Betrouwbaarheid van technische systemen

ANTICIPEREN OP TRENDS

REDACTIE: DR. M.R. DE GRAEF

STT 64

Stichting
Toekomstbeeld
der Techniek

Betrouwbaarheid van technische systemen

Stichting
Toekomstbeeld
der Techniek

De Stichting Toekomstbeeld der Techniek (STT) is in 1968 opgericht door het Koninklijk Instituut van Ingenieurs en is in 2001 gefuseerd met BEWETON. Het werk van STT bestaat voornamelijk uit het uitvoeren van verkenningen op het grensvlak van techniek en samenleving. Door het stimuleren en faciliteren van de kennisuitwisseling tussen mensen van uiteenlopende achtergronden en expertise wordt een brede visie ontwikkeld. Dit proces van 'kennisfusie' is een belangrijk doel van de verkenningen van STT. Het tastbare resultaat is een boek waarin de bevindingen worden vastgelegd. De resultaten worden verspreid op symposia en via de media.

Het bezoekadres van STT is Prinsessegracht 23, Den Haag.
Correspondentieadres:
Postbus 30424, 2500 GK Den Haag, Nederland.
Telefoon +31 70 302 98 30
E-mail info@stt.nl

Betrouwbaarheid van technische systemen

Anticiperen op trends

Redactie: dr. M.R. de Graef

2001

Stichting Toekomstbeeld der Techniek (STT)
Den Haag, Nederland

Colofon

Boekontwerp Salabim, bureau voor vormgeving BNO, Rotterdam
Illustratie omslag Peter A. Weustink (Salabim BNO)
Drukwerk Drukkerij Liesbosch, Nieuwegein

CIP-data Koninklijke Bibliotheek, Den Haag

ISBN 90-804496-5-2
NUGI 841
Trefwoorden betrouwbaarheid, techniek, bedrijfsprocessen, organisatie

Inhoud

Betrouwbaarheid van technische systemen

Nieuwe producten en diensten blijven in een stormachtig tempo op ons afkomen. Een recente uitspraak van een zesjarig kind bij het zien van een niet eens zo oude platenspeler luidde “Wat is dat voor een vreemde cd-speler…”. En dat terwijl vinylplaten gedurende bijna honderd jaar de voornaamste informatiedrager waren voor muziek. Veel mensen zijn nauwelijks gewend aan GSM-telefoons, terwijl GRPS en UMTS er al aankomen. Ook de ontwikkelingen in pc’s blijven hard gaan. Veel mensen beginnen er net aan te wennen dat een pc via een modem en de telefoon verbonden kan worden met Internet op het moment dat deze techniek al grotendeels ingehaald wordt door eerst ISDN en daarna breedbandsystemen als kabelinternet en ADSL. En vergelijkbare innovaties gelden – weliswaar voor eindgebruikers minder zichtbaar – voor professionele systemen.

Het is verbazingwekkend dat dergelijke nieuwe technologieën zo gemakkelijk en in zo’n hoog tempo geaccepteerd worden. Mensen gaan er inmiddels al vanuit dat het de gewoonste zaak van de wereld is een document in een kwartier aan de andere kant van de wereld te kunnen ontvangen, een telefoongesprek met huis te voeren uit een taxi in het midden van Bangkok, of in Zuid-Amerika op elk moment van de dag geld uit de muur te kunnen halen. Groot is dan ook de verwarring als een dergelijk zeer complex systeem een keer niet blijkt te werken. In de zomer van 2001 kwam een groot aantal toeristen op Malta in de problemen wegens het uitvallen van de geldautomaten; het vertrouwen in de techniek was dermate groot dat men geen andere betalingsvoorzieningen had meegenomen.

Ook het gedurende een zekere aanlooptijd niet correct functioneren van een complex systeem als breedbandinternetverbindingen leidde tot zeer veel verontwaardigde reacties van klanten.
Vergelijkbare discussies worden op dit moment gevoerd in de publieke opinie over de beschikbaarheid van het spoorwegnet dat zich op dit moment ook midden in een grote innovatieslag bevindt.

Dit boek staat midden in het spanningsveld tussen enerzijds steeds complexere technische systemen (en de daarbij behorende steeds complexere bedrijfsprocessen) en de steeds toenemende eisen van gebruikers aan de betrouwbaarheid van die systemen. In het boek wordt een aantal recente cases behandeld waarbij de betrouwbaarheid van systemen (of het ontbreken daarvan) een belangrijke rol heeft gespeeld. Al deze cases bevatten voorbeelden van moderne, vaak technologisch complexe systemen of diensten die op een bepaald moment juist niet deden wat ervan verwacht werd. Factoren die hierbij een rol spelen zijn de technologie zelf, de complexiteit van het onderliggende bedrijfsproces, de zeer sterke dynamiek en tijdsdruk van de markt, en de hoge eisen die gebruikers tegenwoordig aan systemen stellen. Tot slot behandelt het boek een aantal richtingen waarin het vakgebied zich zou moeten of kunnen ontwikkelen om ook in de toekomst gebruikers het idee te kunnen geven dat ze ook op de systemen van de toekomst kunnen blijven vertrouwen.

Den Haag, december 2001

Voorzitter STT/Beweton ir. R.M.J. van der Meer

Voorzitter Stuurgroep STT-project
Betrouwbaarheid van technische systemen prof.dr.ir. A.C. Brombacher

Samenvatting

dr. M.R. de Graef

Dit boek is het resultaat van het project 'Betrouwbaarheid van technische systemen' dat in 2001 is afgesloten. In dit project is getracht een overzicht te geven van de ontwikkelingen op het gebied van betrouwbaarheid in uiteenlopende sectoren vanuit de invalshoek van techniek, bedrijfsprocessen en organisatie.

Het boek bestaat uit drie delen. Het eerste deel van dit boek beschrijft de geschiedenis en de gangbare modellen en theorieën van betrouwbaarheid vanuit de drie invalshoeken techniek, bedrijfsprocessen en organisatie. Betrouwbaarheid is een veelomvattend begrip en een eensluidende definitie is lastig te geven. Wat we in het dagelijks leven beschouwen als betrouwbaarheid heet in de techniek ook wel bedrijfszekerheid. Hieronder wordt over het algemeen verstaan de mate waarin een systeem een gespecificeerde functie kan vervullen gedurende een bepaalde tijdsduur. Deze definitie gaat uit van de technische specificatie en deze hoeft niet altijd overeen te stemmen met de eisen die een gebruiker aan een product stelt. De gebruiker zal eerder van een verwachting over het functioneren van een systeem spreken.

Betrouwbaarheid van technische systemen is lange tijd alleen vanuit de techniek benaderd. Hierbij zijn in de loop der tijd de methoden steeds beter geworden. Deze methoden zijn meestal afkomstig uit sectoren waarin van oudsher de noodzaak bestond om technische systemen betrouwbaar te maken en te houden, zoals de vliegtuigindustrie, de chemie, civiele werken en de kernenergie. Hier werden betrouwbaarheidsmethoden ontwikkeld die een systematische aanpak van betrouwbaarheid mogelijk maken. Deze analytische technieken kunnen echter veel breder worden toegepast dan nu het geval is.
De betrouwbaarheid wordt klassiek vaak weergegeven aan de hand van het zogenaamde 'badkuipmodel' of de 'badkuipkromme'. Dit model bestaat uit drie fasen: kinderziekten, normaal gebruik en einde levensduur. Deze voorstelling is te simpel en is tegenwoordig vervangen door een complexere curve die veel meer aansluit bij de praktijk. Voor het analyseren en verbeteren van betrouwbaarheid van huidige en toekomstige producten is niet alleen het juiste mathematische model van belang, maar ook het (bedrijfskundige) proces waarlangs informatie over het falen terechtkomt bij de ontwerper ('information deployment'/terugkoppeling (feedback)).
De terugkoppeling kan op verschillende punten van het bedrijfsproces plaatsvinden.
Om het niveau van terugkoppeling in een bepaald bedrijfsproces te bepalen is het MIR-model (Maturity Index on Reliability) geïntroduceerd. Afhankelijk van het MIR-niveau kan een organisatie de kwaliteit en de betrouwbaarheid beheersen door op een goede manier gebruik te maken van de informatiestromen.
Naast techniek en bedrijfsprocessen is de mens een belangrijke factor in het beheersen van de betrouwbaarheid. Deze rol is vooral onderkend na incidenten waarbij de mens als faalfactor optreedt. Bij deze benadering vanuit de organisatie en het management wordt gekeken naar kenmerken in de technische en de organisatorische context.
De wisselwerking tussen het technisch systeem en zijn omgeving is heel belangrijk voor de betrouwbaarheid van het technisch systeem. Betrouwbaarheid moet integraal vanuit de techniek, de bedrijfsprocessen en de organisatie worden beschouwd. Mogelijk dat daarvoor ook een nieuw conceptueel instrumentarium nodig is, zoals complex adaptieve systemen die door wisselwerking voortdurend veranderen en daardoor evolueren.

De ontwikkelingen met betrekking tot de betrouwbaarheid van technische systemen worden zeer sterk bepaald door een aantal trends, zowel vanuit de techniek als de maatschappij. Dat zijn bijvoorbeeld:

– De toenemende integratie van (steeds complexere) techniek in onze samenleving en de steeds grotere vanzelfsprekendheid waarmee gebruikers verwachten dat deze systemen te allen tijde functioneren.

– De steeds grotere rol van ICT en de steeds grotere afhankelijkheid van informatiesystemen in het maatschappelijk leven.
– De steeds dynamischere bedrijfsstructuren waarbij stabiliteit (door de steeds wisselende economische eisen) en overzicht (door globalisering en uitbesteden) soms ver te zoeken zijn.
– De terugtredende overheid waardoor steeds meer zaken ook op het gebied van de maatschappelijke infrastructuur worden overgelaten aan het private bedrijfsleven.

Dit alles wordt verder gevoed door steeds kortere ontwikkelcycli ('time to market') en steeds complexere technieken en processen.
Deze trends vormen 'bedreigingen' voor de betrouwbaarheid van (toekomstige) technische systemen.

In deel 2 van het boek wordt met behulp van een groot aantal cases duidelijk gemaakt hoe de trends van invloed zijn in verschillende sectoren. Deze cases laten enerzijds zien wat de gevolgen van de trends kunnen zijn en anderzijds welke maatregelen worden getroffen om met deze gevolgen om te gaan.
Doordat de cases door verschillende auteurs zijn geschreven, worden de verschillende visies op het begrip betrouwbaarheid duidelijk.
Uit deel 2 valt af te leiden dat de belangrijke gevolgen van deze trends zijn:
– De toenemende complexiteit van producten maakt het testen en valideren van producten steeds complexer, en daarmee ook duurder en tijdrovender.
– De toenemende complexiteit van (mondiale) bedrijfsprocessen met de daaraan gerelateerde problemen met informatiestromen en informatieoverdracht bedreigen de kennisopbouw van en de kennisuitwisseling over nieuwe producten en technologieën.
– De sterke druk op time to market vereist het gebruik van hoogwaardige voorspellende modellen en technieken.
– Vooral bij sterk innovatieve producten, gebruikt in een complexe omgeving of infrastructuur blijft er (als gevolg van eerder onontdekte productproblemen of onverwachte applicatie- of omgevingsaspecten) een grote kans bestaan dat een aantal problemen met bedrijfszekerheid pas in het veld aan het licht zullen komen. Dit maakt de beschikbaarheid van een goed ontwikkeld, snel en efficiënt terugkoppelsysteem noodzakelijk.

In deel 3 van het boek wordt aangegeven hoe men met de trends kan omgegaan. Er worden richtingen naar de toekomst aangegeven waarin wordt beschreven hoe we de betrouwbaarheid kunnen (blijven) beheersen.
Vroeger werd er vaak naar gestreefd om complexiteit te reduceren. Tegenwoordig ziet men in dat complexiteit een gegeven is, waarop men geen invloed kan uitoefenen.

Om mee te kunnen gaan met de globalisering en de steeds kortere time to market zullen andere ontwikkelprocessen moeten worden ontwikkeld.
Doordat het perspectief van de klant verandert van productgericht naar dienstgericht, zullen systemen techniek steeds minder zichtbaar maken. Men zal dus steeds meer rekening moeten houden met de verwachtingen van de gebruiker en de interactie met de omgeving.

Hierbij zal moeten worden getracht nieuwe vormen van voorspellende modellen te ontwikkelen die behalve de technische risico's ook rekening houden met bedrijfsprocessen en de informatiestromen daarbij. Hiertoe zullen ook de opleidingen aangepast moeten worden. Behalve monodisciplinaire ingenieurs zal er behoefte zijn aan multidisciplinaire deskundigen die (als integrator) zich behalve met de techniek ook met de bedrijfsprocessen en de organisatie bezighouden.

1

1 Overzicht geschiedenis van betrouwbaarheid

dr. M.R. de Graef

Het begin

Betrouwbaarheid speelt al eeuwenlang een belangrijke rol in de samenleving. De behoefte om de betrouwbaarheid te borgen is ook altijd aanwezig geweest. Het begrip betrouwbaarheid stond lange tijd synoniem voor vakmanschap. Ambachtslieden vervaardigden producten en stonden bekend om hun kwaliteit, van ontwerp tot verkoop was het product in handen van deze mensen. Er werden in de Middeleeuwen gilden opgericht, die garant stonden voor het vakmanschap en er ontstonden opleidingen die ervoor zorgden dat deze vakmensen een opleiding kregen. Er bestonden geen grote bedrijven of een overheid die toezicht hield. Er was dus geen speciale aandacht voor betrouwbaarheid en veiligheid, maar deze aspecten waren wel inherent in het systeem aanwezig. Betrouwbaarheid ging om de mensen die de producten ontwierpen, bouwden en onderhielden. Vaak was dat een en dezelfde persoon. Er werden vanzelfsprekend ook voortdurend innovaties doorgevoerd om de betrouwbaarheid te verhogen (zie ook [Brombacher, 1994]).

Deze situatie veranderde met de industriële revolutie, toen individuele werknemers niet langer verantwoordelijk waren voor hun eigen product. Men werkte in een fabriek samen met vaak duizenden anderen en men ging massaproducten fabriceren. Met de invoering van de lopende band ging het nog een stapje verder. Werknemers in fabrieken waren nog slechts verantwoordelijk voor 1 basistaak. Er ontstond een hiërarchie in de bedrijven (management). De werknemers waren niet meer betrokken bij de hele levenscyclus van het product. Men ging zich specialiseren in een bepaalde taak. Waar eerst de gilden verantwoordelijk waren voor het hele proces inclusief de opleiding, werden deze taken nu gescheiden. Dit bracht met zich mee dat ook het begrip betrouwbaarheid een andere dimensie kreeg. Het werd nu noodzakelijk om betrouwbaarheid apart te bestuderen. Ook door de industrialisering nam de productie enorm toe en dus ook de ongelukken en fouten. Betrouwbaarheidsonderzoek was in die beginperiode vaak een kwestie van 'trial and error'. De veiligste en betrouwbaarste bedrijven waren simpelweg die bedrijven die nog bestonden.

Techniek

In eerste instantie richtte het betrouwbaarheidsonderzoek zich op materialen die sterker en dus betrouwbaarder waren (bijv. metaal, stenen, later beton). Als er geen betere materialen voorhanden waren, ging men over op de redundantie. Toen door de industriële revolutie de assemblage-industrie opkwam, werd steeds meer aandacht besteed aan de betrouwbaarheid van componenten. Men deed dat vaak door het kiezen van betrouwbare toeleveranciers; men deed nog niets aan het voorspellen van betrouwbaarheid.
Tijdens de Tweede Wereldoorlog waren vooral elektronische buizen in apparatuur de meest onbetrouwbare component. Er was dus behoefte aan de voorspelbaarheid van de betrouwbaarheid van deze componenten. Men deed dat voornamelijk door een grote database aan te leggen van betrouwbaarheidsdata (zie ook [Denson, 1998]). In de jaren vijftig van de vorige eeuw werd het plan opgevat om de data bijeen te brengen in een handboek. Dit werden de 'military handbooks' met daarin gegevens over de betrouwbaarheid (faaldata) van duizenden (elektronische) componenten. De eerste versie van dit als US MH-217 bekend staande handboek zag het licht in 1962 bij de Amerikaanse marine. Soortgelijke boeken werden opgesteld voor de automobielindustrie en de nucleaire industrie (WASH-1400). Met behulp van deze faaldata kunnen berekeningen worden gemaakt van de faalkans van het totale systeem en kan men dus een voorspelling doen over de betrouwbaarheid van het ontworpen product.

Een andere belangrijke drijfveer is de luchtvaart geweest (zie ook hoofdstuk 12, deel 2). In de luchtvaart ontstond de noodzaak tot betrouwbaarheid door de enorme toename van de burgerluchtvaart in de tweede helft van de vorige eeuw. Deze industrie heeft een goede reputatie opgebouwd op het gebied van betrouwbaarheid.
De wijze waarop men met de technische kant van betrouwbaarheid omgaat veranderde ook in de loop van de eeuwen. Vroeger werden vaak beslissingen genomen op basis van ervaringen uit het verleden (determinisme), later is men steeds meer proberen te gaan voorspellen (probabilisme). In deze benadering kijkt men naar de kans dat een gebeurtenis (falen) kan optreden. Deze probabilistische benadering werd in het begin vooral in de civiele sector gebruikt, maar wordt steeds vaker ook in andere sectoren toegepast, zeker waar het gaat om kritische systemen zoals kerncentrales. In hoofdstuk 3, deel 1 wordt uitgebreid ingegaan op de geschiedenis van het probabilisme en de trends hierin. In relatie tot het voorspellen van de betrouwbaarheid zijn vele methoden ontwikkeld om berekeningen voor de betrouwbaarheid van technische systemen te maken.

In de loop der jaren zijn op het gebied van de technische betrouwbaarheid veel standaarden ontwikkeld die zich vrijwel allemaal specifiek op een bepaald type technisch systeem richten. Deze standaarden moeten voortdurend worden aangepast aan de ontwikkelingen. Ze geven niet de garantie dat de waargenomen betrouwbaarheid overeenkomt met de voorspelde betrouwbaarheid, zoals ook uit hoofdstuk 5, deel 1 blijkt. Uit deze discrepantie kwam ook de noodzaak naar voren om niet alleen de componenten en het ontwerp in dit onderzoek te betrekken, maar ook de procedures die gebruikt worden bij het ontwerpen, bouwen en gebruiken van systemen. De trend is dat standaarden steeds meer generiek worden, en zo worden opgesteld dat ze de betrouwbaarheid waarborgen zonder op specifieke technische details in te gaan (zie ook de hoofdstukken 6 in deel 1, 24 en 30 in deel 2).

Bedrijfsprocessen

In de jaren zeventig werd kwaliteit een belangrijk onderwerp in de industrie, mede hierdoor is de ISO/TC 176-Commissie in 1979 in het leven geroepen die in 1987 de ISO 9000-serie publiceerde. Deze standaard is generiek en is bedoeld om een efficiënte en effectieve organisatie te waarborgen. Het is een gestructureerd model waarin de bedrijfsprocessen (procedures) beschreven worden en aan bepaalde voorwaarden moeten voldoen. Middels uitgebreide audits wordt in een organisatie gecontroleerd of aan de standaard wordt voldaan. Alhoewel ISO 9000 (en aanverwante ISO-standaarden) een organisatie kan helpen bij het verbeteren van de betrouwbaarheid van hun technische systemen, blijkt

vaak dat het geen garantie is. Dit is voor een deel te wijten aan het feit dat de ISO 9000-serie niet integraal op de betrouwbaarheid ingaat (alhoewel de standaard op zichzelf generiek is). Tevens ontbreekt de noodzakelijke terugkoppeling in ISO 9000 grotendeels.
Het zou beter zijn om integraal naar techniek en processen te kijken (zie hoofdstuk 5). Door deze koppeling en terugkoppeling in het bedrijfsproces (MIR-model, zie hoofdstuk 5) is men in staat om de betrouwbaarheid in al zijn facetten beter te controleren. Het voornaamste punt hierin is dat een groot aantal trends – met de steeds korter wordende ontwikkelcycli voorop – het noodzakelijk maken om de technische betrouwbaarheid (de betrouwbaarheid van componenten) te koppelen aan de bedrijfsprocessen.
Hoe de ontwikkeling in de (consumenten)elektronica-industrie verliep, wordt in hoofdstuk 4 geschetst, vooral hoe de terugkoppeling (feedback) uit het veld plaatsvindt. In deze bijdrage staat ook de ontwikkeling van de betrouwbaarheid van componenten naar de integrale betrouwbaarheid van techniek en proces beschreven.

Organisatie

Naast techniek en processen is de mens een belangrijke factor in de betrouwbaarheid van technische systemen. Het meest zichtbaar is die rol waar de mens apparatuur bedient en dus een directe interactie heeft met de techniek, en dus ook invloed heeft. De laatste decennia van de vorige eeuw is men gaan inzien dat betrouwbaarheid ook beïnvloed wordt door de manier waarop het werk is georganiseerd. In hoofdstuk 7 worden de ontwikkelingen op dit gebied geschetst. Hiermee lijkt men weer terug te keren naar de begintijd van de techniek waarin techniek, proces en organisatie in één persoon waren vertegenwoordigd.

Over dit project

In het verleden heeft STT al in meer verkenningen aandacht besteed aan betrouwbaarheid. In ‘De kwetsbaarheid van de stad’ [Laurentius, 1984] wordt zichtbaar gemaakt hoe de samenleving afhankelijk (en dus kwetsbaar) is geworden van water, gas elektriciteit en telecom. ‘Grenzen aan techniek’ [Griethuysen, 1989] heeft als thema de technologische ontwikkelingen en de grenzen daarin. ‘Inspelen op complexiteit’ [Alkemade, 1992] gaat in op de toenemende complexiteit van technieken en hoe daarmee kan worden omgegaan. In ‘Vernieuwing in productontwikkeling’ [Korbijn, 1999] worden de trends met betrekking tot ontwerpprocessen beschreven. Uit krantenberichten lijkt soms

dat de techniek steeds onbetrouwbaarder wordt. Denk bijvoorbeeld aan de tunnelongelukken van de afgelopen tijd. Door de integratie van software in veel systemen wordt de techniek steeds complexer en onzichtbaarder.
Aan de andere kant worden technische systemen steeds betrouwbaarder. Auto's hoeven de eerste 10.000 km niet meer naar de garage; statistisch gezien wordt vliegen steeds betrouwbaarder (en dus veiliger).
Een studie die zich richt op de betrouwbaarheid van technische systemen lijkt dus gerechtvaardigd. In de techniek speelt betrouwbaarheid altijd een rol, maar wordt vaak niet afzonderlijk belicht. In deze studie is getracht over vele sectoren heen gemeenschappelijke aspecten van betrouwbaarheid te vinden. Op deze manier is het mogelijk tussen de verschillende sectoren een kruisbestuiving te laten plaatsvinden.

Uit deze bijdrage blijkt dat betrouwbaarheid vanuit verschillende perspectieven kan worden benaderd: de techniek, de processen en de organisatie. In deze studie is ook voor deze driedeling gekozen. In deel 1 zal een overzicht worden gegeven van een aantal bestaande inzichten op het gebied van betrouwbaarheid en zullen de trends worden geïntroduceerd die voor betrouwbaarheid belangrijk zijn. In deel 2 is een groot aantal cases beschreven die vanuit verschillende sectoren laten zien wat de impact van die trends is en hoe met de trends kan worden omgegaan. In deel 3 wordt in een helikopterview nog eens duidelijk gemaakt wat de impact van de belangrijkste trends kan zijn en zal een aantal richtingen voor de toekomst worden aangegeven.

Referenties

- Alkemade, M.J.A. van (red.) (1992). Inspelen op complexiteit. STT 52. Samsom, Alphen aan den Rijn
- Brombacher, A.C. (1994). Will it really Work? Some Critical Notes on Current Industrial Development Processes. Inaugurele rede. TU Eindhoven
- Denson, W. (1998). The History of Reliability Prediction. IEEE Transactions on Reliability **47**:321-328
- Griethuysen, A.J. (red.). (1989). Grenzen aan techniek. STT 49. Samsom, Alphen aan den Rijn
- Korbijn, A. (red.). (1999). Vernieuwing in productontwikkeling, strategie voor de toekomst. STT 62. STT, Den Haag
- Laurentius, G. (1984). Kwetsbaarheid van de stad. STT 39. Delftse Universitaire Pers, Delft

1

2 Het begrip bedrijfszekerheid

mr.ir. M.J.P. van der Meulen [1]

Inleiding

Dit boek gaat over bedrijfszekerheid [2]. Maar wat is bedrijfszekerheid eigenlijk? Deze vraag stellen is gemakkelijker dan hem beantwoorden. Er zijn veel verschillende meningen. Doel van deze studie is niet een oplossing te vinden en het begrip nu eens en voor altijd te definiëren. Wel is het nodig inzicht te krijgen in de term, en dat kan door de verschillende inzichten in kaart te brengen.

Kijken naar een aantal definities werkt verhelderend. Voor 'dependability' (de Engelse vertaling van het begrip) vinden we in standaarden de volgende definities.

1 Simtech
Max Euwelaan 60
3062 MA Rotterdam

2 Wat in het dagelijks leven onder betrouwbaarheid wordt verstaan is bedrijfszekerheid volgens de technische definitie. Feitelijk is betrouwbaarheid een verdere afbakening van het begrip bedrijfszekerheid.

Definitie 1

The collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance [ESA, ECSS-P-001A, 1997; IEC 300-3-4, 1996; ISO 8402, 1994; ISO 9000-4, 1993; IEC 300-1, 1993; BSI, BS 4778-3.2, 1991; IEC 50 (191), 1990].

Definitie 2

A measure of the degree to which an item is operable and capable of performing its required function at any (random) time during a specified mission profile, given item availability at the start of the mission [USA DoD, MIL-Std-109C, 1994; USA DoD, MIL-Std-721C, 1981].

Definitie 3

Trustworthiness of a computer system such that reliance can justifiably be placed on the service it delivers [Laprie, 1992].

De eerste definitie komt in veel standaarden voor. Dat is dus de meest geaccepteerde variant, zeker in Europa. Het is vooral een kwalitatieve definitie. [ISO 9000-4, 1993] en [IEC 300-1, 1993] voegen er nog een noot aan toe waarmee ze dat onderstrepen: “Dependability is used only for general descriptions in non-quantitative terms.” Kenmerkend is dat deze definitie een paraplubegrip is. Essentieel is de beschikbaarheid met daarnaast de beïnvloedende factoren betrouwbaarheid, onderhoudbaarheid en het onderhoud zelf (vertalen van de Engelse begrippen is moeilijk, en soms vrijwel onmogelijk).

De tweede definitie is van Amerikaanse origine. Hier ligt iets meer nadruk op het kwantitatieve aspect (A measure of ...). Eigenlijk lijkt deze definitie sterk op wat wij betrouwbaarheid zouden noemen.

De derde definitie is van een internationale werkgroep die een begrippenlijst op het vakgebied heeft samengesteld. Het is wederom een kwalitatieve definitie. Ze bestrijkt echter niet de gehele reikwijdte van de eerste definitie, maar lijkt zich tot wat in de eerste definitie betrouwbaarheid heet te beperken, hoewel het begrip trustworthiness toch weer net iets anders kan zijn. Dit begrip heeft een subjectieve bijsmaak. Laprie verzuimt de term ‘trustworthiness’ te definiëren.

Interessant is nu te kijken naar de samenstellende delen van de eerste definitie, waarbij we ons beperken tot definities uit bronnen die de eerste definitie gebruiken.

Availability

The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided [ESA, ECSS-P-001A, 1997; BSI, BS 4778-3.2, 1991; IEC 50 (191), 1990].

Reliability

The probability that an item can perform a required function under given conditions for a given time interval (t1, t2) [CENELEC, prEN50126, 1998; ESA, ECSS-P-001A, 1997; BSI, BS 4778-3.2, 1991; IEC 50 (191), 1990].

Maintainability

The ability of an item under given conditions of use, to be retained in, or restored to a state in which it can perform a required function, when maintenance is performed under given conditions and using stated procedures and resources [ESA, ECSS-P-001A, 1997; BSI, BS 4778-3.2, 1991; IEC 50 (191), 1990].

Maintenance

The combination of all technical and administrative actions, including supervision actions, intended to retain a product in, or restore it to a state in which it can perform a required function [CENELEC, ENV50129, 1998; CENELEC, prEN50126, 1998; ESA, ECSS-P-001A, 1997; BSI, BS 4778-3.2, 1991; IEC 50 (191), 1990].

Wanneer we nu uiteindelijk kijken naar de relaties tussen de definities en de samenstellende delen ervan komen we tot het volgende schema (zie figuur 2.1). De onderliggende kernbegrippen zijn dus: externe hulpbronnen, gebruiks-condities, tijd, de geëiste functionaliteit en menselijk handelen. Over deze begrippen kan het volgende worden opgemerkt.

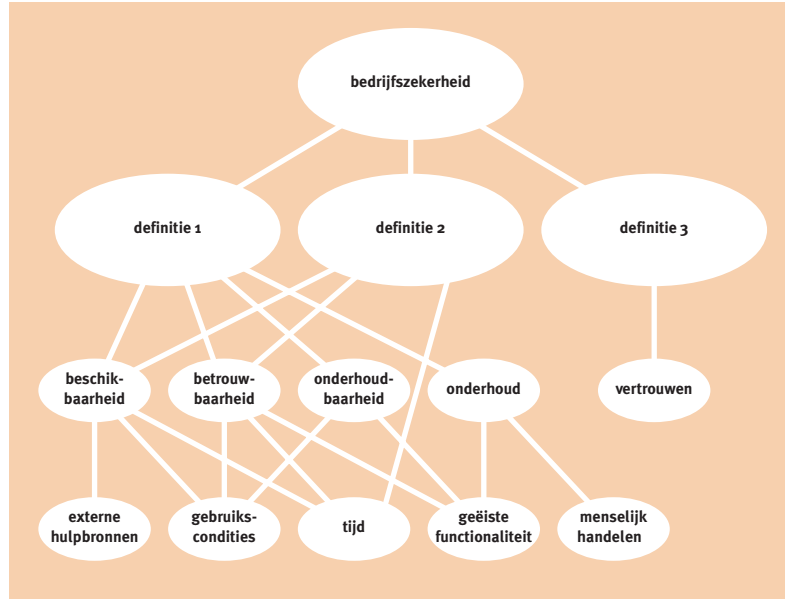
Externe hulpbronnen

De standaarden definiëren het begrip benodigde externe hulpbronnen niet. Bedoeld worden waarschijnlijk hulpmiddelen als voeding en grondstoffen. De gebruiker dient ervoor te zorgen dat deze in voldoende mate aanwezig zijn om het functioneren van het systeem te garanderen. Dit is logisch. Ook is het plausibel dat aan deze externe hulpbronnen wederom bedrijfszekerheidseisen worden gesteld.

Gebruikscondities

De gebruikscondities zijn een gegeven. Wanneer de gebruikscondities anders zijn, kan de bedrijfszekerheid van het systeem niet worden gegarandeerd. Dit kan vaak tot problemen leiden. Dat geldt bijvoorbeeld voor hergebruik van soft-waremodulen. Of denk aan het falen van de Ariane V.

Figuur 2.1
Relaties tussen de definities van bedrijfszekerheid.



Tijd

Zowel beschikbaarheid als betrouwbaarheid hangen sterk af van het begrip tijd. Verschillende eisen hieraan leiden tot een ander ontwerp. Voor vliegtuigen is bijvoorbeeld de missietijd maar enkele uren met extreem strenge bedrijfszekerheidseisen, zodat onderhoud nauwelijks mogelijk is. Dit leidt tot het gebruik van redundante computers. In gevallen waarin de missietijd lang is en het onderhoud eenvoudig, zou dat niet nodig zijn.

Geëiste functionaliteit

Bedrijfszekerheid heeft altijd te maken met geëiste functionaliteit. Niet geëiste functies mogen falen. Belangrijk is te bedenken dat deze 'extra' functionaliteit ongewenste gevolgen voor systemen met een hoge bedrijfszekerheid kan hebben. Het is noodzakelijk aan te tonen dat deze functionaliteit geen nadelige invloed heeft op de bedrijfszekerheid.

Menselijk handelen

Menselijk handelen heeft altijd grote invloed op de bedrijfszekerheid van systemen. Hier praten we enerzijds over handelen tijdens operationeel bedrijf, en anderzijds over handelen dat nodig is voor onderhoud.

De toekomst van het begrip bedrijfszekerheid

Ondanks het feit dat er verschillende definities van het begrip bedrijfszekerheid bestaan, lijkt er een hoge mate van consensus te bestaan over wat het betekent. Definitie 1 lijkt in de wereld het meest geaccepteerd, en dat zal naar verwachting ook zo blijven.

Referenties

- BSI, BS 4778-3.2. (1991). British Standards Institution. BS 4778, Part 3. Availability, Reliability and Maintainability Terms. Section 3.2 Glossary of International Terms. (Equal to IEC 50 (191), 1990)
- CENELEC, prEN50126. (1998). Railway Applications – The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- CENELEC, ENV50129. (1998). Railway Applications; Safety Related Electronic Systems for Signaling
- ESA, ECSS-P-001A. (1997). European Space Agency. ECSS-P-001A. Glossary of terms. Rev. 1
- IEC 50-191. (1990). International Electrotechnical Commission. IEC 50 (191). International Electrotechnical Vocabulary – Chapter 191: Dependability and Quality of Service. (Equal to BS 4778-3.2, 1991)
- IEC 300-1. (1993). International Electrotechnical Commission. IEC 300-1. Dependability Management; Part 1: Dependability Programme Management
- IEC 300-3-4. (1996). International Electrotechnical Commission. IEC 300-3-4. Dependability Management; Part 3: Application Guide; Section 4: Guide to the Specification of Dependability Requirements
- IEC 61508-4. (1998). International Electrotechnical Commission. IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems; Part 4: Definitions and Abbreviations
- ISO 8402. (1994). International Organization for Standardization. ISO 8402. Quality Management and Quality Assurance – Vocabulary
- ISO 9000-4. (1993). International Organization for Standardization. ISO 9000-4. Quality Management and Quality Assurance Standards; Part 4: Guide to Dependability Programme Management. (Equal to IEC 300, 1993)
- Laprie, J.C. (ed.). (1992). Dependable Computing and Fault-Tolerant Systems:5, Dependability: Basic Concepts and Terminology. Springer Verlag, Vienna
- Meulen, M.J.P. van der. (2000). Definitions for Hardware and Software Safety Engineers. Springer, London
- USA DoD, MIL-Std-109C. (1994). USA Department of Defense. Quality Assurance Terms and Definitions
- USA DoD, MIL-Std-721C. (1981). USA Department of Defense. Definitions of Terms for Reliability and Maintainability. (Cancelled by Notice 2, 1995)

1

3 Risicoanalyse: een historisch overzicht

ir. R.W. van Otterloo [1]

Inleiding

De mens is in steeds grotere mate afhankelijk van technische systemen. De functies die vervuld worden door bijvoorbeeld vervoer, communicatie en financiën zijn van levensbelang en kunnen in onze westerse maatschappij niet gemist worden. Al deze functies steunen echter steeds meer op technische systemen. Zelfs een verstoring van enige uren kan al een enorme chaos veroorzaken en grote financiële (en soms ook andere) gevolgen hebben. In vaktermen betekent dit dat onderzoek naar de betrouwbaarheid van technische systemen nuttig is en van groot belang is voor ons allemaal. Op deze wijze redenerend kan men zich afvragen of wij mensen wellicht zelf de noodzaak tot de interesse in betrouwbaarheid in het leven hebben geroepen. Dat maakt het interessant om terug te gaan in de tijd en na te gaan hoe het denken in betrouwbaarheidstermen is ontstaan en hoe het is geëvolueerd.

1 NRG Arnhem
Postbus 9035
6800 ET Arnhem

Betrouwbaarheid van technische systemen

Alvorens in te gaan op het ontstaan van het fenomeen betrouwbaarheid is het verstandig om betrouwbaarheid nader te definiëren. Dat verduidelijkt de mogelijke herkomst (zie ook hoofdstuk 2, deel 1).
Betrouwbaarheid van technische systemen wordt hier gedefinieerd als het beïnvloeden van de kans op falen van dat systeem, dan wel het beperken van faalgevolgen. Dit alles met als doel het afbreukrisico te beperken. De lezer kan zich afvragen wat de overeenkomst is tussen betrouwbaarheid en duurzaamheid. Duurzame systemen gaan lang mee. Als daar in het ontwerp bewust naar is gestreefd, wordt er voldaan aan de genoemde definitie. De kans op falen is namelijk bewust beïnvloed, het afbreukrisico is beperkt. Dit alles maakt het niet makkelijker om een schets te geven van het ontstaan van betrouwbaarheid van technische systemen.

De betrouwbaarheidsanalytische benadering als functie van de tijd

Het eerste begin

Piramiden behoren tot de oudste door de mens gebouwde objecten in de wereld. Ze zijn voortgekomen uit grafheuvels. Ze zijn bewust van een daar niet aanwezig duurzaam materiaal gebouwd en hebben daardoor een lange levensduur. Het afbreukrisico is door deze bewuste keus zeer beperkt. Toch is hier in directe zin geen sprake van betrouwbaarheid. De piramiden zijn vooral gebouwd om de macht van de overleden vorst te symboliseren. Als die symbolische functie erkend wordt, kan men stellen dat daaraan op betrouwbare wijze uiting is gegeven.
In de 6e en 5e eeuw voor Christus werden in Noord-Nederland de eerste terpen opgeworpen. Uitgestrekte kwelders raakten buiten de invloed van de zee, maar overstroomden nog wel incidenteel. Boeren afkomstig van de hogere gronden vestigden zich hier en werden genoodzaakt de natuurlijke verhogingen kunstmatig te versterken en te verhogen. Een aantal van deze terpen zijn in ons landschap nog steeds zichtbaar (bijv. in Ezinge). Hier is men op deterministische wijze met betrouwbaarheid omgegaan.
Het oudste gedeelte van de Chinese muur stamt uit circa 200 voor Christus. Ook dit bouwwerk straalt duurzaamheid uit. Ook hiervan kan men veronderstellen dat bewust naar duurzaamheid is gestreefd, en dat er dus sprake is van betrouwbaarheid. Hout is achterwege gelaten. Er is voor het veel arbeidsintensievere en duurzamere steen gekozen. De hoogte van de muur houdt ongetwijfeld verband met zijn doel om China te beschermen tegen aanvallen van plunderende nomaden. Hoe zou men deze hoogte bepaald hebben? Met 'Structural Reliability'[2],

2 Met Structural Reliability wordt dat gedeelte van de betrouwbaarheidsanalyse bedoeld dat zich niet baseert op historische faalgegevens, maar op sterkteberekeningen. In Structural Reliability wordt de sterkte van een structuur vergeleken met de belasting op die structuur om uit die vergelijking een faalkans te destilleren.

zoals nu dijkhoogten worden uitgerekend? Dat lijkt onwaarschijnlijk, maar toch heeft men natuurlijk geworsteld met de vraag hoe hoog is hoog genoeg?
Alle hiervoor genoemde voorbeelden hebben echter één kenmerk gemeen. Het betreffende betrouwbaarheidsvraagstuk werd op deterministische wijze aangepakt. Men zal zich in die tijden dus meer beziggehouden hebben met het beperken van de faalgevolgen dan met het beperken van de kans op falen.

Mogelijkheden voor risicoanalyse

Mede omdat de technieken ontbraken, was men bij deze vroege ontwikkelingen niet in staat om betrouwbaarheid te analyseren.
De eerste aanzet tot de opkomst van kwalitatieve analyseregels is gegeven door René Descartes (1596-1650). In zijn werk van 1637 genaamd 'Discours de la Méthode' geeft hij een aantal regels die wij heden ten dage terugvinden in risicoanalysetechnieken zoals FMECA[3], gebeurtenissenboom, foutenboom en HAZOP[4].

De vier regels voor onderzoek in het algemeen in dit werk zijn:

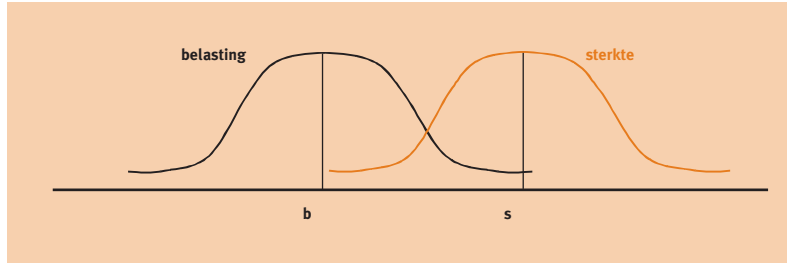
Niets voor waar houden dat niet evident is	**FMECA**
Problemen door verdeling oplossen	**gebeurtenissenboom**
Van het simpele naar het gecompliceerde opklimmen	**foutenboom**
Zo volledig mogelijke opsommingen maken	**HAZOP**

In 1812 publiceerde P.S. Laplace (1749-1827) zijn werk 'Théorie Analytique des Probabilités'. Hierin wordt de klassieke kansrekening behandeld. Deze theorie is een onmisbaar onderdeel van de hedendaagse betrouwbaarheidsanalyse. De tweede editie van dit werk bevatte al de regels van Bayes, ook geen onbekende in de betrouwbaarheidsanalytische wiskunde.
Charles R. Darwin (1809-1882), een Engels natuuronderzoeker die aanvankelijk medicijnen maar later theologie studeerde, schreef het eerste betrouwbaarheidsanalytische werk in 1859, getiteld 'On the Origin of Species by Means of Natural Selection'. Daarin past hij het principe van de hedendaagse Structural Reliability toe op het voortbestaan van specimen.

In figuur 3.1 kan men zien hoe de sterkte van een structuur in een curve met als gemiddelde waarde s kan worden weergegeven. In dezelfde figuur staat ook de belasting op die structuur (curve met gemiddelde waarde b) weergegeven.
De curven als zodanig worden veroorzaakt door de onzekerheden in sterkte en belasting. Het oppervlak dat zich onder beide curven bevindt is een maat voor de kans op falen van de structuur. Daar is immers de sterkte lager dan de belasting. Aan de hand van dezelfde figuur 3.1 kan ook de evolutiegedachte van Darwin uitgelegd worden. Eén specimen bestaat uit grote aantallen die onder-

3 FMECA = Failure Modes Effects and Criticality Analysis. Het is een op brainstormen gebaseerde 'What if methode'.

4 HAZOP = Hazard and Operability Analysis.



Figuur 3.1
Symbolische weergave van het principe van Structural Reliability.

ling minimaal in sterkte verschillen. Dit wordt gesymboliseerd door de curve met als gemiddelde s. (De sterken staan geheel rechts in deze curve. De zwakken uiterst links.) Het grote aantal dat tot dat ene specimen behoort leeft in verschillende biotopen die ieder hun eigen belasting met zich meebrengen. Het vriendelijke biotoop staat links in de b-curve, het veeleisende biotoop staat rechts. Het oppervlak dat zich nu onder beide curven bevindt is een maat voor dat deel van het specimen dat de 'struggle for life' ervaart.

De eerste oefeningen

Tijdens de eerste industriële revolutie (1740-1850) is de behoefte ontstaan aan Systems Reliability[5]. Toch heeft het tot de Eerste Wereldoorlog geduurd, voordat men kwantitatieve betrouwbaarheidsanalyse ging toepassen. Men had in die tijd vliegtuigen met verschillende motoren en dat is de aanleiding geweest om vergelijkingen te gaan maken tussen een- en tweemotorige en twee- en viermotorige vliegtuigen (zie hoofdstuk 12, deel 2). Deze vergelijking had betrekking op het aantal succesvolle vluchten. Deze vergelijkingen waren echter nog kwalitatief van aard. Het heeft tot de jaren dertig geduurd, voordat men overging tot het verzamelen en analyseren van gegevens. Op die manier konden betrouwbaarheid en beschikbaarheid in getallen worden uitgedrukt.

Luchtvaart

De eerste risicoanalytische oefeningen stammen dus uit de jaren dertig en vonden hun oorspong in de luchtvaartindustrie waar gaandeweg ook de eerste betrouwbaarheidscriteria werden opgesteld (niet vaker een onderbreking dan 1 op de 100.000 vlieguren). Door de Tweede Wereldoorlog werd de vliegtuigindustrie verder onder druk gezet en daarmee werden ook de betrouwbaarheidseisen meer expliciet. Dit alles heeft ertoe geleid dat de vliegtuigen die in de jaren zestig werden gebouwd al zo betrouwbaar waren dat zij de grens van 1 op 1.000.000 crashes per vliegtuiglanding haalden.

Spoorwegen

Bij de Spoorwegen heeft men de betrouwbaarheid vooral van toepassing laten zijn op de veiligheid van het vervoer. In eerste instantie is dat deterministisch aangepakt en werkte men met een bewijs van veiligheid. Zo'n bewijs bestond

5 Dat gedeelte van de betrouwbaarheidsanalyse dat gebaseerd is op het ontleden van het te analyseren systeem. Het systeem wordt ontleed tot op de bouwstenen waarvan men op grond van historische gegevens de faalkansen kent. Uit de ontleding is dan weer de faalkans van het totale systeem op te bouwen.

uit vele documenten die betrekking hadden op de veiligheid van het betreffende systeem. In het midden van de jaren negentig zijn de Cenelec-normen ontstaan die daarna geleidelijk zijn ingevoerd. In die normen zijn afhankelijk van het SIL-niveau (Safety Integrity Level, zie hoofdstuk 6, deel 1 en hoofdstuk 26) kwantitatieve betrouwbaarheidseisen gesteld. Die eisen moeten met voorgeschreven methoden (FMECA en foutenboom) aangetoond worden.
Tegenwoordig stelt een afnemer van beveiligingsapparatuur bestemd voor het railvervoer eenvoudig dat deze apparatuur volgens de geldende Cenelec-norm aan een bepaald SIL-niveau moet voldoen. Daarmee staat dan vast welke risicoanalyses er gemaakt moeten worden en aan welke criteria de uitkomsten van die analyses moeten voldoen. Met het invoeren van hoge snelheidslijnen wordt de betrouwbaarheidsanalyse ook veelvuldig voor andere dan veiligheidsstudies aangewend.

Kernenergie

De eerste kernreactor is gedurende de Tweede Wereldoorlog op de campus van de universiteit in Chicago ontwikkeld en beproefd. Het reactorvermogen bedroeg minder dan 1 Watt.
De eerste commerciële kernenergiereactoren stammen uit het eind van de jaren vijftig en het begin van de jaren zestig. Met het op grotere schaal toepassen van kernenergie ontstond ook de behoefte aan het op systematische wijze benaderen van de veiligheid.
Het eerste uitgebreide onderzoek naar ongevallen met kernenergiecentrales stamt uit 1957 en is uitgevoerd door het Brookhaven National Laboratory in de VS. In WASH-740 wordt daarvan verslag gedaan. De gevolgen bleken onacceptabel, maar de kans op zo'n ongeval zou erg klein zijn. In de kernenergie werd tot het begin van de jaren zeventig met het 'single failure'-criterium gewerkt (Het falen van één onderdeel mag niet fataal zijn. Het moet altijd tenminste een combinatie zijn). Ook was het begrip MCA ('Maximum Credible Accident') van toepassing. Hiermee werd het maximale ongeval bepaald waartegen de centrale toch nog beveiligd moest worden. Via het MCA is ook het begrip kans in de veiligheid van kernenergie ingevoerd.
In september 1972 begon professor Norman Rasmussen van het MIT met de Reactor Safety Study, ook wel bekend als WASH 1400. Daarin werden twee verschillende typen kernenergiecentrales door toepassing van de foutenboomtechniek in combinatie met de gebeurtenissenboomtechniek geanalyseerd. Deze eerste PSA (Probabilistic Safety Study) verscheen in conceptvorm in augustus 1974 en heeft sinds dien navolging gekregen over de gehele wereld. In Nederland werd in opdracht van de SEP in 1975 een analoge studie uitgevoerd. In het betreffende RASIN-rapport (Risico Analyse van de Splijtstofcyclus In Nederland) zijn de kernenergiecentrales Dodewaard en Borssele voor het eerst op deze wijze geanalyseerd.

Waterbouw

In Nederland is het Ministerie van Verkeer en Waterstaat als een van de eerste met kansberekeningen begonnen. De watersnoodramp van 1 februari 1953 was de directe aanleiding tot het Deltaplan. In de Deltawet waarmee de Tweede Kamer op 29 oktober 1957 akkoord ging, staat aangegeven dat de dijkhoogten dusdanig moeten zijn dat zij tenminste weerstand kunnen bieden aan een waterstand die 1 maal per 10.000 jaar bij Hoek van Holland voorkomt (daaruit kunnen plaatselijke waterhoogten afgeleid worden). Hier is dus een acceptabele overstromingskans geformuleerd die vervolgens probabilistisch is uitgewerkt. De stormvloedkering in de Oosterschelde die in oktober 1986 in gebruik genomen is is ontworpen en gebouwd op basis van toelaatbare faalkansen. Zelfs de onderhoudsplannen zijn zo dat de destijds toegestane faalkansen voor deelsystemen gerespecteerd worden. Voor de bouw van de stormvloedkering in de Nieuwe Waterweg waarmee men in 1989 is begonnen geldt hetzelfde. De kans dat deze kering niet sluit moest kleiner zijn dan 1 op de 1.000 sluitingen. De kans dat hij tijdens het keren bezwijkt moest kleiner zijn dan 1 per 1.000.000 jaren, en de kans dat hij niet opent kleiner dan 1 op de 10.000 openingen. Het komt wellicht kil over dat dit soort criteria gesteld worden, maar eenmaal overeengekomen zijn ze zeer bruikbaar. Zou dat niet gebeuren, dan blijft men tegen iedere prijs mooier en beter ontwerpen en bouwen.

De huidige situatie

Aan het begin van dit nieuwe millennium is het in de techniek in een aantal situaties gebruikelijk om een probabilistische betrouwbaarheidsanalyse uit te voeren, voordat tot bouwen wordt overgegaan. De redenen hiervoor zijn onder te verdelen in:

- De overheid eist dit (hetzij nationaal, hetzij internationaal). De aanvrager dient eerst een risicoanalyse te overleggen, voordat hij mogelijk toestemming krijgt voor een potentieel gevaarlijke installatie voor kernenergie, chemie of voor een hoge snelheidslijn. De analyse maakt onderdeel uit van de vergunningaanvraag. Internationaal moet aan het ontwerp van vliegtuigen en dergelijke gedacht worden, die ook aan strenge veiligheidseisen moeten voldoen, voordat zij luchtwaardig bevonden worden.
- De economie vraagt om een ontwerpgrens. Nieuwe niet eerder toegepaste systemen, technieken en methoden kunnen bij falen soms tot zware incidenten leiden. De onbekendheid vraagt in zo'n geval om onderzoek vooraf, omdat men wil weten welk risico men loopt en welk niveau van beveiliging verantwoord is.
- Er is een incident geweest. Soms zijn bepaalde technische systemen reeds vele jaren in gebruik, voordat zich een onvoorzien incident met (potentieel)

zware gevolgen voordoet. De eigenaar vraagt zich dan af of het incident structureel is. Een betrouwbaarheidsanalyse kan hier soelaas bieden. Daarmee kan alsnog inzicht worden verkregen in de veiligheid van het technisch systeem. Mocht blijken dat een en ander structureel is, dan kan de voorgestelde wijziging op dezelfde manier op zijn gunstige invloed op het systeem beoordeeld worden.

In zijn algemeenheid kan gesteld worden dat de analysetechnieken en methoden uit de jaren vijftig en zestig stammen. Pas na de opkomst van goed bruikbare faaldatabanken in de jaren zeventig heeft de kwantitatieve betrouwbaarheidsanalyse een vlucht genomen.

Trends

Op 2 december 2000 – dus op de zaterdag voor Sinterklaas – is er in Nederland een recordaantal pinbetalingen gedaan. Stilstaan bij het mogelijk landelijk, regionaal of stedelijk falen van deze betalingsmogelijkheid op die bewuste zaterdag geeft aan hoe afhankelijk de samenleving is van de betrouwbaarheid van technische systemen. Men kan met zekerheid stellen dat deze afhankelijkheid in de toekomst alleen maar zal toenemen. Ook de complexiteit zal verder toenemen. Waar vroeger de overheid opdracht gaf tot het bouwen van infrastructurele voorzieningen en dat in goed overleg met de uitvoerder deed, wordt nu ook aan Publiek Private Samenwerking (PPS) gedacht. Infrastructurele voorzieningen komen steeds vaker volgens het principe van 'design and construct' tot stand. In dat soort situaties wordt met RAM[6]-specificaties gewerkt waarin de RAM-eisen expliciet worden vastgelegd. Er wordt zelfs al met 'Performance Payment Models' gewerkt waarbij de ontwerper of bouwer naarmate hij meer aan de gestelde beschikbaarheidseisen voldoet ook een hogere beloning mag verwachten. Technieken worden ook op een steeds meer uitzonderlijke wijze toegepast. Een windturbine op het land is op vrijwel ieder tijdstip te bereiken en kan dus ook snel weer gerepareerd worden. Voor een offshore windturbinepark (100 kilometer uit de kust) ligt dat veel moeilijker. In het stormseizoen zullen ze juist mankementen gaan vertonen, maar dan zijn ze per schip ook moeilijk te benaderen. Herstellen lijkt uitgesloten, als dat met een drijvende kraan moet gebeuren.

Het is belangrijk om te beseffen dat men met het oog op de toekomst erbij gebaat is faaldata te verzamelen bij het toepassen van betrouwbaarheidsanalyse. Met het ontstaan van nieuwe technieken en uitzonderlijke toepassingen blijft de behoefte aan faaldata voor die specifieke gevallen bestaan. De analysetechnieken en methoden zijn er vaak wel. Zij zullen in de toekomst ongetwijfeld

6 RAM = Reliability, Availability and Maintainability.

nog verbeterd en aangevuld worden, maar zij nemen in waarde toe als ze kwantitatieve resultaten kunnen leveren. Dat kan alleen als er voldoende bruikbare faaldata verzameld zijn.

Gezien de toenemende belangrijkheid van risicoanalyse bij grote en complexe systemen, die vaak grote afbreukrisico's kennen, dient er in de nabije toekomst meer aandacht besteed te worden aan een verdere professionalisering van deze discipline. Gestructureerde en erkende opleidingen en een professionele beroepsvereniging zullen in een grote behoefte voorzien en kunnen het vak op het benodigde hoge peil brengen en houden.

Referenties

- Fullwood, R.R., R.E. Hall. Probabilistic Risk Assessment in the Nuclear Power Industry, Fundamentals & Applications
- Green, A.E., A.J. Bourne. (1972). Reliability Technology
- Reactor Safety Study, an Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. (1975). U.S. Nuclear Regulatory Commission. October
- Rivett, P. Decision Modelling
- William, Ph.D., D. Rowe. (1977). An Anatomy of Risk

1

4 Relatie tussen de diverse bedrijfsprocessen

ir. A.J.M. Huijben[1]

Inleiding

De terugkoppeling over de gerealiseerde betrouwbaarheid is inmiddels op veel gebieden een gangbare werkwijze geworden, maar dat geldt nog niet voor de betrouwbaarheid van een product. Conform de Plan-Do-Check-Act-cyclus (PDCA), geïntroduceerd door Taguchi, is het vanzelfsprekend dat men vaststelt in welke mate de producten aan de gewenste en vermeende betrouwbaarheid voldoen. In de praktijk van elektronische producten is dat nog niet altijd het geval. Dit heeft voornamelijk te maken met de complexiteit van de keten. Veel actoren spelen een rol in de keten en verhinderen daarmee een effectieve en efficiënte terugkoppeling naar de ontwerper en maker.

We illustreren dit door middel van diverse elektronische producten en de analyse van de daarbij behorende keten van actoren. Als uitgangspunt nemen we de definitie van betrouwbaarheid en brengen hierop een verdere nuance aan. Verder wordt een aantal methoden geschetst voor een effectieve terugkoppeling en een data-analyse.

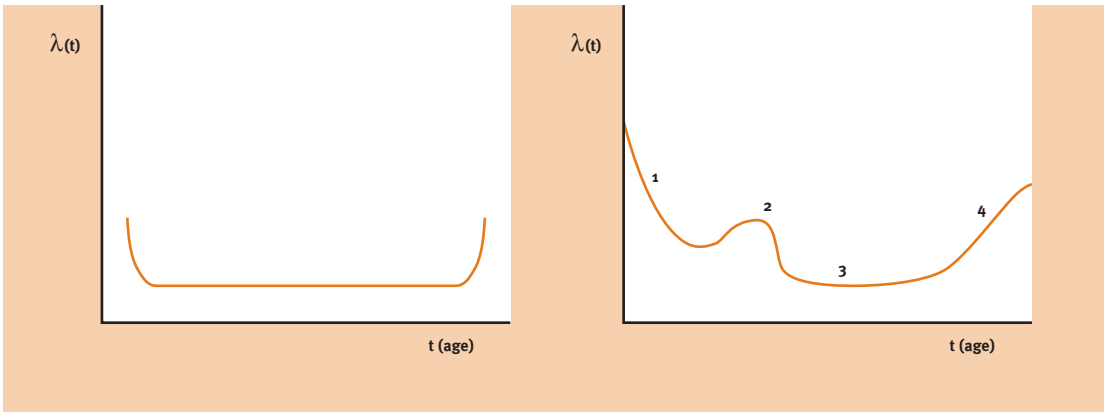
1 Ten tijde van het schrijven van dit artikel was de auteur werkzaam bij Philips Centre for Industrial Technology (CFT), Sector Innovation and Industrial Support, thans als manager Customer Services bij Philips Medical Systems
Postbus 90050
5600 PB Eindhoven

Betrouwbaarheid, de basis

De betrouwbaarheid van een product wordt bepaald door de mate waarin een product zal uitvallen na het in gebruik nemen. Strikt genomen geldt dat betrouwbaarheid de mate is waarin het product een op voorhand vastgestelde *functie* gedurende een gedefinieerde *periode* vervult (zie hoofdstuk 2, deel 1).

Voldoet het product niet aan die eisen, dan noemen we dat falen. De intensiteit van falen zal over de tijd variëren. We kennen allemaal de populaire termen 'producten met kinderziekten' en 'versleten producten'. Hiermee wordt gerefereerd aan vormen van falen die aan het begin, respectievelijk op het einde van de productlevensduur optreden. Dit is geformaliseerd in de badkuipcurve. Stilistisch vertoont een product in het algemeen een intensiteit (lees een kans) van falen zoals aangegeven in figuur 4.1 (links). In de praktijk ziet de curve er vaak veel grilliger uit (rechts).

Figuur 4.1
De badkuipcurve drukt de faalfrequentie uit.



We onderscheiden vroeg falen (1. 'early failure'); vroege slijtage (2. 'early wear-out'); willekeurig en laagfrequent falen (3. 'random' or 'stochastic failure') en ten slotte einde levensduur (4. 'systematic wear-out')

Over elk van deze fasen willen we terugkoppeling krijgen uit de praktijk. Dat wil zeggen dat we ook de eisen aan de betrouwbaarheid op een genuanceerde manier moeten formuleren en dat we bij de analyse van de veldresultaten onderscheid moeten maken tussen de aard en het moment van falen. Kortom, we willen:

- Kwantitatief vaststellen hoe vaak het product faalt (de 'Failure Rate' of 'Field Call Rate'; FCR).
- Dit falen nuanceren over de gebruikstijd van het product; dat wil zeggen als functie van de tijd.
- De onderliggende redenen van falen onderzoeken en vaststellen.

In hoofdstuk 5 (deel 1) van dit boek wordt het MIR-model beschreven. Dit model levert een leidraad bij het systematisch verbeteren van de betrouwbaarheid van het product en is gebaseerd op de hiervoor beschreven wijze van terugkoppeling en analyse.

In het verleden werd de betrouwbaarheid van producten wel beschouwd als een constante eigenschap (de zgn. MTBF; Mean-Time Between Failure) van het product, dus onafhankelijk van de levensduur van het product. Dit is vaak een te beperkte modellering op grond waarvan de betrouwbaarheid slechts op een ongenuanceerde manier kan worden beheerst.

Inmiddels wordt algemeen geaccepteerd dat betrouwbaarheid een tijdsafhankelijke grootheid is en dus varieert met het verouderen van het product. Verder is de mate waarin het product gebruikt en belast is van grote invloed. Dit wordt wel de 'stressor-susceptibility'-theorie genoemd [Brombacher, 1992]. De belasting ('stressor') is een externe factor. De ontvankelijkheid of weerstand ('susceptibility') is een producteigenschap.

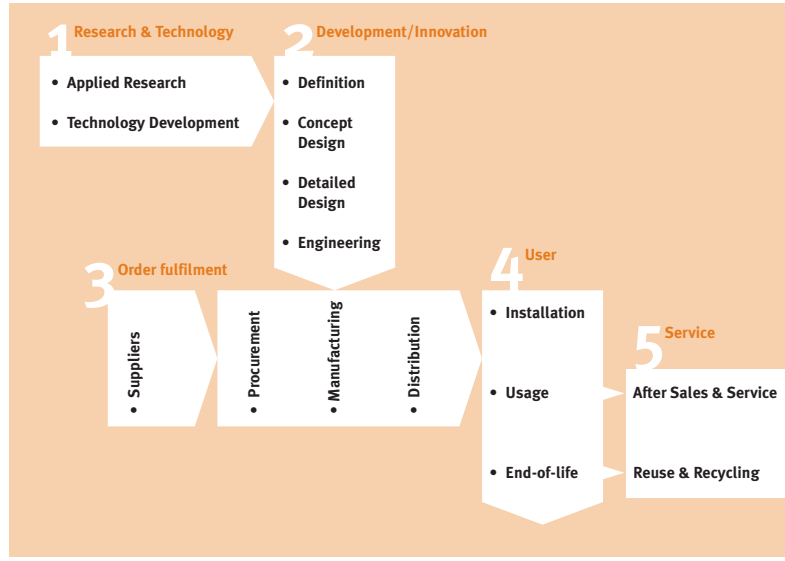
Intuïtief weet u dat ook	**Analogie met arbeidsomstandigheden**
Met welke auto verwacht u de meeste problemen? Een gloednieuwe die nog niet is ingereden, een auto van een jaar die goed is ingereden, of een oude auto van 15 jaar met 200.000 km 'op de klok'? Verder zult u zich bij de aanschaf van een gebruikte occasion afvragen 'Hoe is ermee omgegaan? Wat heeft de auto te verduren gehad'.	Ook hier wordt op een 'stressor-susceptibility'-manier tegen medewerkers aangekeken. 'De medewerker kan veel of iets minder hebben' (susceptibility), maar ook de werkdruk (stressor) is van belang. Een sterke medewerker kan meer hebben. Een medewerker die ook buiten het werk belast wordt, heeft een verlaagde mate van belastbaarheid. Het actuele onderwerp RSI (Repetitive Strain Injury; muisarm) wordt bijvoorbeeld op deze manier benaderd.

Dit alles leidt ertoe dat we bij het ontwerpen van een product of eigenlijk al in de fase waarin de eisen worden geformuleerd het product moeten voorzien van betrouwbaarheidscriteria. Hierbij wordt een aanname gedaan over de manier van gebruik en er wordt geformuleerd hoe vaak het product fouten mag vertonen in elk van de levensfasen. Bij grote aantallen producten spreken we dan meestal over het aantal of percentage producten dat fouten vertoont. Deze aannamen en de daarbij geformuleerde betrouwbaarheidseisen dienen naderhand te worden geverifieerd. Men wil weten in hoeverre het product aan de eisen heeft voldaan om op grond hiervan toekomstige producten eventueel te verbeteren.

Betrouwbaarheid in de diverse fasen

In de diverse fasen die een product doorloopt, zien we de betrouwbaarheid terugkeren (zie figuur 4.2).

Figuur 4.2
De samenhang tussen bedrijfsprocessen.



Bij het definiëren van het product komen betrouwbaarheidscriteria aan bod. Het gaat hier nog slechts om de gewenste betrouwbaarheid van het product. Bij het genereren van productconcepten toetst men het concept aan deze criteria. Zal het product voldoen aan de functionele eisen? In een latere fase als het concept is gekozen en het productontwerp wordt gedetailleerd, worden deze eisen geëvalueerd op de te verwachten betrouwbaarheid en levensduur. Dit wordt vaak middels voorspellende modellen gedaan. Pas als de eerste prototypen van het product verschijnen in de ontwerpfase kan een eerste fysieke inschatting worden gemaakt. Er kan een test worden uitgevoerd, maar er zijn meestal slechts enkele producten – of slechts één prototype van het product – beschikbaar waardoor destructieve testen vaak niet mogelijk zijn. Zodra de eerste proefseries uit productie zijn, kunnen grotere aantallen worden getest. Maar tot dat tijdstip is er nog geen sprake geweest van een product in een werkelijke gebruiksomgeving. De test poogt slechts de realiteit zo goed mogelijk te benaderen. De echte 'proof of the pudding' bestaat uit het versturen en verkopen van de producten, zodat ze in de praktijk gebruikt kunnen worden. 'The real proof is in the eating'. Tijdens het transport kan beschadiging optreden. Tijdens de verkoop kunnen bij de toekomstige gebruiker verkeerde verwachtingen worden gewekt. Dit alles kan ertoe bijdragen dat het product niet of niet correct functioneert of als zodanig wordt gepercipieerd. Dat kan ook gebeuren, doordat de gebruiker het product verkeerd hanteert of voor een verkeerd doel gebruikt.

Misbruik of gebruik

In de praktijk zijn veel voorbeelden van verkeerd gebruik of zelfs van misbruik van producten bekend. Iedereen kent het voorbeeld van het huisdier in de magnetron met als gevolg een klacht van de gebruiker. Onder het Amerikaanse consumentenrecht leidt dit zelfs tot aansprakelijkheidstelling en een bijbehorende schadeclaim.
Ook in Europa zijn dergelijke voorbeelden bekend. Bijvoorbeeld een draagbare telefoon die op het strand met zand en water in aanraking komt. Is de gebruiker hier de schuldige of de producent? Moeilijke vraag, maar een feit blijft dat de consument waarschijnlijk zijn beklag zal doen als het apparaat twee maanden oud is en hierdoor niet meer functioneert. Bovendien zal de 'getroffen' consument in veel gevallen verzwijgen dat het door zijn onvakkundig handelen is ontstaan. Andere voorbeelden zijn videorecorders die door jongere kinderen 'gevoed' worden met een boterham.
In al deze gevallen is het zo dat het feitelijk gebruik en de aanname van de producten over dit gebruik niet met elkaar stroken met als gevolg een klacht. In de meeste gevallen toont de leverancier enige toegeeflijkheid aan de detaillist of verkoper om verdere escalatie te voorkomen.
Wat leren we hiervan? Het is zaak om in de specificatie-, de ontwerp- en de productiefase inspanningen te verrichten om de gebruikscondities, inclusief misbruik zo realistisch mogelijk te evenaren. De beste bron hiervoor is natuurlijk de terugkoppeling uit de praktijk.

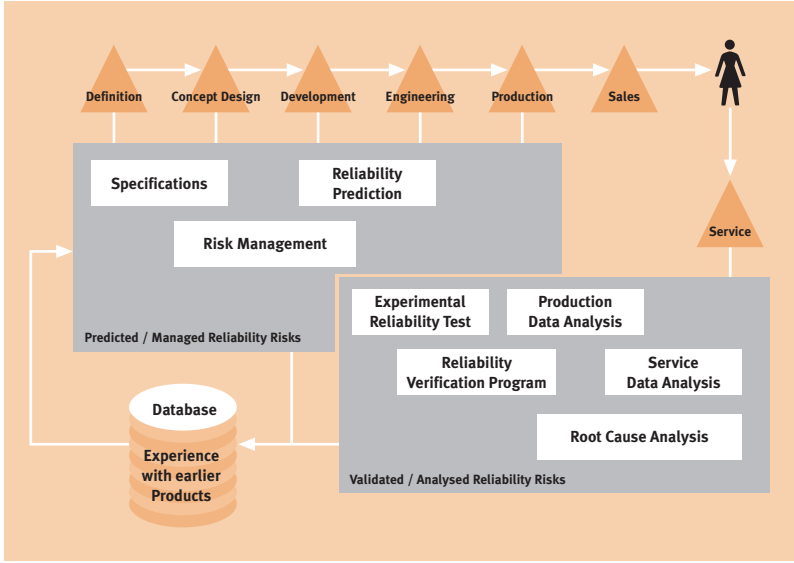
Als we de diverse fasen op het gebied van stressor en susceptibility analyseren, zien we het volgende beeld (zie tabel 4.1 en figuur 4.3).

Tabel 4.1 geeft aan hoe taken kunnen worden gepositioneerd ten opzichte van de diverse fasen van specificatie tot gebruiker. Deze keten wordt vaak door verschillende partijen ingevuld, waardoor de daadwerkelijke terugkoppeling sterk wordt bemoeilijkt en soms zelfs volledig ontbreekt. We bekijken enkele voorbeelden uit de praktijk, waarbij sprake is van een complexe internationale keten die over bedrijven heen loopt.

Tabel 4.1
Analyse van de diverse fasen op het gebied van stressor en susceptibility. Bron: Philips CFT Reliability Group.

Fase	Stressor	Susceptibility
Definitie	Er bestaan slechts matig gedetailleerde beelden over de gebruikscondities. Excessen worden vaak niet meegenomen. Er zijn alleen modelgebruikers die precies doen wat de handleiding voorschrijft.	Het product moet voldoen aan de geformuleerde eisen. Vaak wordt niet in termen van de badkuipcurve gespecificeerd, maar worden doelen gesteld voor: – transportschade; – gemiddelde faalintensiteit (MTBF); – levensduur.

Fase	Stressor	Susceptibility
(Concept-ontwerp)	Er wordt een theoretisch model gemaakt van de belasting die het product moet kunnen doorstaan. Vaak is dat niet tijdsafhankelijk. Er wordt gekeken of de te verwachten krachten de sterkte van het ontwerp niet te boven gaan, bijvoorbeeld door FEA ('Finite Element Analysis', eindige-elementenanalyse). De Monte Carlo-simulatie representeert meer het stochastische en statistische karakter van stressor en susceptibility. Hierbij wordt een aantal willekeurige producten met een bepaalde verdeling in sterkte en susceptibility gekoppeld aan willekeurige krachten. Wel kan in deze fase aandacht besteed worden aan gevoeligheidsstudies. Door te kijken waar bepaalde parameters van het ontwerp gevoelig zijn voor belasting en dus voor betrouwbaarheidsproblemen, kan het product robuust(er) worden gemaakt.	
Engineering	Een of enkele prototypen worden onderworpen aan een niet-variërende belasting. Het stressormodel is dus nog nominaal.	Aangezien er sprake is van een prototype of van een kleine niet-representatieve serie van producten, is er nagenoeg geen variatie in de producten of is deze variatie niet realistisch.
Productie	Het model of de aanname van de belasting is nog steeds niet variabel en dus onvoldoende realistisch. Het aanbieden van producten uit de reguliere productie aan testpersonen die het product zo realistisch mogelijk moeten gebruiken, verhoogt de representativiteit in deze fase.	Bij voldoende omvang van de steekproef mag worden verondersteld dat de gekozen producten realistische eigenschappen hebben en dat de spreiding over deze producten net zo realistisch is.
Distributie	Transportproeven kunnen reeds in de productiefase gedaan zijn. De representativiteit van de belastingen in deze testen is vaak beperkt. Regelmatig proeven uitvoeren in het logistieke traject, bijvoorbeeld door het meesturen van trillingsmeters of versnellingsmeters, verhoogt de representativiteit van de transportbelasting.	De producten zijn volledig realistisch en statistisch voldoende gespreid als er sprake is van testen op het niveau van de 'transporteenheid', bijvoorbeeld grootverpakking, pallet of zelfs een volledig beladen vrachtwagen. Individuele valproeven of trilproeven aan een enkel product ontberen de statistische spreiding over de apparaten. Conclusies over de susceptibility zijn op grond van dergelijke testen dus niet te maken.
Verkoop	De gebruiker krijgt via de verkoper of via de handleiding aangedragen wat een normaal gebruik van het apparaat is. Het komt vaker voor dat (toekomstige) gebruikers een verkeerd en vaak te ruim beeld hebben of krijgen van het toepassingsgebied. Immers, een potentiële koper die de verkoper vraagt naar een gebruiksvorm die op de rand van het acceptabele ligt, brengt hiermee de verkoper sterk in de verleiding om 'ja' te zeggen.	Producten zijn in het algemeen volledig representatief en goed gespreid. Het spookbeeld van het 'maandagochtendapparaat' kent iedereen, maar we mogen veronderstellen dat moderne kwaliteitsnormen in de productie ertoe leiden dat er niet (meer) zoiets bestaat als 'rotte appels' afkomstig uit de reguliere (kwaliteits)productie.
Gebruik	Gebruikers doen de vreemdste dingen met producten. Ga daar maar vanuit. Een efficiënte manier om hierover geïnformeerd te worden kan gevonden worden bij de serviceafdelingen, waar men met de gevolgen van dit gebruik geconfronteerd wordt.	



Figuur 4.3
Analyse van de diverse fasen op het gebied van stressor en susceptibility. Bron: Philips CFT Reliability Group.

Lampen

Diverse soorten lampen (gloeilampen, gasontladingslampen) worden op diverse plaatsen in de wereld geproduceerd, vaak voor een internationale markt. Hierbij is het eerder regel dan uitzondering dat veel van de onderdelen van externe leveranciers worden betrokken.

De fabrikant, assembleur en ontwikkelaar bevinden zich in hetzelfde bedrijf. De onderdelenleverancier en soms ook de assemblagepartij zijn externe relaties. De distributiepartners verzorgen het transport naar de detailhandel, het grootwinkelbedrijf of de OEM-fabrikant[2] (zoals in de automobielindustrie of voor projectverlichting). Dit laatste betekent dat het contact met de klanten en dus ook de serviceverlening door derden wordt afgehandeld. Servicedatabases zijn vaak slechts pover gevuld. Individuele klachten en garantiegevallen zijn in veel gevallen niet eens bij de detailhandel bekend. De doorsnee consument neemt niet de moeite om de gloeilamp terug te brengen als deze sneuvelt. In veel gevallen is het zelfs voor de gebruiker niet eens bekend hoe oud het product was en wanneer en waar het precies is aangeschaft.

Het gevolg is dat geen van de industriële en commerciële partijen enig inzicht heeft in de feitelijke betrouwbaarheid en levensduur van het product. Zelfs al zou men deze informatie hebben, dan is de kans vrij groot dat na analyse de oorzaak in een van de externe processen (onderdelenfabricage, productassemblage of transport) blijkt te liggen. Kortom, de situatie van gestructureerde terugkoppeling van kwantitatieve en kwalitatieve aard is ver weg en waarschijnlijk nooit te realiseren.

2 Original Equipment Manufacturer. Hiermee wordt een fabrikant bedoeld die een product van een ander onder zijn eigen merknaam op de markt brengt.

Computermonitor

Het ontwerp en de productie van computermonitoren vindt plaats op een (beperkt) aantal plaatsen in de wereld van waaruit de distributie over de wereld plaatsvindt. De onderdelen zijn volledig extern geproduceerd; in het gunstigste geval in hetzelfde bedrijf, maar het kan ook een andere divisie of business unit zijn, waarmee dan toch een formele relatie tussen klant en leveranciers bestaat. Het transport wordt door derden verzorgd. Levering vindt plaats aan OEM-klanten die het product onder hun merknaam verspreiden aan de detaillist.
We mogen veronderstellen dat de klant zich wel in alle gevallen bij de verkoop meldt, indien het product niet (goed) functioneert.
Deze gehele keten heeft een aantal voordelen ten opzichte van het voorbeeld van de lampen. De verkopende instantie heeft informatie over het falen van het product. Echter, de partijen in de keten neigen steeds meer naar constructies waarbij de serviceverlening (vervanging, analyse en reparatie) door speciaal

Figuur 4.4
Verlichtingsproduct.
Bron: Philips Lighting.

Figuur 4.5
Computermonitor.
Bron: Philips Consumer Electronics.

hiervoor opgestelde bedrijven wordt verricht. In voorkomende gevallen dient het vergaren en analyseren van betrouwbaarheidsgegevens dan expliciet te worden opgenomen in het samenwerkingscontract. Zo niet, dan zal de service-provider niet meer doen dan strikt genomen noodzakelijk is voor de reparatie en de financiële afhandeling daarvan. Kortom, in een dergelijke constellatie is het mogelijk om het systematisch terugkoppelen van veldgegevens te realiseren. Aangezien we met verschillende bedrijven en nationaliteiten (en dus verschillende talen en culturen) te maken hebben, zijn de beperkingen en tegenwerpingen in de praktijk vaak sterker dan de rationele argumenten om het wel te doen.

Medische systemen

Het derde voorbeeld vinden we in de wereld van de professionele elektronica, namelijk de medische systemen. Het aantal producten is veel kleiner dan in de twee voorgaande voorbeelden.

De ontwikkelafdeling en de productiefaciliteiten bevinden zich vaak in één organisatie. Soms is er sprake van uitbesteding van de ontwikkeling van grote onderdelen of subassemblages. Onderdelen zijn vrijwel altijd ingekocht bij derden. De subassemblage van grotere delen wordt regelmatig ook uitbesteed. De verkooporganisaties verrichten tevens de service van deze systemen, waarbij vaak sprake is van intensieve contacten tussen de serviceafdeling en de gebruikende instantie. Als enige van de drie voorbeelden staan hier industrie en consument of gebruiker direct met elkaar in contact.

De enige hindernis om tot een rijke vorm van terugkoppeling te komen wordt gevonden in culturele verschillen tussen de betrokken partijen. Dit is deels ontstaan, doordat er sprake is van wereldwijde organisaties waardoor de mentale afstand groot is en er sprake is van taalverschillen. Verder speelt een rol dat de mentaliteit en de business drivers in een ontwerp- en productieorganisatie totaal verschillen van die in een serviceorganisatie. Een ontwikkelorganisatie is gericht op innovatie en het vergaren en gebruiken van informatie. Serviceafdelingen zijn primair gericht op snelheid van handelen en kostenbeheersing [Molenaar, in voorbereiding]. In veel cases kan hierin de oorzaak gevonden worden voor de traagheid waarmee de ideale structuur van terugkoppeling ontstaat.

Figuur 4.6
MRI-scanner (Magnetic Resonance). Bron: Philips Medical Systems.

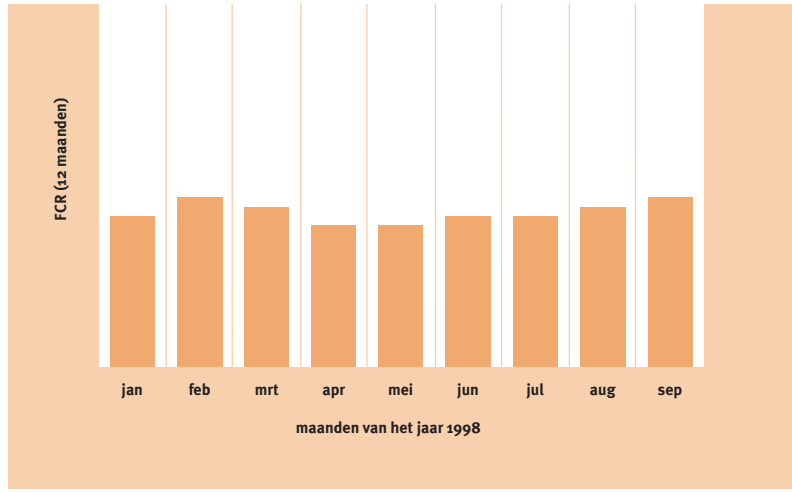
Analyse van velddata

In de vorige paragraaf is geschetst waarom terugkoppeling uit het veld soms niet of slechts moeizaam tot stand komt. In deze paragraaf behandelen we een aantal methoden om velddata te analyseren.
De omvang en het gewenste niveau van detail in de data wordt bepaald door de gewenste analysevormen. De relevante vraag is dus wat willen we concluderen door de data te analyseren? We hanteren hierbij het principe van het MIR-model. Allereerst willen we weten hoe vaak producten falen (MIR 1). Vervolgens willen we weten wat er stuk gaat of faalt (MIR 2) om vervolgens te kunnen analyseren, waardoor dit optrad: de 'root-cause' (MIR 3). Pas daarna is men eraan toe om gerichte verbeteringen in het product of de processen aan te brengen (MIR 4). Hieruit volgt direct het detailniveau van de servicegegevens.

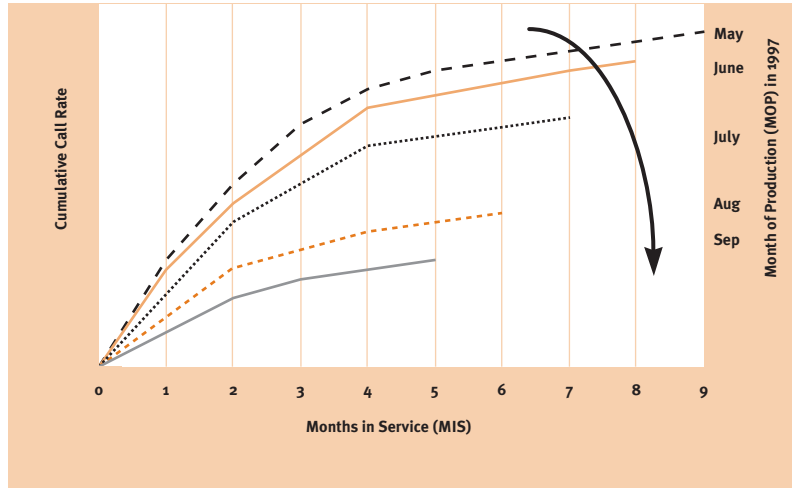
Voor MIR 1 hebben we (slechts) behoefte aan kwantitatieve gegevens. Een percentage dat aangeeft hoe vaak producten falen is voldoende en het tellen van het aantal verkochte en het aantal geretourneerde producten volstaat. De volgende stap (MIR 2) vraagt om overzichten waarin aangegeven is met welk onderdeel of waar in het product iets loos was. Dit kan bijvoorbeeld bestaan uit een lijst van vervangen onderdelen ('spare parts') per reparatie. De analyse van de root-cause vraagt om een omschrijving van de klacht en de uitgevoerde handelingen. Tevens is het van belang om inzicht te hebben in de omstandigheden waaronder de klacht optrad. Hoe meer informatie, hoe liever. Het niet goed functioneren van het computeronderdeel kan veroorzaakt worden door interactie met de omgeving, inclusief de systeemsoftware of de applicatiesoftware. Hier treedt al snel het belangenconflict op. Moet de servicetechnicus al deze gegevens noteren als hij een onderdeel heeft vervangen? Het probleem is opgelost en daarmee af is een veel gehoorde reactie. De MIR 4 stap (verbeteringen ontwerpen) is niet verder afhankelijk van de aangeleverde data. Dus kunnen we constateren dat vooral de stappen MIR 1, 2 en 3 afhankelijk zijn van de beschikbaarheid van veld- en of servicedata.

De kwantitatieve stap MIR 1 lijkt op het eerst gezicht een triviale stap als eenmaal de gegevens beschikbaar zijn. Echter, in de praktijk treedt het volgende probleem op. Bedrijven weten in het algemeen wel hoeveel producten per maand uit de fabriek komen, maar wanneer deze producten worden gebruikt, is minder vanzelfsprekend. Daar komt bij dat bij variërende productie- en verkoopaantallen het verre van triviaal is om het percentage falende producten te berekenen, zelf als men het productie- en faalvolume kent. Een onontbeerlijke bron hierbij is de verkoopdatum van elk gerepareerde product en inzicht in de logistieke pijplijn, waarmee een goede schatting kan worden gemaakt van het totale aantal producten in het veld.

Figuur 4.7
Traditionele rapportagevorm per maand.



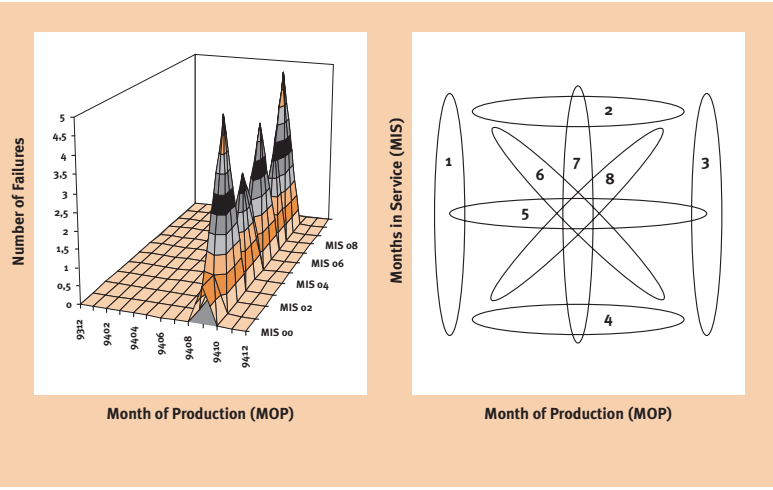
Figuur 4.8
Methode Møltoft.



Vaak wordt de Field Call Rate (FCR) per kalendermaand gerapporteerd. Figuur 4.7 toont de traditionele rapportagevorm (per kalendermaand). In figuur 4.8 zien we de methode volgens Møltoft waarbij de cumulatieve Call Rate als functie van de gebruiksperiode wordt gerapporteerd. Door onderscheid te maken tussen verschillende productieseries is de data veel beter geschikt voor root cause-analyses.

Een ander eenvoudig, maar zeer effectief gereedschap is de MIS-MOP-analyse (zie figuur 4.9). Hiermee kan worden gezocht naar groepen van klachten die tijdens een bepaalde levensduur of in een bepaalde productiemaand zijn opgetreden. MIS staat voor ‘Months in Service’. MOP staat voor ‘Month of Production’.

Figuur 4.9
De MIS-MOP-analyse.



Bij een MIS-MOP-analyse worden alle incidenten of klachten van een bepaald type product in het diagram geplot. Voor de diverse 'bergruggen' zijn plausibele verklaringen te geven:

1 Opstartproblemen in de productie.
2 Einde van de levensduur; systematische slijtage.
3 Aflopende productie met kleinere seriegrootte leidt tot problemen.
4 Verborgen fouten treden kort na ingebruikneming op.
5 Vertraagde foutmechanismen; het product sneuvelt veel vroeger dan zou mogen.
6 Seizoensinvloeden leiden tot fouten in een vaste tijd van het jaar.
7 Fouten ten gevolge van een incident in de fabricage.
8 Het probleem verbetert geleidelijk. Er komen steeds betere, maar geen perfecte producten uit de fabriek.

Tot slot moet worden geconstateerd dat het verrichten van een root cause-analyse weliswaar afhankelijk is van goede en complete veldgegevens, maar de daadwerkelijke analyse vindt plaats door hypothesen te formuleren en deze vervolgens fysiek te toetsen op producten. Dit kan bijvoorbeeld door de vermeende faalmechanismen te forceren door de hierbij behorende belasting te verhogen.

Het effect van snellere innovatie op data-analyse

In veel deelgebieden van de elektronica-industrie is er sprake van een steeds snellere innovatie. Producten volgen elkaar steeds sneller op, waardoor de tijd dat een product op de markt wordt gebracht, steeds korter wordt. De toegestane ontwikkeltijd wordt daarnaast en daardoor steeds korter. Het gevolg is dat er minder tijd is om grondig te werk te gaan in de ontwikkelfase en dat de tijd die

verstrijkt voordat veldgegevens beschikbaar komen, vaak langer is dan de commerciële levensduur van hetzelfde product. Dit dwingt de ontwikkelaar en de fabrikant van deze producten tot een werkwijze waarbij informatie over faalgedrag van producten verder gegeneraliseerd moet worden.

Het effect hiervan is als volgt. In een langzaam innoverende wereld kan men zich veroorloven om de terugkoppeling productspecifiek te laten zijn. Immers, als de informatie beschikbaar komt, kan nog royaal ingespeeld worden op de problemen en kan er nog een herontwerp worden geïntroduceerd. De verbeterde versie zal geruime tijd geproduceerd en verkocht worden, met goed gevolg. Bij een hoge innovatiesnelheid kan dit niet, maar moet men de faalinformatie vertalen naar de competenties van de producerende organisatie, of eigenlijk naar het gebrek aan competenties van die organisatie. In het geval dat opeenvolgende producten door dezelfde mensen worden ontwikkeld of geproduceerd mag men ervan uitgaan dat deze groepen mensen bepaalde sterkten en zwakten vertonen en dat de door deze mensen voortgebrachte producten dus allemaal hieraan leiden. Het is niet vreemd om te veronderstellen dat bepaalde organisaties of bedrijven zwak zijn in elektronica of in kunststof spuitgieten of in hydraulica. Op een dergelijke manier kan de zwakke schakel worden bepaald. Als dit eenmaal is gebeurd, komt echter het lastigste gedeelte, namelijk het systematisch verbeteren of zelfs aanleren van een competentie. In de literatuur over competentiemanagement en kerncompetenties wordt wel gesteld dat het kopiëren van competenties nagenoeg onmogelijk is. Als dit daadwerkelijk zo is, dan rest slechts een oplossing door fusie, bedrijfsacquisitie of samenwerking met partners.

In de virtuele industrie, die is ontstaan onder invloed van het Internet, opereren bedrijven die het merendeel van hun producten laten ontwikkelen en laten produceren. Er worden steeds andere partners en leveranciers gezocht om nieuwe producten te kunnen lanceren, want het gaat steeds om heel andere producten, waarin andere technologieën en dus ook andere competenties gewenst zijn. Dit roept weer een ander dilemma op, namelijk dat het vaststellen van (het gebrek aan) competenties een nauwelijks relevante bezigheid is geworden. Vanwege de organisatiewisselingen kan deze werkwijze niet worden geëxtrapoleerd naar de toekomst en naar toekomstige producten. Dit zal ertoe leiden dat bedrijven die zich in deze context aanbieden met ontwikkel- of productiecapaciteit, hun staat van dienst (en daarmee hun sterkten en zwakten) aantonen aan de hand van hun eerdere productportfolio. Als een bedrijf wordt gevraagd om een bepaald product te ontwikkelen of te produceren, dan mag men ervan uitgaan dat die keuze is gebaseerd op de match tussen de gewenste technologie, en de competenties van het product enerzijds en het bedrijf anderzijds. Als men een complex kunststofproduct of onderdeel wil laten spuitgieten, dan kiest men een

bedrijf dat goed is (gebleken) in soortgelijke kunststofproducten. En daarmee is de gebleken betrouwbaarheid van hun eerdere producten een relevante bron van informatie geworden. En op de eerdere veldgegevens van deze producten zijn de eerder geschetste analysetechnieken van toepassing.
Hiermee is tegelijkertijd de volgende conclusie te trekken. Bedrijven of bedrijfsonderdelen die plotseling een ander soort product gaan ontwikkelen of produceren, zullen daarmee in het algemeen minder resultaat boeken dan met de soort producten die zij daarvoor ontwikkelden of produceerden. Dit laat zich ook doortrekken naar nieuwe distributiekanalen of naar nieuwe markten. Het principe 'schoenmaker blijf bij je leest' geldt hier nog steeds. Een bedrijf dat overweegt om uit te breiden naar andere producten of markten doet er goed aan te overwegen om dat te doen met een partij die daarmee ervaring heeft (opgebouwd).

Complexiteit en betrouwbaarheid van het product

Inleiding

Producten en systemen worden steeds complexer onder andere, doordat steeds meer producten integreren en met elkaar interacteren. Neem als voorbeeld een televisie. De tv anno 2001 zal vaak contact maken met een videorecorder, soms met een pc en soms met een videocamera. In de toekomst komen daar set-topboxen bij en zal de kabelaansluiting veel meer functionaliteit bevatten en meer interactie faciliteren. Dit is nog slechts de functionele interactie van het product. Daarnaast is er nog sprake van de niet-functionele interactie, zoals EMC (overspraakeffecten) of de thermische interactie met de omgeving.

Dit alles leidt ertoe dat producten als geheel steeds complexer worden. Om in die context de betrouwbaarheid te kunnen blijven beheersen, dient zich een aantal methoden aan. Deze paragraaf schetst een aantal mogelijke oplossingen om de toenemende complexiteit het hoofd te kunnen bieden die allemaal gebaseerd zijn op het principe van 'verdeel en heers'.

Systeemdecompositie en architecturen

Een van de wapens tegen complexiteit is systeemdecompositie en architectuurdenken. Productarchitecturen bestaan onder andere op mechanisch, elektronisch en softwaregebied. Voorbeelden van mechanische architecturen zijn universele motoren, een loopwerk voor videorecorders of de beeldbuis van een tv. Deze modulen zijn gespecificeerd naar afmetingen, gewicht en dynamica, onafhankelijk van het product (de set) waarin ze zijn toegepast. Op een zelfde manier herkennen we printplaten ('Printed Circuit Boards', PCB's), waarvan de functionele en niet-functionele eigenschappen zijn beschreven.

Softwarebibliotheken voor softwareontwikkeldoeleinden kunnen als het gevolg van softwarearchitecturen beschouwd worden.
Deze bouwblokken maken het mogelijk dat de systeemontwerper niet alle delen behoeft te (her)ontwerpen, maar gebruik kan maken van bestaande, beproefde modulen. Noodzaak hierbij is dat elk (sub)systeem op een eenduidige wijze is beschreven (gespecificeerd) en getest. De resultaten in de praktijk leiden tot herontwerp van de module. Hierdoor ontstaat een systeem van versies, waarbij compatibiliteit met eerdere versies bewaard dient te worden en faalmechanismen uit het verleden zijn geëlimineerd. De omgeving waarin een module wordt toegepast leidt tot steeds scherpere wensen, waardoor ook een revisie van de modulen gewenst is. Denk aan snellere harddisks of processoren in de pc.

Het geheel van bij een architectuur behorende modulen en subsystemen noemen we een platform. We spreken bijvoorbeeld van een pc-platform. We onderscheiden open en gesloten ('proprietary') platforms. Het pc-platform is een open platform waarbij onafhankelijke producenten delen kunnen aanbieden op grond van een openbaar toegankelijke platformbeschrijving. Dit brengt met zich mee dat men nooit uitputtend kan testen met alle mogelijke randapparaten en configuraties.

Systeem testen

Het testen van modulen is van eminent belang. Tevens hebben we geconstateerd dat modulen en systemen niet uitputtend getest kunnen worden. Het best haalbare is dat een module getest wordt naar de geformuleerde specificaties. We onderscheiden hierin drie niveaus:

- F (Functionaliteit): Vervult de module de gedefinieerde functies?
- R (Robuustheid): Is dit onder alle (gespecificeerde) omstandigheden het geval?
- E (Endurance, duurzaamheid): Blijft de module onder alle omstandigheden werken in de loop der tijd?

De drie niveaus vertonen een duidelijke hiërarchie. Pas nadat de functionaliteit is aangetoond onder nominale omstandigheden, is het zinnig om de robuustheid te testen door de gebruiksomstandigheden te variëren. Technieken als DOE ('Design of Experiments') zijn hierbij noodzakelijk om systematisch het gebruiksgebied te verkennen. Ook dient hierbij buiten het gespecificeerde gebied getest te worden om vast te stellen hoezeer de module overbelast kan worden. Met 'overstress'-technieken als MEOST ('Multi-Environmental Overstress Testing') kan dit op een systematische manier worden gedaan. Na de robuustheid wordt de duurzaamheid geverifieerd door testen. Hierbij wordt het faalgedrag ten gevolge van tijdseffecten vastgesteld. De faalmechanismen zullen op verschillende tijdstippen verschillend zijn en dienen apart opgeroepen te

worden. Hierbij bestaat vaak de behoefte om de test te versnellen. Dit kan alleen met inzicht in het faalmechanisme. Versnellingstechnieken zijn bijvoorbeeld HASS ('Highly Accelerated Stress Screening') en HALT ('Highly Accelerated Life-Testing').

We beschouwen wederom het voorbeeld van het pc-platform. We ontwerpen bijvoorbeeld een pc-insteekkaart. De kaart dient te passen in het hiervoor bedoelde slot in de pc (mechanische interface). Vervolgens moet de pc de kaart herkennen en hiermee interacteren (elektrische en softwarematige interface). De ontwerper wil niet alleen vaststellen of de kaart werkt (functionaliteit), maar ook of dit in alle mogelijke pc's het geval is. Dit laatste kan slechts getest worden in een aantal representatieve pc's. Er zullen echter steeds nieuwe pc's met snellere processoren en met verschillende configuraties verschijnen. Deze verschillen ook in de warmtehuishouding en in hun EMC-gedrag (overspraakeffecten). Het is daarom zinnig om de kaart te testen op hogere dan nu beschikbare klokfrequenties en hogere omgevingstemperaturen. Tot slot wil de ontwerper vaststellen hoe de kaart zich gedraagt in de tijd (duurzaamheid). Het is heel aannemelijk dat de eisen voor een pc-kaart voor particulier gebruik anders (milder) zijn dan voor professioneel (of industrieel) gebruik (robuustheid). Ditzelfde geldt voor de levensduur.

Robuuste technologieën

Een stap verder (en abstracter) dan architecturen en modulariteit vinden we in de robuuste technologieën. Daar waar subsystemen en modulen tastbaar zijn, is een technologie dat niet. Desalniettemin kunnen we spreken van de robuustheid van technologieën. Immers op een zelfde manier als bij fysieke robuustheid kunnen de omstandigheden en de bijbehorende parameters worden gevarieerd. Een robuuste technologie is derhalve een technologie die weinig of niet gevoelig is voor variaties. Dit heeft twee voordelen. Enerzijds komt het natuurlijk de betrouwbaarheid ten goede. Kleine variaties in het productieproces zijn nagenoeg niet merkbaar in de producten. Anderzijds zijn robuuste technologieën bij uitstek geschikt om mee te groeien met de veranderende eisen vanuit de markt. Immers, het is technologisch mogelijk (zonder nadelige effecten) dat parameters variëren. Denk aan kortere cyclustijden, minder materiaalgebruik bij bewerkingsprocessen of toenemende gebruikseisen in de markt.

We beschouwen een voorbeeld van robuuste technologie. Het gaat om het ontwerp en de productie van IC's ('Integrated Circuits'). Aanvankelijk werden IC's ontworpen die functioneerden bij een relatief hoge spanning en stromen.
Bij deze IC's werden relatief hoge spoorafstanden gehanteerd en brede sporen. Onder invloed van de toenemende integratie ging ook de spoordichtheid omhoog. Echter, bij gelijkblijvende spanningen nam hiermee het risico van

doorslag (kortsluiting) enorm toe. Hierdoor ontstond de druk om spanningen en stroomverbruik terug te dringen.
We zien dat er een geleidelijke innovatie en of trend ontstaat om stroomverbruik te reduceren, spoorbreedten te reduceren en de mate van integratie toe te laten nemen. Elk van deze aspecten versterkt de andere.
Een fabrikant die patronen met zeer smalle sporen met een lage variatie kan produceren, zal daarmee in staat zijn om een breed gamma van producten te produceren.

Tot slot

We concluderen dat productbetrouwbaarheid niet los gezien kan worden van de bedrijfsprocessen die deze producten voortbrengen. Naarmate de keten van bedrijven complexer wordt, neemt daarmee de productbetrouwbaarheid af, omdat de kans op miscommunicatie toeneemt en terugkoppeling uit het veld uitblijft. Daar waar in theorie de oplossing simpel is, valt het vaak tegen om dit in de praktijk te implementeren. Organisatorische complexiteit vormt hierbij de bottleneck.

Referenties

- Brombacher, A.C. (1992). Reliability by Design. John Wiley & Sons, Chichester
- Molenaar, P.A., A.J.M. Huijben, D. Bouwhuis, A.C. Brombacher (in voorbereiding). Why do Quality and Reliability Feedback Loops not always Work in Practice?

1

5 Invloed van trends op product-ontwikkeling en op bedrijfszekerheid

prof.dr.ir. A.C. Brombacher[1], *dr. M.R. de Graef, ir. E. den Ouden*[2], *ir. S. Minderhoud*[3], *Y. Lu, MSc*[4]

Inleiding

Op dit moment zijn veel bedrijfsprocessen in beweging. Een toenemende druk op kortere ontwikkelcycli ('time to market'), meer complexiteit van producten en bedrijfsprocessen en steeds meer eisen aan kwaliteit en betrouwbaarheid leiden ertoe dat de productontwikkeling minder eenvoudig te sturen is. Dit artikel[5] bespreekt de relatie tussen de betrouwbaarheid van technische systemen en drie aspecten: kortere ontwikkelcycli, meer complexiteit, en toenemende klanteneisen. Aan de hand van een modelmatige beschrijving van informatie en informatiestromen wordt een aantal problemen met productkwaliteit nader belicht. Een en ander wordt geïllustreerd aan de hand van de resultaten van recent veldonderzoek. Tot slot wordt een aantal mogelijke oplossingsrichtingen gepresenteerd. Hoewel het hier gepresenteerde onderzoek zich vooral richt op producten in de consumentenelektronica, zijn veel van de hier geschetste trends ook van toepassing op andere gebieden waar sprake is van een hoge mate van innovatie en een sterke druk op kortere ontwikkelcycli.

1 Technische Universiteit Eindhoven, Faculteit Technologie Management
Postbus 513
5600 MB Eindhoven

2 Philips CFT, Sector Innovation and Industrial Support
Postbus 218
5600 MD Eindhoven

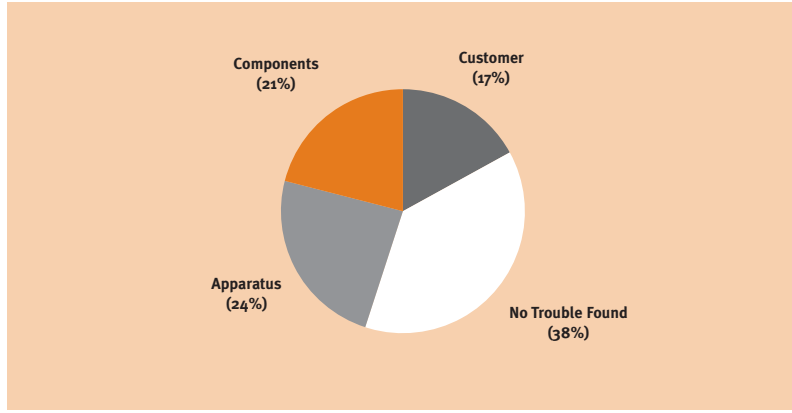
3 Philips CFT, Manager PCP Improvement
Postbus 218
5600 MD Eindhoven

4 Technische Universiteit Eindhoven, Faculteit Technologie Management
Postbus 513
5600 MB Eindhoven

5 Dit artikel is een aanpassing van een eerder verschenen artikel van dezelfde auteurs in [Bedrijfskunde, 2001].

Trends relevant voor bedrijfszekerheid van producten

Veel gangbare literatuur analyseert bedrijfszekerheid als functie van de technische structuur van producten en componenten in deze producten [Henley, 1981]. Ten gevolge van de sterk toegenomen betrouwbaarheid van componenten [Jensen, 1995] en een aantal trends zowel uit de techniek als uit de maatschappij staat deze zuiver technisch gerichte aanpak van betrouwbaarheid sterk ter discussie. Onderzoek door een van de auteurs laat zien dat componenten in veel gevallen slechts in geringe mate problemen met bedrijfszekerheid veroorzaken. Wel speelt de interactie tussen producten en gebruiker en tussen producten onderling een toenemende rol van betekenis [Brombacher, 1996].



Figuur 5.1
Bedrijfszekerheid van moderne consumentenproducten [Brombacher, 1996].

Een mogelijke oorzaak hiervan ligt in een aantal trends in de industrie en maatschappij die een sterke invloed hebben op de kwaliteit en bedrijfszekerheid van (technische) producten. Klassiek wordt kwaliteit veelal gedefinieerd als de mate waarin het product bij aflevering voldoet ('conformance') aan de technische eisen ('specifications'). Traditioneel wordt hieraan vooral aandacht besteed tijdens de productie (uitvoeren en of realiseren van het product). De kwaliteit van het product wordt echter ook in grote mate bepaald door de wijze waarop:

- de klantenwensen door de producent zijn vertaald in een productspecificatie;
- de productspecificatie wordt vertaald in een specificatie van het proces (dat enerzijds in staat moet zijn het gespecificeerde product voort te brengen en anderzijds uitvoerbaar en beheersbaar moet zijn tijdens de eigenlijke productie);
- de specificaties van zowel het product als het proces uiteindelijk worden gerealiseerd;
- de klant in het uiteindelijke product zijn eisen en wensen terugziet ('requirements').

Veel van deze zaken zijn sterk in beweging. Er komt steeds meer technologie ter beschikking, bedrijven doen hun best bedrijfsprocessen steeds efficiënter te laten verlopen, de ketens binnen bedrijfsprocessen worden dankzij zaken als globalisering en outsourcing steeds complexer en bij dat alles stelt de klant ook steeds hogere eisen aan producten. Tijdens een door STT georganiseerde workshop op 23 mei 2000 bleek uit de resultaten van deze workshop een aantal maatschappelijke trends die potentieel een grote invloed hebben (of kunnen krijgen) op de bedrijfszekerheid van huidige en toekomstige technische systemen. Hoewel de participanten bij deze workshop afkomstig waren uit een breed spectrum van de Nederlandse industrie (procesindustrie, voedingsmiddelen, medische industrie, consumentenproducten, bank- en verzekeringswereld, enz.), de overheid en uit onderzoeksinstellingen bleek bij de aanwezigen een brede consensus te bestaan over de volgende invloedsfactoren:

- De toenemende integratie van (steeds complexere) techniek in onze samenleving en de steeds grotere vanzelfsprekendheid waarmee gebruikers verwachten dat deze systemen te allen tijde functioneren.
- De steeds grotere rol van ICT en de steeds grotere afhankelijkheid van informatiesystemen in het maatschappelijk leven.
- De steeds dynamischere bedrijfsstructuren waarbij stabiliteit (door de steeds wisselende economische eisen) en overzicht (door globalisering en uitbesteden) soms ver te zoeken zijn.
- De terugtredende overheid waardoor steeds meer zaken, ook op het gebied van de maatschappelijke infrastructuur, worden overgelaten aan het private bedrijfsleven.

Een en ander betekent dat er enerzijds een steeds grotere druk op bedrijven komt te liggen om bedrijfszekere producten te leveren, terwijl anderzijds diezelfde bedrijven het steeds moeilijker krijgen om de voor bedrijfszekerheid vereiste kennisinfrastructuur te handhaven. De complexere producten stellen hoge eisen aan de kennisinfrastructuur van een bedrijf (men moet in steeds kortere tijd steeds meer over steeds complexere systemen weten), terwijl aan de andere kant de voor deze kennisopbouw vereiste stabiliteit juist lijkt te verminderen; grote delen van de productontwikkelketen worden tegenwoordig uitbesteed aan steeds wisselende partners in soms heel andere delen van de wereld.
Wil een bedrijf in staat zijn bedrijfszekere producten te realiseren, dan betekent dit dat men niet alleen eisen stelt aan het product, maar ook aan het bedrijfsproces waarmee het product tot stand komt, en aan de manier waarop het uiteindelijke product door de klant gebruikt gaat worden[6]. Met andere woorden: wanneer een (eind)product of dienst niet voldoet aan de door de klant aan dat product gestelde impliciete of expliciete eisen, kan onafhankelijk van de door een fabrikant gedfineerde specificaties te allen tijde gesproken worden van een kwaliteits- of bedrijfszekerheidsprobleem. Dit staat in schril contrast tot de

6 In Europa en in de VS verschuift de bewijslast ten aanzien van kwaliteitsclaims steeds meer naar de leverancier. In de VS gaat men als gevolg van de hoge eisen aan 'product liability' (wettelijke aansprakelijkheid van een product) steeds vaker over op een 'no questions asked'-beleid bij het ongevraagd terugnemen van producten. In Europa ziet men een vergelijkbare ontwikkeling, deels dankzij consumenteneisen en voor een deel dankzij wettelijke maatregelen, zoals de wet op de productaansprakelijkheid.

positie die bedrijfszekerheid in het verleden bij veel bedrijven innam. Voor veel producenten was de bedrijfszekerheid van een product alleen relevant in het kader van de veelal beperkte productgarantie. Op dit moment wordt daarom ook door veel fabrikanten de garantie op producten dan ook verlengd (in tijd) en verbreed (naar dekking) [Philips, 1989; Philips, 1999]. Bovendien is op dit moment een producent in het kader van de eerdergenoemde internationale ontwikkelingen op het gebied van de productaansprakelijkheid verantwoordelijk voor een product gedurende de gehele gebruiksduur [Blischke, 1996].

Dit alles maakt het beheersen van kwaliteit en bedrijfszekerheid tijdens de ontwikkeling van een product tot een buitengewoon lastig proces. Een veel groter scala van kwaliteitsaspecten zal gedurende de gehele gebruiksduur van een product moeten worden gecontroleerd. Kernvraag hierbij is hoe men zinvolle parameters vindt waarmee tijdens een ontwikkel- of realisatieproces de mate waarin een product aan deels nog onbekende eisen van toekomstige klanten voldoet, kan worden gemeten. Men dient reeds tijdens de ontwikkeling van een product parameters ter beschikking te hebben waarmee niet alleen het systeemgedrag als functie van het technisch componentgedrag voorspeld en gestuurd kan worden, maar ook het gedrag van het product in interactie met de eindgebruiker gedurende de gehele levensduur van het product. Een aanvullend probleem is dat genoemde parameters zich niet alleen dienen te richten op het product zelf. Oorzaken van problemen met bedrijfszekerheid kunnen liggen in de technische structuur van het product, maar ook in (de structuur van) het bijbehorende bedrijfsproces. Recent onderzoek van Bradley [Bradley, 1999] laat zien dat de oorzaak van veel van deze problemen gezocht kan worden in een slechte afstemming en communicatie in bedrijfsprocessen. Het gaat hier om informatie over problemen die in één deel van het proces wel bekend was, maar in andere relevante delen onbekend bleef. Het is daarom interessant om te onderzoeken welke rol de verspreiding van informatie in moderne bedrijfsprocessen speelt.
De volgende paragrafen zullen daarom aan de hand van een aantal modellen de rol belichten die informatie over bedrijfszekerheid en kwaliteit in het (recente) verleden en in de nabije toekomst in een aantal typen bedrijfsprocessen speelde of mogelijk zal gaan spelen.

Relaties tussen bedrijfsprocessen en kwaliteit en bedrijfszekerheid

Bedrijfsprocessen transformeren invoer naar uitvoer door middel van productiesystemen, informatiesystemen en mensen. Deze processen zijn de primaire processen, waarmee organisaties hun doelstellingen bereiken in termen van

kosten, kwaliteit en tijd. Meer specifiek kunnen deze doelstellingen gedefinieerd worden als:

- optimaal gebruik van materiaal en hulpmiddelen in het primaire proces (kosten);
- de uitvoer van het primaire proces optimaal laten voldoen aan de gestelde eisen aan de kenmerken van het product (kwaliteit);
- de uitvoer van het primaire proces optimaal laten voldoen aan de gestelde eisen aan kwantiteit en tijdigheid (tijd).

Een van de grotere problemen met deze doelstellingen is dat deze 'business drivers' slechts in beperkte mate tijdens het ontwikkel- en realisatieproces te meten zijn. Voor kosten en tijd is het nog gebruikelijk eenvoudige modellen te hanteren tijdens het proces.
Door de voortgang van deze aspecten tijdens het proces van deelactiviteiten te bewaken, tracht men een uitspraak te doen over de voortgang van het proces als geheel. Hoewel – zoals verder in dit artikel besproken zal worden – de genoemde modellen een aantal nadelen hebben, bieden ze tot op zeker hoogte de mogelijkheid om het proces te bewaken en te sturen. Voor kwaliteit bestaan dergelijke eenvoudige modellen niet. Niet alleen ontbreekt consensus over het begrip kwaliteit [Pirsig, 1989], ook is het tot op heden niet mogelijk gebleken kwaliteit volgens de eerdergenoemde klantgerichte criteria op een eenduidige wijze tijdens het proces te meten. De volgende paragrafen van dit artikel zullen hierop nader ingaan.

$$C_{totaal} = \sum_{i=1}^{n} C_{deelactiviteit,i}$$

C_x : Kosten van activiteit X

$$T_{totaal} = \sum_{i=1}^{n} T_{deelactiviteit,i}$$

T_x : Tijd benodigd voor activiteit X

Kwaliteit en bedrijfszekerheid in klassieke ontwikkelprocessen

Er is in een product sprake van een probleem met de kwaliteit of de bedrijfszekerheid op het moment dat een klant ontevreden is over het (niet meer) functioneren van een product. Hieraan kan een breed spectrum van oorzaken ten grondslag liggen; klachten kunnen bijvoorbeeld ontstaan door (al dan niet spontaan optredende) defecten, gebruiksfouten of door een groot aantal andere oorzaken. In veel van de in de jaren vijftig en zestig geschreven literatuur op het gebied van productkwaliteit en bedrijfszekerheid wordt vooral het 'spontaan' falen van componenten gezien als een van de hoofdoorzaken bij het ont-

staan van problemen [Henley, 1981; Coppola, 1984]. Aanbeveling 1, 2 en 3 van de AGREE-commissie (Advisory Group on Reliability of Electronic Equipment) van het US Department of Defence in de VS waren dan ook [Evans, 1998]:

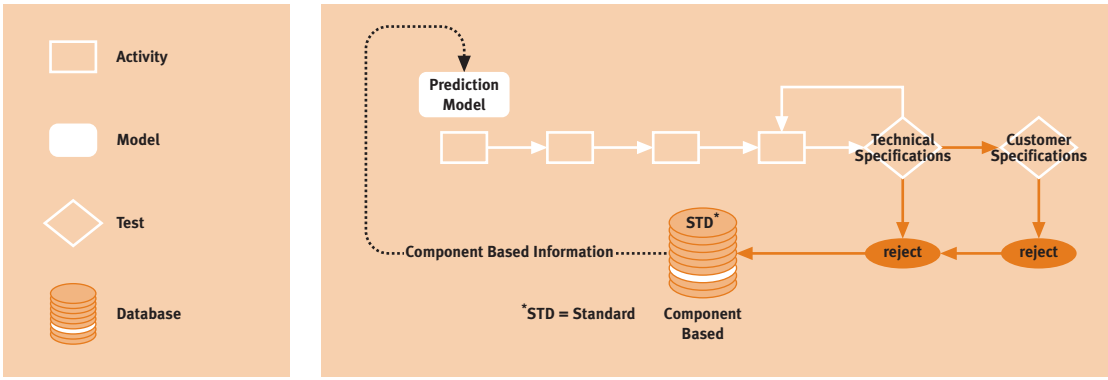
- Het opzetten van een 'field feedback'-systeem voor het vergaren van gegevens uit het veld over het falen van componenten.
- Het ontwikkelen van betere componenten.
- Het verplicht testen op functionaliteit van alle systemen voor gebruik.

Deze AGREE-aanbevelingen zijn vrij direct terug te vinden in de benadering van kwaliteit en bedrijfszekerheid bij ontwikkelstrategieën uit die tijd. Echter, de productontwikkeling is sinds de jaren vijftig vrij sterk in beweging geweest. De vraag is of de benadering van kwaliteit en bedrijfszekerheid gelijke tred heeft kunnen houden met de veranderingen in productontwikkeling. De nu volgende paragrafen zullen aan de hand van een modelmatige beschrijving de relatie tussen productkwaliteit en bedrijfsprocessen laten zien zoals deze zich naar de mening van de auteurs in de loop der jaren ontwikkeld heeft. Vervolgens zullen aan de hand van deze modellen resultaten van veldonderzoek worden gepresenteerd. Deze zullen vervolgens worden gebruikt om te verklaren waarom de huidige benaderingswijzen van kwaliteit niet (meer) toereikend zijn. Tot slot zal een alternatief kwaliteitsmodel worden gepresenteerd dat genoemde nadelen niet lijkt te hebben.

Kwaliteit en bedrijfszekerheid via controle

De aanbevelingen van de eerdergenoemde AGREE-commissie [Erles, 1961] leidden bij productontwikkeling tot een sterke nadruk op de kwaliteit van componenten. Deze benadering is terug te vinden in de handboeken over bedrijfszekerheid uit die tijd [Military Handbook, 1962]. Deze benadering leidt tot het hierna volgende model voor de analyse en optimalisatie van bedrijfszekerheid in productontwikkeling. In dit model nemen twee 'testen' een belangrijke plaats in: de test aan het einde van de productie voor 'conformance to specifications' en de test door de gebruiker gedurende de gehele levensduur van het product. Gegevens uit beide omgevingen werden verzameld en voor zover het componenten betreft verzameld in handboeken en standaarden [Military Handbook, 1987]. In de ontwikkelingsfase van nieuwe producten werd vervolgens met behulp van de aldus verkregen componentmodellen bekeken of het nieuwe product aan de gestelde eisen aan bedrijfszekerheid zou voldoen. Was dit niet het geval, dan werden andere componenten gekozen of als dit geen optie was, werd er gekeken naar (gedeeltelijk) redundante systeemstructuren.

Een groot nadeel van dit proces is de sterk reactieve structuur. Aspecten van nieuwe en of veranderende gebruikers of van nieuwe technologie worden in de productietesten niet meegenomen [Wong, 1988]. Problemen worden geconsta-



Figuur 5.2
Bedrijfszekerheid en kwaliteit in een klassiek bedrijfsproces.

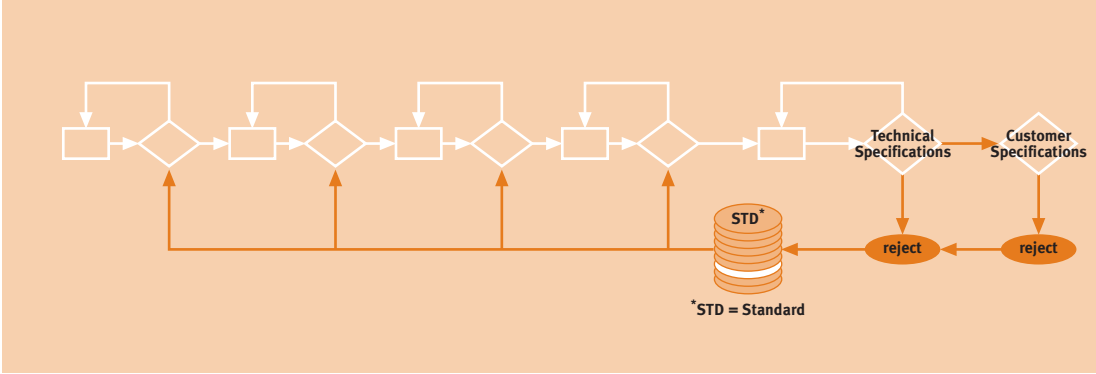
teerd tijdens de productie of in het veld, maar leiden in alle gevallen tot klachten van eindgebruikers of verliezen tijdens productie. In termen van bedrijfsprocessen betekent dit dat alle activiteiten tussen het ontstaan van het probleem en het constateren ervan als verlies kunnen worden aangemerkt. Het systeem is daarmee niet robuust tegen onverwachte klachten en de invloed van nieuwe technologie [Brombacher, 1992; Brombacher, 1994].

Al snel is daarom gezocht naar alternatieve strategieën. Om te voorkomen dat nodeloos kosten worden gemaakt en tijd wordt besteed aan het fabriceren en in de markt zetten van niet (of onvoldoende) werkende producten wordt in modernere bedrijfsprocessen getracht problemen op te sporen bij de bron.

Kwaliteitsanalyse in elke ontwikkelingsfase

In een zogenaamde functionele ontwikkelingsstructuur [VDI, 1973; Pahl, 1984] clustert men gelijksoortige activiteiten. Om te voorkomen dat problemen ver na hun ontstaan opduiken, wordt elke fase van het ontwikkelingsproces afgesloten met een zogenaamde 'phase-gate' of 'milestone'. Tijdens een dergelijke milestone wordt bekeken of er in de betreffende fase geen problemen zijn ontstaan, die verder in het proces tot verspilling hebben geleid. Met betrekking tot kwaliteit en bedrijfszekerheid betekent dit vaak dat men per milestone een serie testen aan het ontwikkelde product uitvoert [Allen, 1971].

Worden verderop in het ontwikkelingsproces of later in het veld toch nog onverwachte problemen gevonden, dan worden de testen dienovereenkomstig aangepast. In de praktijk betekent dit dat op alle activiteiten tussen het via een test opsporen van een probleem en het moment dat een klant hetzelfde probleem uiteindelijk zou vinden kosten en tijd bespaard worden. Door het zogenaamde 'hefboomeffect' [Business Week, 1990] zijn veranderingen vroeg in het ontwikkelingsproces veel goedkoper dan wijzigingen later. Een verandering van een product in het veld is (zie figuur 5.3) meerdere ordegroten duurder dan een wijziging vroeger in het proces en rechtvaardigt daarmee de vaak kostbare testen



Figuur 5.3
Bedrijfszekerheid en kwaliteit in elke fase van het ontwikkelproces.

in dit model. Centraal bij deze benadering staat echter de relatie tussen de test tijdens het ontwikkelingsproces en het uiteindelijke gebruik van een product bij een klant. Bij een valide test zal men problemen reeds tijdens de ontwikkeling kunnen voorkomen. Waar de gekozen testen niet valide zijn, blijven er verschillen (en dus verliezen) bestaan tot op het moment dat de testen worden aangepast. Eigen onderzoek heeft geleerd dat dergelijke aanpassingen gemiddeld drie tot vijf jaar kunnen vergen.
Op deze manier is in termen van regeltechniek een klassiek functioneel ontwikkelingsproces te beschrijven als een systeem dat in sterke mate bepaald wordt door terugkoppeling; men past producten aan op grond van gevonden afwijkingen, hetzij aan het eind van het proces, hetzij tijdens resultaten van productanalyse bij een van de milestones. Deze sterke mate van terugkoppeling resulteert in een vrij conservatief proces. Het starten van een volgende fase voordat een vorige milestone is gepasseerd is niet wenselijk, omdat er altijd afwijkingen gevonden kunnen worden die correcties en aanpassingen noodzakelijk maken. Te vroeg gestarte activiteiten in een volgende fase betekenen in dit kader een extra verspilling van tijd en kosten.

Trends in bedrijfsprocessen

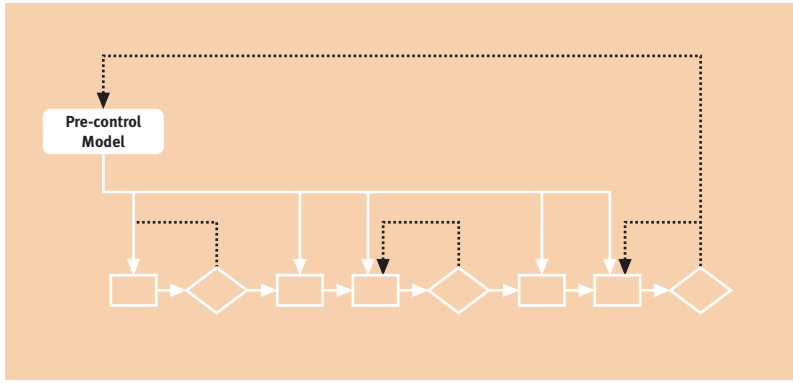
Door de sterke nadruk op verificatie tijdens het proces en de sterke scheiding tussen de functies blijkt een phase-gateproces niet erg slagvaardig. De laatste jaren is er zowel sprake van een sterke druk op kortere ontwikkeltijden [Stalk, 1991; Wheelwright, 1992; Minderhoud, 1999] als – sterk hieraan gerelateerd – van een hoge graad van technische innovatie. Toenemende complexiteit resulteert in sterk toenemende testtijden volgens steeds sneller veranderende (en daardoor onzekerder) testen; de druk op kortere ontwikkeltijden eist juist een sterke verlaging van de totale ontwikkeltijd. Een mogelijkheid om de totaal benodigde tijd in een ontwikkelproces te bekorten zou natuurlijk het parallelliseren van activiteiten in de tijd kunnen zijn. Dit staat echter haaks op de structuur van het phase-gatemodel. Daar start men pas de volgende activiteiten op het moment dat men weet dat voorgaande fasen niet meer aan verandering onder-

hevig zijn. Als het nu op de een of andere manier mogelijk zou zijn de veranderingen (iteraties) in een ontwerpproces los te koppelen van de bijbehorende realisatiefase, dan zou niets een drastische inkorting van de tijd in de weg hoeven staan. Dit principe vormt de basis van een op dit moment veel gebruikte ontwerpstrategie, het zogenaamde 'Concurrent Engineering'.

Concurrent Engineering

Met behulp van methoden zoals Concurrent Engineering [Andreasen, 1987; Minderhoud, 1996; Carter, 1992; Wheelwright, 1992] tracht men in korte tijd zeer complexe producten op de markt te brengen. Concurrent Engineering maakt gebruik van een aantal sterk niet-lineaire aspecten van productontwikkeling. Het phase-gatemodel veronderstelt een verregaande onafhankelijkheid tussen de verschillende fasen. In de praktijk echter [Bradley, 1996] blijken keuzen in het voortraject in zeer sterke mate het natraject te bepalen. Theoretisch lijkt een vroegtijdige optimalisatie van alle aspecten inclusief bedrijfszekerheid en kwaliteit iteraties in het natraject te kunnen voorkomen. Dit maakt vervolgens theoretisch althans tijdreductie door middel van het parallelliseren van activiteiten mogelijk. Als men weet dat bepaalde componenten gedurende het verdere proces niet veranderen, kan men deze componenten (of als ander voorbeeld spuitgietmallen) gerust vroeg bestellen. Dit maakt echter dat het eerder geschetste beheersmodel niet kan voldoen. Men kan niet uitgaan van onafhankelijkheid tussen de fasen, als men juist vooral al in de vroege fasen deze afhankelijkheid gebruikt.

Kent men de kosten per activiteit, de benodigde tijd per activiteit en de onderlinge invloedsfactoren, dan is het mogelijk een ontwerpproces reeds in de vroege fasen te optimaliseren naar kosten en tijd. Wil Concurrent Engineering goed functioneren, dan zal een dergelijk model ook voor kwaliteit moeten gelden. Hoewel de voordelen van Concurrent Engineering bijzonder aantrekkelijk zijn, is de rol van kwaliteit en bedrijfszekerheid in een dergelijk proces relatief onduidelijk. De volgende paragrafen zullen daarom nader op deze aspecten ingaan.



Figuur 5.4
Concurrent Engineering: vroegtijdige optimalisatie in het voortraject.

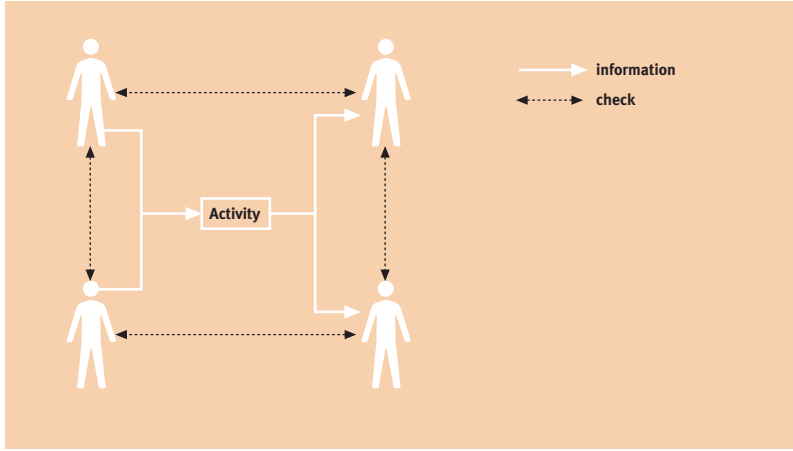
Veldonderzoek naar rol kwaliteit en bedrijfszekerheid in moderne ontwikkelprocessen

Het beheersen van de kwaliteit en de bedrijfszekerheid in een modern bedrijfsproces vertoont veel overeenkomsten met het regelen van een regelkring zoals gebruikelijk is in de regeltechniek. Er is een aspect – in dit geval productkwaliteit of bedrijfszekerheid – dat alleen zuiver te meten is aan het einde of de uitgang van een proces. De stuurfactoren (en de invloed van deze stuurfactoren) waarmee tijdens het proces de uitgangsfactor (kwaliteit) te beïnvloeden is, zijn slechts ten dele bekend. Volgens Eisenhart en Brown [Brown, 1995], maar ook volgens het eerdergenoemde onderzoek van Bradley [Bradley, 1999] speelt (gebrek aan) communicatie een zeer belangrijke rol bij het ontstaan van problemen met kwaliteit en bedrijfszekerheid in het veld. Wil men echter een beeld hebben van de relatie tussen productkwaliteit en de kwaliteit van informatiestromen, dan zal men deze informatiestromen op de een of andere manier moeten kunnen analyseren en kwalificeren. In de nu volgende paragrafen worden achtereenvolgens het ontwikkelen van analysemodellen voor kwaliteitsinformatiestromen en de kwalificatie van deze informatiestromen besproken. De ontwikkelde technieken worden vervolgens toegelicht aan de hand van de resultaten van veldonderzoek. Ten slotte zullen deze analysemodellen gebruikt worden om problemen met kwaliteit en bedrijfszekerheid in de huidige ontwerpprocessen te verklaren en voor toekomstige processen te voorspellen.

Modelleren en analyseren van kwaliteitsinformatiestromen

Gedurende het ontwikkelproces beïnvloeden veel activiteiten direct of indirect de kwaliteit van producten. Deze activiteiten vormen de basis voor de gebruikte informatiestroommodellen. Voorbeelden zijn ‘Failure Mode en Effect Analysis’ (FMEA), maar ook kwalificatiesystemen van componenten of het gebruik van ‘Quality Function Deployment’ (QFD)-matrices. Deze activiteiten genereren informatie over de (toekomstige) kwaliteit van een product. De gegenereerde informatie is echter alleen zinvol, als deze informatie ook daadwerkelijk gebruikt wordt. Vandaar dat per activiteit ook onderzocht wordt wie de gebruikers of klanten van deze informatie zijn. Bij het vormen van een kwaliteitsinformatiemodel gaat men voor het bepalen van de relevante activiteiten uit van activiteiten zoals beschreven in de formele beschrijving van een ontwerpproces. Bij het bepalen van de klantinformatie is het gebruik van formele documenten en structuren beslist onvoldoende [Lu, 1999; Petkova, 1999]. Het is goed mogelijk dat formeel beschreven activiteiten niet (goed) uitgevoerd worden of dat de informatie, gegenereerd door een dergelijke activiteit niet (goed) bereikt wordt. Daarom gebruikt men interviews bij het bepalen van de relaties tussen klant en toeleverancier waarbij bij de toeleverancier en bij de gebruiker van de informatie wordt gecontroleerd of de informatiestroom daadwerkelijk werkt. Indien

Figuur 5.5
Modelleren van kwaliteitsinformatie-stromen: validatieproces.



nodig – bijvoorbeeld bij tegenstrijdige resultaten uit het interview – wordt een en ander geverifieerd aan de hand van documenten.

Met behulp van een dergelijk model is het mogelijk te bepalen welke informatie welk deel van de organisatie bereikt. Het model zegt echter niets over de aard of de kwaliteit van de informatie. Daarom is als tweede stap in het ontwikkelen van een kwaliteitsinformatiestroommodel gezocht naar een kwalificatie van de gebruikte informatie.

Het MIR-concept: kwaliteit van informatiestromen

In de regeltechniek gaat men er vanuit dat bij het besturen van systemen relevante informatie wordt gebruikt. Bij het analyseren van kwaliteit en bedrijfszekerheid hoeft dit laatste, gegeven de opbouw van figuur 5.1 beslist niet altijd het geval te zijn. Daarom gebruiken de auteurs naast het eerdergenoemde informatiestroommodel ook een kwaliteitsindex voor deze informatie. Met behulp van de zogenaamde 'Maturity Index on Reliability' (MIR) [Lu, 1999; Brombacher, 2000] wordt gekeken of de kwaliteitsinformatie:

1 juist gemeten wordt (MIR-niveau 1: 'how much');
2 de juiste actoren in het proces bereikt zijn (MIR-niveau 2: 'where');
3 informatie bevat om de juiste oorzaak('root-cause')van een probleem met kwaliteit of bedrijfszekerheid te analyseren (MIR-niveau 3: 'why');
4 zodanig gestructureerd is dat herhaling van fouten voorkomen wordt (MIR-niveau 4: 'what to do').

Deze vier MIR-niveaus worden samen met het eerder geïntroduceerde informatiestroommodel gebruikt om te analyseren welke structuur een bedrijf gebruikt bij het beheersen van kwaliteit en bedrijfszekerheid. Tevens kan de structuur van een aldus verkregen MIR-model worden gebruikt om te analyseren of de gebruikte kwaliteitsstructuur past bij de eisen die zijn opgelegd door het ontwerp-

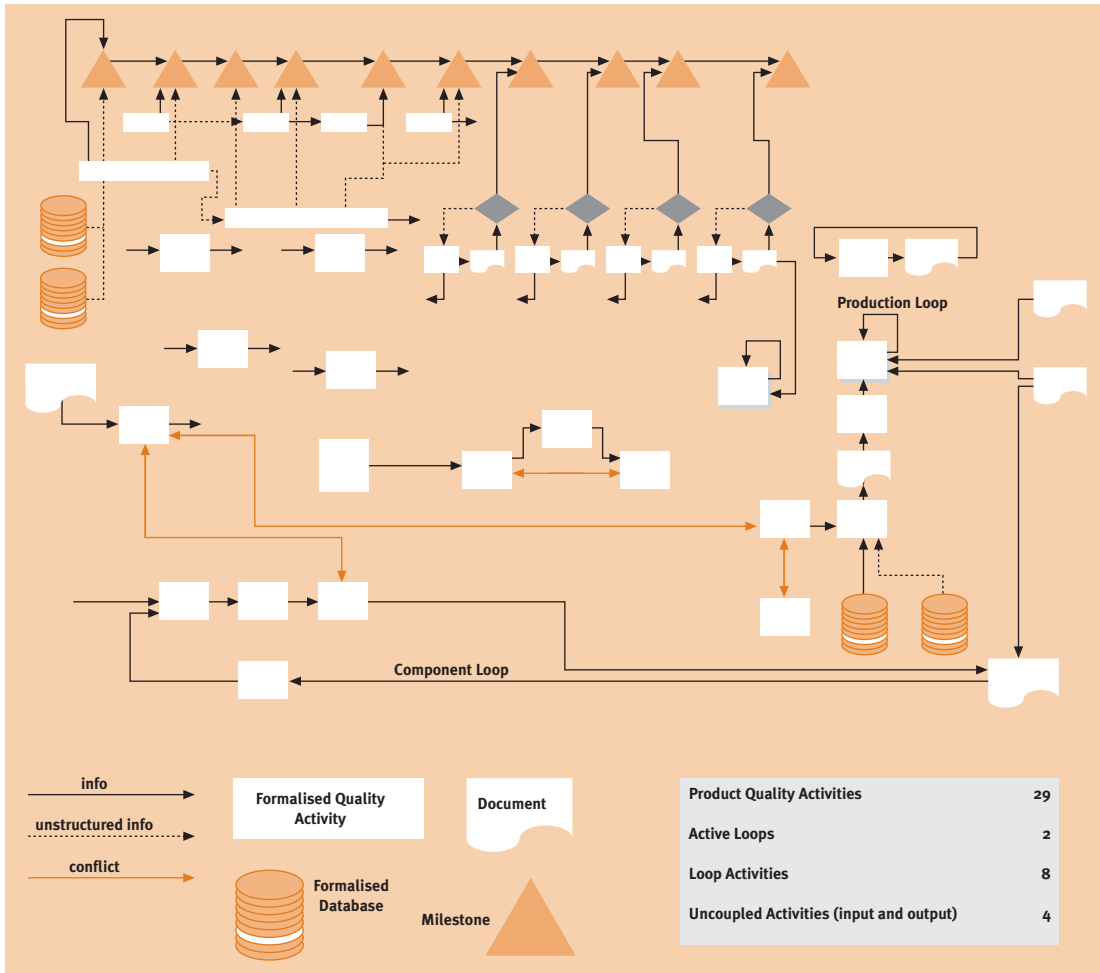
proces. De nu volgende paragraaf zal als voorbeeld een dergelijk (uit veld-onderzoek verkregen) MIR-model presenteren en aan de hand van dit model uitspraken doen over de mate waarin het mogelijk is in een dergelijke structuur de kwaliteit te beheersen en te verbeteren.

Veldonderzoek naar kwaliteitssystemen in tijdgedreven ontwikkelingsproces

In de periode 1995 tot heden zijn in de organisaties van de auteurs dertig MIR-modellen volgens de eerdergenoemde methode ontwikkeld. Figuur 5.6 geeft een sterk vereenvoudigde weergave van een dergelijk onderzoek weer [Lu, 1999].

Het hier geanalyseerde proces kent een groot aantal formeel gedefinieerde kwaliteitsactiviteiten (voorbeelden: FMEA, diverse kwaliteitstesten, simulaties en dergelijke). In het proces bestaan slechts twee regelkringen; systemen waar afwijkingen in het verwachte productgedrag op de een of andere manier worden

Figuur 5.6
Vereenvoudigd voorbeeld resultaten MIR-onderzoek.



teruggevoerd in het ontwikkelproces. De eerste regelkring is een regelkring voor de kwaliteit van componenten. Per component wordt bijgehouden hoe vaak deze component in het productieproces faalt en bij onverwacht gedrag wordt contact opgenomen met de toeleverancier (MIR-niveau 2). De informatie blijkt echter niet gedetailleerd genoeg om de oorzaak te vinden (MIR-niveau 3) met als gevolg dat correctieve acties vaak een beperkt effect hebben. Een andere regelkring zorgt voor kwaliteitsbewaking in het productieproces. Bij afwijkingen in de kwaliteit van dit proces wordt met behulp van een aantal nauwkeurig omschreven analyse-instrumenten een root-causeanalyse uitgevoerd (MIR-niveau 3) waarna correctieve actie volgt. Er zijn echter geen borgingsmechanismen aanwezig om herhaling van een zelfde probleem bij toekomstige generaties producten te voorkomen (MIR-niveau 4). Hieruit valt af te leiden dat er met betrekking tot de kwaliteit veel activiteiten, maar weinig regelkringen bestaan. De resultaten van veel activiteiten worden verder niet in het proces gebruikt. Productoptimalisatie van de kwaliteit en bedrijfszekerheid vindt vrijwel geheel in het natraject (productie) plaats. Dit maakt dat een dergelijk proces op het gebied van kwaliteitsbeheersing veel overeenkomsten vertoont met een klassiek 'quality by inspection'-model. Een iets verdergaande analyse laat weliswaar een groot aantal milestones zien die echter geen deel uitmaken van actieve regelkringen. Ook kan men per milestone een groot aantal testen terugvinden, maar de resultaten van deze testen worden wegens tijdsdruk nauwelijks gebruikt. Ook dit bevestigt het eerdergenoemde beeld van een klassieke quality by inspection-organisatie. Als echter gekeken wordt naar de eisen die aan het hier geschetste proces gesteld worden, dan blijkt dat het hier gaat om een proces met een zeer grote druk op korte ontwikkeltijden en een zeer hoge graad van innovatie. Met andere woorden: een proces dat sterke gelijkenis vertoont met het eerder geschetste model van Concurrent Engineering. Verder onderzoek leert dat – hoewel dit bedrijf verder tracht Concurrent Engineering in te voeren (minder milestones, vroege productoptimalisatie, enz.) – dit niet lukt op het gebied van kwaliteit en bedrijfszekerheid. De vereiste 'voorspellende modellen' voor kwaliteit en bedrijfszekerheid zijn door dit bedrijf niet gevonden of niet ingevoerd. In termen van Concurrent Engineering is het bedrijf dan ook als volgt te karakteriseren:

– Structuur ontwerpproces: Concurrent Engineering.
– Kwaliteitsbeheersing: quality by inspection.

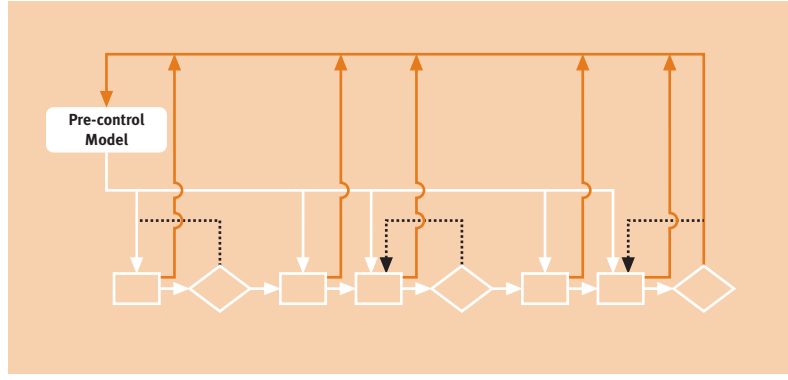
Dit betekent dat terwijl het bedrijfsproces juist een vroegtijdige optimalisatie van alle aspecten eist, de optimalisatie van kwaliteit en bedrijfszekerheid plaatsvindt in een fase van maximale kosten, maximaal tijdsbeslag en minimale flexibiliteit.

Een vergelijking tussen dertig van deze MIR-projecten laat zien dat dit probleem niet typisch is voor het hier genoemde geval, maar eigenlijk overal optreedt waar eisen aan korte ontwikkeltijden gecombineerd worden met een hoge graad van innovatie. Dit schept dan ook de vraag of het praktisch mogelijk is om de eisen van Concurrent Engineering te koppelen aan een goed kwaliteitsbeheers-systeem. Voor het uitvoeren van een rigide testprogramma volgens het phase-gatemodel is de tijd tekort en een goed Concurrent Engineering-voorspelmodel lijkt te ontbreken. Een veelgehoorde klacht hierbij is dat het voorspellen van productkwaliteit vooral voor nieuwe klanten(wensen) in combinatie met nieuwe technologie bijzonder lastig is. Men verwacht dat dergelijke problemen alleen nog maar zullen toenemen door de eerdergenoemde trends in kwaliteit en bedrijfszekerheid.

Een mogelijk alternatief: het iteratieve model

De auteurs stellen daarom een uitbreiding van het eerdergenoemde Concurrent Engineering-model voor, namelijk het iteratieve model. Bij het iteratieve model gaat men enerzijds ervan uit dat men zoveel mogelijk problemen in een vroeg stadium tracht te voorkomen ('pre-control'), maar dat anderzijds nieuwe tech-nologieën en nieuwe klanten een zeer snelle en gedetailleerde terugkoppeling noodzakelijk maken.

Om reden van doelmatigheid (zie de eisen die gesteld worden aan een proces met Concurrent Engineering) zal deze terugkoppeling steeds zo vroeg mogelijk moeten plaatsvinden. Niet passief wachten op de rapportage van fouten, maar actief vroegtijdig zoeken naar mogelijk optredende afwijkingen. De hierbij gekozen strategie vertoont daarmee enige gelijkenis met strategieën die worden gebruikt bij de ontwikkeling van software [Yazdani, 1999].



Figuur 5.7
Iteratief ontwikkelproces.

Conclusies

Kwaliteit en bedrijfszekerheid van consumentenproducten zijn op dit moment sterk in beweging. Niet alleen nemen de klanteneisen op dit gebied toe in tijd en in dekking, ook worden steeds complexere producten in steeds kortere tijd gerealiseerd. Dit artikel laat zien dat het binnen deze veranderende randvoorwaarden niet eenvoudig mogelijk is kwaliteit en bedrijfszekerheid slechts op een manier te hanteren. Quality by inspection is niet of slechts op lange termijn mogelijk bij nieuwe technologie. De milestones in een phase-gatemodel leveren bij een toenemende complexiteit en meer klanteneisen een ontoelaatbare vertraging op. En Concurrent Engineering in de zuivere vorm eist in dat geval een maturiteit van de (modellen van) zowel de technologie als het ontwerpproces, waaraan niet eenvoudig kan worden voldaan.

ontwerpproces	type regelkring (in proces)	tijdconstante	effectiviteit	type regelkring (aanpassings-mechanisme processen)	tijdconstante
Quality by inspection	nvt	nvt	afhankelijk van eindtest	via handboeken / standaarden	4-5 jaar
Phase-gate	per milestone	frequentie milestones	afhankelijk van kwaliteit milestones	updaten inhoud milestones	2-3 jaar
Concurrent Engineering	pre-control	tijdconstanten van pre-control-model	afhankelijk van pre-control-model	alleen via resultaten offline-studies	geen
hybride	per milestone*	frequentie milestones	afhankelijk van kwaliteit milestones**	?	?
iteratief	pre-control + terugkoppeling	tijdcontanten van leerlussen	afhankelijk van snelheid en effectiviteit leerlussen	updaten knowledge base	weken

* aantal milestones voor hybride vorm << phase-gatemodel

** aantal aspecten in milestones << phase-gatemodel

Tabel 5.1
Verschillende modellen van product-ontwikkelingsprocessen en de rol van kwaliteit in dergelijke processen.

Resultaten van eigen onderzoek [Brombacher, 2000] laten zien dat veel bedrijven een hybride ontwikkelingsproces hanteren, waarbij elementen (activiteiten) uit een van de genoemde modellen zijn overgenomen, maar waarbij niet langer aan de aan deze elementen gestelde randvoorwaarden wordt voldaan. De toegevoegde waarde van dergelijke activiteiten lijkt dan ook uiterst gering. Tabel 5.1 geeft een vergelijking tussen verschillende modellen van productontwikkelingsprocessen en de rol van kwaliteit in dergelijke processen.

Aan het kiezen van een bruikbare benadering voor kwaliteit en bedrijfszekerheid lijkt dus allereerst het kiezen van een adequate productontwikkelingsstrategie vooraf te gaan. Hierbij zouden volgens de resultaten van dit artikel de volgende criteria gebruikt kunnen worden:

- Welke markt- en of technologie-eisen aan tijd en graad van innovatie (technisch gezien en voor de klant) worden gesteld aan het proces?
- Welke regelstructuur (product- en procesniveau) hoort daarbij?
- Wat zijn de gewenste tijdconstanten van de regelkringen?
- Welke basisstructuur (een van de genoemde modellen) volgt hieruit?

Het onderzoek laat zien dat het modelleren en analyseren van informatiestromen niet alleen een goed inzicht geeft in het gebruik en de doelmatigheid van de gebruikte kwaliteitsinstrumenten. Uit de aard van de gebruikte regelsystemen is af te leiden welk type kwaliteitssysteem daadwerkelijk werkt. De resultaten van dit onderzoek laten zien dat het operationele kwaliteitssysteem slechts zelden voldoet aan de eisen die het productontwikkelingsproces hieraan stelt. Het hier geschetste iteratieve kwaliteitsmodel biedt wellicht een oplossingsrichting om problemen met kwaliteit en bedrijfszekerheid bij veranderende bedrijfsprocessen het hoofd te bieden.

Referenties

- Allen, T.J. (1971). Communications, Technology Transfer and the Role of Technical Gatekeeper. R&D Management
- Andreasen, H.M., L. Hein. (1987). Integrated Product Development. IFS Publications
- Blischke, W.R., D.N.P. Murthy. (1996). Product Warranty Handbook. Marcel Dekker, New York
- Bradley, W. (1999). Analysis of Industrial Accidents. Symposium The Reliability Challenge. Finn Jensen Consultancy, London
- Bralla, J.G. (1996). Design For Excellence. Mc Graw-Hill
- Brombacher, A.C. (1992). Reliability by Design. John Wiley & Sons, Chichester
- Brombacher, A.C. (1994). Will it really Work? Some Critical Notes on Current Industrial Design Processes. Inaugural Lecture. Eindhoven University of Technology
- Brombacher, A.C. (1996). Predicting Reliability of High Volume Consumer Products; some Experiences 1986–1996. Symposium The Reliability Challenge. Finn Jensen Consultancy, London
- Brombacher, A.C. (2000). Designing Reliable Products in a Cost and Time-Driven Market: a Conflict or a Challenge. Inaugural Lecture. Eindhoven University of Technology, February

- Brombacher, A.C., e.a. (2001). Bedrijfszekerheid van technische systemen bij veranderende bedrijfsprocessen, Bedrijfskunde, tijdschrift voor modern management **2:**49-59
- Brown, S.L., K.M. Eisenhardt. (1995). Product Development: Past Research, Present Findings and Future Directions. Academy of Management Review **2,** Vol. 20
- Carter, D.E., B. Stilwell Baker. (1992). Concurrent Engineering. Mentor Graphics Corporation
- Coppola, A. (1984). Reliability Engineering of Electronic Equipment: A Historical Perspective. IEEE Transactions on Reliability, September
- Cost of non-Quality. (1990). Business Week, April 30
- Erles, D.R. (1961). Reliability Application and Analysis Guide. The Martin Company
- Evans, R.A. (1998). Electronics Reliability: A Personal View. IEEE Transactions on Reliability, September
- Henley, E.J., H. Kumamoto. (1981). Reliability Engineering and Risk Assessment. Prentice Hall
- Jensen, F. (1995). Electronic Component Reliability. John Wiley & Sons
- Lu, Y., H.T. Loh, Y. Ibrahim, P.C. Sander, A.C. Brombacher. (1999). Reliability in a Time-Driven Product Development Process. Quality and Reliability Engineering International
- Lu, Y., H.T. Loh, A.C. Brombacher, E. den Ouden. (2000). Accelerated Stress Testing in a Time-Driven Product Development Process. International Journal on Production Economics
- Military Handbook Reliability Prediction of Electronic Equipment (MIL-HDBK-217). (1962). United States Navy
- Military Handbook Reliability Prediction of Electronic Equipment (MIL-HDBK-217E). (1987). United States Department of Defence
- Minderhoud, S. (1996). The Principles of Concurrent Engineering in Practical Cases. Seminar Concurrent Engineering for Product & Tooling Development in the Precision Engineering Industry. PEDEC and GINTIC, Singapore
- Minderhoud, S. (1999). Quality and Reliability in Product Creation – Extending the Traditional Approach. Quality and Reliability Engineering International, December
- Pahl, G., W. Beitz. (1984). Engineering Design, A Systematic Approach. Design Council, London
- Petkova, V.T., P.C. Sander, A.C. Brombacher. (1999). The Role of the Service Centre in Improvement Processes. Quality and Reliability Engineering International
- Philips Product Warrantee. (1989). Philips Consumer Electronics
- Philips Product Warrantee. (1999). Philips Consumer Electronics
- Pirsig, R.M. (1989). Zen and the Art of Motorcycle Maintenance. Bantam

– Stalk, G., T.M. Hout. (1991). Competing against Time. The Free Press, New York
– VDI-Richtlinie 2222. (1973). Sheet 1, Konzipieren technischer Produkte. VDI-Verlag, Dusseldorf
– Wheelwright, S.C., K.B. Clark. (1992). Revolutionizing Product Development: Quantum Leaps in Speed, Efficiency and Quality. The Free Press, New York
– Wong, K.L. (1988). Off the Bath Tub onto the Roller-Coaster Curve. Proceedings Annual Reliability and Maintainability Symposium. IEEE
– Yazdani, B., C. Holmes. (1999). Four Models of Design Definition: Sequential, Design Centred, Concurrent and Dynamic. Journal of Engineering Design **1**: 25-37, Vol. 10

1

6
Veiligheid in de procesindustrie

ing. R.Th.E. Spiker[1]

Inleiding

De veiligheid in de procesindustrie kent een lange historie, maar de laatste paar jaar zijn er in internationaal verband aanzienlijke wijzigingen in de standaardisatie opgetreden. Berekeningen aan betrouwbaarheid en het aantonen van de betrouwbaarheid van de genomen veiligheidsmaatregelen spelen hierin een grote rol. Maar om de veiligheid waarover we hier spreken duidelijk uiteen te zetten, is het nodig om aan de volgende gebieden enige aandacht te schenken.

1 Yokogawa Industrial Safety Systems B.V.
Postbus 20020
7302 HA Apeldoorn

Veiligheid van productie

De veiligheid waarover we hier spreken is de veiligheid van productieapparatuur in de procesindustrie zoals ketels, reactorvaten, tanks, allerlei roterende machines ten opzichte van de mens en zijn omgeving. Hieronder vallen ook transport (treinen, vliegtuigen) en medische apparatuur.
In deze uiteenzetting beperken we ons tot de procesindustrie. Recente grote ongelukken zoals in tabel 6.1 zijn vermeld hebben de industrie, de regeringen en de burgers met de neus op de feiten gedrukt. Ingewikkelde grote productieprocessen in de procesindustrie kunnen ook grote calamiteiten veroorzaken.

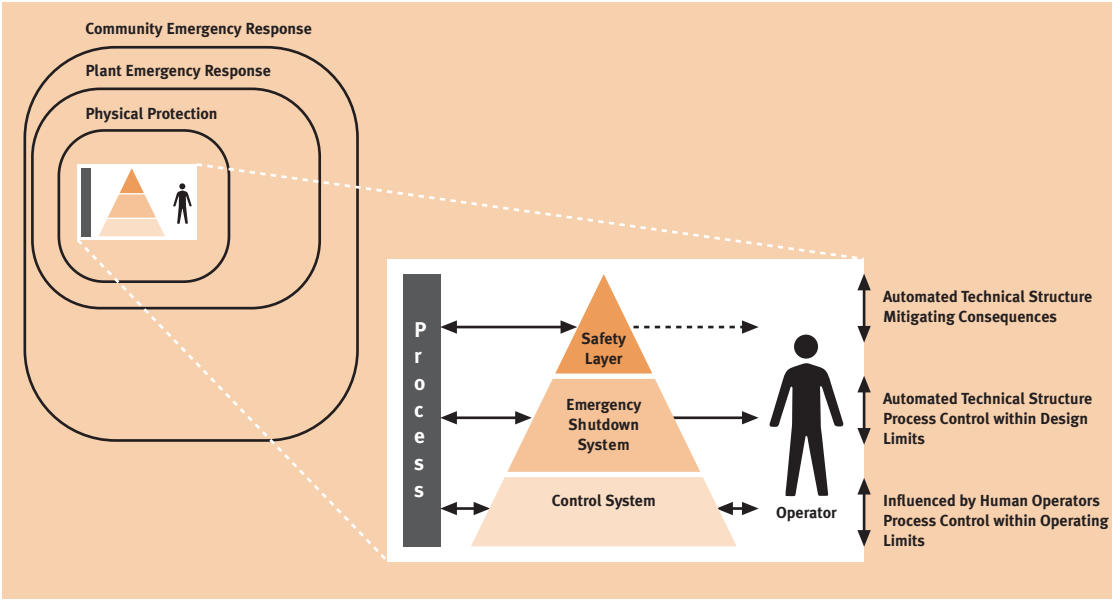
Tabel 6.1
Lijst van bekende industriële ongelukken.

datum	Locatie	type ongeluk	enige cijfers
01.06.74	Flixborough (Groot-Brittannië)	explosie na uitstoot van cyclohexane	28 doden 104 gewonden 3.000 geëvacueerden
01.07.76	Seveso (Italië)	uitstoot van dioxine	200 gewonden 730 geëvacueerden
03.12.83	Bhopal (India)	lekkage van methylisocyanate	2.800 doden 50.000 gewonden 200.000 geëvacueerden
26.04.86	Chernobyl (USSR)	nucleaire reactorexplosie	31 doden 299 gewonden 135.000 geëvacueerden
06.07.88	Piper Alpha (Noordzee)	explosie en brand op een productieplatform	167 doden

Historische achtergronden

Deze ongelukken staan bij de meeste mensen nog in het geheugen gegrift. Elk jaar gebeuren er in de procesindustrie echter kleine en grote ongelukken die alleen in de technische procestijdschriften worden gemeld. Ongelukken met de trein, de luchtvaart en medische ongelukken die geregeld plaatsvinden laten we hier buiten beschouwing.
Waar het hier om gaat zijn de abnormale condities in de betreffende productieprocessen die vaak wel zijn herkend tijdens de uitgevoerde risicoanalyses, maar waarvoor geen of te geringe of inadequate maatregelen zijn getroffen, of waarbij het onderhoud van de veiligheidsmiddelen onvoldoende was.
Ook niet uit te sluiten zijn de vaak niet voorziene gelijktijdigheid van effecten of een onvoorziene reeks van gebeurtenissen in het proces die ogenschijnlijk onafhankelijk zijn, maar later wel degelijk een afhankelijk karakter blijken te hebben.

Het gaat hier om industriële machines en processen die vroeger werden gestuurd door mensen (operators), maar tegenwoordig door computers met de operator als supervisor.
Wanneer bepaalde zaken uit de hand lopen door een fout in de computer of een onvoorziene situatie, dan wordt de operator voor de potentiële gevaarlijke situatie gewaarschuwd door allerlei alarmeringen. Deze alarmen kunnen ontstaan door een verkeerde onderhoudshandeling die door de computer niet wordt herkend (een onvolkomenheid in de programmering), of een combinatiefout van de operator, de computer en het proces, en soms van het onderhoud. In sommige situaties is de tijd te kort voor een operator om in te grijpen. Een mens heeft tijd nodig om de situatie te herkennen en de juiste maatregelen te nemen, specifiek in het holst van de nacht. In andere gevallen is de situatie te complex om binnen een veilige tijd tot een juist (door mensen gevormd) oordeel te komen.
Om deze problemen te voorkomen, zijn beveiligingssystemen ontwikkeld die zowel mechanisch als elektrisch, als elektronisch kunnen zijn.
Een van de eerste mechanische systemen is het veiligheidsventiel op een ketel, maar ook de oude wisselbedieningen bij de spoorwegen kenden mechanische en elektrische vergrendelingen.
Speciale veiligheidskleppen die snel en volledig kunnen afsluiten of openen, en aangestuurd worden door pressostaten en thermostaten als meetsonde in combinatie met een relais zijn voorbeelden van elektrische beveiligingen.
De modernste beveiligingssystemen bestaan uit computers die speciaal zijn ontworpen voor veiligheidstaken en waarbij zeer veel aandacht is besteed aan interne foutdetectie met ook speciale veilige meetsensoren en uitvoerorganen zoals veiligheidskleppen.



Figuur 6.1
Relaties tussen proces, besturing, beveiliging en samenleving.

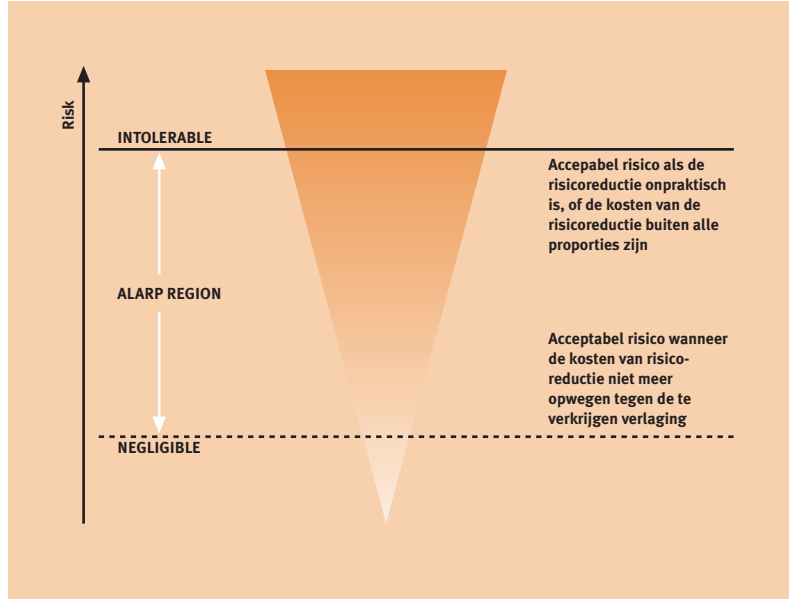
Figuur 6.1 toont de relaties tussen het proces, de diverse besturingen, de beveiligingslagen en de omliggende publieke samenleving.

De acceptatiegraad van een zeker risico, zowel individueel als door de gemeenschap (groep) is de laatste jaren sterk onderhevig aan veranderingen. Een persoonlijk risico veroorzaakt door anderen wordt steeds minder geaccepteerd en de burger vindt dat de staat daarvoor zorg moet dragen. Anderzijds wordt vaak achteloos omgegaan met eigen risico's die door de burger zelf worden veroorzaakt. Het probleem van de staat is nu wat een acceptabel risico voor de burger is. De procesindustrie heeft Internationaal het ALARP (As Low As Reasonable Possible)-model omarmd om risicomanagement mogelijk te maken.
De basis van dit model gaat uit van de gedachte dat het acceptabele risico van een industriële activiteit niet groter mag zijn dan het natuurlijke risico dat de burger loopt door getroffen te worden door algemeen aanwezige gevaren zoals overstromingen, aardbevingen, blikseminslag.

Het risico veroorzaakt door een industrieel proces kan nu in drie delen worden uitgesplitst:
- Een risico dat te groot is om acceptabel te zijn en niet kan worden gereduceerd.
- Een risico zo klein dat het kan worden verwaarloosd.
- Een risico dat zonder extra maatregelen onacceptabel zou zijn, maar wel kan worden gereduceerd.

Hier komt het ALARP-model om de hoek kijken. Figuur 6.2 toont het basismodel.

Figuur 6.2
Risiconiveaus in het ALARP-model.



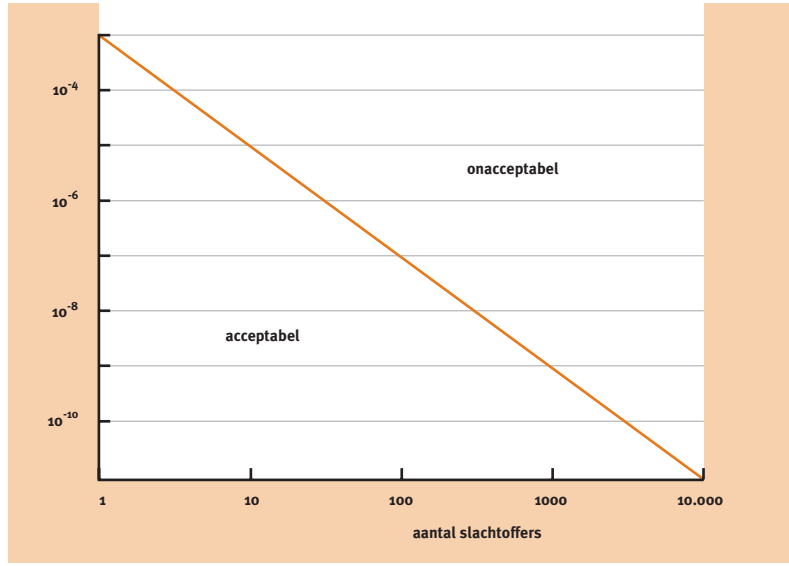
Het zal duidelijk zijn dat het middenniveau een bron van discussie is en in elk land anders wordt gedefinieerd. De reductie van het risico in dit middenniveau wordt bepaald door de totale kosten van die reductie, de regels van het betreffende land en wat door een bepaalde maatschappij als aanvaardbaar of verdedigbaar wordt gezien.

Situatie in 2001

Voor het eerst in de geschiedenis is twee jaar geleden een internationale standaard voor beveiligingssystemen in de proces-, de machine-, de transport- en de medische industrie tot stand gekomen. Hieraan is meer dan tien jaar gewerkt en de consequenties voor sommige industrieën en landen kunnen ingrijpend zijn.
Deze standaard, de IEC 61508 en de daaruit voortvloeiende applicatiegerichte beveiligingsstandaard voor de procesindustrie IEC 61511, is anders dan de reeds aanwezige nationale Duitse en Engelse standaarden.
De 'oude' standaarden waren 'prescriptive' ofwel 'dicterend'. Dit houdt in dat nauwkeurig werd voorgeschreven welk type beveiliging en hoeveel beveiliging in bepaalde procesomstandigheden nodig waren. Ook de beveiligingsapparatuur zelf werd strikt omschreven.

De IEC 61508/61511 echter is opgesteld vanuit de gedachte dat nieuwe ontwikkelingen niet moeten worden belemmerd en dat veel wegen naar Rome leiden.
De standaard is daarentegen 'performance based' ofwel 'resultaat'gericht.
Elk type beveiliging mag worden gebruikt en in elke gewenste hoedanigheid, maar de gebruiker moet op ieder moment kunnen aantonen dat de geïnstalleerde beveiliging adequaat is (met de juiste risicoreductie en technisch functionerend). Hiertoe is voor een levenscyclus ('lifecycle')benadering en een 'verdedigbare' beslissing als rapportagemethode besloten. Dit laatste houdt in dat voor elke technische veiligheidsbeslissing en voor alle materiaalkeuzen een geschreven rechtvaardiging moet worden opgesteld. Specifiek betekent dat een beschrijving van de reden waarom de gebruiker er zeker van is dat de benodigde risicoreductie wordt verkregen en op welke technische gegevens dat feit is gebaseerd.
Aan 'Safety Management' – het opstellen van allerlei test- en handelingsprocedures voor de operator en de onderhoudstechnici – wordt grote aandacht geschonken en daarbij worden eisen gesteld aan de opleiding en ervaring van zowel de leidinggevende als de uitvoerende technici.
De standaard zelf laat zich niet uit over 'hoeveel risicoreductie moet worden toegepast' en wat een aanvaardbaar risico is.
De interpretatie hiervan verschilt van land tot land. In de meeste landen worden

geen grenzen gesteld door de respectievelijke regeringen. Men laat dit over aan de gebruiker en deze moet bij een calamiteit aantonen dat de beveiliging voldoende was. Dit kan problemen opleveren, want een adequate referentie ontbreekt nu. Door jurisprudentie waarvan in het verleden is aangetoond dat het werkt, en technische artikelen van vele soorten procestoepassingen met hun reductie, wordt getracht een referentiekader te krijgen.
Nederland onderscheidt zich door in een wet risicogrenzen te stellen aan industriële activiteiten. Zowel individuele als groepsrisicocriteria zijn vastgelegd. Het individuele risicocriterium geeft een acceptabel risicoprofiel voor individuele personen en maakt geen onderscheid in de grootte van een bepaald ongeval. Ook voor het groepsrisico zijn criteria opgesteld en hier komt het feit naar voren dat een bepaald individueel risiconiveau acceptabel is, maar dat hetzelfde niveau voor een groep onacceptabel is.
De huidige risicoacceptatiecriteria in Nederland zijn weergegeven in figuur 6.3.



Figuur 6.3
Risicoacceptatiecriteria in Nederland.

In het ALARP-model wordt het middenveld door de betreffende procesindustrieën nu ingevuld met behulp van HAZOP-analyses (Hazard and Operability Analysis) en RAS (RISK Assessment Studies), ook wel QRA genoemd (Qualitative Risk Analysis).
Gedurende de HAZOP-analyse worden in een team alle mogelijke deviaties van het proces systematisch en in een logische volgorde onder de loep genomen en alle potentiële gevaren vastgelegd en de mogelijke consequenties omschreven. In een tweede sessie met daarbij alle disciplines vertegenwoordigd (denk daarbij aan proces-, mechanische, elektrotechnische en instrumentatietechnici, ervaren operators van identieke processen en technici met ervaring in milieu en arbeidsveiligheidswetgeving) wordt per potentieel gevaar de mogelijke

frequentie ervan bepaald, maar ook de mogelijke consequenties voor de veiligheid van personen, milieuverontreiniging, productieverliezen, beschadiging en of verlies van bedrijfsmiddelen en bedrijfsreputatie.
Hierbij moet worden opgemerkt dat alleen de veiligheidsvoorzieningen voor mens en milieu zijn vastgelegd in de betreffende standaard en dat alle overige genoemde beveiligingsobjecten een vrije keuze van de gebruiker mogen zijn.
Per potentieel gevaar wordt de benodigde risicoreductie bepaald en uitgedrukt in een benodigd 'Safety Integrity Level' (SIL) en deze wordt uitgedrukt in een kans. Dit SIL is dan de maatstaf per benodigde veiligheidsfunctie.
De IEC 61508/61511 onderkent 4 Safety Integrity Levels. (SIL 1–2–3–4). Per niveau zijn in de standaard duidelijke aanwijzingen te vinden voor de realisatie, de installatie en de validatie van de beveiligingen en die worden dwingend opgelegd. Bij niet voldoen is de betreffende beveiligingsfunctie bij een gebruiker niet in overeenstemming met de standaard.
In de standaard wordt ook veel aandacht geschonken aan de juiste procedures voor alle werkzaamheden aan het desbetreffende proces en aan gericht en specifiek omschreven periodiek onderhoud van alle apparatuur in de beveiligingsketen.
Modificaties aan de beveiligingsapparatuur moeten de levenscyclusstructuur en -volgorde weer volledig doorlopen en de mogelijke invloed van deze modificaties op alle andere beveiligingsketens moet strikt worden nagegaan en vastgelegd.
Kortom de gehele weg van ontwerp van een beveiliging tot het ontmantelen ervan wordt omschreven en is genormeerd.
Een ander aspect is de dwangmatigheid om deze standaard toe te passen.
Op dit moment gaat men in Engeland door de HSE (Health & Safety Executive, te vergelijken met ons Ministerie van VROM) redelijk strikt op wettelijke basis met deze standaard om, maar voor alle andere staten ontbreekt deze wettelijke basis (nog).
Wat is nu de drijfveer voor de industrie om toch deze standaard te gaan toepassen?
Specifiek de grote wereldwijd opererende firma's zijn gevoelig voor kritiek over de veiligheid van hun bedrijfsprocessen. Bij een calamiteit gaat het publiek ervan uit dat er een schuldige moet zijn. De desbetreffende firma moet dan kunnen aantonen dat de geïnstalleerde beveiligingen adequaat zijn ontworpen en onderhouden.

Voordat de internationale beveiligingsstandaard een feit was, ontbrak er een uniform referentiekader om adequaat beveiligingen te kunnen beoordelen.
Met de nieuwe standaard in de hand kan elke (aan)klager die een schadevergoeding wil, nagaan of de betreffende beveiligingen in overeenstemming zijn met de overeengekomen internationale standaard. Dit is mogelijk, omdat het

volledig documenteren van alle genomen technische beslissingen over en uitvoeringen van de veiligheid nu verplicht is en een duidelijk 'auditable trail' (te controleren spoor) moet worden opgesteld.
Het niet nakomen van de gestelde eisen en het niet adequaat documenteren hiervan kan worden gekenmerkt als 'nalatigheid'. Dit gaat vaak gepaard met het betalen van enorme schadevergoedingen die in geval van nalatigheid vaak boven de verzekerde bedragen kunnen uitgaan. Dit is dan nog afgezien van de negatieve publiciteit die hieruit kan voortkomen.

Literatuur

- Rouvroye, J.L. (2001). Enhanced Markov Analysis as a Method to Assess Safety in the Process Industry. Ph.D. thesis Eindhoven University of Technology
- IEC 61508. Functional Safety of Electrical/Electronic/Programmable Electronic Safety Related Systems. International Electrotechnical Commission, Geneve
- Bijlage bij brief aan de Tweede Kamer. (1994). Vergaderjaar 1993-1994, 22.666, nr. 6. 13 Juni
- Apell. (1999). Awareness and Preparedness for Emergencies at Local Level. List of Selected Accidents. UNEP Division of Technology, Industry and Economics (UNEP/TIE). Paris

1

7 Rol management en organisatie in veiligheid en betrouwbaarheid: een kort overzicht

dr. T.W. van der Schaaf [1]

Inleiding

Moderne benaderingen van procesbeheersing in bedrijven gaan er allemaal vanuit dat dit altijd het resultaat is van complexe interacties tussen de drie basiscomponenten: mens, techniek en organisatie. In deze bijdrage bekijken we de rol van de organisatie (en het bijbehorende managementdeel van de personeelsleden) bij de aspecten veiligheid en betrouwbaarheid voor de totale procesbeheersing.

1 Technische Universiteit
Eindhoven, Faculteit Technologie Management
Postbus 513
5600 MB Eindhoven

Geschiedenis

De belangrijke rol die tegenwoordig algemeen wordt toegekend aan de factor organisatie is van vrij recente datum. Volgens psycholoog James Reason (een van de goeroes van dit moment op het gebied van veiligheidsmanagement) doorloopt elke technologie achtereenvolgens drie fasen:

– In het begin wordt de oorzaak (en de oplossing) van elk probleem gezocht in de techniek (de zgn. 'engineering age').
– Daarna wordt (vaak na een aantal incidenten met een duidelijke menselijke invloed) de mens als faalfactor 'ontdekt' (de zgn. 'human error period').
– Ten slotte komt dan (na een of meer zeer complexe (bijna-)ongevallen) uiteindelijk ook de rol van het management en de organisatie in beeld (de zgn. 'socio technical era').

Deze fasen bleken duidelijk terug te vinden in de geschiedenis van een 'oude' technologie als de spoorwegen, maar evenzeer in de veel recentere ontwikkelingen in bijvoorbeeld de kernenergieopwekking. Deze drie zienswijzen zijn dus niet tijdgebonden, maar fasen waar elke nieuwe technologie blijkbaar 'doorheen moet' op weg naar volwassenheid.

Latente en actieve factoren

Reason zelf heeft een belangrijke rol gespeeld bij de overgang van het denken in termen van het zoeken naar 'schuldigen' (vaak degenen op de werkvloer die een machine bedienden of de gebruikers van een product) naar het 'systeemdenken'. Daarbij richt de aandacht zich vooral op de kenmerken van de technische en organisatorische context waarin werknemers hun taken moeten vervullen. Of zoals hij het noemt "blunders at the sharp end" (ook wel actieve fouten genoemd) worden als het ware 'uitgelokt' door verkeerde managementbeslissingen "at the blunt end" (de zgn. latente fouten).

Onvermijdelijke ongevallen

Een tweede invloedrijke bijdrage uit de gedragswetenschappen is die van Charles Perrow, een van de (dissidente) leden van de presidentiële onderzoekscommissie naar aanleiding van de bijna-meltdown van de kerncentrale op Three Mile Island vlakbij Harrisburg in 1979. Deze socioloog van Harvard stelt in zijn boek 'Normal Accidents' dat bepaalde productieprocessen (zoals kernenergieopwekking) inherent onbetrouwbaar zijn, zodat ongevallen dan 'normaal' te verwachten zijn, ongeacht de kwaliteit van het management en het overige

personeel. De combinatie van zeer complexe interacties tussen de processen met een strak gekoppelde organisatie leidt volgens hem tot zeer kwetsbare systemen waarin elke storing zich snel verspreidt door het hele proces zonder dat de organisatie dat tijdig kan waarnemen en corrigeren [Perrow, 1984].

Zoeken naar de zondebok

Ondanks al deze inzichten echter worden nog steeds veel incidenten teruggevoerd tot degenen die 'het laatst met hun vingers aan de knoppen hebben gezeten'. Een voorbeeld is de beruchte East Midlands vliegtuigramp uit 1989 (zie hoofdstuk 12, deel 2) waarbij de piloten na het gedeeltelijk uitvallen van een motor de andere (nog goede motor) uitzetten, waarna het vliegtuig tijdens de landingsfase alsnog neerstortte. Zowel de media als de rechtbank legden de volledige schuld bij "die stomme piloten". Verder onderzoek echter liet zien dat er een groot aantal ernstige latente fouten waren, zoals ontwerpfouten in de (nog gloednieuwe) motoren, ergonomisch slecht ontworpen instrumenten en onvoldoende training van de piloten in dit totaal nieuwe type cockpit, het negeren door de Britse RLD van een reeks van lessen uit eerdere ongevallen waarbij de bemanningen ook niet duidelijk wisten in welke motor zich problemen voordeden. Al deze latente factoren lagen geheel buiten de invloedsfeer van de bemanning, en waren vooral gedreven door kostenbesparing.

Positieve uitzonderingen

Gelukkig kan het ook beter, getuige de succesverhalen die verzameld zijn door Karlene Roberts en haar collega's uit Berkeley, Californië. In de luchtverkeersleiding en op vliegdekschepen hebben zij naar de kenmerken gezocht van 'High-Reliability Organizations' (HRO's) die zich ondanks hun vaak zware belasting en hoogtechnologisch gehalte eigenlijk geen enkel ongeval kunnen veroorloven. Deze organisaties waren in staat om in geval van grote druk of onverwachte problemen snel 'om te schakelen' van een zeer bureaucratische vorm van procesbeheersing (volledig gebaseerd op het strikt volgen van uitgekauwde vaste procedures) naar een flexibele gedecentraliseerde 'professionele' organisatievorm waarin ieders inbreng van laag tot hoog essentieel was. Dit was mogelijk doordat de volgende houding tot risico's continu bevorderd werd:

- het rapporteren van fouten, maar zonder het maken van fouten toe te laten;
- persoonlijk initiatief tot het aangeven van zwakke plekken in de bestaande procedures;
- het vermijden van risico's, maar zonder rigide te worden;
- elkaar in de gaten houden bij kritische taken zonder bemoeizuchtig te worden.

Zo'n positieve 'veiligheidscultuur' alleen was niet voldoende. Er waren ook aanzienlijke investeringen in het kennisniveau en in de motivatie van alle personeelsleden nodig, een continue onderlinge communicatie, en een zeer gevarieerde teamsamenstelling.

Cultuurniveaus

Hoe komen we nu van een 'zondebok'cultuur naar die van een lerende, zich continu verbeterende organisatie? Ron Westrum [Westrum, 1992] heeft dit groeipad op een heldere wijze in drie fasen verdeeld die nogal lijken op de MIR-niveaus van Brombacher (zie hoofdstuk 5, deel 1):

- een 'pathologische' organisatie ontkent of onderdrukt problemen, straft 'whistle blowers', omzeilt zelfs veiligheidswetgeving, en ontmoedigt nieuwe ideeën;
- een 'bureaucratische' (of 'calculatieve') organisatie doet het minimaal vereiste aan risicomanagement en wel volgens het boekje, maar gaat alleen iets nieuws (en dan nog op beperkte schaal) proberen als het zich direct terugbetaalt;
- een 'generatieve' organisatie ten slotte is steeds actief op zoek naar tekenen dat het beter kan, traint en beloont het melden, stimuleert nieuwe ideeën en is bereid tot vergaande interne wijzigingen.

Ontwerpconsequenties

Wat betekent het bovenstaande nu voor ontwerpers van complexe technische producten? In de eerste plaats zal duidelijk zijn dat een organisatie nooit geheel vrij kan zijn van latente fouten, zodat ook de daaruit voortkomende ontwerpen altijd hun ingebakken faalwijzen zullen hebben. Een volwassen organisatie zal dit niet willen ontkennen, maar juist deze mogelijkheid van verborgen zwakke plekken in het ontwerp continu willen benadrukken, en meldingen van mogelijke symptomen daarvan steeds verwelkomen. Vervolgens zal men zo diep mogelijk de patronen in de faaloorzaak van deze symptomen willen onderzoeken, om ze vervolgens tot ontwerpverbeteringen te laten leiden. Nog beter is het om tevens reeds in het product de mogelijkheden in te bouwen die de gebruiker straks in staat moeten stellen om eventueel toch optredende storingen tijdig te detecteren, te diagnosticeren, en vervolgens te corrigeren. Dit optredende 'herstelgedrag' bij de eindgebruiker (zie hoofdstuk 33, deel 2) is tenslotte weer zeer bruikbare feedbackinformatie voor de ontwerpers. Door op deze manier enerzijds de faalfactoren in het product steeds verder te minimaliseren en de herstelmogelijkheden voor de gebruiker te maximaliseren, kunnen de veiligheid en de betrouwbaarheid van het product continu verbeterd worden.

Referenties

- Heinrich, H.W., D. Petersen, N. Roos. (1980). Industrial Accident Prevention, a Safety Management Approach. McGraw-Hill, New York
- Petersen, D. (1989). Techniques of Safety Management, a Systems Approach. Aloray, New York
- Perrow, C. (1984). Normal Accidents: Living with High-Risk Technologies. Basic Books, New York
- Reason, J.T. (1990). Human Error. Cambridge University Press, Cambridge
- Reason, J.T. (1997). Managing the Risks of Organizational Accidents. Ashgate, Aldershot
- Roberts, K.H. (1989). New Challenges in Organisational Research: High-Reliability Organisations. Industrial Crisis Quarterly **3**(2):111-125
- Schaaf, T.W. van der, D.A. Lucas, A.R. Hale (red.). (1991). Near Miss Reporting as a Safety Tool. Butterworth-Heinemann, Oxford
- Turner, B.A., N.F. Pidgeon. (1997). Man-Made Disasters. Butterworth-Heinemann, Oxford
- Westrum, R. (1992). Cultures with Requisite Imagination. In: J. Wise, D. Hopkin, P. Stager (red.). Verification and Validation of Complex Systems: Human Factors Issues. Springer Verlag, Berlijn

1

8
De complexiteitsparadox: over mechanische en adaptieve systemen

dr.ir. J.F.L.M. Brukx[1], *dr. G.L. Wackers*[2]

Kijken door een andere bril

De deelnemers aan dit STT-project hebben een toename van complexiteit genoemd als een van de belangrijke tendensen in de ontwikkeling van hedendaagse technische systemen. Dit zou erop kunnen wijzen dat er iets fundamenteels aan de hand is. Wat precies bedoeld wordt met een toename van complexiteit is echter niet op voorhand duidelijk. Bijna tien jaar geleden heeft men in een ander STT-project [Alkemade, 1992] reeds geconcludeerd dat complexiteit een relatief en subjectief begrip is en dat het daardoor moeilijk is een eenduidige definitie en maat van complexiteit te ontwikkelen.
Komt de perceptie van complexiteitstoename voort uit het feit dat er een wezenlijke verandering in de aard van het systeem is opgetreden? Of is het een kentheoretisch probleem? Zijn technische systemen gewoonweg door hun omvang en ingewikkeldheid niet meer volledig in hun functioneren te begrijpen? Zijn zij niet meer kenbaar? Dat hoeft namelijk niet te betekenen dat zij wezenlijk in hun aard veranderd zijn. Het zou ook kunnen dat de toegenomen belangstelling voor complexiteit te maken heeft met de opkomst van 'nieuwe wetenschappen' die de wereld op een andere manier conceptualiseren. Een nieuwe manier van kijken kan aspecten zichtbaar maken die in het oude perspectief onderbelicht bleven.

1 Syntelligens
Laan van Nederhoven 96
3334 BN Zwijndrecht

2 Universiteit Maastricht,
Capaciteitsgroep
Maatschappijwetenschap en
Techniek
Postbus 616
6200 MD Maastricht

In deze bijdrage willen we nader ingaan op deze nieuwe manier van kijken. We zullen dit doen aan de hand van twee metaforen. Met metafoor bedoelen we hier in brede zin de manier waarop we het een begrijpen in termen van het ander. De ene metafoor representeert de manier van kijken, zoals die zich ontwikkeld heeft sinds de Wetenschappelijke Revolutie. We zullen deze aanduiden met de term machinemetafoor. De andere manier van kijken komt voort uit een beweging die nu ongeveer twintig jaar aan de gang is. Daarin probeert een groeiend aantal wetenschappers uit uiteenlopende gebieden, zoals neurale netwerken, kunstmatige intelligentie, ecologie en chaostheorie een theoretisch raamwerk te ontwikkelen waarin het totale verschijnsel complexiteit gevangen wordt en dat zowel licht werpt op de werking van de natuur als op het reilen en zeilen van de mensheid [Waldrop, 1994]. Deze wijze van kijken ontbeert echter nog een eenvoudige en heldere metafoor. Bij gebrek aan beter zullen we hiervoor de term complex adaptief systeem (CAS) gebruiken. We zullen echter niet proberen complexiteit te definiëren of een overzicht te geven van de zeer uiteenlopende manieren waarop in verschillende wetenschappelijke disciplines het begrip complexiteit wordt gebruikt.

Machinemetafoor

Wetenschapshistorici hebben gewezen op de fundamentele veranderingen in het wereldbeeld die hun intrede deden in de periode die we nu achteraf als de Wetenschappelijke Revolutie aanduiden. Dijksterhuis vatte deze veranderingen samen als de ‘mechanisering van het wereldbeeld’.
De natuurkunde nam hierin het voortouw door het universum op te vatten als een grote, zich voorspelbaar gedragende machine die mechanisch verklaard en mathematisch beschreven kon worden. De mechanisering van het wereldbeeld had ingrijpende gevolgen voor opvattingen over de materie en voor het begrip van causaliteit. Newton vatte materie op als zijnde samengesteld uit kleine, ondeelbare deeltjes met niets daartussen. Aristoteles’ stelsel van vier verschillende vormen van causaliteit werd vervangen door het moderne causaliteitsbegrip dat een nauw spatiotemporeel verband veronderstelt tussen oorzaak en gevolg. Bovendien werd een lineair proportioneel verband verondersteld tussen de grootte van de oorzaak en de grootte van het gevolg. Dit mechanistische wereldbeeld gaf aanleiding tot een experimentele, reductionistische en interventionistische wetenschapsopvatting. Een maakbare wereld kon door technologisch ingrijpen veranderd en ten gunste van de mens verbeterd worden.
De wereld was volledig kenbaar en daardoor in principe althans beheersbaar, controleerbaar en voorspelbaar. In de technologisch veranderde wereld was de mens de bron van de nieuwe orde en werd hij steeds als controlerend en sturend centrum vooronderstelt.

Hoewel Newton niet alleen verantwoordelijk was voor deze omslag in de manier waarop we de wereld begrijpen, wordt zijn naam ermee verbonden, en daarmee met een van de pijlers van onze moderne westerse cultuur.

"Newtonian science, the underpinning of civilization from the 1700s to the present, is rooted in physics and mathematics – rule bound disciplines that require data 'up front' in order to operate. The core of the paradigm, the laws of motion, suggest that the world is a well-behaved machine. It offers the promise of a law-abiding and predictable universe, a belief strengthened by the notion that relationships between cause and effect are simple, clear, and linear. The 'if X ..., then Y' view of the world prevailed for two centuries, delighting scientists whose ultimate goal was to predict and control." [Tetenbaum, 1998].

Deze mechanistische manier van kijken ligt ook besloten in de wijze waarop de hedendaagse ingenieur denkt over het ontwerpen van technische systemen, en over de technische beheersbaarheid en betrouwbaarheid daarvan. Dit denken vanuit de machinemetafoor vinden we ook terug bij managers en bestuurders, vooral in hun houding over bestuurbaarheid en beheersbaarheid van organisaties.

Complexe adaptieve systemen

De tweede manier van conceptualiseren sluit aan bij de relatief nieuwe theorievorming onder complexiteitstheoretici. Sinds enkele decennia houden mathematici en theoretisch natuurkundigen zich intensief bezig met juist die groep fenomenen die de Newtoniaanse natuurkunde lange tijd links heeft laten liggen: complexe, non-lineaire fenomenen; fenomenen die in hun gedrag het proportionele verband tussen oorzaak en gevolg missen en daardoor onvoorspelbaar en moeilijk beheersbaar zijn.

Fysici richtten hun aandacht op weersystemen, op turbulenties in vloeistofstromen, op faseovergangen tussen de vaste, vloeibare en gasvormige toestanden van stoffen en op fluctuaties in de populaties van organismen in ecosystemen. Deze 'chaos'-theoretici ontdekten relatief simpele patronen in de ogenschijnlijke wanorde van de natuur, orde in de chaos [Gleick, 1987; Lorenz, 1993]. Biologen keken met nieuwe ogen naar de fantastische orde en de verbazingwekkende diversiteit die we in de levende natuur aantreffen. Die orde kon niet langer door de invloed van de Darwinistische evolutie op moleculair DNA verklaard worden. Zij veronderstelden dat deze biologische orde ontstond op basis van simpele wetmatigheden die de interactie tussen elementen van een complex dynamisch systeem beheersen. Om hun groeiende begrip van deze fenomenen

onder woorden te brengen introduceerden zij nieuwe 'begrippen', nieuwe concepten. Dit nieuwe begrippenapparaat is nog onaf en sterk in ontwikkeling. Niet alle pogingen om inzichten uit de complexiteitstheorie te vertalen naar het domein van technische systemen zijn even geslaagd. Desondanks levert deze manier van kijken een interessante heuristiek op die ons in staat stelt nieuwe vragen te stellen.

Dergelijke systemen worden aangeduid met de term complexe adaptieve systemen [Waldrop, 1994; Zimmerman, 1998]. Zo beschrijft Stacey [Stacey, 1998] een complex adaptief systeem als volgt: "[a] complex adaptive system consists of a number of components, or agents, interacting with each other according to sets of rules called schemas in such a manner as to improve their behaviour and thus the behaviour of the system which they comprise. In other words, in a complex adaptive system, agents interact in a manner that constitutes learning. Complex adaptive systems operate in an environment that consists of other complex adaptive systems so that the systems and its environment together form a coevolving supra-system that, in a sense, learns its way into the future."

Complexe adaptieve systemen maken deel uit van een omgeving die zelf weer een complex adaptief systeem vormt. Zij zijn open en veranderen als reactie op veranderingen in hun omgeving, terwijl zij zelf als gevolg van hun eigen adaptaties hun omgeving veranderen. Door de niet-lineaire wisselwerking tussen co-evoluerende complexe adaptieve systemen wordt zowel differentiatie als samenhang gegenereerd. Voorbeelden van complexe adaptieve systemen zijn onder andere de hersenen, het immuunsysteem, ecologieën en culturele en sociale systemen. In wezen is elke collectie van mensen, zoals industrieën, ondernemingen, afdelingen van organisaties of teams te beschouwen als een complex adaptief systeem.
In dit complexiteitsperspectief ligt het primaat bij de interacties tussen elementen van het systeem. Het zijn deze lokale interacties die tenslotte de eigenschappen, het gedrag of de orde van het systeem als geheel genereren. Goodwin spreekt in dit verband over een generatief veld van relaties [Goodwin, 1994][3]. Het systeem zelf is de bron van die eigenschappen die daarom 'emergent' genoemd worden.

Zo is het adaptief vermogen een emergente eigenschap die afhankelijk is van het aantal koppelingen tussen elementen van het systeem. Wanneer het aantal koppelingen een bepaalde kritische grens overschrijdt, veranderen de gedragseigenschappen van het systeem. Het overgangs- of grensgebied wordt de 'rand van chaos' genoemd. Het systeem bevindt zich dan in een toestand die ligt tussen statische onveranderlijkheid (evenwicht) aan de ene kant en volstrekte chaos (onvoorspelbaarheid, instabiliteit, geen lerend vermogen of herinnering)

3 Met betrekking tot het ontstaan van structuren in organismen lokaliseert Goodwin generatieve velden op het niveau van het organisme. Goodwin herintroduceert op deze manier het organisme in zijn (theoretische) biologie als een zelfstandige en zelforganiserende bron van orde, van biologische organisatie, waarop enerzijds DNA en anderzijds de omgeving invloed uitoefenen.

aan de andere kant. De rand van chaos wordt gekenmerkt door 'begrensde instabiliteit' waarin adaptief, lerend en innovatief vermogen gecombineerd worden met voldoende organisatie om ervaringen als herinneringen op te slaan en te benutten.
De onafhankelijkheid van complexe adaptieve systemen van een extern organiserend en structurerend principe (DNA of mens of ingenieur) verleent hen 'zelforganiserende' eigenschappen. Ons (zelf)bewustzijn is een voorbeeld van zo'n emergente zelforganiserende eigenschap die gegenereerd wordt door de talloze interacties tussen de neuronen in ons brein.
De lokale interacties in complexe adaptieve systemen lijken te bestaan uit eenvoudige wetmatigheden. In de virtuele wereld van een computer kunnen vrijwel alle uit de populatiedynamica bekende biologische fenomenen gesimuleerd worden met behulp van 'organismen' die bestaan uit enkele simpele regels die hun onderlinge interacties beschrijven. Het ordelijke gedrag van een vlucht vogels of een school vissen kan met slechts enkele regels in een programmeertaal gesimuleerd worden [Lewin, 1993]. Een simpel stapel- en trekmodel waarin de notie van DNA helemaal niet voorkomt, kan alle bloemvormen genereren die we kennen [Linden, 1997].

Dit conceptuele zoeklicht op emergente eigenschappen en zelforganisatie betekent niet dat er geen plaats meer is voor intentioneel en doelgericht handelende mensen of organisaties. Hun actie vindt echter altijd plaats als interactie in een complex adaptief systeem waarvan zij deel uitmaken. Op een globaal niveau kan het gedrag van het systeem niet geheel vanuit de intenties van individuen verklaard worden.

Generatieve velden en technische systemen

Welke plaats moeten we nu binnen dit perspectief aan technische systemen toekennen? Enerzijds kan het ontwerpen en bouwen van een technisch systeem gezien worden als een poging om materie-, energie- en informatiestromen controleerbaar en beheersbaar te maken en af te grenzen van een onvoorspelbare omgeving. Dat past in het perspectief van de machinemetafoor. Tegelijkertijd kan niet ontkend worden dat een technisch systeem gebouwd wordt door en voor mensen, dat wil zeggen dat het zowel in de 'generatieve fase' als in de 'gebruiksfase' onderdeel is van een complex adaptief systeem dat we organisatie noemen.
Dit onderscheid tussen het technische van 'het technische systeem' en het sociale van de organisatie is geen wezenlijk onderscheid dat gelegen is in de aard der dingen, maar is zelf een resultaat van de (differentiërende en samenhang genererende) werking van complexe adaptieve systemen. Het technisch

systeem en het onderscheid tussen systeem en omgeving worden tegelijkertijd geproduceerd in wat we met Goodwin zouden kunnen noemen een generatief veld van (interactieve) relaties tussen actoren.[4]

Behalve de generatieve fase in de levenscyclus van een technisch systeem is ook de gebruiksfase van belang. Na de productie van een artefact vindt verplaatsing naar een nieuwe 'onderhouds- en gebruikscontext' plaats. Hoewel door vormen van al dan niet aan techniek gedelegeerde controle op afstand een voortdurende invloed vanuit de productiecontext soms mogelijk is, komt het technisch systeem onvermijdelijk onder de invloedsfeer van het complexe adaptieve systeem dat de gebruikscontext vormt. Het technisch systeem wordt opgenomen in een nieuw veld van relaties. Zonder die relaties zou het slechts een dood ding zijn. De relaties met onderhouds- en gebruiksorganisaties zijn wezenlijk voor het vermogen van het technisch systeem om zijn beoogde functie te kunnen blijven uitvoeren. Adaptieve processen in de onderhouds- en gebruiksorganisatie zijn dan ook van directe invloed op dat functionele vermogen, op de conditie van het systeem, en daarmee dus ook op de betrouwbaarheid van de technologie.

Optimalisering en kwetsbaarheid: twee kanten van een medaille

In de managementliteratuur zijn de afgelopen jaren diverse artikelen en boeken verschenen die proberen complexiteitstheoretische noties te vertalen naar een nieuwe manier om over het gedrag van bedrijven (en populaties van bedrijven) na te denken. Geïnspireerd door de miraculeuze wijze waarop succesvolle soorten in biologische systemen zich aan hun omgeving of biotoop hebben aangepast, en door de harmonieuze wijze waarop in het lichaam van een organisme gespecialiseerde en gedifferentieerde weefsels en organen samengevoegd zijn tot een organisch functionerend geheel, wordt vaak een bijna automatisch verband gelegd tussen adaptieve processen en lerend vermogen. Dit verband is aantrekkelijk, omdat het een beeld oproept van een bedrijf dat op basis van een innovatief, lerend vermogen in staat is in een snel veranderende markt steeds weer de weg naar de toekomst te vinden.

Adaptieve processen hebben vaak echter een lokaal karakter en zijn niet gericht op het leren of overleven van het geheel. Er is niet altijd één coherente doelstelling. Doelstellingen met betrekking tot bijvoorbeeld veiligheid, economisch rendement en regelmatigheid in het leveren van diensten en goederen hoeven niet met elkaar te sporen. In een organisatie kunnen fricties en breukvlakken ontstaan die informatiestromen afbreken of ombuigen. Adaptieve processen

4 Een 'generatief veld' valt niet samen met de notie van een afgrensbare organisatie. Het kan bijvoorbeeld gaan om actoren (mensen, teams, afdelingen) die in een bedrijf of organisatie werken. Maar zij kunnen ook in verschillende organisaties werken. Relaties kunnen gericht zijn op samenwerking, maar ook gedomineerd worden door competitie.

die volgens lokale criteria als 'leren' worden opgevat, kunnen resulteren in een grotere kwetsbaarheid van het geheel [Rosness, 1992[5]; NOU, 2000[6]]. Een grotere kwetsbaarheid die zich kan uiten in een groter aantal incidenten, ongevallen en technisch falen, is de keerzijde van de medaille van het adaptief vermogen van complexe systemen. Lokale adaptaties die bijdragen aan een beter functioneren van het geheel en soms zelfs noodzakelijk zijn om het geheel op een aanvaardbare manier te kunnen laten functioneren, dragen in andere omstandigheden bij aan het falen van het systeem. De notie van kwetsbaarheid heeft betrekking op de toestand of conditie van een systeem en niet op gebeurtenissen (ongevallen, technisch falen) die in veiligheids- en betrouwbaarheidsstatistieken worden opgenomen. Twee voorbeelden kunnen dit verduidelijken.

John Law laat in zijn analyse van een treinongeval bij Ladbroke Grove in de buurt van het Paddington Station in London zien dat het strikt volgen van voorgeschreven veiligheidsprocedures tot gevolg zou hebben dat dagelijks in Engeland ergens het treinverkeer stil zou komen te staan met alle gevolgen van dien. Veiligheidsvoorschriften eisten van verkeersleiders dat steeds als er een 'signaalsituatie' ontstaat die aangeeft dat een trein door 'rood' is gereden het treinverkeer in de omgeving stilgelegd moet worden. Verkeersleiders hadden echter geleerd dat in de meeste gevallen waarin zich een dergelijke situatie voordeed de machinist zelf al de trein tot stilstand had gebracht. Binnen 20 seconden belde de machinist de verkeersleiding om te bevestigen dat dit inderdaad het geval was. In afwijking van de formele voorschriften ontwikkelde zich – door lokale adaptaties – een praktijk waarin eerst even werd afgewacht voordat actie ondernomen werd. Die praktijk leidde er echter ook toe dat niet op tijd werd ingegrepen, toen een trein echt door rood reed en op een andere passagierstrein botste. Law[7] concludeert dat: "if the prevailing practice of the signalmen across the network was in fact to 'wait and see' then this was a system imperfection which actually helped to keep the wheels turning almost all of the time. Or more generally, that … system imperfections are necessary if systems are to run at all."

Snook laat in zijn analyse van het neerschieten van twee Black Hawk helikopters van de Amerikaanse landmacht door twee F15-jachtvliegtuigen van de Amerikaanse luchtmacht in Noord-Irak zien dat een in het ontwerp van het Pentagon in hoge mate geïntegreerde 'task force'-organisatie (Provide Comfort) door lokale adaptaties na verloop van tijd 'ontkoppeld' raakt [Snook, 2000]. Voor het functioneren van de organisatie als geheel bleef dit enkele jaren lang zonder gevolgen, omdat zich nooit situaties voordeden die een hoge integratie vereisten. Dat veranderde toen twee helikopters van de Amerikaanse landmacht de 'no fly-zone' binnenkwamen vóór de eerste F15-jagers en zonder dat de vluchtleiding in het AWACS-vliegtuig van hun aanwezigheid op de hoogte

5 Rosness definieert kwetsbaarheid als "[a] set of characteristics of an open system which limits its ability to survive and perform its mission when exposed to adverse conditions which the system was not designed, constructed or developed to tolerate."

6 Dit Noorse rapport zegt over kwetsbaarheid "Vulnerability is an expression of the functional problems a system will encounter when it is subjected to an undesired event, as well as the problems the system will have in reestablishing its operation after the event has occurred. Vulnerability is tied to a possible loss of value. In this context systems can for example be a state, the national energy supply, a company or a stand alone data system. To a large extend vulnerability is self-inflicted. It is possible to influence vulnerability, to limit or reduce it."

7 Zie http://www.comp.lancs.ac.uk/sociology/soc055jl.html

was. De helikopters werden zowel elektronisch als visueel (verkeerd) geïdentificeerd als vijandige helikopters en conform bestaande gevechtsinstructies neergeschoten.

Snook noemt dit soort gedrag in een organisatie 'practical action'. Het is lokaal gezien efficiënt; het is verkregen uit praktische ervaring en is verankerd in de logica van de taak en het wordt gerechtvaardigd door dagelijkse routinematige herhaling. Dit naar lokale standaarden efficiënte en door lokale ervaring gelegitimeerde gedrag is het gevolg van lokale adaptaties die resulteren in wat Snook een 'practical drift' noemt, waardoor in de loop van de tijd de oorspronkelijke sterk gekoppelde organisatie vervangen wordt door een serie van lokale adaptieve subunits (AWACS, US Airforce, US Army) die elk hun eigen versie van 'de regels' rechtvaardigen.
Het begrip 'drift' verwijst naar een verandering in de loop van de tijd, naar een beweging weg van, een afwijking van een ideaal, doel of standaard [Ciborra, 2000 [8]]. Volgens Snook is het: "this disconnect, this delta, this gap between the locally emergent procedures actually being followed in various subgroups from those that engaged actors assume are dictating action, that constitutes a general set of conditions that increases the likelihood of disastrous coordination failures."

De uit lokale adaptaties en drift resulterende kwetsbaarheid is een emergente, dynamische eigenschap van het systeem die lange tijd of het grootste deel van de tijd verenigbaar is met een aanvaardbaar functioneren van het systeem als geheel [9] [Perrow, 1999].

Paradoxen voor de toekomst

Wat betekent dit alles voor de toekomst? Voor de betrouwbaarheid van complexe technische systemen? Voor het management van complexe organisaties? Charles Handy [Handy, 1995] schrijft in zijn boek 'Beyond Certainty': "We must not let our past, however glorious, get in the way of our future."

We moeten onderkennen dat de benaderingen en strategieën die in het verleden succesvol zijn gebleken dat niet noodzakelijkerwijs in de toekomst hoeven te zijn. We hoeven niet te ontkennen dat in het westen de Newtoniaanse mechanistische wijze van denken (in wetenschap, technologie en management) ons de welvaart heeft gebracht die we vandaag ervaren. Tegelijkertijd is de wereld door de technische systemen die in de loop van de 20e eeuw werden gebouwd, veranderd op een wijze waardoor wij haar niet meer kunnen begrijpen en beheersen met datzelfde conceptuele en praktische instrumentarium. Dit levert

8 Ciborra e.a. gebruiken het begrip 'drift' om aan te geven dat de uitkomst van top-down beleidsinvoeringsprocessen de neiging hebben om 'off-mark' te zijn.

9 Er zijn ook noties van kwetsbaarheid die een statisch of structureel karakter hebben. Een enkelvoudige lijn voor datatransmissie van A naar B is kwetsbaarder dan een cirkelvormige of een netwerkconfiguratie. In de anatomie van het technisch systeem kan dan een achilleshiel geïdentificeerd worden. 'Normal Accidents' van Perrows kan ook gelezen worden als een argument over de structurele kwetsbaarheid van sterk gekoppelde en complex-interactieve systemen.

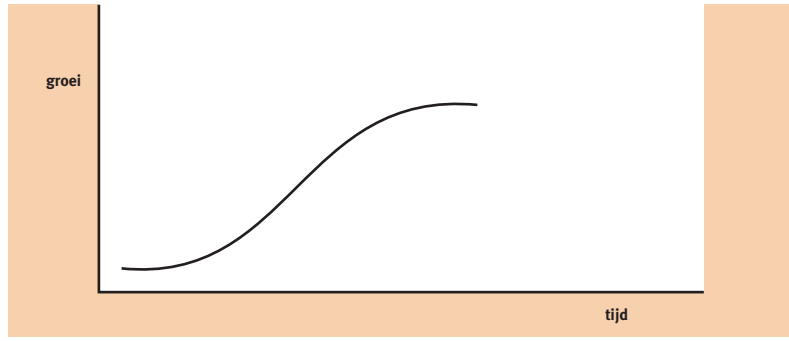
paradoxale situaties op. Complexiteitstheoretici suggereren dat deze problemen niet meer door 'meer kennis' in het oude Newtoniaanse paradigma kunnen worden opgelost. De ontwikkelingen in de laatste decennia op het gebied van de transporttechnologie en de informatie- en communicatietechnologie (ICT) hebben ertoe geleid dat de interactiviteit en de onderlinge afhankelijkheid tussen mensen, dingen en processen enorm is toegenomen. Dit gegeven en de toenemende diversiteit door de wereldwijde trend van individualisering en de toename in de snelheid waarmee veranderingen zich voltrekken en elkaar opvolgen, maken dat de wereld steeds complexer geworden is. Waar we vroeger dingen en gebeurtenissen in een bepaalde tijdsinterval als onafhankelijk van elkaar mochten beschouwen, en er een direct, vaak lineair verband was tussen oorzaak en gevolg, lijkt dit nu steeds minder toelaatbaar. Wanneer de complexiteit van een systeem een bepaalde kritische grens overschrijdt, gaat het zich gedragen als een complex adaptief systeem met zelforganiserend vermogen en emergente eigenschappen. Het gedrag laat zich slechts voorspellen in patronen, doch niet in details. Tenzij we in staat of bereid zouden zijn om de mate van complexiteit in onze wereld sterk te reduceren, zullen we nieuwe strategieën moeten ontwikkelen die ons in staat stellen om met die onzekerheid en onvoorspelbaarheid om te gaan.

In de managementliteratuur kunnen we concrete formuleringen van het paradoxale spanningsveld tussen machine- en CAS-metaforen aantreffen, evenals eerste aanzetten voor nieuwe strategieën. We zullen er een aantal kort bespreken om aan te geven in welke richting gedacht wordt.

De industriële paradox

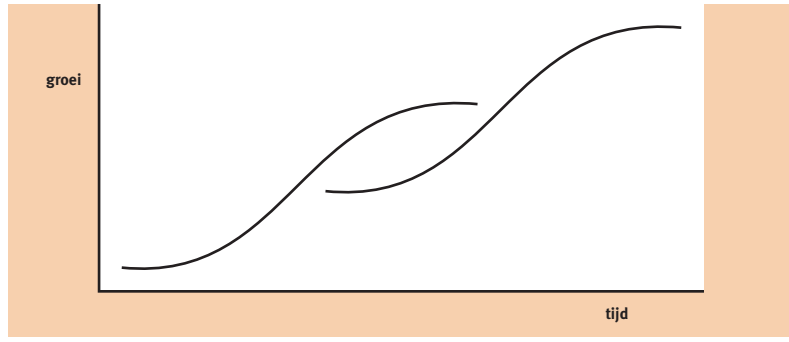
In zijn boek 'Mass Individualisation', bespreekt Ton van Asseldonk [Asseldonk, 1998] de industriële paradox waarmee industriële ondernemingen in het huidige tijdperk worden geconfronteerd. "Aan de ene kant wordt de markt steeds grilliger en minder voorspelbaar, terwijl aan de andere kant het bedienen van deze onvoorspelbare wensen de basis van industriële productiviteit vernietigt en daarmee de welvaartscheppende kracht van het systeem als geheel." Van Asseldonk bedoelt hier met een industriële onderneming een onderneming die ontstaan is vanuit het mechanistische denken waarop de industriële revolutie gebaseerd is. Hij stelt dat "de enige manier om deze paradox op te lossen is de wijze van ordening van de functionele elementen in de procesketen te veranderen. In plaats van de centraal geleide functionele ordening die zo typisch is voor de Tayloriaanse (en Newtoniaanse) manier van organiseren is een nieuwe vorm van ordening noodzakelijk. Een ordening die ontstaat uit de interactiviteit tussen de functionele elementen zelf." Met andere woorden, een ordening die voortkomt uit het zelforganiserend vermogen van de organisatie. Ordening door zelforganisatie die beïnvloed kan worden door het wijzigen van de condities.

Charles Handy [Handy, 1994] bespreekt in 'The Age of Paradox' deze paradox aan de hand van de zogenaamde Sigmoid-curve of groeicurve. Deze S-vormige curve (zie figuur 8.1) geeft het verloop weer van veel groeiverschijnselen, zoals die in de natuur, in de maatschappij en in het bedrijfsleven voorkomen. Voorbeelden hiervan zijn ons eigen groeiverloop, de opkomst en de ondergang van een rijk zoals de Sovjet-Unie, de levenscyclus van een product, de groei en het faillissement van een onderneming. De curve begint met een gebied waar iets nieuws ontstaat dat langzaam begint te groeien, vaak met vallen en opstaan. Vervolgens komt er een fase waarbij de groei ondersteund en versterkt wordt door allerlei leerprocessen, waarvan de resultaten geconsolideerd worden in de vorm van het ontstaan van structuren, vaak zowel in fysieke, in organisatorische als in culturele zin. Deze structuren zijn er vervolgens de oorzaak van dat deze leerprocessen hun limiet bereiken en er een periode van stagnerende of soms zelfs afnemende groei ontstaat.
Als we de curve op zich bekijken, suggereert zij dat er aan de groei van dingen een einde komt. In sommige gevallen is dit ook zo, denk bijvoorbeeld aan onze eigen groei.



Figuur 8.1
S-vormige curve.

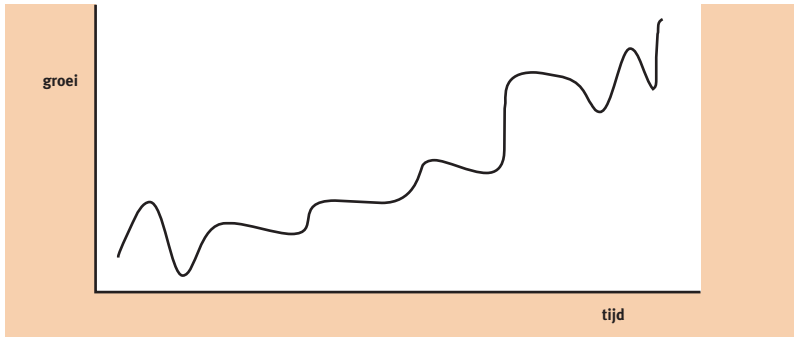
Doch voor andere systemen, zoals organisaties hoeft dit niet het geval te zijn, mits tijdig op een nieuwe groeicurve wordt overgegaan (zie figuur 8.2).
Het probleem is echter dat we niet precies weten op welk punt van de curve we zitten en dat de beslissing over de overgang naar een nieuwe S-curve dient te



Figuur 8.2
Organisaties met een nieuwe groeicurve.

geschieden op een moment dat er nog geen tekenen van stagnatie zijn in de oude curve. De tweede curve – of het nu een nieuw product of een nieuwe manier van werken of een nieuwe technologie betreft – zal wezenlijk verschillen van de oude. Het overgangsgebied is een tijd van grote onzekerheid en verwarring. Enerzijds dient het succes van de ontwikkeling uit het verleden waarop de oude curve is gebaseerd, te worden geëxploiteerd, terwijl anderzijds de uitdagingen van de toekomst dienen te worden geëxploreerd. Dit wordt ook wel het exploitatie- en exploratiedilemma genoemd (Asseldonk, 1998).

Verschillende groepen mensen of ideeën concurreren met elkaar over de toekomst. Het probleem wordt nog bemoeilijkt door het feit dat de getekende groeicurve een zogenaamde gemiddelde trendcurve is, doch dat in een bedrijfscontext de actuele datacurven meestal zeer sterke fluctuaties vertonen (zie figuur 8.3), waardoor het S-vormige verloop niet of moeilijk te onderkennen is.

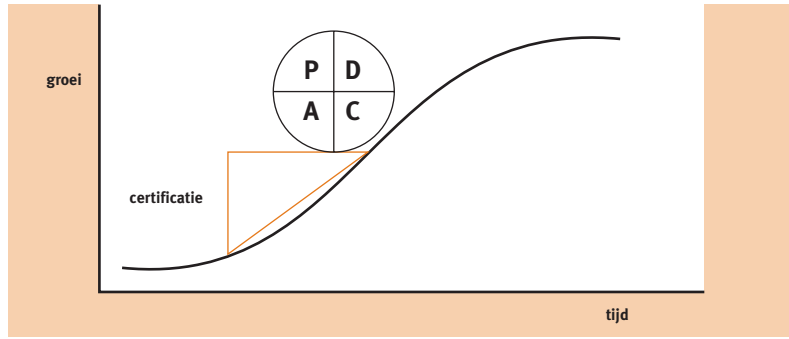


Figuur 8.3
De actuele datacurven in een bedrijfscontext.

Het paradoxale is dat het in stand houden van het succes van de oude curve gebaseerd is op het beheersmodel en dat voor de exploratie van toekomstige kansen en uitdagingen de beheersgedachte dient te worden losgelaten, opdat nieuwe mogelijkheden op basis van zelforganisatie kunnen ontstaan. De genoemde ontwikkelingen in transport en ICT zorgen ervoor dat de tijdseenheid op de horizontale as krimpt en de opeenvolging van S-curven zich in een steeds hoger tempo voltrekt. Dit betekent dat het exploitatieproces en het exploratieproces zich gelijktijdig dienen te voltrekken. Het probleem hierbij is echter dat de mensen die hierbij betrokken zijn, zijn opgevoed met een mechanistisch wereldbeeld. Ze denken dus vanuit de machinemetafoor, terwijl het exploratieproces in een situatie van grote onzekerheid een zoekstrategie vereist die gebaseerd is op de theorie van complexe adaptieve systemen. Bovendien hebben certificeringsprocessen het adaptief vermogen van de organisatie beperkt.

Het certificeren is bedoeld om het continue verbeterproces dat aan de S-curve ten grondslag ligt te formaliseren. Het doel hierbij is om de verkregen verbeteringen te waarborgen. In figuur 8.4 is dit schematisch weergegeven. De wig stelt

het certificeringsprogramma voor dat de zogenaamde Deming-cirkel PDCA ('Plan, Do, Check, Act') dient te borgen. Hierbij worden de structuren (procedures, contractvormen, cultuur, e.d.) waarin het succes van het verleden is geformaliseerd versterkt, waardoor het moeilijker wordt om discontinue overgangen naar nieuwe S-curven te maken.



Figuur 8.4
Formaliseren van het continue verbeterproces dat aan de S-curve ten grondslag ligt.

Formele en informele subsystemen in organisaties

Ralph Stacey [Stacey, 1998a] behandelt de paradox die voortkomt uit het spanningsveld tussen de machinemetafoor en de theorie van complexe adaptieve systemen in termen van wat hij noemt het formele of legitieme subsysteem en het informele of schaduwsubsysteem in een organisatie.
Het formele of legitieme systeem van een organisatie is het voorgeschreven netwerk van relaties in termen van hiërarchie, haar bureaucratie en haar formeel goedgekeurde ideologie of expliciet gedeelde cultuur. Het informele of schaduwsysteem wordt al geruime tijd onderkend, maar wordt vooral beschouwd als een bron van traagheid en weerstand tegen veranderingen die geïnitieerd worden door het legitieme systeem.
Traditionele benaderingen van verandermanagement zijn erop gericht om het informele systeem te 'ontdooien' en de organisatie van de ene evenwichtstoestand via een overgangsperiode van instabiliteit naar een nieuwe evenwichtstoestand te brengen, die beter aangepast is aan de omgeving om vervolgens die evenwichtstoestand weer te 'bevriezen'. De onderliggende op een beheersmodel gebaseerde aanname is dat een organisatie van de ene evenwichtstoestand naar de andere gebracht kan worden door de a priori-intentie van het legitieme systeem.

Vanuit het perspectief van een theorie van complexe adaptieve systemen heeft het informele of schaduwsysteem een essentiële en positieve rol in de aanpassing en de levensvatbaarheid van een organisatie onder condities van turbulentie, ambiguïteit en onzekerheid in de omgeving. Hier spelen zich processen van zelforganisatie in complexe netwerken van informele (en formele) relaties af.

De condities voor zelforganisatie komen voort uit de voortdurende spanning tussen stabiliteit en instabiliteit, met andere woorden tussen het legitieme systeem en het schaduwsysteem. Dit is de toestand van de zogenaamde begrensde instabiliteit (de rand van chaos). Factoren die ervoor zorgen dat een complex adaptief systeem in een toestand terechtkomt van begrensde instabiliteit, zijn de stroom van informatie en energie in het systeem, de veelheid aan interacties, de diversiteit van de interacterende personen, het gebruik van verschil in machtsverhoudingen en het niveau van opgewondenheid of onrust (Stacey, 1998a).

Het paradoxale zit hem in het feit dat het legitieme systeem het schaduwsysteem dient te onderkennen, te aanvaarden en te faciliteren zonder het te willen controleren en beheersen. Op deze wijze kan in een organisatie het vermogen ontstaan van voortdurend te leven in verandering in plaats van zichzelf te zien als bewegend van A naar B.
Indien het zelforganiserend karakter van het schaduwsysteem niet wordt onderkend, wordt ook de eerder besproken toename van kwetsbaarheid ten gevolge van practical drift niet opgemerkt, voordat een catastrofaal falen van het systeem die kwetsbaarheid onontkoombaar demonstreert.

Reflectie

Met wortels die terugreiken tot Newton vindt de beheersgedachte in het huidige managementdenken een stevige grondslag in de algemene systeemtheorie en cybernetica. Hierbij wordt voorondersteld dat de wereld maakbaar en beheersbaar is, mits voldoende kennis en informatie aanwezig is. Zo spreekt Stafford Beer in 'The Brain of the Firm' [Beer, 1981] over cybernetica als de 'science of control' en over management als de 'profession of control'. Het gebruik van het woord management met zijn connotatie van beheersen is niet beperkt gebleven tot het bedrijfsleven, maar het gebruik ervan omvat gebieden zo divers als management van het milieu, van energie, van de gezondheidszorg, van onderwijs, of zelfs management van emoties. Of nog ambitieuzer management van de aarde.
Wij hebben de aandacht willen vestigen op de vraag of de toename in de complexiteit van technische en of organisatorische systemen een nieuw conceptueel instrumentarium en een nieuw handelingsrepertoire vereist. We hebben geprobeerd op een tentatieve manier een alternatief perspectief te schetsen.
We hopen hiermee aan te zetten tot reflectie en zelfreflectie op de toenemende complexiteit van onze door technische systemen bevolkte omgeving en de consequenties van ons handelen. We zouden ons hierbij de volgende vragen kunnen stellen.

Als het waar is dat er omstandigheden zijn die om een andere aanpak vragen, hoe kunnen we ze dan herkennen?
Volgens Stacey [Stacey, 1992] is er een aantal kwalitatieve indicatoren die kenmerkend zijn voor toestanden van begrensde instabiliteit, zoals de stroom van informatie en energie in een systeem, het aantal interacties, de diversiteit van de interacterende personen, het niveau van onrust en het verschil in machtsverhoudingen. Hoe kunnen deze in de praktijk van organisaties geoperationaliseerd worden?

Als we de toestand van begrensde instabiliteit hebben onderkend, wat zijn dan de instrumenten en mogelijkheden om de processen van zelforganisatie zodanig te beïnvloeden dat ze in het voordeel werken van het totale systeem zonder te vervallen in het willen beheersen?
Uit deze bijdrage moge duidelijk zijn dat er geen recepten of kant-en-klare managementinstrumenten bestaan om de betrouwbaarheid van technische systemen te waarborgen onder condities van toenemende complexiteit, turbulentie en onzekerheid. Men zal al denkend, lerend en communicerend samen met anderen zowel in als buiten de organisatie de reis in de toekomst moeten durven maken. Kauffman formuleert dit pregnant als volgt.
"The question of what kinds of complex systems can be assembled by an evolutionary search process not only is important for understanding biology, but may be of practical importance in understanding technological and cultural evolution as well. The sensitivity of our most complex artifacts to catastrophic failure from tiny causes – (for example the Challenger disaster, the failed Mars Observer mission, and power-grid failures affecting large regions) suggests that we are now butting our heads against a problem that life has nuzzled for enormously longer periods. How to produce complex systems that do not teeter on the brink of collapse. Perhaps general principles governing search in vast spaces of possibilities cover all these diverse evolutionary processes, and will help us design (or even evolve) more robust systems." [Kaufman, 1995].

Referenties

- Alkemade, M.J.A. (1992). Inspelen op complexiteit. STT-publicatie nr. 52. STT, Den Haag
- Asseldonk, T.G.M. van (1998). Mass Individualisation, PhD thesis, Katholieke Universiteit Brabant, Tilburg
- Beer, S. (1981). The Brain of the Firm. John Wiley & Sons, New York
- Ciborra, C.U. e.a. (2000). From Control to Drift. The Dynamics of Corporate Information Infrastructures. Oxford University Press, Oxford

- Gleick, J. (1987). Chaos. Making a New Science. Abacus, London
- Goodwin, B. (1994). How the Leopard Changed its Spots. The Evolution of Complexity. Weidenfeld and Nicolson, London
- Handy, Ch. (1994). The Age of Paradox. Randon House. Harvard Business School Press, USA
- Handy, Ch. (1995). Beyond Certainty. Randon House, London
- Kauffman, S. (1995). At home in the Universe. p157. Pinguin Group, London
- Lewin, R. (1993). Complexity. Life at the Edge of Chaos. J. M. Dent, London
- Linden, F. van der. (1997). Wiskunde in de kiem. Natuur & Techniek **65**, 12: 64–73
- Lorenz, E.N. (1993). The Essence of Chaos. UCL Press, London
- NOU. (2000). Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet. Norges offentlige utredninger 2000:24. Statens forvaltningstjeneste Informajsonsforvaltning
- Perrow, C. (1999). Normal Accidents. Living with High-Risk Technologies. Edition with an Afterword and Postscript on the Y2K problem. Basic Books, New York
- Rosness, R. (1992). Vulnerability in Complex Systems. Directions for Research. Working Paper. NTNU, Trondheim
- Snook, S.A. (2000). Friendly Fire. The Accidental Shootdown of U.S. Black Hawks over Northern Iraq. Princeton University Press, Princeton, N.J.
- Stacey, R. (1992). Managing Chaos, Dynamic Business Strategies in an Unpredictable World. Kogan Page, London
- Stacey, R. (1998a). Intervening in the Shadow Systems of Organisations. Complexity and Management Papers 4, Complexity and Management Centre, University of Hertfordshire, United Kingdom
- Stacey, R. (1998b). Foresight in Complex Systems. Management Papers 2. Complexity and Management Centre, University of Hertfordshire, United Kingdom
- Tetenbaum, T.J. (1998). Shifting Paradigms: From Newton to Chaos. Organizational Dynamics **26**, 4:21-32
- Waldrop, M.M. (1994). De rand van chaos; over complexe systemen. Uitgeverij Contact, Amsterdam/Antwerpen
- Zimmerman, B.J., (1998). http://www.edgeplace.com/think/main_prime6.html

2

9 Inleiding

dr. M.R. de Graef

In dit deel van het boek zijn 24 cases verzameld uit diverse sectoren en disciplines. Het geheel is een brede waaier van verschillende visies op het begrip betrouwbaarheid.
In hoofdstuk 5 van deel 1 is een overzicht van een aantal trends gegeven die een rol spelen in betrouwbaarheid. Deze trends zijn niet altijd direct gerelateerd aan betrouwbaarheid.
Om de gevolgen van deze trends te illustreren zijn (bestaande) cases beschreven. Op deze wijze wordt snel duidelijk wat de gevolgen van de trends kunnen zijn en wordt een aantal maatregelen besproken.
Uit de verschillende werkgroepen (techniek, bedrijfsprocessen en organisatie) is gevraagd om hiervoor cases te leveren. De werkgroepen Techniek en Bedrijfsprocessen hebben individuele cases geleverd. De werkgroep Organisatie heeft in een aantal groepjes gewerkt aan cases over luchtvaart, ziekenhuis, chemische industrie en ICT.

De cases in de hoofdstukken 10, 12, 13, 14, 27, 30, 31 en 32 zijn door de werkgroep Techniek geschreven. De werkgroep Bedrijfsprocessen heeft de hoofdstukken 15, 16, 17, 18, 19, 20, 28 en 29 geleverd en de werkgroep Organisatie schreef de hoofdstukken 22, 23, 25 en 26. De cases laten niet uitsluitend de invalshoek van de werkgroep zien, maar dat aspect heeft wel de nadruk. Een aantal hoofdstukken is geschreven door auteurs die niet aan de werkgroepen deelnamen, maar wel hun visie op het begrip betrouwbaarheid weergeven.
De meeste cases laten de negatieve gevolgen zien als de trends doorzetten. Een aantal cases laat zien hoe getracht is met deze trends om te gaan. Dat kan zowel preventief zijn door methoden als risicoanalyse te gebruiken of reactief zoals bijvoorbeeld in de bijdrage over het herstellen van fouten (hoofdstuk 33, deel 2) duidelijk wordt.

Alhoewel deze cases allemaal over een specifiek technisch systeem gaan, is het betrouwbaarheidsaspect van deze cases vaak generiek, zoals ook blijkt uit deel 3 van dit boek, waarin in een helikopterview de belangrijkste trends uit de cases worden besproken.
De uitdaging voor u als lezer ligt er dan ook in om de cases te lezen, zonder al te specifiek naar het desbetreffende technisch systeem te kijken en op die manier de generieke zaken te herkennen.
Door de verschillende deskundigen zelf een case te laten schrijven ontstaat een aardig overzicht van de verschillende visies op het begrip betrouwbaarheid.
Als lezer kunt u er met uw eigen bril naar kijken en zo weer andere aspecten van deze cases zien.
In deel 3 zal een aantal aspecten worden beschreven die een integrale aanpak van betrouwbaarheid mogelijk maken.

2

10 Informatie- en communicatietechnologie, de nieuwe Achilleshiel?

ir. H.A.M. Luiijf [1]

Inleiding

Onze westerse en specifiek de Nederlandse samenleving wordt in sterk toenemende mate afhankelijk van diensten die zijn gebaseerd op informatie- en communicatietechnologie (ICT). Onze informatiesamenleving is daarbij afhankelijk van het goed functioneren van een zeer complex geheel van elektronische diensten, programmatuur, computers, netwerkschakelsystemen, netwerken, transmissiesystemen (bijv. microgolfverbindingen, glasfibers, koperkabels) en spanningsvoorzieningen. Er is sprake van een keten aan diensten die geleverd worden door verschillende bedrijven of onafhankelijk werkende onderdelen van grote conglomeraten (bijv. de KPN Telecom Universeel Transport Netwerkdienst) [Van Till, 2001].

1 TNO Fysisch en Elektronisch Laboratorium, Afdeling Telematica en Beveiliging
Postbus 96864
2509 JG Den Haag

Organisaties die de risico's in de informatiebeveiliging van vertrouwelijkheid, betrouwbaarheid en beschikbaarheid op een gebalanceerde wijze willen reduceren, voeren regelmatig een zogenaamde kwetsbaarheids- en afhankelijkheidsanalyse uit. Programma's als ESAKA of CRAMM kunnen hulp bieden bij deze analyse en genereren een reeks maatregelen gebaseerd op de ingevoerde gegevens.
Een organisatie die voor haar diensten aan eindgebruikers een zeer hoge graad van beschikbaarheid eist, zorgt ervoor dat zij niet alleen de computerdiensten binnenshuis dubbel uitvoert en een uitwijk in geval van calamiteiten regelt, maar ook de beschikbaarheid van externe communicatieverbindingen zeker stelt door met haar toeleveranciers 'service level agreements' (SLA) en harde garanties af te sluiten. Deze leveranciers zijn op hun beurt echter vaak afhankelijk van derden of van een onafhankelijk opererend intern onderdeel, waarmee zij een vergelijkbare SLA afsluiten.

Met een glasvezel die aan de voorkant het terrein op komt, een tweede glasvezel aan de achterzijde naar een andere wijkcentrale en een beschikbaarheidsgarantie van 99,99% lijkt alles goed geregeld, totdat Murphy toeslaat.
De hierna volgende case is een condensatie van werkelijke ervaringen van verschillende bedrijven tijdens dezelfde calamiteit. Het voorbeeld is ter wille van de duidelijkheid van de complexiteit en de verwevenheid van onze ICT-diensten een gedramatiseerde versie van ware gebeurtenissen. De Rijksdienst voor het Wegverkeer (RDW) te Veendam heeft hierbij als een van de getroffen bedrijven vanwege de vele bekende informatiediensten als hypothetisch voorbeeld van de complexe problematiek gediend. De relatie tussen functies, verantwoordelijkheden en personen is dan ook fictief.

Case

De gegevens van Nederlandse voertuigeigenaren en hun voertuigen worden geregistreerd in registers die door de RDW worden beheerd. De RDW voorziet de burger binnen bepaalde kaders zoals het privacyreglement van informatie uit deze registers. Aan de hand van de registers controleren de RDW en het Centraal Bureau Motorvoertuigen (CBM) of de bezitter van een voertuig heeft voldaan aan de voertuigverplichtingen. De computersystemen in Veendam leveren een aantal on line elektronische diensten voor particulieren, automobielbedrijven, politie en verzekeringen. Bekende diensten zijn het overschrijven van kentekens op postkantoren, de afgifte van rijbewijzen op gemeentehuizen, de uitgifte van nieuwe kentekens, het opvragen van de verzekeringsstatus en het eigendom door de politie, de lijst van gestolen voertuigen, de APK-afmeldingen en de APK-status. Gebaseerd op deze afmeldingen voeren controleurs steekproeven uit.

Alles bij elkaar gebruiken zo'n 30.000 gebruikers dagelijks de on line-diensten van de RDW.

De RDW heeft veel telefoonlijnen in gebruik, onder andere voor een 'call centre' met een groot aantal ICT-werkplekken waar geautoriseerden informatie uit de informatiesystemen kunnen opvragen of bijvoorbeeld APK-afmeldingen kunnen opgeven. Om bij het opgraven van een kabel niet zonder telefonie- en fax-verkeer te zitten, heeft de telefoniemanager, die verantwoordelijk is voor de telefooncentrale en de spraakdiensten, een dubbele kabelaansluiting met gescheiden routering naar twee verschillende wijkcentrales gecontracteerd. KPN Telecom als telefonieleverancier geeft voor die dienst een zeer hoge beschikbaarheidsgarantie, waarbij ze geld zullen restitueren als het afgesproken beschikbaarheidspercentage niet gehaald wordt. Volgens de accountmanager van de telefonieserviceprovider geeft dat een betere beschikbaarheid dan een computercentrum ooit kan bereiken! Daarnaast zijn de telefooncentrales van een aantal kantoren van de RDW elders in Nederland met elkaar verbonden via dezelfde verbindingen.

Al het dataverkeer uit Nederland komt binnen via dezelfde kabelbundels, maar vallen onder de verantwoordelijkheid van een manager die verantwoordelijk is voor de datanetwerken. Hij heeft de contractuele afspraken uitbesteed aan de telefoniemanager; tenslotte komen de verbindingen binnen via hetzelfde koppelpunt van de telecommunicatieleverancier. Om gezien de uithoek van het land extra zekerheid te hebben, is bovendien in het geval van een calamiteit een alternatieve datanetroutering tussen zowel Stadskanaal als Arnhem met de RDW-locatie Veendam mogelijk via straalzenders. Kostbare voorzorgen om te zorgen dat de 30.000 gebruikers van de informatiesystemen onbelemmerd auto's kunnen overschrijven, de politie vanuit de auto direct kan nagaan of een verdacht voertuig als gestolen te boek staat, sloopbedrijven een kenteken kunnen intrekken, of garages APK-meldingen kunnen doorgeven.

Beide managers hadden gebaseerd op risico-inschattingen de nodige maatregelen getroffen om de beschikbaarheid van zowel telefonie als dataverkeer optimaal te garanderen naast allerlei maatregelen om intern ook de beschikbaarheid van het call centre en de computers aan vergelijkbare hoge eisen te laten voldoen. Met de telecommunicatieleverancier waren zware SLA's afgesloten om die vereiste hoge beschikbaarheid zeker te stellen. En voor het geval een dragline onvoorzichtig zou zijn, waren er gescheiden kabelroutes naar verschillende wijkcentrales, en straalverbindingen. Wat zou er dan nog mis kunnen gaan?

Om enkele minuten over acht op 15 juni 1999 sloeg een aannemer een damwandplank in de haven van Groningen. Het was de zoveelste plank, al ging deze

iets taaier de grond in. De aannemer kon niet bevroeden dat dit kwam, omdat hij op enkele meters diepte vier glasvezelkabels aan het doorklieven was. Deze kabels van het KPN universeel transportnetwerk verbonden de hoofdcentrales in Noord-Nederland en vormden gezamenlijk de enige hogecapaciteitsverbindingsweg in het noorden. Onmiddellijk waren de provincie Groningen en grote delen van Friesland en Drenthe verstoken van vaste en mobiele telefonie, werd 1-1-2 onbereikbaar, en vielen alarmmeldingen, fax- en dataverkeer, geld- en pindiensten en de Internettoegang uit. Pas aan het einde van de werkdag was een aantal diensten beperkt bruikbaar. Herstel van de volledige capaciteit kostte echter meer tijd. Eén bedrijf had overigens ontzettend veel geluk, ze hadden net een minuut voor het wegvallen van de communicatie een brandmelding aan 1-1-2 doorgegeven.

Bij de RDW leek het er eerst op dat de rest van Nederland die ochtend traag opstond, het was na achten erg rustig bij het call centre... er kwam geen enkel telefoontje. Even later ontving de telefoniemanager de klacht dat uitgaand bellen niet lukte. Hoe bereik je in zo'n geval de storingsdienst van KPN Telecom? Gelukkig waren er enkele mobiele KPN-telefoons aanwezig, maar die bleken alleen lokaal te kunnen bellen, de KPN-storingsdienst bleek onbereikbaar. Pogingen om mobiele telefoons van de tweede en nog een andere mobiele operator te gebruiken strandden ook. Om snel tot landelijke dekking te komen, hebben deze operators voor de koppeling van de antennemasten transmissiecapaciteit ingehuurd bij hun concullega KPN. Medewerkers die erop uitgestuurd werden, rapporteerden dat in een groot gebied noch vast, noch mobiel telefoonverkeer mogelijk was. Dit probleem hield de telefoniemanager druk bezig. Dat ook de datalijnen geen verbinding hadden, was voor hem van lagere prioriteit. Intern bleek de responsetijd van de computers veel sneller dan normaal. Telefonische pogingen van RDW-medewerkers elders in het land om te klagen over het gebrek aan informatiediensten eindigden aldaar in een blokkeertoon. Hetzelfde gold voor alle andere afnemers van informatiediensten. Het duurde dan ook geruime tijd, voordat de datanetwerkmanager in de gaten kreeg dat zijn dataverbindingen weinig 'bitten' transporteerden, al kwam er wel iets binnen via een alternatief pad. Maar klachten bleven uit...

De telefoniemanager kon hem vertellen dat de kabelbundels aan de voor- en achterzijde geen telefoon- en dataverbindingen gaven. Geen probleem, in het geval van dataproblemen met de rest van Nederland had de RDW de alternatieve routering via straalverbindingen met het KPN-datanet geregeld. Voor het omzetten van de grote datastromen naar de straalverbindingen moesten echter de juiste mensen bij KPN de routering van deze stromen wel even omzetten. Het probleem was overduidelijk, zij waren door gebrek aan telefonie- en faxverkeer onbereikbaar. Gegeven de grote omvang van de storing was het netwerkbedrijf

van KPN dermate in de weer om het transmissieverkeer elders in Nederland in goede banen te leiden en te proberen sommige delen van Noord-Nederland alternatief te ontsluiten, dat men geen initiatieven nam om alternatieve paden voor eindgebruikers in te stellen.

Analyse

Nadrukkelijk gaat het hier niet om een analyse van de case zelf, maar om aan te geven dat de complexiteit van ICT nog steeds slecht beheersbaar is, zeker als daarbij veel interne en externe actoren (dienstenaanbieders) betrokken zijn. Dit geval is geen op zichzelf staand eenmalig incident. Gevallen van chaos bij een groot deel van het Nederlandse spoorwegnet door elektriciteitsuitval bij de dienstleiding in de zuidelijke regio van de NS staan bij vele tienduizenden reizigers nog op het netvlies. Maar ook de uitval van Internet in Alphen aan de Rijn door sabotage van een wijkcentrale door een lawinepijl; en de uitval van het Internet van Casema gedurende 24 uur zijn voorbeelden van calamiteiten in de Nederlandse informatie-infrastructuur die men bijna dagelijks in de krant kan lezen.

Door de liberalisatie van de telecommunicatiemarkt blijkt de overheid geen directe zeggenschap en controle meer te hebben over de actoren. De ontwikkeling van het nieuwe fenomeen Internet valt sowieso buiten de directe overheidscontrole. Voor marktactoren geldt echter vrijwel hetzelfde. Binnenshuis kun en moet je zelf controleren – je eigen broek ophouden. Daar waar sprake is van een (vaak nog) onduidelijke keten van actoren (elektriciteitsleverantie, transmissienetwerkoperator, netwerkoperator, TTP[2]-dienst, dienstenverlener), is het moeilijk de informatie-infrastructuur in de dynamische omgeving beheersbaar en betrouwbaar te houden.

Hierbij geldt ook nog eens de kwetsbaarheidsparadox van Steetskamp en Van Wijk [Steetskamp, 1994]: “Naarmate een land minder kwetsbaar is in zijn voorzieningen, komt iedere verstoring van de productie, distributie en consumptie van die voorzieningen des te harder aan.” De perceptie van een betrouwbare voorziening zorgt ervoor dat deze vaker gebruikt gaat worden, waardoor de gevolgen van een verstoring nog extremere vormen kunnen aannemen.

De overheid kan opteren voor een nuloptie, niets doen. De dagelijkse reeks kleine en middelgrote incidenten zal als een walvis af en toe boven komen. Even een incident, daarna al snel weer vergeten. Zolang de Tweede Kamer niet ernstig bezorgd is en geen indringende vragen stelt, komt de regering daarmee weg. Dat gaat goed, totdat er een grootschalig incident op de elektronische

2 TTP = Trusted Third Party, een organisatorisch-elektronische oplossing die bij het elektronisch zaken doen de zekerheid biedt dat een partij inderdaad de partij is die het zegt te zijn; dit is te vergelijken met het notariaat.

snelweg optreedt. Als het kalf verdronken is, komt dan pas de vraag hoe het zover heeft kunnen komen?
De liberalisatie van de telecommunicatie in Nederland is zover doorgevoerd dat er voor de overheid niets anders op zit dan om zelf als 'operator' een veel betere greep op de kritische informatie-infrastructuur te krijgen. De Zweedse overheid heeft overigens besloten om delen van de glasvezelinfrastructuur weer in eigen hand te nemen, waardoor zij verantwoordelijk is voor de adequate aansluiting van alle steden en dorpen en tevens voor betrouwbaarheidsgaranties zorgt.

Marktpartijen in Nederland hebben ieder voor zich een groter of kleiner deel van de betrouwbaarheidspuzzel in handen. Ze kunnen op de scheidingsvlakken met hun toeleveranciers weliswaar een SLA vastleggen, maar er kan snel een beroep op 'overmacht' gedaan worden. Te betalen boetes wegens het niet nakomen van de SLA zijn vervelend, maar is een verrekening achteraf. De dienstverlening van de ketenafhankelijke inkopende partij is ondertussen geschaad en is onbetrouwbaar voor de klant.

Een oplossing ligt dus in het midden. Een betrouwbare informatie-infrastructuur kan alleen ontstaan als alle betrokken actoren (overheid en markt) het betrouwbaar functioneren van gehele ketens van diensten als gezamenlijk nationaal belang zien. Pas dan wordt er in voldoende mate geïnvesteerd in redundantie, training in crisisbeheersing en concullegiale hulp bij ongelukken. Pas daarna is er sprake van het beheersen van incidenten.

Conclusies

Door de dynamiek van de telecommunicatiewereld, de steeds grotere verwevenheid van communicatiediensten en de convergentie – het steeds dichter naar elkaar toe groeien – van datacommunicatie, telefonie en andere communicatiemiddelen ontstaat zoveel complexiteit dat de kwetsbaarheid en afhankelijkheid van telecommunicatiesystemen nauwelijks te doorgronden zijn. Voor accountmanagers en telefonie- en datacommunicatiemanagers die SLA's en contracten voor een optimale beschikbaarheid van zulke systemen afsluiten is het dan ook bijna ondoenlijk om de gehele keten aan risico's te doorgronden.

Het contracteren van een tweede telecommunicatiepartij om extra betrouwbaarheid te garanderen, lijkt een goed alternatief. Echter, enkele kilometers verder kan uit kostenoverwegingen een en dezelfde glasvezel gebruikt worden. Noch de accountmanager, noch u als contractafsluitende partij weet hiervan, al is het voor beide partijen duidelijk dat een dergelijke verbinding als calamiteitenverbinding geldt. En, indien alle voorzorgsmaatregelen getroffen zijn en de

verbinding vandaag via twee gescheiden routeringen loopt, kan marktwerking morgen ertoe leiden dat extra capaciteit bij de concullega ingehuurd moet worden en dat nu net uw verbinding door het netwerkbedrijf alsnog in die ene kwetsbare bundel of die ernaast terechtkomt. Ondenkbaar is dat niet; om een stad niet te vaak open te leggen voor het trekken van glasvezels, laten sommige steden slechts één consortium van een aantal tele- en datacommunicatieleveranciers tegelijkertijd graven. De glasvezels liggen daarbij als massieve (in een hap door te graven) bundels broederlijk naast elkaar.

Ontwikkelingen in de ICT, steeds meer behoefte aan informatie en convergentie zullen op korte termijn tot een nog grotere afhankelijkheid van telecommunicatiesystemen leiden. Een aantal voorbeelden is te vinden in [Luiijf, 2000]. Als we geen rekening houden met die afhankelijkheid, zullen er geen alternatieve vormen van communicatiemedia meer zijn in het geval van een grootschalige calamiteit. De voorbereiding op de millenniumovergang gaf al een eerste indicatie van de potentiële problemen, onder andere met het nationale noodnet. Elektriciteitsbedrijven toonden hun gebrek aan vertrouwen dat ze de volledige ketenafhankelijkheid goed geanalyseerd hadden door veldtelefoons uit een museum te halen.
Wil Nederland de ambitie van het kabinet waarmaken om in de wereld van E-commerce en M(obile)-commerce tot de top-10 landen te gaan behoren, dan zal de onderliggende informatie-infrastructuur betrouwbaarder moeten worden. Het verkrijgen van inzicht in de complexe materie en de wijze waarop verantwoordelijken de ketenproblematiek en -kwetsbaarheid in kaart kunnen brengen, is een onderwerp dat veel studie waard is. Het gaat immers vaak om slechts één faalmoment: één glasvezel, één integrated circuit van een kwartje, een simpele softwarefout, een ventilator die dreigt uit te vallen.

Samenvattend kan worden gesteld dat vanuit deze optiek de volgende megatrends (zie deel 1 van dit boek) een rol spelen bij de betrouwbaarheid van de informatie-infrastructuur:

- *Betrouwbaarheid*: de consument stelt steeds hogere eisen aan betrouwbaarheid, zie de eerder besproken dubbele betrouwbaarheidsparadox.
- *Deregulatie en liberalisatie*: de betrouwbaarheid van diensten die een marktpartij biedt kan een concurrentieaspect zijn, waardoor 'betere' betrouwbaarheid geboden wordt dan in het geval van een (overheids)monopolist. Echter door de opsplitsing in veel actoren kan de betrouwbaarheid in de integrale keten sterk verminderen en zijn grootschalige incidenten nauwelijks beheersbaar, tenzij in publiek-privaat partnership samen aan meer betrouwbaarheid gewerkt wordt.
- *Kortere ontwikkeltijd* waardoor bij de invoering van nieuwe communicatie- en informatiediensten voldoende kennis en ervaring ontbreken. Dit wreekt

zich en is zichtbaar als uitrolproblemen, onbeheerste calamiteiten, onvoldoende redundantie, het niet waarmaken van de betrouwbaarheid waarop de klant volgens zijn perceptie recht heeft. Een perceptie die gebaseerd is op de marketingactiviteiten die (soms ver) voorlopen op de technische dienstverlening.

– *Toenemende dynamiek*: de snelle ICT-ontwikkelingen zorgen voor een enorme dynamiek in de ontwikkeling van ICT-infrastructuren: iedere 1 tot 1,5 jaar een nieuwe generatie apparatuur, iedere 2 tot 3 jaar een geheel nieuwe technologie, het gaat steeds sneller. Daarbij worden steeds meer infrastructuren gebaseerd op Internettechnologie en daardoor is er sprake van convergentie in de kernactiviteit van infrastructuren voor vaste en mobiele telefonie, dataverkeer, semafonie, satelliettoegang, betalingsverkeer, meten en regelen van energie en andere distributiesystemen, keren en beheren van onze waterhuishouding, en telematicadiensten. Tevens is er sprake van verwevenheid, doordat diensten geboden worden die door verschillende infrastructuurketens heenlopen zoals e-mail naar SMS, gesproken e-mail via de mobiele telefoon, GPRS/WAP-diensten om enkele voorbeelden te noemen. Gedegen infrastructuurontwerpen waarbij rekening is gehouden met betrouwbaarheidseisen kunnen door de dynamische marktwerking snel hun waarde verliezen.
– *Marktconcurrentie*: druk op de efficiëntie, omdat zo goedkoop mogelijk opereren soms ten koste gaat van redundantie. Ook wordt capaciteit bij concullega's ingekocht, indien de realisatietijd of de lage bezettingsgraad bij de aanleg van eigen middelen minder efficiënt is: mobiele operators huren bijvoorbeeld vaste verbindingen van KPN Telecom. Het resultaat is dat in bepaalde gebieden alle operators dezelfde glasvezelbundel gebruiken, waardoor op één plaats een kabelbreuk ('single point failure') ontstaat en een klein incident onverwacht kan leiden tot een grootschalige verstoring van de samenleving.
– *Complexiteit*: hoe de potentiële risico's van de eerdergenoemde verwevenheid en convergentie in een dynamische wereld vertaald moeten worden in ontwerpcriteria van een dienstenafnemer en hoe deze vervolgens in de praktijk beheersbaar blijven als veel actoren dynamisch wisselen van onderliggende infrastructuren (vandaag verschillende infrastructuren, morgen door dezelfde glasvezel), is een onderwerp waarnaar nog veel onderzoek verricht moet worden. Overheidsregels die negatief uitpakken: om niet iedere week een trottoir open te hebben liggen, eist de overheid steeds vaker dat infrastructuuroperators consortia vormen om gezamenlijk bundels glasvezelpijpen in de ondergrond te stoppen, anders geeft men geen graafvergunning af. De consequentie hiervan is dat de bundels van alle operators dicht bij elkaar liggen en gelijktijdig gevoelig zijn voor een 'drag-and-cut' incident. Het openleggen van het trottoir om een doorsneden kabel of glasvezel te mogen

repareren is in een aantal gemeenten ook 'vergunningsplichtig', waardoor de reparatietijd soms weken bedraagt als gevolg van administratieve procedures. Dit alles werkt negatief op de betrouwbaarheid en de beschikbaarheid van meer informatie-infrastructuren tegelijkertijd.

Referenties

- Infodrome. (2001). Het KWICT-instituut. Regulerend én stimulerend naar een betrouwbare ICT-infrastructuur. Infodrome, Amsterdam. www.infodrome.nl/download/pdf/deb_kwets.pdf
- Luiijf, H.A.M., M.H.A. Klaver. (2000). Bitbreuk. De kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij. Infodrome essay. Infodrome, Amsterdam. www.tno.nl/instit/fel/refs/pub2000/luiijfbitbreuk.doc
- Steetskamp, I., A. van Wijk. (1994). Stroomloos, kwetsbaarheid van de samenleving: gevolgen van verstoringen van de elektriciteitsvoorziening. Rathenau Instituut, Den Haag
- Till, J. van, R. de Boer, C.H.C. van de Sandt, P. Maclaine Pont, H.A.M. Luiijf, M.H.A. Klaver, J. Huizenga. (2001). Samen werken voor veilig Internetverkeer: Een e-Deltaplan. Ministerie van Verkeer en Waterstaat/DGTP. www.tno.nl/instit/fel/ts/resources/kwint.pdf
- Vries, J.M. de. (2001). Beleidsnota Kwetsbaarheid op Internet (KWINT). Tweede Kamer der Staten-Generaal, 26643 nr. 30

2

11 Betrouwbaarheid digitale ruimte door marktwerking en publiek-private samenwerking

drs. F.J.G. van de Linde [1]

Inleiding

De wereld heeft de duizelingwekkende ontwikkeling van elektronische communicatie omarmd. Tussen de eerste analoge telegraaf en de draadloze digitale videotelefoon op het schoolplein ligt niet veel meer dan een eeuw. De sublieme technische werking en de betekenis voor de samenleving tarten ieders voorstellingsvermogen, ook van de hoogst opgeleide professionals en de meest ervaren deskundigen. Het is niets minder dan een technisch en sociaal wonder.

1 RAND Europe
Newtonweg 1
2333 CP Leiden

Zo nu en dan worden we geconfronteerd met de gevolgen van niet goed functionerende elektronische informatie- en communicatiesystemen. Ergernis is meestal de beperkte schade die erdoor wordt aangebracht, bijvoorbeeld in de vorm van lange wachttijden, onbereikbaarheid over mobiele of vaste netwerken of verlies van gegevens. Maar naarmate die systemen de wereld met steeds fijnmaziger communicatienetwerken omspannen, meer gebruikers en aanbieders gemakkelijker toelaten tot de digitale ruimte die erdoor wordt gecreëerd, en sterker vervlochten raken met vitale functies van onze samenleving, zoals voeding, energie, transport, misdaadbestrijding en defensie kan ook de kans toenemen dat de gevolgen van niet functioneren zwaarder wegen dan ergernis. Een kleine, al dan niet opzettelijke verstoring in een uithoek van de digitale ruimte kan een sneeuwbal- of cascade-effect veroorzaken en tot economische schade[2] leiden, en misschien zelfs levensbedreigende situaties veroorzaken[3]. Maar de digitale ruimte kan zich alleen goed ontwikkelen als deze voldoende betrouwbaar is. Het is daarom nodig over werkbare betrouwbaarheidsmaatregelen na te denken.

Werkbare betrouwbaarheidsmaatregelen

Deze gedachte is niet nieuw. In het verleden werd bij betrouwbaarheid in eerste instantie gedacht aan technische betrouwbaarheid. Daarom zijn netwerken en communicatieprotocollen ontworpen, zoals Internet die bestand zijn tegen het uitvallen van gedeelten van de fysieke infrastructuur, bijvoorbeeld doordat een graafmachine een kabel beschadigt. Dat heeft goed gewerkt. Het grootste gevaar dat de technische betrouwbaarheid nog bedreigt is een te geringe capaciteit om aan de snel ontwikkelende vraag te voldoen. Maar zolang de bandbreedte van communicatiekanalen, de schakelsnelheid van knooppunten en de opslagcapaciteit van geheugens blijven toenemen, blijven aanbod en vraag in redelijke verhouding tot elkaar staan. Bovendien schept het aanbod de vraag, niet andersom.

Naast de noodzaak van het waarborgen van technische betrouwbaarheid, dient nu ook de aantasting van de betrouwbaarheid door niet technische factoren te worden bestreden. Die strijd is van een heel andere aard. Juist omdat informatie- en communicatiesystemen internationaal toegankelijk zijn kan immers één enkele vandaal bijvoorbeeld met een lawine van e-mail capaciteitsproblemen veroorzaken of nog erger met een kwaadaardig virus functies van het netwerk lamleggen. Criminelen kunnen zich op uiteenlopende manieren door misbruik van de digitale ruimte trachten te verrijken bijvoorbeeld door in te breken in persoonsgegevens, door digitale valsemunterij of door betalingen te incasseren zonder de koopwaar te leveren. Daarbij maken zij gebruik van de mogelijkheden zich onafhankelijk van tijd en plaats te organiseren. Ook wordt het Internet

2 Het 'I love you'-virus richtte volgens VNO-NCW in Nederland voor 50 Mf schade aan. Wereldwijd wordt de schade door informatieverlies als gevolg van vandalisme op vele tientallen miljarden dollars geschat.

3 'Critical Infrastructures' worden door overheden al tijden erkend, ook de nationale informatie-infrastructuur. Het Britse kabinetsbureau definieert "Critical are those parts of our infrastructure that are so important that an attack would have serious economic and social consequences and would be of immediate concern to the Government."

gebruikt om de uitwisseling van illegale en ongewenste inhoud te faciliteren, zoals nazistische teksten en kinderporno, of uitwisseling van illegale kopieën zonder betaling van het intellectuele eigendomsrecht. Cyberterrorisme ten slotte is de politiek gemotiveerde aanval op de digitale ruimte.
Hoewel een enkele vandaal veel ellende kan aanrichten, is het voorkomen ervan juist niet gemakkelijk door een enkele partij te realiseren, net als in de 'gewone' wereld. Dat is het gevolg van de wereldwijde vertakking en vervlechting van de digitale ruimte waarbij de verantwoordelijkheden zijn gedelegeerd aan een keur van private partijen en organisaties die in een los verband samenwerken, en met overheden die op grote afstand opereren, vaak op basis van controle achteraf, of het nu gaat om misbruik, fraude, vandalisme, terrorisme of marktwerking.
Er is echter ook behoefte aan maatregelen vooraf, waardoor gebeurtenissen die de betrouwbaarheid van de digitale ruimte aantasten zoveel mogelijk worden voorkomen. Daarom moeten alle internationaal betrokken partijen de handen ineenslaan. Gezien het wereldomspannende karakter van de problematiek staan internationale samenwerking van overheid en industrie voorop. Hun gezamenlijke opdracht is om de betrouwbaarheid van de digitale ruimte te bevorderen zonder dat voor de toegang en het gebruik te grote belemmeringen worden opgeworpen.
Deze gezamenlijke inspanning begint nu op gang te komen. Na een start in – hoe kan het ook anders – de VS, maakt de EU thans een snelle inhaalslag, daarbij gesteund door supranationale instanties zoals de Raad van Europa (Cybercrime Convention), de EC [4], de ISO [5] en de OESO [6]. Daarbij bestaat er een opvallende consensus over rechten, plichten, verantwoordelijkheden en procedures.

Hoewel in veel gevallen, en zeker in het geval van Internet, de nationale overheid de belangrijkste speler is geweest in het initiëren en opzetten van de digitale ruimte, zijn de belangrijkste spelers nu te vinden in de private sector. Die sector kent als geen ander de kwetsbaarheden van alle componenten van de digitale ruimte en heeft ook kennis van de feitelijke gebeurtenissen die de werking hebben aangetast of kunnen aantasten. De overheid heeft weliswaar ook inzicht in kwetsbaarheden, maar niet in dezelfde kwetsbaarheden of met hetzelfde detail als het bedrijfsleven. Bovendien zullen de private en publieke sector die informatie niet als vanzelfsprekend met elkaar willen delen. Overheid en bedrijfsleven hebben nu eenmaal verschillende doelen. De overheid is er voor het nationale belang, het bedrijfsleven voor de winst en de aandeelhouder. Bovendien is het bedrijfsleven er allerminst van overtuigd dat we ons zorgen moeten maken over een 'Cyber Pearl Harbour' [Anderson, 2001]. Ten aanzien van het risico (kans maal gevolg) blijven de partijen vaak steken in schermutselingen over karikaturale hypothesen van vandalisme en – vooral – terrorisme. Maar misschien blijft het risico wel gelijk, doch verandert het de komende jaren van 'kleine kans, groot gevolg' naar 'grote kans, klein gevolg', zo betoogt vooral

4 Creating a safer information society by improving the security of information infrastructures and combating computer-related crime; Communication from the European Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the regions COM (2000) 890, Brussels, March 2001

5 ISO/IEC JTC 1/SC27, June 1999, Common Criteria Standard

6 OECD, Cryptography Policy Guidelines, 27 March 1997

de private sector. Men tilt er niet zo zwaar aan; het Y2K-probleem viel immers ook enorm mee. Het potentiële risico van het niet functioneren van andere kritische infrastructuren, vooral die van elektriciteit wordt veel groter gevonden. Dat blijkt niet alleen uit de praktijk, het werd ook beargumenteerd in een veel geciteerde publicatie van RAND [Ware, 1998] op dit gebied, waarin voor de eerste keer de interdependentie tussen verschillende infrastructuren helder aan de orde werd gesteld. Ook is de economische impact van kwetsbaarheid (niet betrouwbaar) moeilijk te meten, zodat het moeilijk is uit te rekenen hoeveel de investering in betrouwbaarheid uiteindelijk oplevert. Tenslotte heerst de overtuiging dat een 100% betrouwbare digitale ruimte nooit werkelijkheid kan worden. Dat wordt ook in Nederland onderschreven [KWINT, 2001]. Dat betekent dat ook in de digitale ruimte risico's niet kunnen worden weggenomen, maar dienen te worden beheerst, conform de modernste algemene opvattingen over risico [Beck, 1992].

De spelers in de digitale ruimte zijn voornamelijk privaat, en het zijn er veel. Ze zijn voortdurend wereldwijd actief (7x24x365). Daarmee is een dynamische innovatiekracht gemobiliseerd die haaks staat op de kolomsgewijze organisatie van overheden [Rathmell, 2000]. Als gevolg daarvan zullen beleidsactiviteiten van overheden niet de benodigde snelheid kunnen halen om de betrouwbaarheid van de digitale ruimte in technische zin te kunnen beïnvloeden. Dat levert een belangrijk leerpunt op. Regelgeving dient van algemene, niet technische aard te zijn.

Marktwerking en publiek-private samenwerking

Tijdens een internationale publiek-private workshop, georganiseerd door RAND Europe in Den Haag in juni 2001 [Rand, 2001], werd door een deelnemer de vergelijking gemaakt met de ontwikkeling van de auto. De ICT zou zich nu in het T-Fordstadium bevinden. Als gevolg daarvan verwachten deskundigen veel meer van de marktgedreven technologische ontwikkeling dan van regelgeving. ICT wordt steeds betrouwbaarder in plaats van minder betrouwbaar (net als bij de auto) en markten zijn beter geschikt om risico te reguleren dan overheden. Dat biedt een tweede belangrijk leerpunt dat ook voor overheden een aanknopingspunt kan vormen, namelijk het bevorderen van marktwerking op het punt van betrouwbaarheid. Marktgedreven oplossingen, inclusief het kunnen verzekeren van cyberrisico's, bieden de voorkeur boven internationale verdragen die zo'n beetje de langzaamste methode zijn om iets voor elkaar te krijgen, aldus een van de deelnemers aan de bovengenoemde workshop.
Misschien vindt u het een weinig geruststellende gedachte om op marktmechanismen te moeten vertrouwen als het om betrouwbaarheid van ICT gaat.

Immers, het marktdenken bepaalt soms iets te vanzelfsprekend het beleidsaanzien van onze tijd, en lang niet alle gevolgen van deregulering zijn gunstig, zoals bij de Nederlandse Spoorwegen. Sommige sectoren worden zelfs angstvallig van deregulering gevrijwaard, zoals het Nederlandse drinkwatersysteem. Maar ICT is nu juist hét voorbeeld van goed geslaagde liberalisering in de VS en Engeland en later in de toonaangevende Europese lidstaten. Dat volgt uit talloze evaluaties van het liberaliseringsbeleid van de telecomsector. Het is dan ook om die reden begrijpelijk dat de publieke en private sectoren wereldwijd op een zelfde manier denken over de acties die moeten worden ondernomen om de betrouwbaarheid van de digitale ruimte te bevorderen, namelijk het bevorderen van marktwerking en publiek-private samenwerking.

Dit betekent dus dat er ook een rol voor de overheid is weggelegd. De overheid dient toe te zien op het voorkomen van marktfalen en marktwerking te bevorderen. In de digitale ruimte kan dat door alle partijen om te beginnen van zoveel mogelijk informatie te voorzien. Transparantie is het sleutelwoord. Als bijvoorbeeld duidelijk is welke dienstverleners in de digitale ruimte meer betrouwbaarheid bieden dan anderen en het is de prijs waard, dan zullen partijen kiezen voor betrouwbare dienstverleners. Dit kan de overheid bevorderen door met de sector te streven naar duidelijkheid over de betrouwbaarheid van diensten en producten.

De overheid kan bovendien met R&D-steun zowel voor technologisch onderzoek als voor beleidsonderzoek zoals 'benchmarking' en 'best practices studies' bevorderen dat bedrijven en instellingen onderzoek doen naar technologie voor betrouwbaarheid zoals 'smartcards', betrouwbare tussenpartijen die certificaten kunnen verstrekken ('Trusted Third Parties', TTP's[7]), encryptie en de bijbehorende infrastructuur die daarop is gericht ('Public Key Infrastructure', PKI). Veel hiervan is al op Europese schaal met bestaande wetgeving of in aanzet geregeld, inclusief de verplichting dat op de betrouwbaarheid van TTP's wordt toegezien.

Het is de taak van de overheid om bedrijven ertoe aan te zetten betrouwbaarheidsinspanningen te doen. Vaak zullen bedrijven en organisaties dit graag onderling en met brancheorganisaties vormgeven, bijvoorbeeld via zelfcertificatie. Een illustratief en origineel voorbeeld is het samenwerkingsverband van forensische IT-specialisten[8].

Taken die niet door de markt worden opgepakt vormen het primaat van de publieke sector. Daarbinnen valt bijvoorbeeld het oprichten van 'Early Warning Services' en crisismanagement voor verschillende vormen van 'cybercrime'. Verschillende Europese landen hebben dit inmiddels gedaan, bijvoorbeeld in de vorm van 'Computer Emergency Response' teams (CERT's), of ze zijn ermee bezig. In de VS bestaan er goede ervaringen mee, zoals met het 'Infraguard'-programma van het National Infrastructure Protection Center (NIPC) dat het

7 TTP = Trusted Third Party, een organisatorisch-elektronische oplossing die bij het elektronisch zaken doen de zekerheid biedt dat een partij inderdaad de partij is die het zegt te zijn.

8 European Network of Forensic Science Institutes (www.enfsi.org) is een associatie van forensische laboratoriumdirecteuren in Europa (van Portugal tot Rusland). Er is een speciale werkgroep voor IT Forensics.

mogelijk maakt gebeurtenissen in een vroeg stadium te identificeren. Bovendien wordt uitwisseling van informatie in en tussen private en publieke sectoren in de VS vergemakkelijkt door de zogenaamde Information Sharing and Analysis Centers (ISAC's). Enkele Europese landen kennen ook vergelijkbare samenwerkingsverbanden die dit ondersteunen, zoals de Information Assurance Advisory Council (IAAC) in het Verenigd Koninkrijk. In het kader van diverse Europese projecten wordt daaraan verder gewerkt, ook door RAND Europe, vooral in het kader van het 'Dependability Development Support Initiative[9].

Ten slotte blijft de overheid als wetgevende macht belangrijk. In de Filippijnen kon de bedenker van het 'I Love You'-virus niet worden vervolgd bij gebrek aan wetgeving. Dat is een situatie die – met internationale richtlijnen – snel wereldwijd dient te worden aangepakt. De Europese Commissie streeft naar harmonisatie van nationale wetgevingen op dit punt. Een opmerkelijk recent besluit in dit verband regelt de gelijkwaardigheid van gewone versus digitale handtekeningen.

De internationale beleidsontwikkeling geeft aan dat er consensus bestaat over de opvatting dat wereldwijd de verantwoordelijkheid voor een betrouwbare digitale ruimte zo dicht mogelijk bij de aanbieders en afnemers dient te worden gelegd. Het beleid in de digitale ruimte wordt daarmee een getrouwe kopie van het beleid in de dagelijkse wereld. En de ontwikkeling van beide werelden wordt gekenmerkt door toenemende transparantie, marktwerking en duidelijke rechten en plichten waarop alle belanghebbenden worden afgerekend.

Referenties

- Anderson, R.H. (2001). Cooperation between the Private Sector and the Government in Critical Infrastructure Protection: Lessons Learned from the US Experience. 5th International Conference on Technology, Policy and Innovation, The Hague. June
- Beck, U. (1992). The Risk Society. Towards a new Modernity. Sage Publications, London
- Beleidsnota Kwetsbaarheid op Internet (KWINT). (2001). Ministerie van Economische Zaken, Ministerie van Verkeer en Waterstaat, juli
- RAND. (2001). Cyber Security: What does the Private Sector Expect from Governments? A Transatlantic Perspective. RAND Europe, Leiden. April 9
- Rathmell, A. (2000). Protecting Critical Information Infrastructures. IST 2000. The Information Society for All. Nice. 6-8 November
- Ware, W.H. (1998). The Cyber-Posture of the National Information Infrastructure. RAND, Washington

9 www.ddsi.org

2

12
Het betrouwbaar ontwerp van een modern straalverkeersvliegtuig

ir. R.D. Boers [1]

Inleiding

De commerciële luchtvaart begon omstreeks 1920 met vliegtuigen die in de meeste gevallen rechtstreeks waren afgeleid van de militaire luchtvaart uit de Eerste Wereldoorlog. De gewenste betrouwbaarheid van militaire bommenwerpers was door de aard van ontwerp en gebruik (korte ontwerpcycli, korte gebruiksduur) te laag voor het civiele vervoer van personen en vracht. Door de lage gewichten en snelheden (typische waarden van de Fokker F II uit 1920 met een maximum startgewicht van 1.900 kg, en een snelheid van ca. 120 km/u) en dus lage energie-inhoud waren ongevallen vaak niet catastrofaal. Eerder gebeurde het dat een noodlanding gemaakt moest worden door het uitvallen van een (soms de) motor, waarbij in glijvlucht gedaald werd en op een weiland werd geland.

1 Inspectie Verkeer & Waterstaat,
Divisie Luchtvaart, Unit
Luchtvaartuigen
Postbus 575
2130 AN Hoofddorp

Figuur 12.1
Fokker F II (1920), passagiersaantal 5, gewicht 1.900 kg, kruissnelheid 120 km/u, motorvermogen 185 pk, actieradius 1.200 km. Bron: Fokker Heritage Trust.

Dit waren ongevallen die in relatief goed weer plaatsvonden en daardoor meestal goed afliepen. Heel anders werd de situatie in slecht weer. Vooral in de loop van de jaren twintig van de 20e eeuw werd hoger en sneller gevlogen en daar kwamen atmosferische effecten als windstoten en ijsafzettingen aan te pas. Ongevallen werden navenant steeds ernstiger en liepen vaker catastrofaal af. De kennis over de atmosfeer moest in die periode net zo opgebouwd worden als de kennis over het ontwerpen van een civiel vliegtuig zelf.
De eerste constructiemethode en de meest succesvolle in die tijd was een rompconstructie bestaande uit een gelast staalbuisframe, bedekt met linnen of soms triplex of bij het motorgedeelte met metaal waarin dan een passagierscabine was geplaatst. De vleugel was meestal geconstrueerd als een een- of tweeliggerconstructie waarvan het voorste deel was bekleed met triplex om torsie te kunnen opnemen, de resterende oppervlakken met linnen. Deze methode was voor die tijd licht en toch voldoende sterk. De betrouwbaarheid van de constructie werd uiteraard bepaald door de kwaliteit van de lassen, het linnen en het triplex. Hoewel de passagiersluchtvaart in Europa omvangrijker was, kwam de luchtvaart vooral in de VS op gang door de stimulerende werking van lucratieve postcontracten. Dat leidde ertoe dat snelheid van steeds groter belang werd. Snelheid komt in de eerste plaats voort uit meer motorvermogen, en de ontwikkeling van steeds grotere motorvermogens was daarom in die tijd zeer belangrijk in de VS. Maar een deel van de snelheidswinst kan ook worden ingeruild voor meer laadvermogen, en hoewel postcontracten niet direct om grotere vliegtuigen vroegen, was er vooral in Europa een tendens om steeds meer passagiers te vervoeren. In het begin van de jaren dertig van de 20e eeuw kwam er in Amerika een deregulering op gang, waardoor de hoge postsubsidies werden verlaagd. Luchtvaartondernemingen waren daarom ook daar mede aangewezen op passagiersvervoer. Dit gebeurde aanvankelijk met ‘klassiek’

geconstrueerde vliegtuigen: een staalbuisromp met een houten vleugel. Aan deze beginperiode kwam in 1931 een eind met het ongeval van een Fokker F 32, destijds een der grootste passagiersvliegtuigen, dat het gevolg was van onontdekt houtrot in de vleugel. Bij een vlucht in zwaar weer bezweek de vleugel. Als gevolg van dit ongeval werd deze constructiemethode niet langer toegestaan in de VS. Hiermee brak het tijdperk van de geheel metalen vliegtuigconstructie aan.

Ontwikkeling

Met de komst van het geheel metalen vliegtuig kon ook de stroomlijnvorm van vliegtuigen gestalte krijgen. Inmiddels was in de jaren twintig en dertig van de vorige eeuw veel onderzoek gedaan naar de invloed van de eigenschappen van de atmosfeer en van de materiaalkeuze op het ontwerp van vliegtuigen. Met de tegelijkertijd snelle ontwikkeling van steeds krachtiger motoren is er in die tijd sprake van een grote ontwikkeling in ontwerpfilosofieën. De lijndiensten gingen steeds langere afstanden overbruggen en om de vlieger in staat te stellen een groot en zwaar vliegtuig langere tijd te besturen werden hydraulische en pneumatische systemen toegepast, en nieuwe langeafstandsnavigatie-instrumenten gebruikt. Vooral automatisering begon op te komen, aanvankelijk in de vorm van een automatische piloot die het vliegtuig in de goede vliegstand houdt, en daarmee de vlieger rust gunt op de lange afstand. Een belangrijk element daarbij was de ontdekking van de kunstmatige horizon waardoor blind vliegen mogelijk werd. Weer later wordt automatisering ook toegepast om vrijwel alle vliegtuigsystemen te kunnen beheersen en controleren.

Figuur 12.2
Douglas DC 4 boven New York aan het begin van een oceaanvlucht op weg naar Amsterdam (1946). Passagiersaantal 44, gewicht 33.140 kg, kruissnelheid 330 km/u, totaal motorvermogen 4 x 1.350 = 5.400 pk, actieradius 3.150–4.600 km. Bron: KLM Aerocarto Arnhem.

Parallel daaraan neemt de betrouwbaarheid van vliegsystemen gestaag toe en tegen het eind van de jaren veertig in de 20e eeuw vliegen passagiersvliegtuigen met circa 100 inzittenden over oceanen en woestijnen in vrijwel alle weersomstandigheden.

In dit groeiproces zijn enkele schoksgewijze stappen te onderkennen die van grote invloed zijn geweest op de methode van ontwerpen en het niveau van betrouwbaarheid van vliegtuigsystemen. Dat zijn de introductie van straalmotoren en propellerturbinemotoren, de invloed van metaalmoeheid met het daaraan gerelateerde scheurgedrag van een vliegtuigconstructie, de introductie van elektronica in vliegtuigsystemen, en de automatisering van het vliegtuig als geheel systeem gezien.
De straalmotor verving met zijn relatief klein aantal ronddraaiende onderdelen de complexe zuigermotor, waarin veel verschillende onderdelen zowel reciproke als ronddraaiende als beide bewegingen maken. Uit die tijd stamt ook het voorschrift dat vliegtuigen bestemd voor vluchten over oceanen met drie of meer motoren moesten zijn uitgerust; in de civiele praktijk waren dat altijd viermotorige vliegtuigen.
Het veel grotere specifieke vermogen van een straalmotor maakte ook plotseling grotere afmetingen, grotere gewichten en dus een groter laadvermogen van vliegtuigen mogelijk.
Daardoor kon er op grotere hoogte gevlogen worden, waarmee grotere snelheden bereikt konden worden. Maar dat leidde ook tot een zwaardere belasting van de vliegtuigromp door de wisselende belasting van de drukcabine.
Metaalmoeheid als fenomeen was wel bekend, maar de invloed van scheurgedrag van een complete vliegtuigconstructie zoals een romp was vanuit ontwerptechnisch oogpunt nog onvoldoende bekend. De ongevallen in 1953 en 1954 met de Comets, een der eerste straalverkeersvliegtuigen, zijn illustratief. Deze ongevallen lieten zien dat de wisselende belasting die de romp onderging met het op druk brengen op grotere hoogte gevolgd door het drukloos maken bij de landing, leidden tot het ontstaan van kleine beginscheuren, vooral aan scherpe vormovergangen. Bij de groei van de scheurlengte wordt op een zeker moment een kritische lengte bereikt, waarna de scheur instabiel verder groeit. Dit gaat bij een onder druk staande drukcabine van een vliegtuig explosief. Na een buitengewoon grootschalig onderzoek door Britse luchtvaartonderzoeksinstellingen in de periode van 1954 tot 1958 werd dit gedrag herkend en goed beschreven. Daarna ging de kennis over hoe een instabiele scheurgroei in het ontwerp te vermijden met sprongen omhoog. Tegenwoordige vliegtuigconstructies hebben nu een vormgeving, waardoor explosieve instabiele scheuruitbreiding normaliter niet meer kan voorkomen.
Een ander gevolg van deze schaalvergroting was de noodzaak om de werkbelasting van de bemanning steeds meer beheersbaar te houden.

Langeafstandsvluchten van 10 tot 14 uur waren gewoon geworden en de beperkingen van het menselijk kunnen leidden ertoe dat steeds meer geautomatiseerde elektronische systemen toegepast werden. Deze laatste ontwikkeling strekte zich later ook uit tot vliegtuigen die kortere afstanden aflegden, de navigatie-eisen en de vliegtuigcomplexiteit stonden geen weg terug meer toe. Ook de toenemende drukte in de omgeving van luchthavens veroorzaakte een toenemende werkdruk in de cockpit.

Trends

Uit het voorgaande kan een aantal trends gesignaleerd worden, die van belang zijn voor de case die hier wordt beschreven.
Naarmate de luchtvaart volwassen wordt, neemt de werkdruk van vliegers geweldig toe. Dat leidt ertoe dat met de stand van de techniek de automatisering in de cockpit voortdurend toeneemt, zowel op het gebied van de controle over het complexe vliegtuig, als van de navigatie. Daarbij dient niet alleen de langeafstandsnavigatie te worden inbegrepen, maar ook de lokale navigatie rondom de luchthavens, vooral het naderingsgedeelte van de vlucht, waarbij de verkeersleiding steeds grotere aantallen vliegtuigen zo snel mogelijk en zonder vertraging op de landingsbaan moet brengen. De ontwikkeling van nieuwe software die deze functies kan vervullen gaat daarom steeds sneller. Een achtergebleven gebied hierin is de beoordeling van menselijke factoren. Deze ontwikkelingen hebben invloed op de methoden van testen van nieuwe constructietechnieken en systeemtechnologieën. Het wordt moeilijk om bijvoorbeeld alle eigenschappen van een nieuwe toepassing van software te onderkennen in het ontwerpproces en adequaat te testen. Door de omvang van beproevingsprogramma's kost het luchtvaartautoriteiten steeds meer moeite de certificering van deze technologische ontwikkeling te beheersen. Er is een groeiende tendens om steeds meer van deze verantwoordelijkheden 'dan maar' te delegeren naar de terzake deskundige industrie.

Kenmerken van het moderne vliegtuigontwerp

In de loop der jaren werden het ontwerp en de bouw van een verkeersvliegtuig steeds duurder door de hiervoor gesignaleerde trends. Afhankelijk van de inrichting die een vliegtuigoperator wenst, is de prijs van een tweemotorig korteafstandsvliegtuig voor circa 120 passagiers ongeveer 60 miljoen dollar en voor een viermotorige Jumbo circa 300 miljoen dollar, en die prijzen stijgen nog steeds.

Daarmee wordt het noodzakelijk om zowel de technische als de economische levensduur van een verkeersvliegtuig steeds voldoende lang te maken om uit de kosten te komen en voldoende rendement op het geinvesteerde kapitaal te halen. Een kenmerkende technische levensduur voor een korteafstandsvliegtuig is 90.000 cycli (start en landing, de bepalende belastingsgevallen voor de levensduur). In tijd gerekend is dat (aannemende een gemiddeld daggebruik van 10 uur en een gemiddelde vluchtduur van 2 uur) circa 18.000 dagen, dus meer dan 45 jaar. Een van de eerste Fokker F 27 Friendship uit 1958 was in 2000 nog steeds in gebruik, een periode overbruggend van 42 jaar!
Om de enorm toegenomen drukte in en om luchthavens het hoofd te kunnen bieden, dient de werkdruk in de cockpit zo laag mogelijk gehouden te worden. Dat wordt bereikt door enerzijds een vergaande automatisering van de diverse vliegtuigsystemen en anderzijds een toenemende integratie van de verkeersleiding op de grond en de navigatie aan boord van het vliegtuig. Vooral systemen die besturing en controle door de vliegers vereisen zijn tegenwoordig geautomatiseerd, zoals het brandstofmanagementsysteem (zorgen dat de brandstof in de diverse veelal gescheiden tanks regelmatig gebruikt wordt, zodat geen asymmetrische gewichtsverdeling van het vliegtuig ontstaat). Verder kunnen het aanpassen van het vermogen van de motoren aan het voortdurend dalende vliegtuiggewicht (vanwege het gebruik van brandstof) of de bediening van de drukcabine (de druk in de cabine zodanig opbouwen en aflaten, dat de cabine niet onnodig belast wordt en het comfort voor de passagiers optimaal blijft) worden geautomatiseerd. Dat geldt vaak ook voor de ijsdetectie en -bestrijding. Bij moderne vliegtuigen worden al deze functies zodanig geïntegreerd met de automatische piloot dat op ieder moment van de vlucht de vliegtuigconditie optimaal is, ook wat de navigatie betreft.

Figuur 12.3
Boeing 737-500 (1990) voor de korte en middellange afstand. Passagiersaantal ca. 120, kruissnelheid ca. 800 km/u, motorvermogen 2 x 10.000 = 20.000 kg, stuwkracht (komt bij 800 km/u overeen met ca. 47.500 pk), actieradius ca. 4.400 km. Bron: Jean-Charles Dayot.

De meeste verkeersvliegtuigen zijn tegenwoordig uitgerust met een uitgebreidere automatisering van het hiervoor genoemde brandstofmanagementsysteem, de zogenaamde 'auto-throttle', een automatische gasbediening waarmee de stuwkracht van de motoren voortdurend wordt aangepast aan de fase van de vlucht, inclusief vliegmanoeuvres. Daarbij wordt van de vliegers een goed en diepgaand begrip gevraagd van de onderliggende ontwerpfilosofieën, vooral bij onverwachte gebeurtenissen, zoals faalcondities van vliegtuigsystemen, vogelaanvaringen, zeer zware turbulentie. De mens/machine-interactie is daarbij mede bepalend voor de veiligheid van de vlucht en de personen aan boord. In de hiernavolgende case wordt daarvan een voorbeeld gegeven.

Case tweemotorig modern straalverkeersvliegtuig

Het ongeval

Bij een nieuw type tweemotorig straalverkeersvliegtuig voor circa 130 passagiers trad ongeveer 11 minuten na vertrek tijdens de klim naar kruishoogte een motorstoring op. Rook werd door het ventilatiesysteem (dat lucht van de motorcompressor betrekt) de cockpit in geblazen, zodat de vliegers concludeerden dat een motor in brand was gevlogen. Tevens verloor een van de motoren stuwkracht. Normaliter zou een asymmetrische krachtenverdeling de vliegers fysiek geïnformeerd hebben welke motor gefaald zou hebben. Het vliegtuig was uitgerust met een automatische piloot en een auto-throttle en daarom was er geen merkbare verdraaiing om de topas, zodat onbekend bleef welke motor een lagere stuwkracht gaf. Het vliegtuig is zo ontworpen dat het op één motor kan vliegen. De voornaamste taak voor de bemanning zou nu zijn om de gefaalde motor uit te zetten. De klim werd afgebroken, het vliegtuig werd op een horizontale stand gebracht en met de gashandels werd het motorvermogen daarop afgestemd, dat wil zeggen verlaagd ten opzichte van het startvermogen. Even later zou het vermogen nog verder teruggebracht worden om een daalvlucht te beginnen naar het uitwijkveld, dat zich slechts circa 20 minuten vliegen verderop bevond. De copiloot waarschuwde de verkeersleiding en haalde de procedure 'motor uitzetten' tevoorschijn. Bij de procedure motor uitzetten dient vastgesteld te worden welke van de twee motoren gefaald heeft. Daarvoor bestaat in de cockpit geen directe indicator. De gangbare techniek om dit vast te stellen is om van de meest waarschijnlijk gefaalde motor het gas terug te nemen en te zien of daarmee de problemen verdwijnen. Als dat niet het geval is, dan heeft de andere motor gefaald. De vliegers waren van mening dat de rechtermotor in brand stond, want de motorinstrumenten gaven voor de rechtermotor een lagere prestatie aan, en ze draaiden het gas van die motor dus terug. Het schudden nam inderdaad af en de vliegers sloten vervolgens de rechtermotor af. Er zou uitgeweken worden naar het dichtstbijzijnde vliegveld. Bij onderzoek naar het ongeval

bleek later dat de linkermotor gefaald had door een breuk in een aantal compressorbladen.Tijdens de vlucht was dat de vliegers echter niet bekend. Gedurende de vlucht naar het uitwijkveld werd geleidelijk al gedaald met laag motorvermogen, maar voor het neerlaten van de vleugelkleppen en het landingsgestel is meer motorvermogen nodig. Vlak voor de laatste naderingsfase raakte de linker (dus draaiende) motor nog verder beschadigd door het afbreken van steeds meer compressorbladen. Vanaf dat moment kon deze motor geen vermogen meer leveren, en aangezien de goede rechtermotor uitgezet was, verloor het vliegtuig hoogte en raakte enige tientallen meters voor de baan de grond. Het vloog tegen een talud langs de snelweg aan de kop van de baan en brak in diverse stukken. Er waren 47 doden te betreuren. Er waren in totaal 126 passagiers aan boord.

Elementen in de oorzaakketen

De linkermotor verloor direct na de start een stuk van een compressorblad (door onjuiste certificatie). Daardoor ontstond een onbalans en de beschadigde motor gaf rookontwikkeling, maar leverde nog wel vermogen.
Het vliegtuig was uitgerust met een automatische gasbediening (de auto-throttle, die ervoor zorgt dat er geen (al te grote) asymmetrische stuwkracht ontstaat). Door de beschadiging in de linkermotor bij klimvermogen gaf dit systeem direct veel extra brandstof aan de linkermotor om de asymmetrische stuwkracht te compenseren. Om dat goed te kunnen doen, verlaagde het systeem daarom tevens de brandstoftoevoer naar de goede motor. Dat is te zien op de motorbrandstofdrukinstrumenten die laten zien dat het vermogen van de rechtermotor naar beneden gaat. Dat wordt zichtbaar door het toerental van de 'fan' (een

Figuur 12.4
Cockpit Boeing 737-500. Links en rechts, en boven elkaar twee beeldschermen met vliegtuigcondities en navigatiegegevens. In het midden motorindicaties.

grote lagedrukcompressor aan de voorzijde van de motor).Nadat even later het gas van de rechtermotor werd teruggehaald (om na te gaan welke motor gefaald had) werd dit systeem echter automatisch uitgeschakeld, zodat de extra brandstoftoestroom ook ophield. Daardoor eindigde meteen het schudden van het vliegtuig en de rookontwikkeling, zodat de bemanning ervan overtuigd raakte dat de rechtermotor gefaald had, en dat het dus correct was om die uit te zetten.
Een fysieke aanduiding dat de linkermotor stuwkracht verloor was er niet, omdat de automatische piloot dit compenseert en dat correct doet.
Er is in de cockpit een vibratieniveau-indicator (van de motoren) aangebracht, maar in de voorgaande versie was dit instrument zo onbetrouwbaar dat geen enkele vlieger deze indicator serieus nam. In deze versie was de vibratieniveau-indicator echter een elektronisch instrument dat zeer betrouwbaar was. Ook waren de cockpitinstrumenten in dit nieuwere model van dit type verkeersvliegtuig voor het eerst op beeldschermen afgebeeld, maar aangezien de functies van de motorinstrumenten niet verschilde van de oudere versie, was door het management van de luchtvaartmaatschappij (noch overigens door de luchtvaartautoriteit) conversietraining geëist.
Hierdoor ontstond een verkeerde beslissing en was een ongeval onafwendbaar, terwijl het systeem geacht werd zo betrouwbaar te zijn dat het nu juist zo'n ongeval had moeten en kunnen voorkomen.

De betrouwbaarheidsgrenzen van het totaalsysteem

Hier volgt een korte opsomming van de betrouwbaarheidsgrenzen van het totaalsysteem[2].

- De indicatie is betrouwbaar, maar de aflezing is verkeerd begrepen of geïnterpreteerd.
- De faalconditie (beschadigde motor) wordt niet in directe zin, maar indirect aan de vliegers gepresenteerd (verlaagde vermogensindicatie door toerental goede motor, compensatie van de asymmetrie).
- Aanvullende (reddende) informatie (namelijk aan welke kant de brandende motor zich bevindt) wordt door het cabinepersoneel niet doorgegeven.
- Door de snelle sequentie van gebeurtenissen (schudden, daalvlucht, landingsfase, onverwachte motordegradatie binnen ca. 25 minuten) kregen de vliegers geen gelegenheid de situatie te analyseren.
- Gebrekkige training door de luchtvaartmaatschappij en het ontbreken van eisen daartoe van de luchtvaartautoriteit hebben een bijdrage geleverd.
- Uit een analyse van het ongeval blijkt dat dit ongeluk een gevolg is van een keten van gebeurtenissen die alle met 'AND poorten' aan elkaar zijn verbonden (zie kader in hoofdstuk 32). Eén schakelverbreking had het ongeval kunnen voorkomen.

2 Onder totaalsysteem wordt in dit kader verstaan het geheel van vliegtuig- en motorontwerp, beproeving en of certificatie, en bemanning.

De lessen ter lering

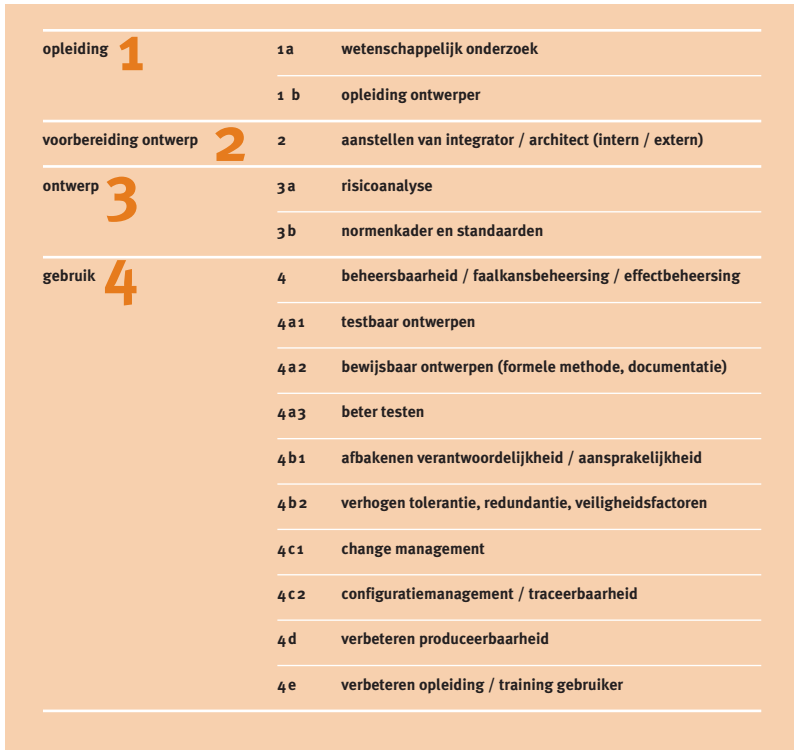
De wortel van het kwaad ligt in het feit dat de motoren van dit model vliegtuig een iets hoger vermogen konden leveren door een kleine vergroting van de 'fan'bladen. Omdat de toename van de afmetingen slechts circa 10% bedroeg, stelden de certificatieautoriteiten geen nieuwe testcyclus verplicht. Ook een nieuwe beschouwing van alle mogelijke faalcondities en hun gevolgen werd niet nodig geacht. Zou dat wel gebeurd zijn, dan was het hiervoor beschreven scenario hoogst waarschijnlijk onderkend. Dan was òf de mogelijke breuk van het fanblad vermeden door een grotere sterkte toe te passen, òf was het aflezen van de instrumenten aangepast.
Men dient met grote voorzichtigheid om te gaan met de conclusie dat een modelwijziging slechts weinig invloed heeft en dat een conversietraining van de bemanning dus niet nodig is.
In dit geval werd de minimale toename van de afmetingen van de kleine motor en de toepassing van nieuwere instrumenten met beeldschermaflezing een fatale combinatie, toen men niet tot additionele bemanningstraining overging. Het ontwerp van de mens/machine-interactie heeft onvoldoende aandacht gekregen, waardoor de aflezing van de motorinstrumenten fout geïnterpreteerd werd. In samenhang hiermee dienen de vliegers over voldoende diepgaande kennis en begrip van de diverse vliegtuigsystemen en hun automatiseringskenmerken te beschikken ('Hoe gedraagt het systeem zich in diverse scenario's?'). Aan deze eis zit echter een grens: een vlieger kan bij de huidige vliegtuigen niet meer de academische kennis bezitten die de ontwerper heeft.

De betrouwbaarheidsketen, de analyse van de betrouwbaarheid en de onbetrouwbaarheid van het vliegtuigontwerp

De hoofdparameters die van invloed zijn op het niveau van de betrouwbaarheid van het vliegtuigontwerp laten een aantal stappen zien die gedurende het ontwerpproces en het daaropvolgende gebruik in sommige gevallen wel en in andere gevallen geen hiaten vertonen (zie figuur 12.5).

Het begin van een goed ontwerp ligt in een voldoende ontwikkeld wetenschappelijk niveau van de ontwerper. Bij het ontwerpen van vliegtuigen en vliegtuigsystemen is in het algemeen wel sprake van een voldoende wetenschappelijk niveau: ingenieurs met een vliegtuigbouwkundige, werktuigbouwkundige of elektronische achtergrond zijn direct betrokken en verantwoordelijk voor het initiële ontwerp. Naarmate het ontwerp vordert, komt steeds meer de vraag naar voren of de diverse onderdelen op een effectieve manier geïntegreerd zijn. Vooral de automatisering van de besturing van de huidige vliegtuigen is essentieel voor een veilig (en dus betrouwbaar) ontwerp. De generatie van straalverkeersvliegtuigen die in het begin van de 21e eeuw op de markt verschijnen, bevatten in veel gevallen een verminderde inherente stabiliteit, en zijn dus met

Figuur 12.5
Punten die van invloed zijn op de betrouwbaarheid van een technisch systeem tijdens de levenscyclus.



een 'fly-by-wire'-systeem uitgerust. Het ontwerp van deze vliegtuigen omvat veel sensoren die allerlei vliegtuigposities, bewegingen en gedragingen meten en in een computer verwerken, waarna de correctieve stuuruitslagen gecommandeerd en automatisch uitgevoerd worden (zie voor een nadere toelichting het kader hierna).
Als de integratie in dit werkveld onvoldoende is toegepast of wanneer bepaalde aspecten over het hoofd zijn gezien, kunnen de gevolgen catastrofaal zijn.

Een vliegtuigvleugel levert bij het bewegen door de lucht een opwaartse kracht op, maar ook een moment. Helaas is de fysica van de vleugel zodanig dat dit moment (bij de meeste toegepaste vleugelvormprofielen) destabiliserend werkt. Dat wil zeggen dat als de invalshoek door bijvoorbeeld een windstoot groter wordt, de liftkracht ook groter zal worden. Het vliegtuig zal willen stijgen. Het destabiliserend moment heeft als eigenschap dat de vergroting van de invalshoek juist groter wordt, zodat er nog meer liftkracht ontstaat. Dit proces gaat door totdat de kritische invalshoek bereikt wordt, waarna de vleugel zijn liftkracht in het geheel verliest, en de zwaartekracht als enige verticaal gerichte kracht overblijft. Om dit effect teniet te doen, wordt een achtervleugel (soms een voorvleugel) toegepast die zodanig gedimensioneerd wordt dat de destabiliserende momenten worden opgeheven door een resulterende kracht van de combinatie van vleugel en achtervleugel. Dat levert dan een stabiliserend moment aan het vliegtuig als geheel op. Hiervoor is in principe geen roeruitslag aan de achter-

vleugel vereist. Daarmee wordt de verstoring tegengewerkt, en dat is het kenmerk van stabiliteit. Verminderde stabiliteit beoogt hetzelfde effect te bereiken, maar nu door op de juiste momenten een roeruitslag te geven. Het grote voordeel hiervan is dat de achtervleugel kleiner kan worden, waardoor gewicht en weerstand verminderen. Nadeel is echter dat deze roeruitslagen voortdurend met een frequentie tot enkele Herz moeten worden aangebracht. Een menselijke vlieger is hiertoe niet in staat. Een computergestuurd vliegtuig uitgerust met elektrisch aangestuurde roeren is wel in staat continu te berekenen welke uitslag hoe groot, wanneer en hoe lang gegeven moet worden. Dat kan alleen als deze aansturing elektrisch gebeurt. Dat is het 'fly-by-wire'-principe. Airbus past dit systeem al toe in enkele modellen die ook een inherente verminderde stabiliteit bezitten. Boeing past wel fly-by-wire toe, maar niet op burgervliegtuigen met verminderde stabiliteitseigenschappen, en mist dus het gewichtsvoordeel zoals eerder is uiteengezet.

Nadat bij het ontwerp alle voorziene integratiestappen zijn gemaakt, behoren de risico's te worden getoetst, die ontstaan als twee of meer functies niet of onjuist aan elkaar gekoppeld worden. Daarmee wordt bereikt dat een bepaalde conditie bij het werkelijke gebruik niet tot catastrofes zal leiden. Bij het ontwerp van de gedigitaliseerde motorafleesinstrumenten van het in deze case beschreven straalverkeersvliegtuig is er sprake van een onvoorzien effect door de integratie van de menselijke interpretatie bij het aflezen van deze instrumenten en de betekenis ervan. Daaraan gekoppeld is de uitrusting van het vliegtuig met een automatische stuwkrachtregelaar (auto-throttle). Omdat bij het falen van de ene motor de auto-throttle een verlaging van de stuwkracht aan de goede motor de juiste handeling was van dit systeem, werd echter de menselijke aflezing geïnterpreteerd als een indicatie van het falen van die goed werkende motor.
In de integratie werd een onvolledig normenkader toegepast, namelijk dat een terugval of daling (van de aanwijsnaald van het instrument) wel een vermindering van de stuwkracht van de ene motor betekent, maar dat in het geval van een falende motor een andere norm gehanteerd moet worden. De boodschap aan de vlieger zou moeten zijn 'deze daling is terecht'. Hier is dus sprake van het niet onderkennen van de relatie tussen normen, risicoanalyse en integratie. Deze relatie is dus onvolledig getest in de ontwerpfase. Dit is te onderkennen als een hiaat in de stappen 2 (aanstellen van een integrator/architect) en 3 (risicoanalyse/normenkader en standaarden). Zie voor deze stappen figuur 12.5. Gegeven het feit dat deze relatie niet onderkend werd in het ontwerpproces, zouden er nog andere elementen geweest kunnen zijn die dit ontwerp hadden kunnen redden?
Een belangrijke stap in de introductie van ieder nieuw ontwerp van een complex apparaat als een schip, een vliegtuig of het besturingssysteem van een chemische fabriek is de training van de bestuurder of gebruiker ervan. Ook al zou de eerdergenoemde relatie onvoldoende uitgedacht zijn, bij realistische trainingen

op het apparaat zelf of op een goed gevalideerde simulator zou het gedrag van het ontwerp waarschijnlijk wel op de juiste wijze geinterpreteerd worden. Een goede koppeling tussen de ketenstappen 4 (effectbeheersing) en 4e (training) (zie figuur 12.5) zou de situatie mogelijk gered hebben. Ook voor een training geldt echter weer dat er een goede koppeling moet zijn op integratieniveau en op het gebied van de normen: de training zou in het geval van het tweemotorig straalverkeersvliegtuig een oefening 'motoruitval aan één kant' moeten bevatten. Overigens wordt in de luchtvaart deze conditie altijd geoefend. Maar in deze case werd voorzover bekend geen simulatoroefening gehouden, zodat deze situatie onbekend bleef.

Een andere relevante vraag is of er mogelijkheden waren om deze fatale onbetrouwbaarheid te vermijden in het samenspel tussen de ontwerper (in dit geval de vliegtuigfabriek) als exponent van het bedrijfsleven en de overheid die als luchtvaartautoriteit de maatschappelijke verantwoordelijkheid voor de veiligheid van de samenleving draagt.

Historisch gezien is er een tendens waarneembaar, waarin de overheid geleidelijk steeds meer afstand neemt van de industrie. Waar de directeur van 's Rijks Studie Dienst voor de Luchtvaart nog zelf een testvlucht met de Fokker F-VIIA uitvoerde – en dat overigens in enkele dagen kon doen – beslaat het huidige testvliegprogramma van een straalverkeersvliegtuig tussen 1.000 en 2.000 vlieguren. Dat is een programmaduur van 2 à 3 jaar. De overheid heeft weliswaar zelf ook testvliegers in dienst, maar die vliegen niet meer dan een testprogramma van circa 5 tot 10% van die duur. Daarbij worden meestal bepaalde eigenschappen in bepaalde condities (zoals slecht weer of hoge werkbelasting) getoetst binnen het testprogramma van de vliegtuigfabrikanten. Ook het toetsen van de veiligheidseisen die de overheid aan het vliegtuigontwerp stelt, wordt in toenemende mate gedelegeerd aan de fabrikant onder allerlei complexe kwaliteitsborgingserkenningen. Dit impliceert dat de fabrikant in toenemende mate zelf moet beoordelen of aan alle ontwerpkwaliteiten wordt voldaan. Terzijde zij opgemerkt dat voor de opzet (ontwerp) van dit delegatieproces dezelfde ketenbenadering dient te worden toegepast.

Ten slotte kan de vraag gesteld worden of de mens dan maar niet geheel uit de kringloop gehaald moet worden als het hiervoor beschreven ongeluk een rechtstreeks gevolg was van een menselijke interpretatiefout. Dat komt neer op een volledig geautomatiseerd vliegtuig dat geen input van menselijke vliegers meer nodig heeft.

Is dat mogelijk? De stand der technologie laat toe dat vliegtuigen inderdaad geheel automatisch kunnen vliegen. Vanaf de start, de stijgvlucht, de navigatie tijdens de kruisvlucht, de nadering en de landing, inclusief het afdraaien van de landingsbaan ligt dit binnen de mogelijkheden. Wat echter nog niet onderzocht is is de maatschappelijke acceptatie: zowel aan de kant van het reizend publiek als aan de kant van luchtvaartautoriteiten, fabrikanten en luchtvaartmaat-

schappijen staat men huiverig tegenover zo'n ontwikkeling. Dit heeft vooral te maken met de betrouwbaarheid van het ontwerp in marginale condities, zoals de situatie dat een motor is uitgevallen (niet echt bijzonder ontwerptechnisch gezien), als er geland moet worden in slecht winterstormweer (ook niet bijzonder meteorologisch gezien), of als de wind ten opzichte van de richting van de landingsbaan een zijwindcomponent heeft die tegen de limieten van het vliegtuig zit (op zich ook niet echt bijzonder). Ieder element op zichzelf is niet bijzonder gevaarlijk of onvoorzien. De combinatie van deze omstandigheden wordt echter in het geval van een volledig automatisch vliegtuig zonder menselijke vlieger in termen van een betrouwbaar ontwerp (nog?) als onrealistisch gezien. Er is geen enkel inzicht of alle stappen in de stappenketen van de betrouwbaarheid voldoende afgedekt zijn. Ook zouden vooralsnog de psychologische barrières bij een publieke acceptatie onoverkomelijk zijn.

Uitgaand van figuur 12.5 kan dus geconcludeerd worden dat als een niet volledig betrouwbaar ontwerp tot catastrofale condities (dus als mensenlevens verloren gaan) leidt, de grootst mogelijke aandacht moet worden gegeven aan de relaties tussen de ontwerpelementen 2 (aanstellen van een integrator/architect) en 3 (risicoanalyse/normenkader en standaarden). Vervolgens moeten de stappen 4 (effectbeheersing), 4a1 (testbaar ontwerpen) en 4a3 (beter testen) intensief worden toegepast.

2

13 Belang integraal software testen en de mislukte marsmissies

ir. R.J. Baarda[1]

Inleiding

De ruimtevaart levert vanaf het begin een grote hoeveelheid voor het betrouwbaarheidsdenken relevante, herkenbare en algemeen bekende cases. Ruimtevaartsystemen kunnen getypeerd worden als:

- complex zowel qua technische samenstelling als de wijze van ontwikkelen door vele gespecialiseerde organisaties;
- vernieuwend, omdat vaak nieuwe technieken (bijv. ionenaandrijving) en materialen (bijv. hitteschilden) moeten worden ontwikkeld waarvan de betrouwbaarheid initieel onbekend is;
- onder tijdsdruk ontwikkeld.

1 IQUIP Informatica B.V.,
Afdeling Software Control
Postbus 263
1110 AG Diemen
http://www.iquip.nl

Op het gebied van betrouwbaarheid heeft de ruimtevaartindustrie een enorm 'trackrecord' opgebouwd.
Om tegemoet te kunnen komen aan de kritiek van de Amerikaanse politiek dat er tussen de successen te veel tijd zat en dat ze te duur waren, heeft NASA de Amerikaanse ruimtevaartprogramma's vanaf de jaren negentig aangestuurd vanuit de 'faster, better, cheaper' (FBC)-aanpak.
Deze aanpak heeft bij het Marsprogramma geleid tot meer relatief kleinere missies. De eerste drie missies zijn geslaagd, maar hierna is een aantal missies niet volbracht. De systemen werkten uiteindelijk niet naar behoren, omdat ze onvoldoende betrouwbaar waren.
In deze case worden twee van deze mislukte missies behandeld. Dit gebeurt aan de hand van de publieke NASA-rapporten [2] die het verloop van de missie beschrijven, de oorzaken analyseren en aanbevelingen voorstellen. Deze beschrijving geeft geen compleet overzicht van alle oorzaken (voor een uitgebreide analyse zie de rapporten op de website), maar spitst zich toe op het testaspect. Dit testen speelt een grote rol in deze cases.

Trends

Deze case dient als illustratie van de trends.

Toenemende druk op doorlooptijd

De markteisen zijn verschoven van groot en goed (dus relatief langzaam) naar sneller (korte time to market) en kleiner en dus eventueel iets minder goed.

Toenemende kennis

Het management en de 'ontdekker' van kennis besteden te weinig aandacht aan het doorgeven (dat is vastleggen en distribueren) van kennis, waarbij de toename van inhoudelijke kennis een uitdaging is en projectmanagementkennis aan de nieuwe generatie moet worden overgedragen. In een omgeving die gekenmerkt wordt door een korte time to market kan er echter geen kennisborging plaatsvinden (zie ook hoofdstuk 5, deel 1).

Toenemende complexiteit

Toenemende complexiteit leidt tot meer verschillende overzienbare eenheden waarbij de integrale werking een zorgenkind is. De enorme toename van de hoeveelheid software vereist een meer defensieve testaanpak. Door de eisen aan time to market komt het testen en zeker het hertesten na foutherstel echter onder druk.

2 Zie www.nasa.gov/newsinfo/marsreports.html

De mislukte marsmissies

Het NASA Marsprogramma

Het Marsprogramma van de NASA omvat een aantal onbemande missies met specialistische taken. Het is gestart in 1994 als eerste programma volgens de FBC-aanpak. De eerste missie in dit programma, de Mars Global Surveyer (MGS, 1996), was op zich zelf een groot succes en toonde de mogelijkheden van deze aanpak aan. De volgende missie, de Mars Pathfinder (Marslander I, 1997), was ook een groot succes. Ook de Deep Space missie (DS-1, 1998), bedoeld om nieuwe technologie als ion-aandrijving en autonome besturing te beproeven, slaagde.
Hierna ging het mis. In 1999 mistte de in 1998 gelanceerde Mars Climate Orbiter (MCO) zijn Marsbaan door een navigatiefout en vervolgens verging de Mars Polar Lander (MPL) op Mars, doordat de remraketten te vroeg afsloegen. De oorzaak van de laatstgenoemde fout lag in een opeenstapeling van fouten tijdens de ontwikkeling en onvoldoende training van de bemanningsleden op aarde.
In de volgende paragrafen wordt nader ingegaan op de specifieke aspecten van deze twee mislukte missies. Generieke onderzoeksresultaten worden in de laatste paragraaf behandeld.

De Mars Climate Orbiter

Wat er gebeurde

De Mars Climate Orbiter (MCO) is een satelliet die vanuit een baan rond Mars het marsklimaat in kaart zou brengen. De MCO heeft Mars echter gemist. Achteraf bleek dat gedurende de vlucht van de aarde naar Mars er reeds koersafwijkingen waren. De bemanning van het vluchtleidingscentrum herkende deze echter niet. Pas toen de afwijking duidelijk werd, werd vanaf de aarde ingegrepen in het autonome koersbepalingssysteem. De tijd was echter te kort om de MCO weer op de goede koers te brengen.

Analyse

De verkeerde koersaanwijzingen werden veroorzaakt door de onjuiste interface tussen twee softwaresubsystemen. Het ene subsysteem communiceerde in Engelse maten (‘inch’, ‘foot’) en het andere in het metrische stelsel (meters). De subsystemen waren gemaakt door verschillende organisaties.

Citaat uit het NASA-rapport: “Thousands of functions can be correctly performed and one mistake can be mission catastrophic. Mistakes are prevented by oversight, test and independent analysis, which were deficient for MCO. Specifically, software testing was inadequate.”

Een tester zou op basis van de specificaties al snel hebben gezien dat de systemen met verschillende metrieke stelsels werkten en dus niet goed konden communiceren. Ook het daadwerkelijk uitgebreid testen van de samenwerking van de twee systemen is niet uitgevoerd. Verschillen tussen meter en foot zijn dusdanig dat de fout gevonden had kunnen worden.
Kostenbesparingen door het niet uitvoeren van deze testen zijn niet voorhanden, maar vallen in het niet bij de mislukte missie.
De voor navigatie verantwoordelijke bemanning in het vluchtleidingscentrum had de koersafwijking tijdens de vlucht naar Mars niet opgemerkt. Dit gebrek aan opmerkzaamheid bleek terug te voeren tot een tekort aan bemanningsleden in het vluchtleidingscentrum en een gebrek aan kennis bij de bemanning. Het kennisgebrek bij de bemanning kwam door gebrek aan training. Het corrigeren van de onjuiste koers na ontdekking kostte de bemanning te veel tijd, en dat was te wijten aan een gebrek aan training van deze procedure.

De Mars Polar Lander-missie

Wat er gebeurde

De Mars Polar Lander (MPL) was samen met een aantal meetapparaten naar Mars gestuurd. Tien minuten voor de landing van de MPL zouden de meetapparaten in de ruimte worden gebracht en de MPL zou een zachte landing maken. Omdat na het geplande scheidingsmoment noch met de MPL noch met de meetapparaten communicatie mogelijk bleek, is geconcludeerd dat het geheel neergestort was.
Er is uitgebreid onderzoek gedaan naar de mogelijke oorzaken van het mislukken. Als meest waarschijnlijke oorzaak is aangegeven dat het uitklappen van de landingspoten in de sensoren valse elektrische signalen deed ontstaan die de besturingsprogrammatuur de indruk gaven dat de MPL de grondoppervlakte had bereikt. Daarop werden de remraketten uitgezet, zodat de MPL een te harde landing op Mars maakte.

Zoals in het rapport staat: “During the test of the Lander system, the sensors were incorrectly wired due to a design error. As a result the spurious signals were not identified by the systems test, and the systems test was not repeated with the properly wired touchdown sensors. While the most probable direct cause of the failure is premature engine shutdown, it is important to note that the underlying cause is inadequate software design and systems test.”

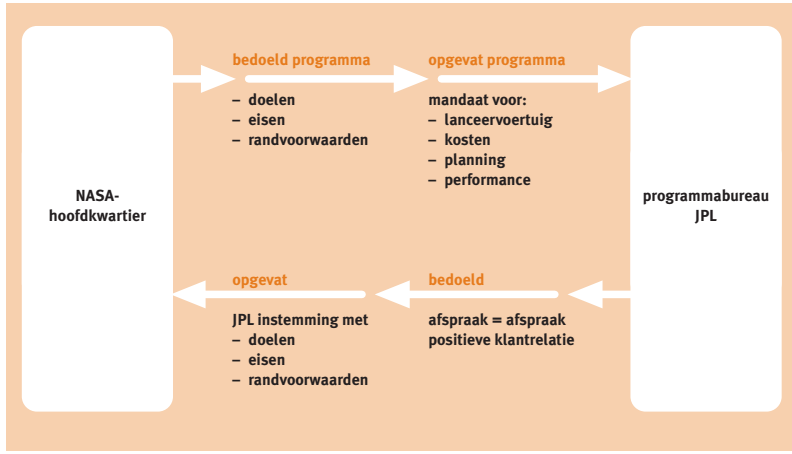
Analyse

Het is niet abnormaal dat sensoren valse signalen afgeven, maar maatregelen om dit op te vangen waren niet opgenomen in de software-eisen (ontwerpfout). Tijdens het testen bleek dat de bedrading onjuist was aangebracht (ontwerpfout), zodat het valse signaal en de gebrekkige afhandeling tijdens het testen

niet geconstateerd zijn. Na het aanpassen van de bedrading is de sensortest niet herhaald (testfout). De gehele installatie is dus niet werkend beproefd. De les dat testen naast maakfouten ook ontwerpfouten vindt was blijkbaar verloren gegaan. Tijdens de eerste test was immers een ontwerpfout gevonden (bedrading) die de goede werking van het uitklapmechanisme verhinderde. Door tijdgebrek is de test niet herhaald. De tweede ontwerpfout (opvangen valse sensorsignalen) is hierdoor niet gevonden.
Overigens bleek het uitgevoerde testprogramma voor de verloren meetapparaten onvoldoende te zijn geweest om een goede werking zeker te stellen. Men had er vanwege de tijdsdruk voor gekozen om de geplande algehele systeemtest niet uit te voeren!

Algemene conclusies en aanbevelingen

De meest fouten hadden voorkomen kunnen worden als er voldoende aandacht besteed was aan het voorkomen dan wel het opsporen van fouten (door testen en revisie). Omdat het traject snel moest worden uitgevoerd met een beperkt budget, is ervoor gekozen te bezuinigen op testwerk in plaats van op de veelheid van eisen. De slaagkans van de missie fungeerde als sluitstuk van het project. Deze keuze heeft te maken met de wijze van aansturing door het programmamanagement en de onervarenheid van het jonge projectmanagement. De veelheid aan projecten uitgevoerd door onderaannemers werd gecoördineerd door het programmabureau dat is ondergebracht bij JPL (Jet Propulsion Laboratory). Het NASA-hoofdkwartier stuurde het programmabureau JPL aan. Tussen de opdrachtgever NASA en het programmabureau bestonden grote misverstanden over doelen, eisen en randvoorwaarden. Het programmabureau interpreteerde zelfstandig de NASA-planningeisen als harde 'project'doelen
(zie figuur 13.1).



Figuur 13.1
Doel en interpretatie door NASA-hoofdkwartier en JPL.

De omslag van programmadoelen (een geslaagde missie) naar planningdoelen werd versterkt door een relatief jonge groep projectmanagers die vooral bezig waren met het maximaal invullen van de functionele eisen binnen de gestelde tijd. Deze keuze van 'de einddatum is heilig, desnoods met iets minder kwaliteit' is niet in overleg met NASA gemaakt. Het risico van een niet haalbare missie werd niet expliciet ingecalculeerd. In extreme bewoordingen kan gesteld worden dat er gelanceerd is zonder dat men de zekerheid had dat het geheel zou werken.

Aanbevelingen

Missiekritische producten vereisen een grondig test- en verificatieprogramma waarop vroegtijdig geanticipeerd dient te worden.
Bij een korte time to market moet in de besturing van het project schaalbare functionaliteit ingebouwd worden, zodat tegenslagen opgevangen kunnen worden door minder functionaliteit in plaats van minder testen. Het sleutelwoord is risicomanagement.
Ondanks tijd- en budgetdruk moeten gezonde ontwikkelprincipes niet losgelaten worden. Zonder uitputtend te zijn:

1 Efficiënte onafhankelijke revisies door competent personeel.
2 Overzicht, analyse en testen in stand blijven houden met het oog op het voorkomen van het falen van de missie.
3 Verantwoordelijkheden en gezag duidelijk definiëren; dus niet alleen op tijd en binnen het budget, maar ook goed werken.
4 Ga pas 'life' als je getest hebt, en test terwijl je 'life' bent.
5 Bepaal de risico's en bewaak de risico's.

Ten slotte

NASA heeft het probleem van de strijdigheid van deadlines versus tijdvretend testwerk aangepakt met de oplossing 'denken in risico's'. Enerzijds dienen de projecten te rapporteren op basis van risico's, anderzijds wordt intern gestuurd op basis van risico's.
Om de risicoreducerende maatregel 'testen van de integrale werking' te versterken, dient men zo vroeg mogelijk met het inrichten van het integratietestproces te beginnen. Om dit inrichten zeker te stellen, is het verstandig om de rol van de testmanager met een specifiek persoon te bemensen. Deze testmanager kan zich in de vroege fase van het project ook uitstekend bemoeien met de risicoanalyse en het testplan over alle ontwikkelingsstappen heen, omdat iedere ontwikkelings- of integratiestap een eigen (detail)testplan kent.

Bij het aansturen van het testproces is een teststrategie nodig. In de teststrategie wordt op basis van risico's vastgesteld welke delen zwaar en welke licht getest worden. Als illustratie volgt een uitwerking voor het testen van softwaremodulen. Voor softwaremodulen wordt bepaald welke modulen 'rood' (falen geeft grote risico's) en welke 'groen' (falen heeft minder risico's) moeten worden. Het testen van rode modulen krijgt dan meer prioriteit dan het testen van groene modulen.

Software heeft als nadeel dat niet alle fouten in een redelijke tijd tegen redelijke kosten gevonden kunnen worden. In het ontwikkelproces van software legt testen beslag op een aanzienlijk deel van het budget (tientallen procenten). Waar software in samenhang met sensoren en actuatoren werkt, zal in simulatoren geïnvesteerd dienen te worden die het gedrag van sensoren, actuatoren en hun onderlinge werking kunnen simuleren.
De trend is dat in technische systemen steeds meer software toegepast wordt. De ontwikkelkosten van bijvoorbeeld de volgende generatie Mercedes S-klasse zal voor 40% bestaan uit softwareontwikkeling tegen 30% voor de 2000-generatie. De 2000-generatie omvat circa 1 miljoen regels code. Omdat software niet eenvoudig per satelliet te verspreiden is, zal iedere auto voor iedere softwarefout teruggeroepen moeten worden. Dergelijke fouten zijn een kostbare geschiedenis en zullen tevens het vertrouwen in het merk schaden. Testen wordt dan belangrijk om de kans op zo'n fout te verkleinen. Door de grotere hoeveelheid software in het technische systeem zal de hoeveelheid testwerk toenemen.
Het opereren in het spanningsveld maakt het vinden van alle fouten onmogelijk. Deze aanpak vereist het maken van een teststrategie. Hierin wordt op rationele gronden bepaald welke subsystemen (en hun interfaces) hoe diepgaand getest moeten worden (zie de literatuur voor meer informatie hierover).

Literatuur

– Perry, W. (1995). Effective Methods for Software Testing. John Wiley & Sons, New York
– Pol, M., R. Teunissen, E. van Veenendaal. (1999). Testen volgens TMap. Tutein Nolthenius, 's-Hertogenbosch

2

14
Bouwvergunningen voor tunnels Hogesnelheidslijn-Zuid

ir. M.N.J.H. Wijnands [1,2]

In een veld vol tegenstellingen overeenstemming bereiken over de veiligheid van een prestigieus miljardenproject. De uitgangspositie voor het verlenen van bouwvergunningen voor de tunnels van de Hogesnelheidslijn-Zuid (HSL-Zuid) had nauwelijks uitdagender kunnen zijn.

Dit artikel belicht de standpunten van de HSL-Zuid en haar onderhandelingspartners en schetst hoe de overeenstemming tot stand kwam.

1 Holland Railconsult
Postbus 2855
3500 GW Utrecht

2 De auteur werkte van 1997 tot en met 1999 bij de Projectorganisatie Hogesnelheidslijn-Zuid (HSL-Zuid), waarvan het laatste jaar als onderzoeksleider tunnelbrandveiligheid. Hij was betrokken bij het overleg tussen HSL-Zuid, de brandweer, de GGD en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties over de bouwvergunningen voor de tunnels.
De auteur schreef dit artikel op persoonlijke titel. Zijn visie komt niet noodzakelijkerwijs overeen met die van de Projectorganisatie HSL-Zuid. De Projectorganisatie is van mening dat open communicatie en vrije meningsvorming van groot belang zijn voor de veiligheid.

Project Hogesnelheidslijn Amsterdam-Parijs

In de Projectorganisatie HSL-Zuid werkt het Ministerie van Verkeer en Waterstaat samen met de ingenieursbureaus DHV en Holland Railconsult.

De belangrijkste tunnels in het tracé zijn van noord naar zuid:
- boortunnel onder het Groene Hart, ca. 7 km lang;
- 'cut-and-cover'-tunnel Rotterdam Noordrand, ca. 2 km lang;
- zinktunnel onder de Oude Maas, ca. 1,5 km lang;
- zinktunnel onder de Dordtse Kil, ca. 1,5 km lang.

Waarom zijn deze tunnels in het tracé opgenomen? De tunnel onder het Groene Hart moest er komen vanwege hart voor het groen: politiek Den Haag koos voor de tunnel om het milieu in het Groene Hart te sparen. Ook wilde men ervaring opdoen met het boren in slappe grond. De overige tunnels zijn gepland vanwege het tracé, de inpassing of de kosten.

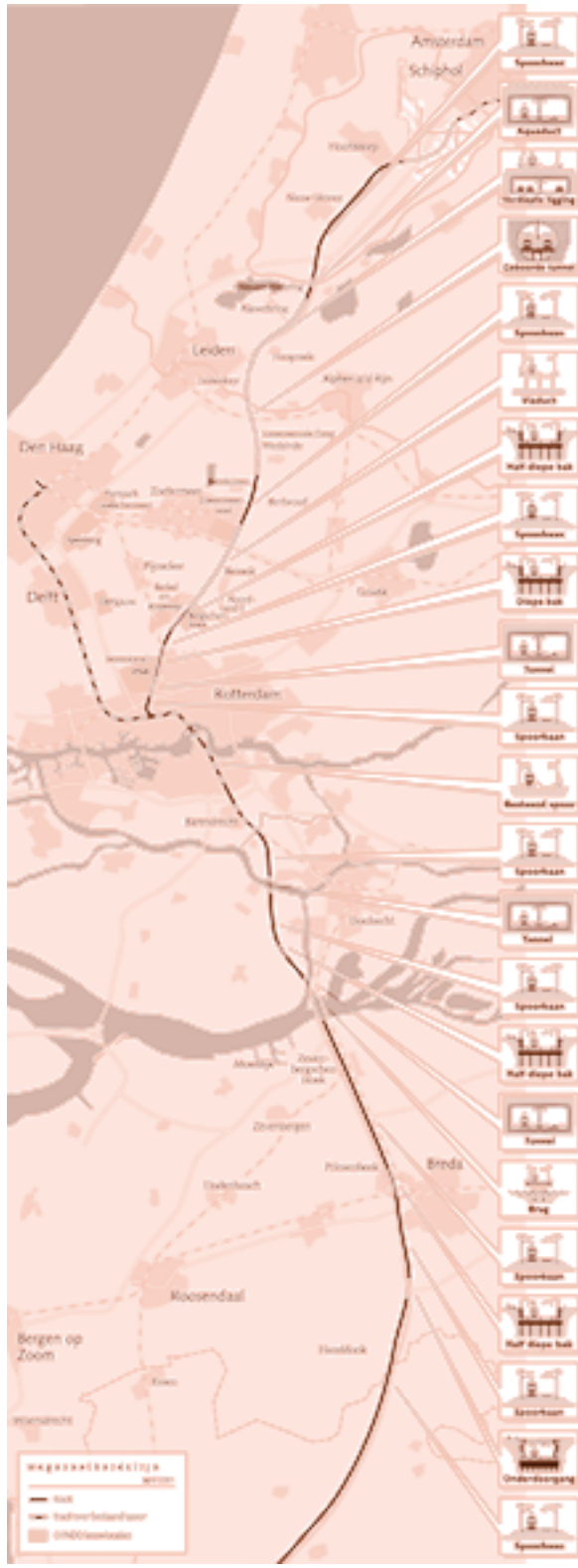
De veiligheid van tunnels

Sociale veiligheid scoort hoog. Ontwerpers van fietstunneltjes weten uit ervaring dat dit een zeer belangrijk aspect is. In de perceptie van mensen zijn tunnels om die reden eng; je wilt er liefst zo snel mogelijk weer uit zijn. Het letterlijk en figuurlijk enge karakter ervaren veel mensen elke keer opnieuw, als ze in een tunnel zijn.
Fysieke veiligheid daarentegen scoort laag. Sociaal veilig ingepakt in een auto of trein rijden velen dagelijks door tunnels. Het is de vraag of zij zich realiseren wat er fout kan gaan. De opmerkelijke reeks van recente tunnelbranden zal zijn sporen in de perceptie van het publiek zeker achtergelaten hebben, maar de vraag is of het veel meer dan sporen zullen zijn.
Anno 2000 kan een Amsterdamse wethouder over de metrotunnels beweren dat 'het absoluut veilig' moet zijn; bij een vluchtdeur die alleen te openen is, als je aan een kabel trekt en gelijktijdig een rooster induwt, 'moet een instructiebordje komen' [Volkskrant, 2000]. Wat mogen wij verwachten van het publiek, als een bestuurder al zoveel onwetendheid ten toon spreidt? In de Volkskrant verscheen geen enkele ingezonden brief met een reactie. Navraag leerde dat er nauwelijks brieven waren binnengekomen, met in elk geval als uitzondering een brief van de auteur van dit artikel.

Het 'onaanvaardbaar' over de eerdergenoemde situatie met het instructiebordje wordt wèl publiekelijk uitgesproken door Frank Steyvers en Dick de Waard, functiepsychologen aan de Rijksuniversiteit Groningen, in een door Hans

Figuur 14.1

Het tracé van de Hogesnelheidslijn-Zuid. Het nieuw te bouwen Nederlandse tracé loopt van Hoofddorp naar Rotterdam en van Barendrecht naar de Belgische grens. De tak naar Den Haag is bestaand spoor. In de tekening zijn de verschillende baantypen aangegeven, waaronder vier tunnels. Bron: Projectorganisatie Hogesnelheidslijn-Zuid.



Masselink geschreven artikel in Trouw van 26 januari 2001 [Trouw, 2001] in het katern 'de Verdieping' met als prikkelende titel 'Het sprookje van de veilige tunnel'. De brand in de skikabeltrein in een tunnel in het Oostenrijkse Kaprun op 11 november 2000 met ruim 150 dodelijke slachtoffers heeft recent laten zien hoe gevaarlijk treintunnels kunnen zijn. De bijna-ramp in 1996 in de Kanaaltunnel met zijn peperdure servicetunnel was al een teken aan de wand. Automobilisten zijn gewaarschuwd door de rampen in de Mont-Blanc-tunnel en de Tauern-tunnel. Misschien is het verschil in perceptie te wijten aan de mate waarin het gevaar voelbaar is. Mensen voelen de risico's bij sociale veiligheid instinctief aan. Je realiseren dat er risico's bij fysieke veiligheid zijn met weinig kans dat ze ook inderdaad voorkomen, vergt waarschijnlijk een zekere kennis en nieuwsgierigheid of wellicht discipline, omdat deze risico's verder van je af staan.
Misschien ook vertrouwt men op de brandweer als redder. Dat is tegelijk een makkelijke rationalisatie van psychologische verdringing. Maar helaas, hoezeer de brandweer zich ook zal inzetten, als een treinbrand in een tunnel zich snel ontwikkelt, komt zij te laat.

HSL-Zuid en hulpverleners aan één tafel

Tunnels zijn bouwwerken en voor bouwwerken zijn bouwvergunningen nodig. Een bouwvergunning vraag je aan bij de gemeente waarin het bouwwerk zal worden neergezet. Ziehier de wettelijke verplichting van de Projectorganisatie HSL-Zuid tot een bouwvergunningaanvraag voor haar tunnels in de diverse gemeenten.
De gemeente zal de aanvraag beoordelen op tal van aspecten. Voor de veiligheid vraagt zij advies aan de brandweercommandant, die op zijn beurt meestal zijn preventieofficier, vaak de GGD en soms de politie bij zijn advies betrekt. Ziehier de rol van de hulpverlening als toetser van de veiligheid. De hulpverleningsdiensten zijn deze rol de laatste jaren steeds meer pro-actief gaan invullen en willen reeds invloed uitoefenen op momenten dat de grote ontwerpbeslissingen nog genomen moeten worden.
Op deze wijze kwamen de HSL-Zuid en de hulpverleningsdiensten als onderhandelingspartners aan tafel te zitten. Wat maakte deze situatie nou zo moeilijk? Het ligt voor de hand dat de partijen niet dezelfde belangen hadden en dat geld altijd een rol speelt. Maar er speelt meer, zoals hierna duidelijk zal worden. De partijen beschikten over onvoldoende kennis en ervaring op dit specifieke gebied. Enerzijds was dat een gelukkig toeval, maar anderzijds was het lastig: er was weinig casuïstiek over ongevallen. Experimenten waren wel gedaan, maar beperkt: treinstellen zijn te duur voor het vergaren van betrouwbare gegevens over uiteenlopende typen materieel en branden. Er was wel bekend dat er internationale normen waren voor de brandveiligheid van treinen, maar niet

bekend was wat deze precies inhielden. Risicoanalyses voor treintunnels waren in Nederland nog niet gedaan op de wijze zoals dat voor de HSL-Zuid zou gaan gebeuren.

Als een onderwerp weinig houvast geeft in een onderhandelingsproces, hebben de 'krachten' vrij spel. Wat was dit krachtenspel? Wat waren de tegenstellingen? Deze krachten zijn beschreven aan de hand van de onderstaande verzonnen dialoog.

HSL-Zuid, brandweer en GGD in fictieve dialoog

Aan tafel zitten vertegenwoordigers van de Projectorganisatie HSL-Zuid (de manager veiligheid, de onderzoeksleider tunnelbrandveiligheid, de coördinator tunnelinstallaties en de overlegsecretaris), de brandweer (een brandweercommandant, een preventieofficier en een tunnelexpert), de GGD (een deskundige op het gebied van het verband tussen blootstelling aan giftige stoffen en de gevolgen ervan voor de mens) en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (een medewerker van de Directie Brandweer en Rampenbestrijding). Het Ministerie is geen directe partij in de onderhandelingen, omdat de verlening van de bouwvergunningen een zaak is van de gemeenten, die autonoom zijn. Het Ministerie heeft in deze vooral een coördinerende rol.

Laten we eens kijken hoe zo'n vergadering zou kunnen lopen. Uiteraard trekt men tijd uit voor een kennismaking en een versteviging van de inmiddels gegroeide respectvolle en veelal hartelijke persoonlijke betrekkingen. Maar als de inhoudelijke discussie gestart is, zijn het vooral de belangen die de toon bepalen.
De hiernavolgende fictieve dialoog is kunstmatig geconstrueerd. Allerlei zaken die over meer vergaderingen verspreid gespeeld hebben en op allerlei manieren zijn behandeld en gecommuniceerd, zijn in één dialoog bij elkaar gebracht. Posities en vragen die in een vergadering door achtergronden of non-verbale communicatie duidelijk werden, zijn scherper weergegeven, omdat het onderhavige medium in ruimte en tijd alleen het hier en nu kent en als expressiemiddel alleen het woord.

HSL-Zuid: Onze leidraad voor de veiligheid is het Integraal VeiligheidsPlan HSL-Zuid, opgesteld door Railned Spoorwegveiligheid in samenwerking met het Ministerie van Verkeer en Waterstaat. Daarin zijn de normen beschreven voor het aanvaardbaar persoonlijk en groepsrisico. Zij zijn tot stand gekomen na zorgvuldige afweging onder voorwaarde dat de HSL ondanks de veel hogere snelheid minstens net zo veilig is als het conventionele spoor.

Hulpverleners: Tja, daar hebben wij weinig boodschap aan. Wij toetsen aanvragen voor bouwvergunningen gewoon aan het Bouwbesluit. Dat doen we al jaren zo.

HSL-Zuid: En wat zegt het Bouwbesluit over tunnels?

Hulpverleners: Voor gebouwen is het Bouwbesluit heel duidelijk: maximaal 30 m naar de nooduitgang, gebaseerd op 30 seconden adem inhouden en 1 m per seconde loopsnelheid.

HSL-Zuid: Dat geldt zeker niet voor tunnels?

Hulpverleners: Nee, niet direct, want een tunnel is geen gebouw. Voor een bouwwerk in het algemeen geldt de eis dat vluchten binnen een redelijke tijd mogelijk moet zijn.

HSL-Zuid: Het Bouwbesluit bevat dus eigenlijk geen normen voor tunnels.

Hulpverleners: Het Bouwbesluit zegt wel degelijk iets. Als het gaat om onze interpretatie van het begrip 'redelijke vluchttijd', dan kijken we naar de norm voor gebouwen. We baseren ons dan op 30 seconden adem inhouden en 1 m per seconde loopsnelheid en komen dan uit op een maximale loopafstand van 30 m en dus nooduitgangen om de 60 m. Trouwens, een tunnel mag dan in het Bouwbesluit slechts een bouwwerk zijn, in de Woningwet is een tunnel wèl een gebouw.

HSL-Zuid: Dat kan niet de bedoeling zijn. Zo worden tunnels onbetaalbaar in Nederland. Wij werken in dit land al jaren met een vluchtpad van 1,20 m breed en nooduitgangen om de 150 m, als ze niet te duur zijn, of anders om de 300 m. Zo staat het in de ontwerpvoorschriften van de Nederlandse Spoorwegen. Daarop hebben we al onze kosten begroot. Waarom zou dat plotseling niet voldoende zijn?

Hulpverleners: De voorschriften van de Nederlandse Spoorwegen, waar jullie al jaren mee werken, worden niet genoemd in het Bouwbesluit. En trouwens, waar zijn ze op gebaseerd? Zijn ze ooit getoetst op veiligheid bij een brand? Elke club kan wel met zijn eigen voorschriften aankomen. Wij werken met het Bouwbesluit en voeren gewoon de wet uit. Dat is trouwens wel lastig, want sommigen onder ons voelen ook wel aan dat het Bouwbesluit niet direct geschreven is voor tunnels. Maar ja, we kunnen als brandweer geen beleid maken. Dat moet de politiek doen. Maar die komen er niet uit en wij zitten er mee. Toch zijn wij ook de beroerdsten niet. Als jullie kunnen aantonen dat 150 of 300 m gelijkwaardig is aan 60 m, doordat jullie bijvoorbeeld de rook wegzuigen, dan vinden we dat prima.

HSL-Zuid: Toch is een tunnel iets heel anders dan een gebouw. Daarvoor zouden eigenlijk specifieke, realistische normen moeten komen.

Commentaar: Hier staan verschillende normen tegenover elkaar: het Integraal VeiligheidsPlan HSL-Zuid en het Bouwbesluit (met eventueel het gelijkwaardigheidsbeginsel). Daardoor is er geen gemeenschappelijk vertrekpunt.

HSL-Zuid: Het Integraal VeiligheidsPlan HSL-Zuid (IVP) is probabilistisch. Met kwantitatieve risicoanalyses kan men laten zien dat men aan de eisen van het IVP voldoet. Dit is de traditie bij het Ministerie van Verkeer en Waterstaat. We hebben intern en extern opdrachten voor deze risicoanalyses uitgezet.

Hulpverleners: Wat zeg je? Probabilistisch? Wij beschouwen veiligheid deterministisch. Aan kansen hebben we geen boodschap, want als wij in actie moeten komen, is de kans gelijk aan 1. Onze maatschappelijke en wettelijke opdracht is het redden van mensen. Uiteraard hechten we veel belang aan preventie, maar het Bouwbesluit blijft de norm voor vluchtwegen. Dat is ook de traditie bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, de coördinator op het gebied van veiligheid.

HSL-Zuid: Wat jullie over preventie zeggen, is niet helemaal consequent. In onze visie is het zo dat er minder vluchtwegen nodig zijn, als een trein goed beveiligd is tegen brand. De kans op een ongeval moet meespelen. Het kan toch niet zo zijn dat we èn onze nek uitsteken in Europa voor het veiliger maken van treinen èn ook nog eens peperdure vluchtvoorzieningen moeten aanleggen?

Commentaar: Hier staan verschillende visies op veiligheid tegenover elkaar: probabilistisch en deterministisch. Er is geen gemeenschappelijke reisgids.

HSL-Zuid: Onze risicoanalyses laten zien dat we voldoen aan ons Integraal VeiligheidsPlan. Ze zijn trouwens uitgevoerd door TNO.

Hulpverleners: Die kwantitatieve risicoanalyses van jullie vinden wij weinig overtuigend. De modellen zijn moeilijk te doorgronden en de getallen geven weinig zekerheid. Als we ons even opstellen als advocaat van de duivel: het ziet er allemaal makkelijk manipuleerbaar uit; je kunt alles wel uit een computer laten komen. En lijkt de werkelijkheid de modellen niet te logenstraffen? Kijk bijvoorbeeld naar de Kanaaltunnelbrand. Er is zeer veel geld uitgegeven aan veiligheid, alles is vooraf onderzocht en geanalyseerd en toch was er al in 1996 bijna een catastrofe van ongeveer 30 doden.

HSL-Zuid: Wij beschouwen kwantitatieve analysen als objectief. Zo maak je veiligheid objectief en weeg je veiligheidsguldens en veiligheidsrendement zorgvuldig tegen elkaar af. Waarom gaan jullie daar niet in mee? We zijn ons wel bewust van de onzekerheden in het model en de getallen, maar beter kan niet, want dit is wat ons probabilistische normenkader voorschrijft.

Hulpverleners: Jullie benaderingswijze is wel een beetje technocratisch. Kwantitatieve risicoanalyses verpakken het rampbesef in modellen, doden worden tot getallen en deze getallen zijn acceptabel zolang ze onder de norm blijven. Wij kennen de gevolgen van rampen vaak uit eigen ervaring. Voor ons zijn doden geen getallen, maar menselijk leed en niet zelden trauma's voor onszelf.

HSL-Zuid: Je mag je niet laten leiden door emoties. Het gaat hier om het afwegen van geld tegen veiligheid en dat moet je op een goede manier doen. Je kunt hier nu wel het onderste uit de kan proberen te krijgen, maar kun je al dat geld niet veel beter uitgeven aan preventie in het verkeer? Aan bijvoorbeeld scootertjes is vast nog heel wat te doen. Als je daar een goed budget in steekt, neemt het aantal verkeersdoden fors af. Dan voer je integraal veiligheidsbeleid in Nederland.

Commentaar: Als de methoden en achtergronden verschillen, verschilt ook de benadering. Er is geen gemeenschappelijk taalgebruik.

Hulpverleners: Tja, als jullie niet meegaan met onze denkwijze, stellen we gewoon de 60 m uit het Bouwbesluit verplicht. Sowieso horen we steeds hetzelfde: jullie risicoanalyses wijzen uit dat jullie aan je eigen normen voldoen, maar dat zijn gewoon niet ònze normen.

HSL-Zuid: Dat is geen onderhandelen. Wij moeten die vergunning hebben om door te gaan. Jullie zijn niet verplicht deze te verlenen en kunnen rustig wachten op onze voorstellen en ze dan bekritiseren. Als jullie vinden dat we proberen de zaak door te drukken, nemen jullie het Bouwbesluit in de hand en zeggen '60 m'.

Commentaar: Er is geen gemeenschappelijk streefpunt in de tijd.

HSL-Zuid: Durven jullie eigenlijk wel ergens ja tegen te zeggen? Het lijkt erop dat jullie bang zijn om je te committeren.
(Onuitgesproken gedachten:) We voelen ons eigenlijk een beetje machteloos in dit spel. Dat onderhandelen is toch heel iets anders dan ons eigen project. Dit is niet zozeer een technocratisch als wel een intermenselijk proces en dat is lastig. Je bent afhankelijk van een partij waar je geen greep op hebt. Wij als HSL-Zuid willen het liefst de handen vrij en alle opties openhouden voor het bespelen van de markt. Het moet toch een aantrekkelijk product zijn voor vervoerders?

Veiligheid vraagt om eisen aan vervoerders: beperking van de treincapaciteit, eisen aan het materieel en allerlei procedures. Daar zitten ze niet op te wachten. Ook dat is lastig.

Hulpverleners: (Onuitgesproken gedachten:) Wij voelen ons klem zitten tussen de druk van een miljardenproject en onze maatschappelijke verantwoordelijkheid. En dat nog eens met weinig middelen, want specialistische kennis heeft de gemiddelde gemeentelijke brandweer niet in huis en budget voor eigen opdrachten aan onderzoeksinstituten is er ook niet. Ten slotte is er geen duidelijke wetgeving. (Hardop uitgesproken:) We zien de bui al hangen: als er een ramp gebeurt, worden wij aangewezen als zondebok. Bij het publiek leeft een illusie over de effectiviteit van de hulpverlening bij een tunnelramp. Maar goed, wij – althans sommigen onder ons – beseffen ook wel dat we niet zonder resultaat uit dit proces kunnen stappen. Dat zou ons aanzien zeker geen goed doen. Onze positie is ook niet eenvoudig. Misschien moet de politiek het maar zeggen.

HSL-Zuid: Misschien wel ja. Wij zitten ook in een lastige positie, want wij hebben als aanvrager van de bouwvergunning de bewijslast op onze schouders, die nog eens extra zwaar is, omdat jullie positie zo moeilijk is.

Commentaar: Aan beide kanten liggen de posities moeilijk.

HSL-Zuid: Wij vinden bronaanpak – preventie dus – essentieel. Wij gaan dus eisen stellen aan de brandveiligheid van de treinen. Uit de risicoanalyses blijkt namelijk dat vluchtvoorzieningen maar weinig effect hebben, als een rijtuig eenmaal volledig in brand staat.

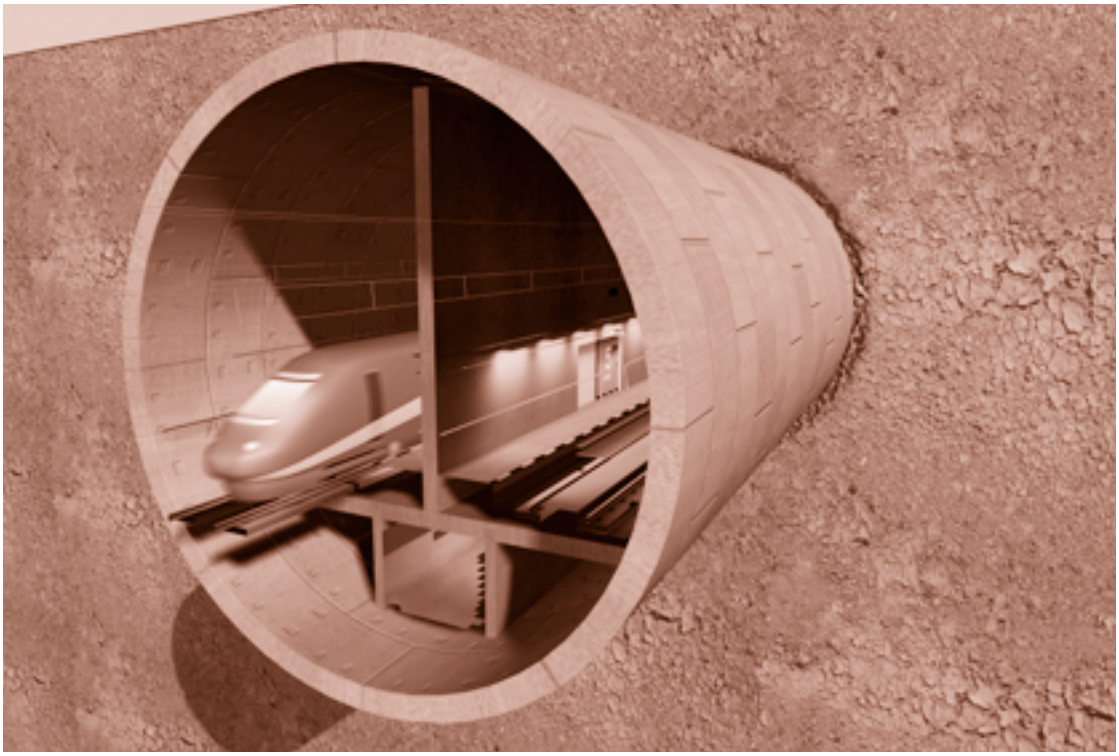
Hulpverleners: Wij zijn het volkomen met jullie eens dat bronaanpak het meeste effect heeft. Maar hoe staat het met de mogelijkheid van het stellen van eisen aan treinen, gezien de harmonisatie en interoperabiliteit in Europa? Elke buitenlandse hogesnelheidstrein moet toch door onze HSL-tunnels kunnen rijden? Zorg eerst maar eens voor een handtekening van de minister.

Commentaar: Als er dan goede oplossingsvoorstellen op tafel liggen, kunnen er haalbaarheidscomplicaties spelen. De speelruimte voor oplossingen is soms beperkt, niet alleen financieel.

Hoe HSL-Zuid de bouwvergunningen kreeg

Ondanks de hiervoor genoemde complicaties hebben de gemeenten de bouwvergunningen voor de tunnels verleend. De Projectorganisatie HSL-Zuid heeft de veiligheid van de tunnels ondergebracht in een stafafdeling die rechtstreeks onder de projectdirecteur valt. Dat is voor geen enkel ander aspect van het ontwerp gedaan. Het geeft aan dat veiligheid op het hoogste niveau zeer serieus genomen werd.

Begin 1998 is een overleg gestart tussen HSL-Zuid, brandweer en GGD uit de betrokken gemeenten en regio's en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties als coördinator van de hulpdiensten.
Er was veel werk voor onderzoeksinstituten en adviesbureaus. TNO MEP te Apeldoorn en TNO Bouw / Centrum voor Brandveiligheid te Rijswijk hebben in opdracht van HSL-Zuid onderzoeken gedaan naar onder andere de emissiebrontermen (soorten en hoeveelheden van verbrandingsproducten per eenheid van brandvermogen) bij brand, de brandbaarheid van treinen en de voortplanting van hitte en rook in een tunnel; eveneens hebben zij een kwantitatief risicoanalysemodel voor de tunnels opgesteld en berekeningen uitgevoerd.
Ingenieursbureau DNV te Rotterdam heeft in een gezamenlijke opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en HSL-Zuid de veiligheid van de Groene-Hart-tunnel onderzocht.
Vertegenwoordigers van de hulpverleningsdiensten zijn zoveel mogelijk betrokken geweest bij de onderzoeken. Deskundigen van de onderzoeksinstituten werden betrokken bij de onderhandelingen.
HSL-Zuid heeft resultaten van onderzoeken in het overleg met de hulpverleners gepresenteerd, ook als de resultaten niet direct gunstig waren. Een voorbeeld hiervan is dat treinen harder en sneller kunnen branden dan men dacht: in het ergste van de representatieve scenario's bereikt een treinbrand binnen 5 à 10 minuten een vermogen van maar liefst 60 MW, driemaal zo hoog als werd aangenomen in de Nederlandse spoorwegwereld.
HSL-Zuid heeft waarschijnlijk meer geld uitgegeven aan onderzoek naar brand in tunnels dan enig ander project in Nederland. Op deze wijze draagt zij ook bij aan de ontwikkeling van kennis in Nederland. Dit is ook een van de doelen van het project.
Een belangrijke maatregel die HSL-Zuid heeft toegezegd is dat nieuwe treinen zó brandveilig moeten zijn dat een brand minstens 15 minuten in de trein moet blijven, voordat rook en hitte de tunnel instromen. Deze tijd moet voldoende zijn voor de reizigers om zichzelf in veiligheid te brengen. Hoe de vervoerder deze 15 minuten realiseert, is zijn eigen zaak. Dat kan bijvoorbeeld met behulp van een mistsprinkler.



Figuur 14.2
Plaatje uit het virtual reality-model van de boortunnel onder het Groene Hart. Een tussenwand verdeelt de monobuis in twee helften. Per helft is er één spoor. Zichtbaar is het vluchtpad en een vluchtdeur om te vluchten naar de andere buis. Bron: Holland Railconsult, Groep Visuals.

De minister van Verkeer en Waterstaat heeft voor HSL-Zuid een 'Safety Committee' ingesteld met als leden de hoogleraren R. van der Heijden, E. Horvat, J. Vrijling en inmiddels ook T. Regtuit. De functie van dit comité is die van onafhankelijk beoordelaar en bekrachtiger van de veiligheidsbesluiten met als doel het veiligheidsbeleid van HSL-Zuid maatschappelijk décharge te verlenen. In de loop van de onderhandelingen heeft het comité een onafhankelijke rol boven de partijen gekregen, een soort commissie van wijze mannen, die de partijen tot elkaar wist te brengen.

Een andere convergerende factor van buitenaf werd gevormd door gemeentelijke besturen die in de laatste fase van de onderhandelingen een rol zijn gaan spelen. Uiteindelijk zijn zij het ook die de bouwvergunningen moeten verlenen. Bij beide partijen groeide het besef dat ze in zekere zin tot elkaar veroordeeld waren. Het niet tot een akkoord komen zou niet aan de buitenwereld te verkopen zijn. Niet iedereen dacht er zo over, maar het was wel de overwegende opvatting.

Ten slotte – maar zeker niet het minst belangrijk – groeide tussen de partijen een inhoudelijke consensus over de materie. Je zou misschien kunnen zeggen dat hiervoor in een zo ingewikkelde zaak nou eenmaal een bepaalde hoeveelheid tijd staat.

HSL-Zuid en haar onderhandelingspartners hebben vanuit zeer verschillende startposities onder moeilijke randvoorwaarden een proces doorlopen dat uit-

eindelijk tot resultaat heeft geleid. Het spel is stevig gespeeld, maar dat past bij veiligheid als een zo belangrijk aspect van de maatschappelijke inpassing van de HSL-Zuid in Nederland.

Persoonlijke visie

In de verzonnen dialoog zijn verschillende factoren die de onderhandelingen bemoeilijkt hebben terug te vinden. Deze factoren zijn niet allemaal even gemakkelijk weg te nemen.
De gemakkelijkste maatregel lijkt wel de aanwijzing van een onafhankelijke, gezaghebbende overlegvoorzitter vanaf het begin van de onderhandelingen. Deze stelt de agenda's vast, geeft alle partijen huiswerk mee, houdt hen aan een tijdschema en zorgt voor evenwichtige inspanningen. Het Safety Committee had, als het eerder was ingesteld, deze rol kunnen vervullen of iemand uit zijn midden of namens hem daarvoor kunnen aanwijzen.
Aan de kant van de brandweer zou een landelijk kenniscentrum de rol van tegenspeler van een miljardenproject kunnen vervullen. Zo'n kenniscentrum zou kennis in huis moeten hebben, een budget voor mede-opdrachtgeverschap voor onderzoeken moeten krijgen en voldoende gezag bij de immers autonome gemeentelijke korpsen moeten hebben.
De overheid zou duidelijke normen voor tunnels kunnen vaststellen, of op zijn minst een procedure zoals een veiligheidseffectrapportage. Dat laatste is zeker geen nieuw idee en het eerste zeker geen nieuwe verzuchting.
In elk geval zou gewerkt kunnen worden aan een synthese tussen de deterministische en de probabilistische benadering. Op het determinisme is aan te merken dat het geen rekening houdt met de kans op een ongeval. Het kan daardoor een te emotionele benadering worden, waarin men blind wordt voor een bewuste afweging van kosten tegen baten. Ter illustratie: de Volkskrant kopt op 6 september 2001 op pagina 3: "Amsterdamse metrotunnel erg onveilig" en schrijft: "De Amsterdamse metrotunnel is zo onveilig dat bij brand 'een aanzienlijk aantal' dodelijke slachtoffers kan vallen"; aan de kans op een ongeval refereert het artikel in het geheel niet.
Het probabilisme daarentegen kan ontaarden in een de-pc-is-geduldig-excercitie door modellencowboys die een monopolie op de waarheid claimen. Dit lijkt een karikatuur, maar is misschien waarschijnlijker dan men denkt: men kan makkelijk blind worden voor de werkelijkheid en terechtkomen in een situatie waarin men het model, waarin men al zoveel tijd geïnvesteerd heeft, overeind probeert te houden. Dat die werkelijkheid meer fantasie heeft dan de modellenbouwer, blijkt nog eens uit een artikel in de Metro van 6 september 2001: een vrouw werd onwel op de wc en drukte daarbij een spuitbus met luchtverfrisser langdurig in, waarna de grote hoeveelheid vrijgekomen gas door een los

stroomdraadje in een fitting in een vuurzee veranderde. Risicoanalysemodellen gaan over faalkansen; maar wat zijn de faalkansen van de modellen? Determinisme en probabilisme zijn gezonde tegenwichten voor elkaar. In een project als de HSL-Zuid komen de twee aan één tafel samen, waardoor de tegenwichtwerking vanzelf ontstaat. Niettemin zou een methodische synthese van determinisme en probabilisme de totstandkoming van wederzijds begrip en overeenstemming versnellen en daardoor tijd en kosten besparen.

Tot slot

Fysieke veiligheid heeft het van nature moeilijk. Ze vraagt voortdurende aandacht, zorg en geld, maar is pas zichtbaar als het fout gaat. De recente rampen in Enschede (13 mei 2000) en Volendam (1 januari 2001) hebben laten zien hoe fout het kan gaan, als de voortdurend noodzakelijke aandacht en zorg ontbreken.

Een spanningsveld tussen de nodige en de verleende aandacht zal altijd blijven bestaan. In dat spanningsveld zullen trieste gebeurtenissen zich blijven voordoen. Gegarandeerd foutloze systemen ontwerpen en invoeren is voor mensen onmogelijk. Daarnaast lijken mensen van tijd tot tijd geprikkeld te moeten worden om alert te blijven. Dat geldt in het groot voor de politiek en het bestuur, die geprikkeld lijken te moeten worden door ongewenste gebeurtenissen op helaas grote schaal.
Hopelijk leidt de discussie die is losgebarsten na de ramp in Volendam tot een cultuur waarin pro-activiteit het blijvend wint van reactiviteit. Daarbij hoort een stringent handhavingsbeleid. Daarbij hoort ook een helder normenkader voor tunnels. Inmiddels werkt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties samen met het Ministerie van Verkeer en Waterstaat aan het project MAVIT: Maatschappelijk Aanvaardbaar Veiligheidsniveau voor Infrastructuur en Transport. De doelen van dit project zijn: 1. veiligheid in het overleg brengen, vóórdat het besluit voor het bouwen van het object is genomen en 2. normen voor de veiligheid van tunnels voor gebruikers en hulpverleners (preventie, zelfredzaamheid en inzet hulpdiensten) vaststellen. Het zou een goede zaak zijn, als het project ook tot een integratie van de deterministische en de probabilistische benaderingswijze leidt. Het in dit artikel beschreven proces was mede aanleiding voor MAVIT. Zo brengt de HSL-Zuid niet alleen de reiziger van Amsterdam naar Parijs, maar zet zij ook het Nederlandse veiligheidsbeleid op het spoor naar een hoger niveau.

Figuur 14.3
Sfeervol en enigszins bedrieglijk plaatje uit het virtual reality-model van de boortunnel onder het Groene Hart. De grote hoofdletter-A-achtige constructie is een vluchtschacht, waardoor reizigers uit de niet getroffen buis naar het maaiveld kunnen vluchten. Deze bevindt zich naast en boven de tunnel ter hoogte van de kop van de trein, waar ook de vluchtdeur zichtbaar is, maar lijkt veel dichterbij te staan en deel van de tunnel uit te maken. In de hoek linksonder is een doorkijkje naar de tunnelwand van de andere tunnelhelft gegeven. Bron: Holland Railconsult, Groep Visuals.

Referenties

– de Volkskrant. 29 november 2000
– Masselink, H. (2001). Het sprookje van de veilige tunnel. Trouw, 26 januari, de Verdieping

2

15
Nieuw sorteersysteem PTT Post

ir. J.A.M. ten Dam [1]

De achtergronden

In het begin van de jaren negentig ontstond bij PTT Post grote zorg over de ontwikkeling van het postvolume. De snelle groei van het faxverkeer, de lagere verzendfrequentie in het financiële berichtenverkeer en de toenemende concurrentie zetten de traditionele postgroei onder druk. Dit gevoegd bij een jaarlijkse groei met 100.000 adressen (de omvang van de steden Delft en Zoetermeer) leidde tot een sombere verwachting van de winstgevendheid van het Postbedrijf. Actie was dus geboden. De belangrijkste actie was het plan om de sortering van de briefpost (alle post die zonder aanbellen bezorgd kan worden) maximaal te automatiseren. Hiertoe werd een project gestart (Briefpost 2000) met als doelstellingen:

- Het automatisch sorteren van 90% van de 22 miljoen brieven per dag tot op bestelloop (de post die een postbode meeneemt op zijn ronde).
- Het maximaal automatisch lezen van adressen (ca. 90%).
- Het terugbrengen van het aantal sorteercentra van 12 naar 6. Voor deze 6 centra moeten nieuwe uniforme gebouwen gebouwd worden.
- Het project realiseren in de periode 1992-1998.
- Het behalen van een kostenbesparing van 300 miljoen gulden per jaar.

1 PTT Post B.V., Afdeling Sortering
Postbus 30250
2500 GG Den Haag

Voor het uitvoeren van dit plan was 1300 miljoen gulden nodig.

Een belangrijke voorwaarde was dat zowel tijdens als na de reorganisatie de kwaliteit van de postbezorging niet zou verslechteren. De klant, die steeds hogere eisen stelt aan kwaliteit en betrouwbaarheid, zou er dus geen nadelige gevolgen van mogen ondervinden.

De grote postvolumen werden van oudsher door de klant gesorteerd aangeleverd. Verwerking op de sorteercentra werd hiermee omzeild. Deze klanten hadden hiervoor investeringen gedaan in software en hardware en kregen voor deze sorteeractiviteiten een korting. Door dit project zou dit vanaf 1 januari 1999 niet meer nodig zijn. Van de uiteindelijk gerealiseerde besparingen is 70 miljoen teruggegeven aan de markt.

Het project

Voor het uitvoeren van het project Briefpost 2000 werd een kleine projectgroep (10 man) gevormd die verantwoordelijk was voor het procesontwerp, de aanschaf van machines, de huisvesting en de organisatorische consequenties.

De belangrijkste pijler van het project was het maximaal automatisch sorteren. Om de mogelijkheden hiervan te verkennen werden alle belangrijke leveranciers van sorteerapparatuur benaderd. Onderzocht werd welke sorteerapparatuur in een periode van ongeveer 3 jaar operationeel zou kunnen zijn.
Daarnaast werden alle postorganisaties bezocht die actief waren op het gebied van automatisch sorteren. Uiteindelijk is op grond van efficiëntie gekozen voor het aanschaffen van machines voor het sorteren van kleinere briefformaten, machines voor grotere briefformaten (A4, tijdschriften) en machines voor kleine pakjes.
Voorts werd besloten een splitsing te maken tussen de transportsystemen en de informatica. Bij informatica gaat het om het digitaliseren van beelden van brieven, het lokaliseren van adresvelden en het automatisch lezen van adressen. Ook het kunnen raadplegen van onder andere het telefoonboek, de bestanden van de Kamers van Koophandel en het postcodebestand maakt hiervan deel uit. Wanneer een adres uiteindelijk niet automatisch leesbaar is, wordt de brief op een computerscherm geprojecteerd en de postcode ingetoetst. De gevonden sorteerinformatie gaat terug naar de machine waar de betreffende brief zich op dat moment bevindt.

De aanschaf

Uit alle beschikbare informatie is een procesontwerp gedefinieerd. Op basis daarvan zijn functionele specificaties opgesteld die als 'longlist' aan geselecteerde leveranciers zijn gestuurd. De reacties op deze lijst hebben geleid tot een 'shortlist'. Voor de uiteindelijke selectie van de leveranciers voor de verschillende machinetypen is gebruik gemaakt van de deskundigheid van KPN Research dat op dit gebied kan bogen op een langdurige expertise.

Omdat de verwerving van grote bouwlocaties, het verkrijgen van bouwvergunningen en het bouwen zelf drie jaar in beslag zou nemen, ontstond de ruimte om voor deze nieuw te ontwikkelen machines een proefbedrijf in te richten. Hier zou gedurende één jaar getest en gemodificeerd kunnen worden. Daarnaast vond PTT Post het belangrijk onderzoek te doen naar de werkorganisatie en de ergonomie die als gevolg van het nieuwe procesontwerp sterk zouden veranderen. Ook de integratie van de mechanische transportsystemen met de diverse IT-componenten zou hier uitvoerig getest worden.

Machines voor het sorteren van kleinere formaten waren in Nederland al sinds 1978 gereed. Voor de grotere poststukken was dit een eerste ervaring.
In enkele landen waren recent voorzichtige pogingen ondernomen op dit gebied. Er waren in 1992 slechts vijf leveranciers die deze apparatuur aanboden. Hiervan bleven er twee over na de eerste selectieronde. Bij de finale beoordeling en keuze speelden naast de inhoud van de offertes ook aspecten mee als:

- eerdere prestaties op dit gebied;
- algemene prestaties van de leverancier;
- financiële draagkracht van het bedrijf;
- projectorganisatie van de leverancier;
- professionaliteit van de betrokken projectgroep.

Het resultaat

Uiteindelijk is het niet gelukt 90% van de grotere poststukken automatisch te sorteren. Het bleek voor de leverancier een onmogelijke opgave om aan de contractuele verplichtingen wat betreft specificaties en levertijd te voldoen. Vooral de in folie verpakte postzendingen die meestal in grote hoeveelheden aangeboden worden veroorzaakten veel problemen. Niet alleen het separeren van de poststukken, maar ook het opnemen van beelden die na digitalisering automatisch gelezen moeten kunnen worden, bleek te moeilijk. Een andere complicatie vormde de sterke toename van allerlei bijlagen (cd-rom's sleutelhangers, enz.). Duidelijk is dat de leverancier te veel vertrouwde op globale oplossingen, op

Figuur 15.1
Het nieuwe sorteersysteem van PTT Post. Bron: PTT Post.

zijn ervaring met de bouw van sorteermachines en op de professionaliteit van de eigen organisatie.
Door het niet halen van de levertijd was het niet mogelijk de machine uitgebreid te testen in het hiervoor bedoelde proefbedrijf. Met de markt was immers afgesproken dat vanaf 1 januari 1999 de klanten de post niet meer hoefden te sorteren. Als gevolg hiervan werden veel problemen pas zichtbaar tijdens de operationele fase. Onbekendheid met bediening en onderhoud gevoegd bij voortdurende wijzigingen leidden tot een slechte performance (kosten en kwaliteit).
Naast problemen met de leverancier en de techniek waren meer factoren van invloed op de afronding van dit project.

In 1992 werd ervan uitgegaan dat na een lichte stijging in de eerste jaren het postvolume in 1998 weer terug zou zijn op het niveau van 1992. Daarna zou het volume verder dalen. In werkelijkheid was het volume in 1998 ruim 20% hoger dan in 1992. Daarnaast is het aanbod verschoven naar het einde van de week (de attentiewaarde van post is het hoogst op zaterdag). Van dit hogere volume is het percentage folie in deze periode meer dan verdubbeld. Folieleveranciers zijn in staat geweest dunnere folie te produceren bij gelijkblijvende sterkte. Dit dunnere folie is slechter machinaal te sorteren. De markt bleek dus veel dynamischer dan verwacht.

Waar de werkloosheid in 1992 aanzienlijk was, is er aan het einde van de jaren negentig juist sprake van een tekort aan arbeidskrachten. Aanvankelijk was de grootste zorg hoe men 5.000 FTE's (voltijdbanen) kon verminderen zonder gedwongen ontslagen. Momenteel is de grootste zorg hoe men de arbeidsplaatsen vult. Deze ontwikkeling is versterkt door de concentratie van twaalf naar zes sorteercentra.

In deze zes nieuwe sorteercentra waren de processen, de productiemiddelen, de werkruimte, de arbeidsomstandigheden, de fysieke belasting, de werktijden, de werkzaamheden, de collega's, de leidinggevenden, en de locatie anders. Voor de 10.000 betrokken medewerkers was deze stapeling van veranderingen zeer ingrijpend.

PTT Post vervult meer dan de meeste andere bedrijven een publieke functie. Zij kan bij achterblijvende prestaties niet alleen bij klanten, maar ook in de media op veel aandacht rekenen. Meer dan in het verleden kan de klant kiezen uit meer aanbieders zowel voor fysieke als elektronische distributie. Dit vraagt om meer openheid en communicatie. Ook bij het niet halen van verwachtingen.

De integratie van de verschillende transportsystemen met complexe netwerken en software gaf nog een andere complicatie. De investering in de integrerende software, die de verschillende systeemcomponenten als een geheel moet laten werken, vertegenwoordigde slechts 10% van de totale investering in het machinepark. De leverancier van deze software was vanwege het financiële risico niet bereid de verantwoordelijkheid voor de systeemintegratie voor haar rekening te nemen. Uiteindelijk heeft PTT Post dit zelf moeten doen.

Bij een zo lang lopend complex project bestaat het gevaar dat de verdeling van de verantwoordelijkheden tussen de eigen projectgroep en die van de leveranciers diffuus wordt. Er ontstaan gemakkelijk situaties waarbij de projectgroepen er belang bij hebben negatieve informatie niet tijdig en open naar de moederorganisaties te communiceren.

De complexiteit van het volledig vernieuwde bedrijfsproces is sterk toegenomen. Gevoegd bij de afgenomen flexibiliteit als gevolg van de vergaande automatisering leidt dit tot een verhoogd afbreukrisico.

De maatregelen

Na de problemen in kaart gebracht te hebben, is samen met de leverancier een nieuwe 'reduced base-line'[2] vastgesteld. Hiermee zijn na een lang modificatietraject de uiteindelijke operationele specificaties gedefinieerd. Met deze nieuwe specificaties is bepaald welke post(verpakkingen) automatisch sorteerbaar zijn. De machineoperators zijn opgeleid om dit onderscheid te kunnen maken en hierdoor de prestaties van de automatische sorteermachine te verbeteren. Met klanten wordt continu geprobeerd de aangeboden post binnen de specificaties te laten vallen. Wanneer dit niet lukt, vraagt PTT Post klanten voorgesorteerd aan te bieden. Als ook dat niet slaagt, wordt de post handmatig gesorteerd.

2 reduced base-line is de in de praktijk haalbaar gebleken performance.

Om het proces te kunnen beheersen, is een systeem van vooraf melden opgezet. Dit houdt in dat dagelijks met grote aanbieders wordt gecommuniceerd over hoeveelheden, machinegeschiktheid, sorteergraad en plaats en tijd van aanbieding.

2

16 Verantwoordelijkheid voor ketens in het Internet

drs. A. Jonk [1]

Inleiding

In pogingen om de kwaliteit en efficiëntie van bedrijfsprocessen te verhogen speelt ICT een belangrijke rol als 'enabler'. Bijvoorbeeld het virtuele organisatieconcept [Dael, 1997] is gebaseerd op het idee dat allerlei activiteiten door ICT steeds minder aan tijd en plaats gebonden zijn. Telewerken, netwerkbedrijven, innovatie-uitbestedingsvormen zoals ASP ('Application Service Providers', een techniek waardoor bedrijven geen beheer over en onderhoud van software meer hoeven te voeren, maar deze programmatuur over het Internet kunnen gebruiken en toepassen in het eigen bedrijfsproces). Andere vormen van innovaties, zoals 'Just in Time', leunen ook sterk op ICT. Wezenlijk is echter dat in de context van procesinnovaties de relaties tussen opdrachtgever en opdrachtnemer altijd duidelijk overeind blijven. Voor een consument bijvoorbeeld is Nike de schoenleverancier, al heeft deze fabrikant bijna zijn hele productie, distributie en ontwerp uitbesteed. Nike is een integrator en eindverantwoordelijke voor de kwaliteit van het product en de wijze waarop het geproduceerd wordt [Klein, 2000].

1 Het Expertisecentrum
Jan Willem Frisolaan 3
2517 JS Den Haag

Zoals gezegd leunt menige verandering in de organisatie op ICT. Meer specifiek kan gesteld worden dat zo'n verandering in toenemende mate op het gebruik van het Internet leunt. ICT en het Internet zijn dan ook de enablers van de trends zoals ze in dit boek besproken worden. Flexibiliteit, toenemende kennisintensiteit en toenemende dynamiek zijn niet voorstelbaar zonder de mogelijkheden die ICT en het Internet bieden. ICT is echter meer dan een neutrale facilitator, het kent ook zijn eigen karakteristieken en problemen.
Een van de trends die aan de analyse in dit boek ten grondslag liggen is die van de toenemende complexiteit. Als sinds de jaren zeventig is het idee dat een perfect werkend softwareprogramma te schrijven is. Software maakt echter per definitie fouten, en doet dat per definitie op onverwachte en vervelende momenten. De vervlechting van ICT en bedrijfsprocessen wordt daarmee ernstig gecompliceerd. De beschikbaarheid van ICT is weliswaar hoog, maar onduidelijk en nooit gegarandeerd. Dit geldt in zeer sterke mate voor het Internet. Daarin speelt niet alleen het individuele falen van systemen een rol, maar het complexe gedrag van samenwerkende en onderling afhankelijke systemen. Daarmee komt de kwetsbaarheid van het Internet in beeld.

Organisaties zullen graag risico's willen afdekken die zij als gevolg van de afhankelijkheid van de ICT-infrastructuur van het Internet lopen. Deze risico's zijn niet gering. De President's Commission on Critical Infrastructure Protection stelde in 1997 in een rapport dat veel sectoren, zoals de verzekerings- en bankbranche een uitval van communicatie-infrastructuren van drie dagen niet zouden overleven [Critical Foundations, 1997]. De mogelijke schade is dus groot en het risico daarop is niet nihil. Zoals het rapport 'Samen werken voor veilig Internetverkeer; Een e-Deltaplan' [Stratix, 2001] opmerkt:
"Nederland was op 25/12/1998 een dag lang grotendeels onbereikbaar op het Internet door uitval van de AMS-IX ten gevolge van kortsluiting in een transformator in het laagspanningsnet aan de rand van het WCW-terrein. Kritische 'routers' en andere apparatuur op de AMS_IX 'backbone' waren niet op noodstroomvoorzieningen aangesloten."
Maar bij wie kunnen organisaties voor het afdekken van een dergelijk risico terecht? In deze bijdrage wordt de specifieke organisatievorm die het Internet mogelijk maakt besproken in relatie tot de beschikbaarheid, en de mogelijkheid die beschikbaarheid te verhogen.

De Internet Service Provider (ISP)

De toegangspoort voor organisaties tot het Internet wordt gevormd door een Internet Service Provider (ISP). Met de ISP kunnen afspraken in de vorm van een SLA (Service Level Agreement) over betrouwbaarheid en kwaliteit gemaakt worden. Maar die afspraken hebben een beperkte reikwijdte. De algemene voorwaarden van XS4ALL, Internet Provider te Amsterdam, stellen bijvoorbeeld nadrukkelijk:

"14.1 Onder overmacht wordt verstaan alle van buiten komende oorzaken die redelijkerwijs niet voorzienbaar waren en als gevolg waarvan XS4ALL niet in staat is haar verplichtingen jegens de klant na te komen. Hieronder zijn onder meer, maar niet uitsluitend, begrepen storingen in de verbinding met het Internet, storingen in de telecommunicatie-infrastructuur, storingen in netwerken."[2].

Met ISP's kunnen afspraken gemaakt worden over bijvoorbeeld de beschikbaarheid van hun modems, over de 'up-time' van de hard- en software[3]. Feitelijk houden daarmee de mogelijkheden voor een organisatie die toegang tot het Internet wil krijgen op. Ook andere ISP's hebben namelijk vergelijkbare voorwaarden, en dat is niet zonder reden. ISP's hebben zelf beperkte invloed op de kwaliteit en de werking van het onderliggende netwerk van datatransporteurs waarop zij hun diensten baseren, en kunnen daarom ook geen garanties aan hun eigen klanten afgeven.

Drie organisatieniveaus

Grofweg kunnen de organisaties die het Internet vormen worden onderverdeeld in drie lagen: de toegangsproviders (zoals XS4ALL), de gegevenstransporteurs (zoals KPNQwest, UUNET) en de (fysieke) netwerkleveranciers (zoals Versatel, UPC en KPN). Bovenop deze structuur zitten de afnemers van informatie, de toepassingen en de aanbieders van informatie (zoals websites).[4]

Op het fysieke niveau wordt de beschikbaarheid vooral negatief beïnvloed door kabelbreuken. Hoewel wezenlijk voor de beschikbaarheid van het Internet als geheel – menig anekdotisch verhaal speelt zich op het niveau van kabelbreuken af – inhoudelijk is het een weinig spannende materie.

Op IP-niveau zijn netwerken met een grote verscheidenheid aan IP-transporteurs met elkaar verbonden. Soms via directe verbindingen tussen twee netwerken, soms via grote interconnectiepunten zoals de Amsterdam Internet Exchange (AMS-IX). De topologie van dit netwerk verandert voortdurend, onder andere als gevolg van de sterke groei van het Internetverkeer en het aantal aanbieders van transportdiensten. Vanzelfsprekend zijn alle leveranciers van transportdiensten verantwoordelijk voor de kwaliteit en betrouwbaarheid van hun diensten, en concurreren daar ook mee. Omdat ze echter op basis van onderliggende contracten in een constant veranderende omgeving werken – de route die een pakketje data over het Internet aflegt tussen oorsprong en bestemming is hoogst onvoorspelbaar – is er geen partij die opdrachtnemer is voor de hele route die een pakketje data aflegt. Het Internet is bewust zo ontworpen om maximaal robuust te zijn tegen verstoringen van het netwerk, zoals de uitval van knooppunten of hele delen van het netwerk. Als er geen centrale partij is, kan het netwerk immers niet uitgeschakeld worden door de centrale partij aan te vallen. De voordelen van dit type netwerkorganisatie zijn dan ook evident; naast robuustheid is ook het aanpassingsvermogen aan veranderende markt-

2 http://www.xs4all.nl/voorwaarden/index.html

3 Kwaliteitsgaranties op het deel tussen de gebruiker en zijn toegangspoort tot het Internet zijn overigens wel wezenlijk, aangezien de meeste verstoringen zich op dat traject afspelen. Tijdens het schrijven van dit artikel kon de auteur slechts ruwweg de helft van de tijd bij zijn ISP terecht, omdat het lokale netwerk van die provider overbelast was. In dit kader zijn de acties van de consumentenorganisaties tegen de kabelprovider Chello interessant.

4 Zie voor een eenvoudig overzicht van internetcomponenten htpp://www.navigators.com/internet_architecture.html. Overigens is deze markt continu in beweging, waarbij bedrijven wisselende combinaties van de verschillende diensten aanbieden.

omstandigheden (nieuwe leveranciers van transport- en andere diensten hebben lage toetredingskosten) imposant. Het is moeilijk voorstelbaar dat één bedrijf, Internet Inc.?, in staat zou zijn geweest een dergelijke mondiale groei en verspreiding te realiseren, als zij geheel verantwoordelijk was geweest voor de kwaliteit en de uitrol van het netwerk.
Communicatieprotocollen zijn wezenlijk voor een open ICT-infrastructuur als het Internet. In tegenstelling tot 'popular belief' is de ontwikkeling hiervan geen anarchistisch proces, maar vindt besluitvorming over zaken als het IP-protocol, naamgeving en adressering in duidelijk hiërarchisch geordende organen zoals de IETF (Internet Engineering Taskforce) [5] plaats. Opgemerkt moet worden dat de marktmacht van een (of enkele samenwerkende) partij(en) dit systeem kan doorbreken. De pogingen om de ontwikkeling van HTML te coördineren zijn gestrand op de macht van aanvankelijk Netscape en vervolgens Microsoft [6].
De beste omschrijving voor dit type (meta-)organisatie, waarin samenwerkende organisaties standaarden ontwikkelen en op basis van deze standaarden een pakket diensten leveren, is een 'best effort'-netwerk.

Het Internet heeft een aantal specifieke kwetsbaarheden, waarvan sommige samenhangen met haar karakteristiek als best effort-netwerk. Als voorbeeld beschrijven we de karakteristieken van de topologie van het netwerk en de heterogeniteit van het netwerk.

Topologie

De meest in het oog springende kwetsbaarheid zijn de eigenschappen die de topologie van het netwerk met zich meedraagt. Zoals gesteld wordt de topologie van het netwerk niet ontworpen, maar wijzigt organisch al naar gelang de veranderende omgevingsfactoren. Wel is de topologie van het netwerk van sterke invloed op de betrouwbaarheid van het netwerk en haar robuustheid tegen verstoringen. Het beste voorbeeld hiervan is de 'Single Point of Failure' (SPOF), een enkel knooppunt in het netwerk waarvan uitval een groot deel van de functionaliteit van het netwerk uitschakelt. Nederland kende een SPOF voor het Internetverkeer van en naar het buitenland in de AMS-IX, zoals aan het begin van deze bijdrage werd vermeld. Het opsporen en opheffen van SPOF's (door het introduceren van redundantie) is een belangrijke taak. De vraag is echter wie dat moet doen, gegeven het gedistribueerde karakter van het netwerk en de afwezigheid van een centrale autoriteit. Hier is een mengvorm van overheidsinitiatief (geïnspireerd op het maatschappelijk belang van de betrouwbaarheid van ICT-infrastructuren (zie voor een argumentatie hiervan [Luiijf, 2000]) en zelfsturing in de vorm van samenwerking tussen de bedrijven die gezamenlijk het netwerk vormen.
Meer in algemene zin – een SPOF is een extreem voorbeeld – is de graad van connectiviteit in het netwerk van belang voor de robuustheid en betrouwbaar-

5 http://www.ietf.org/

6 Natuurlijk kunnen hierbij nuanceringen geplaatst worden, zoals dat het hier meer de inhoud van berichten betrof dan het communicatieprotocol van het bericht.

heid. Dat is vooral het geval als gekeken wordt naar de bedreiging van overbelasting. Wanneer een communicatielijn maximaal is belast, zullen vertragingen optreden terwijl extra verkeer omgeleid wordt naar omliggende knooppunten. Het risico dat deze knooppunten overbelast raken is niet gering, zodat de overbelasting zich als een olievlek over het netwerk kan verspreiden. Meer connectiviteit in een netwerk verhoogt het aantal mogelijke routes dat data tussen twee knooppunten kan nemen exponentieel, waarmee de kans op deze olievlekwerking evenredig verlaagd wordt. De laatste jaren is de connectiviteit in het Internet sterk toegenomen. Het Nederlandse Internet heeft inmiddels ook geen SPOF meer.

Naast connectiviteit wint het netwerk ook sterk aan robuustheid als op verbindingen restcapaciteit aanwezig is. Verkeer dat over uitgevallen verbindingen getransporteerd zou worden moet immers geherrouteerd kunnen worden. Hier wringt het concept van een best effort-netwerk, bestaande uit zelfstandige ondernemingen die hun delen van het netwerk zo efficiënt mogelijk trachten te exploiteren met gunstige eigenschappen van het netwerk in zijn geheel. Immers, een transporteur zal altijd proberen zijn lijnen dicht tegen de maximale capaciteit te bezetten, en de restcapaciteit zo klein mogelijk te houden. De aggregatie van suboptimaliseringen door individuele partijen leidt in dit soort gevallen per definitie niet tot een optimale inrichting van het netwerk vanuit de invalshoek van maximale beschikbaarheid. Omdat er voor dit probleem geen echte oplossingen zijn, worden deze gezocht in het aanbrengen van prioriteiten in datatransport. De nieuwe versie van het IP-protocol zal daarom voorzien in de mogelijkheid om prioriteiten aan te brengen. Nu is het zo dat het netwerk geen onderscheid maakt tussen e-mail en andere data die nodig is voor meer tijdkritische toepassingen. Met de invoering van deze nieuwe versie zal de beschikbaarheid van het Internet vanuit de optiek van de gebruikers (die beschikbaarheid meten in termen van de benodigde snelheid van de gebruikte toepassingen) sterk kunnen stijgen zonder dat voor dezelfde hoeveelheid data extra netwerkcapaciteit noodzakelijk is.

Heterogeniteit

De meest in het oog springende calamiteiten op het Internet de laatste jaren zijn rappe en agressieve verspreidingen van virussen. Deze werden naast kwaadwillende daders veroorzaakt door een combinatie van onoplettende gebruikers en de dominantie van Microsoft Outlook. Hetzelfde gebeurde met de Microsoft IIS-webservers die in juli 2001 ten prooi vielen aan de Code Red Worm.

Wanneer een groot deel van de gebruikers in een netwerk van dezelfde programmatuur gebruikmaken, wordt het netwerk kwetsbaar voor fouten in die programmatuur. Dit is een typisch netwerkeffect, alleen al omdat deze effecten onzichtbaar zijn voor individuele gebruikers (of niet in de afwegingen betrokken

kunnen worden), en er geen correctiemechanismen bestaan. Een parallel in de dierenwereld is De Cheetah-populatie in de wereld die op basis van haar aantallen geen direct gevaar meer lijkt te lopen. De genetische variatie in de populatie is echter door het bijna uitsterven van de soort in vroeger tijden buitengewoon gering. Daardoor wordt de diersoort nog altijd met uitsterven bedreigd. Het gebrek aan genetische variatie maakt de Cheetah immers zeer kwetsbaar voor ziekten [Cheetah, Microsoft, 1994]. Hetzelfde geldt overigens voor de reuzenpanda.

Niet alleen virussen maken een netwerk kwetsbaar voor homogeniteit (wat als de dominante versie van Outlook een serieuze, maar niet gedetecteerde millenniumbug had bevat?), maar over het algemeen wordt wel in termen van opzettelijke verstoring naar homogeniteit gekeken. Het virusvoorbeeld toont al aan dat uitval van hardware of software vaak gecorreleerd is aan de leverancier van die hard- of software. Dit gebeurt terwijl een gelijktijdige uitval van knooppunten in een netwerk dit netwerk ernstig kan verstoren. In 'Nature' [Albert, 2000] stond onlangs een onderzoek beschreven dat duidelijk maakt hoe fragiel het verkeer over een netwerk als het Internet is. Wanneer (willekeurig) 1% van de knooppunten uitvalt, vermindert de effectiviteit van het Internet met 50%. Wanneer 4% van de knooppunten uitvalt, functioneert het netwerk niet meer. De vrees dat de Code Red Worm het hele Internet had kunnen platleggen was zeker niet ongegrond.
Opzettelijke verstoring krijgt begrijpelijkerwijs veel aandacht in literatuur over het Internet[7]. Fouten in het communicatieprotocol, de software en de hardware in het netwerk kunnen door het open karakter van het Internet relatief eenvoudig opgespoord en uitgebuit worden. Het is zeker zo dat de dominante software in het netwerk het belangrijkste aanvalsobject is voor opzettelijke verstoring.
In de context van dit artikel is het interessant om te zien op welke wijze door de organisaties die het Internet vormen aan bevordering van de beschikbaarheid wordt gedaan. Het Computer Emergency Response Team Coordination Center (CERT/CC)[8] coördineert de bestrijding van aanvallen (zoals inbraak en virussen) op (delen van) het Internet. Bij het CERT zijn vele nationale, sectorale en lokale CERT's aangesloten die voor verdere kennisverspreiding zorgen. De CERT's worden gefinancierd door overheidsorganisaties en private partijen.
Impliciet wordt de beschikbaarheid van het Internet door de samenstellende partijen bevorderd, doordat alle partijen hun eigen diensten zo betrouwbaar mogelijk maken, onder andere door te streven naar een hoge connectiviteit met de buitenwereld. Verbetering van de beschikbaarheid wordt naast meer mogelijkheden voor tarifering mogelijk gemaakt door het uitbreiden van het IP-protocol met informatie over prioriteiten.

7 Information Warfare.

8 http://www.cert.org/

Conclusies

Organisaties die hun bedrijfsvoering of dienstverlening op een ICT-infrastructuur als het Internet baseren dienen zich bewust te zijn van de inherente kwetsbaarheden van het Internet. De risico's die zij lopen als gevolg van uitval van het Internet kunnen zij niet afdekken bij een ISP. Daarom zullen organisaties voor zover mogelijk risico's bij hun klanten moeten leggen en tegelijkertijd streven naar redundante voorzieningen om uitval van hun communicatie-infrastructuur te kunnen opvangen[9]. Het gebruik van het Internet verhoogt de complexiteit van het bedrijfsproces, hetgeen nooit zonder tegenmaatregelen gedaan mag worden.

Het organisatieprincipe van een best effort-netwerk kent specifieke kwetsbaarheden, zoals blindheid voor zwakten van de topologie van het netwerk en het gevaar van te grote homogeniteit van de elementen in het netwerk. Deze zwakten zijn moeilijk te ondervangen en vragen om een actieve rol van overheden enerzijds, en zelfsturing door de organisaties waaruit het netwerk bestaat anderzijds.

Het best effort-netwerk Internet bevat veel mechanismen om de beschikbaarheid van dit netwerk te bevorderen, maar tegelijkertijd kan de beschikbaarheid niet gegarandeerd worden. Dit levert de paradoxale situatie op dat het netwerk wellicht zo betrouwbaar is als het in het praktijk blijkt te zijn, juist omdat er geen centrale instantie is die de betrouwbaarheid kan garanderen. De toetredingskosten voor nieuwe leveranciers zijn door de opzet zo laag dat het netwerk als geheel volop recht kan doen aan de dynamische marktomstandigheden waarin het verkeert.

Of het principe van best effort-netwerken zich in andere sectoren zal manifesteren valt te bezien. Op weinig terreinen zijn parallelle ontwikkelingen te zien, al kan wel gewezen worden op het 'Open Source'-softwareontwerp zoals Linux, waarin veel van de karakteristieken van Internet zijn terug te vinden.

De combinatie van strakke standaardisering en of interfaceontwerp en vrije toetreding zou ook in de verkeerssector denkbaar zijn, al vereist dit een vergaande vorm van herontwerp van wetgeving, bijvoorbeeld op het terrein van het openbaar vervoer (met stations als interconnectiepunten). Ook hierbij zal de afweging tussen een zo hoog mogelijke, maar uiteindelijk onvoorspelbare betrouwbaarheid of iemand kunnen afrekenen op een redelijk betrouwbaarheidsniveau een bijna diabolische afweging zijn.

9 In zijn meest simpele vorm is dit zichtbaar bij intensieve Internetgebruikers, zoals telewerkers die verschillende accounts bij verschillende ISP's hebben, en het liefst verschillende toegangstechnieken (kabel, telefoon) gebruiken.

Referenties

- Albert, R. e.a. (2000). Error and Attack Tolerance of Complex Networks. Nature
- Critical Foundations; Protecting America's Infrastructures. (1997). The Report of the President's Commission on Critical Infrastructure Protection. Oktober
- Dael, R. van, C. Metselaar (red.). (1997). De virtuele organisatie. Kluwer Bedrijfsinformatica & NGI
- Klein, N. (2000). No Logo. Flamingo, London
- Luiijf, H.A.M., M.H.A. Klaver. (2000). Bitbreuk, de kwetsbaarheid van de ICT-infrastructuren en de gevolgen voor de informatiemaatschappij. Infodrome. 28 maart
- Cheetah Microsoft (R) Encarta. Copyright (c) (1994) Microsoft Corporation. Copyright (c) 1994 Funk & Wagnall's Corporation
- Stratix/TNO-FEL. (2001). Samen werken voor veilig Internetverkeer; Een e-Deltaplan. In opdracht van het Ministerie van Verkeer en Waterstaat

2

17 De betrouwbaarheid van optische disksystemen

ir. A. Huijben[1], *prof.dr. S.B. Luitjens*[2]

Introductie

Deze case beschrijft het resultaat van een onderzoek naar de betrouwbaarheid van consumentenproducten bestemd voor de massamarkt. De producten zijn Compact Disc (CD)-spelers en Digital Versatile Disc (DVD)-systemen. Terugkoppeling uit de markt is essentieel voor een goed beeld van de betrouwbaarheid. Hier wordt verslag gedaan van een semi-kwantitatief onderzoek naar de faalkans. Op grond van de analyse wordt duidelijk dat het voor juiste uitspraken over de betrouwbaarheid belangrijk is de goede maat te kiezen. Vaak wordt alleen het aantal garantieclaims per tijdseenheid geregistreerd (Field Call Rate, FCR). Voor het verbeteren van de betrouwbaarheid lijkt het aan te bevelen om het aantal fouten per tijdseenheid te registreren en de data te interpreteren met gebruikmaking van de hazardfunctie.

1 Philips Medical Systems,
Manager Customer Services
Postbus 90050
5600 PB Eindhoven

2 Philips Research
Prof. Holstlaan 4
5656 AA Eindhoven

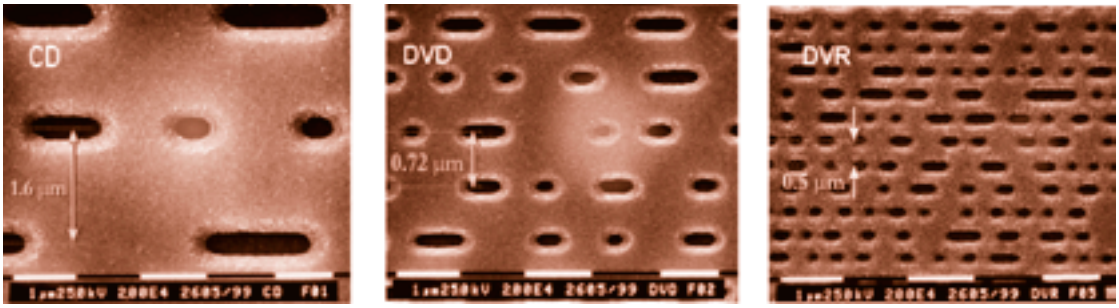
Na een inleiding over de technologische ontwikkelingen op het gebied van de optische dataopslag gaan we in op de resultaten voor een aantal CD- en DVD-producten. De studie van de betrouwbaarheidskentallen en faalmechanismen geeft de mogelijkheid om gericht de betrouwbaarheid van het bestaande product te verbeteren. Ook kunnen er alvast maatregelen genomen worden voor een optimale betrouwbaarheid van toekomstige producten. Wel moet een adequate manier gebruikt worden om informatie over betrouwbaarheid te verzamelen. In de conclusies en aanbevelingen wordt hierop ingegaan.

Technologische ontwikkelingen

Opslagsystemen gebaseerd op optische technologie zijn tegenwoordig zeer bekend. De Compact Disc (CD) is in het begin van de jaren tachtig van de vorige eeuw gelanceerd door Philips en Sony voor het weergeven van muziek. Men kan zeggen dat dit het begin van het digitale tijdperk is, omdat de muziek als digitale informatie op de disk is opgeslagen. De CD noemen we de eerste generatie optische disksystemen. Tegenwoordig hebben we niet alleen CD-spelers, maar ook CD-recorders die in staat zijn geluid op te nemen. Na ruim tien jaren dient zich de tweede generatie aan. Nieuwe technologieën zijn ter beschikking gekomen met als gevolg dat het opslaan van videoinformatie ook mogelijk wordt. Dat is de DVD-speler voor het afspelen van DVD-video's. Ook de DVD-technologie wordt binnenkort uitgebreid met apparaten die het mogelijk maken videoopnamen te maken.
In laboratoria over de hele wereld wordt ondertussen gewerkt aan de derde generatie optische opslagsystemen voor audio en video, maar ook voor dataopslag in de pc. Dit systeem wordt aangeduid met DVR[3] en maakt gebruik van zeer geavanceerde technologie voor laser en plaat.

De onderliggende technologie van deze optische disksystemen is vergelijkbaar. Het principe van de drie generaties berust op een halfgeleiderlaser die details op de plaat aftast en in beeld en geluid omzet of de gegevens in de pc ter beschikking stelt. Doorbraken in de fysica en technologie van voornamelijk platen en lasers maakt deze vooruitgang mogelijk. Door het toepassen van lasers die licht produceren met een steeds kleinere golflengte is het mogelijk steeds kleinere details te zien en dus meer informatie op de plaat op te slaan. Als een gevolg daarvan is de capaciteit van de optische disks toegenomen van 650 MByte voor de CD, naar 4,7 GByte voor de DVD tot 22 GByte voor DVR. Een illustratie vinden we in figuur 17.1.

3 DVR betekent Digital Video Recorder.



Figuur 17.1
Opnamen met een scanning elektronenmicroscoop van details op een CD, een DVD en een DVR-plaat. De kleur van het laserlicht en de grootte van het actieve gebied is aangegeven. De kleur verandert van infrarood (CD) naar blauw (DVR). Verandering van de kleur rood naar blauw komt door de kleinere golflengte van het licht. Bron: [Password Magazine, 2000].

Betrouwbaarheidsstudie [4]

Het doel van de studie was het verschaffen van inzicht in de betrouwbaarheid van CD-spelers, DVD-spelers en de evolutie op dit terrein. Op die manier zou kunnen worden aangegeven wat van belang zal zijn bij de volgende generatie disksystemen en waarop gelet zou moeten worden om de betrouwbaarheid verder te verbeteren. Het onderzoek heeft zich toegespitst op CD-spelers, CD-wisselaars, CD-recorders en DVD-videospelers op de Nederlandse markt.

Betrouwbaarheidsverbetering en –kentallen

Zowel vanwege de toenemende garantietermijn als vanwege de kosten verdient betrouwbaarheid aandacht. Ook is een betrouwbaar product de manier om de klant optimaal tevreden te stellen. De toegang tot betrouwbaarheidsgegevens uit het verleden is daarbij van eminent belang om de betrouwbaarheid te kunnen verbeteren.

Tijdsdruk door steeds kortere ontwikkelcycli leidt ertoe dat de producthistorie vaak onbenut blijft. Dat heeft tot gevolg dat er onvoldoende wordt gereageerd op optredende fouten die dientengevolge steeds opnieuw in opeenvolgende producten optreden.

Daarnaast zien we dat vaak het aantal garantieclaims per tijdseenheid wordt geregistreerd (de FCR) in plaats van het aantal fouten als functie van de leeftijd van het product (kalendertijd versus leeftijd of ouderdom). De hazardfunctie drukt de foutkans of foutfrequentie uit als functie van de ouderdom van het product. Daarmee is het mogelijk om ervaringen over verschillende producten te aggregeren, ook al zijn deze op een verschillend tijdstip geproduceerd, verkocht of in gebruik genomen. We ‘vegen’ hiermee als het ware alle producten van een bepaald type bijeen. Zo wordt de faalkans als functie van de gebruiksduur (leeftijd) van het product verkregen. In het meest algemene geval leidt de hazardfunctie tot de badkuipcurve zoals in hoofdstuk 4 van deel 1 is beschreven.

4 De studie is uitgevoerd door universitair afstudeerder L. Toscano van de Technische Universiteit Eindhoven in samenwerking met Philips.

Terugkoppeling van velddata

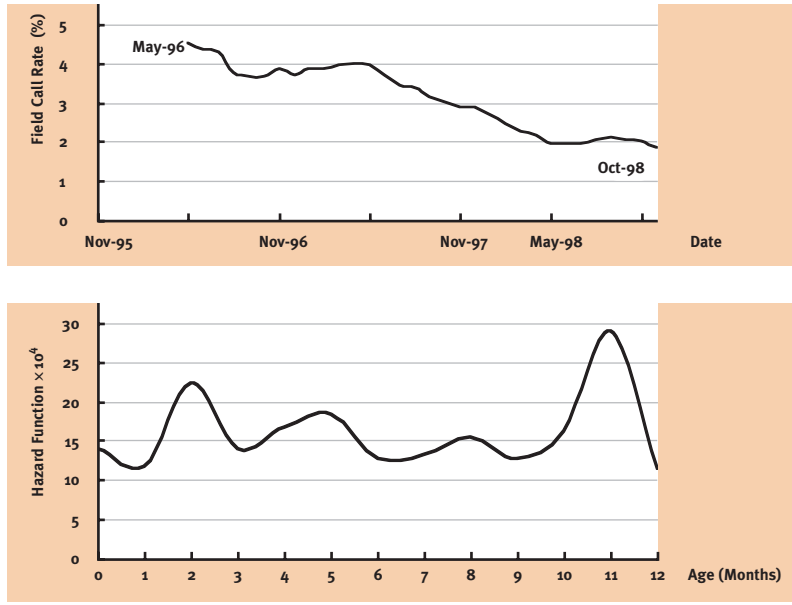
De producten waar het in deze studie om gaat worden vaak door derden gerepareerd. Door deze vorm van uitbesteding van de serviceactiviteiten wordt de terugkoppeling van servicegegevens aanzienlijk bemoeilijkt, omdat men over de grenzen van bedrijven heen dient te organiseren en te communiceren. Dit leidt ertoe dat de gegevens minder compleet en minder correct blijken te zijn. Door het uitbesteden wordt de producent slechts geïnformeerd over de fouten die in de garantieperiode optreden vanwege de geassocieerde financiële consequenties.

De organisatie volgt de FCR op basis van garantieclaims. Reacties kunnen plaatsvinden op grond van wijzigingen in het aantal claims ('calls'). Hierin schuilt een aanzienlijke vertraging, waardoor pas laat actie kan worden ondernomen. Immers een wijziging in het product zal gedurende een periode van 12 maanden zichtbaar worden in de markt. Pas na 1 jaar echter zijn alle apparaten in de markt van het nieuwe soort. Bovendien gaat bij het toepassen van de FCR alle informatie over specifieke, leeftijd gerelateerde problemen van het product verloren.

Data-analyse

De CD-speler, de oudste van de vier onderzochte producten, werd in 1982 op de markt geïntroduceerd. De CD-wisselaar werd in 1988 en de CD-recorder werd eind 1997 op de markt gebracht. De eerste DVD-speler werd in 1998 geïntroduceerd. Voor het onderzoek waren alleen gegevens beschikbaar voor de periode na 1994, hetgeen de data-analyse aanzienlijk beperkte. Voor verschillende producten zijn in de studie de FCR-functies en de hazardfuncties berekend.
Een representatief voorbeeld van de resultaten is te zien in figuur 17.2. Het betreft een speler waarvan de productie in 1995 is gestart en die tot eind 1998 in productie bleef. De bovenste figuur is de FCR (uitgedrukt in procenten). We zien dat de FCR aanzienlijk daalt. De interpretatie is dat dit een gevolg is van een verbetering van de productkwaliteit in de loop der tijd. Immers het gemiddelde aantal keren dat het product gedurende de garantietermijn faalt neemt af. In de onderste figuur zien we de hazardfunctie voor hetzelfde product. De resultaten zijn geanalyseerd over een gebruiksperiode van een jaar (de garantietermijn). We zien significante veranderingen in het promillage van de fouten. Deze curve is te vergelijken met de eerder beschreven badkuipcurve. De detailinformatie leert iets over de faalkans als functie van de leeftijd van het product. Het maximum bij de start van de periode is te wijten aan fouten die direct na in gebruikneming optreden (vroeg falen) of fouten die veroorzaakt worden door vroege slijtage. Aan het einde van de garantietermijn zien we eveneens een verhoging. Dat komt vaker voor en vindt zijn verklaring in coulance van de detailhandel. Dealers accepteren vaak geretourneerde producten die net buiten de garantie

Figuur 17.2
Field Call Rate versus hazardfunctie (Failure Rate Function).



of nog onder de garantie vallen. Het is zeker niet veroorzaakt door falen aan het einde van de levensduur, omdat die na een jaar nog lang niet bereikt is. Deze curve is een krachtig middel om de betrouwbaarheid gericht te verbeteren, zeker als ook de oorzaak van het falen (de 'root-cause') bekend is.

Conclusies en aanbevelingen

Het doel van het project was het formuleren van aanbevelingen voor de volgende generatie disksystemen. Tijdens het project bleek een aantal organisatorische beperkingen van invloed te zijn op de kwaliteit van de velddata en daarmee op het kunnen formuleren van aanbevelingen.

Conclusies

- Een gestructureerde analyse van veldreparaties zou kunnen worden uitgebreid met 'root-causeanalyses' (analyse over de achtergrond van de oorzaak). Indien dit achterwege wordt gelaten, blijft de oorzaak van het falen onbekend en zal het probleem opnieuw optreden.
- Het verkrijgen van 'root-cause'-informatie uit veldgegevens is moeilijk.
- FCR is meer een instrument voor kostenbeheersing dan voor betrouwbaarheidsverbetering.
- De besproken vertraging bij het veranderen van de productbetrouwbaarheid verhindert een pro-actieve en snelle reactie.
- De kwaliteit van veldgegevens kan worden verbeterd. In het algemeen zijn de integriteit en de volledigheid beperkt.

– Het is moeilijk om veldgegevens te krijgen die afkomstig zijn van producten die buiten de garantie vallen.
– Ondanks dit alles was het mogelijk om een kwantitatieve analyse uit te voeren op grond waarvan toekomstige FCR-niveaus voorspeld konden worden.
– Met behulp van de hazardfunctie kon worden aangegeven op welke leeftijd de meeste veldfouten optreden.

Aanbevelingen

Op basis van de hier beschreven studie kon worden aangegeven hoe veldgegevens uitgebreid zouden moeten worden en welke analyse hierop toegepast zou kunnen worden.
Het draait dan vooral om:

1 De uitbreiding van servicedata met een omschrijving van de faalkarakteristieken.
2 Het opzetten van specifiek op foutanalyse gerichte activiteiten naast de reguliere service en reparatieactiviteiten.
3 Het uitbreiden van de kwantitatieve (Call Rate gerichte) data-analyse met kwalitatieve (faalmechanisme gerelateerde) analysen.
4 Het inbedden, dan wel onderkennen van betrouwbaarheidsinformatiestromen in de bedrijfsprocessen. Dat wil zeggen expliciet om betrouwbaarheidsinformatie vragen aan (externe) servicebedrijven.

Dit alles zal betekenen dat het verzorgen van de terugkoppeling over faalgedrag en faalfrequentie van producten een reguliere taak wordt van de serviceorganisatie, en dus niet alleen het repareren van deze producten.

Generalisatie

Hoewel deze case is gebaseerd op een specifieke range van producten, de bijbehorende data en bijbehorende organisaties, zijn de conclusies redelijk universeel en overdraagbaar. In veel gevallen zijn de veldgegevens van serviceafdelingen niet bedoeld voor betrouwbaarheidsanalyses en daarom ook slechts beperkt bruikbaar voor dit doel. Mits compleet en correct, vormt deze bron echter waardevolle informatie voor verbeteracties. Het uitbreiden van veldgegevens en de bijbehorende analyse is in veel gevallen de eerstvolgende stap op weg naar een verbetering van de betrouwbaarheid.

Referenties

– Password Magazine. (2000). Philips Research, Vol. 2. januari
– Toscano, L.M. (2000). Reliability of Third Generation Optical Storage Systems. Msc-thesis. Technische Universiteit Eindhoven. augustus

2

18 Punctualiteit in het reizigersvervoer per trein

prof.dr. R. Dekker[1], *drs. M.J.C.M. Vromans*[2]

Inleiding

Geen week lijkt voorbij te gaan zonder geklaag over vertragingen in het openbaar vervoer [Volkskrant, 2000]. De betrouwbaarheid van de uitvoering van onder andere de dienstregeling van de Nederlandse Spoorwegen lijkt daarbij lager te zijn dan ooit het geval is geweest. In deze bijdrage zullen we dat nader bekijken.

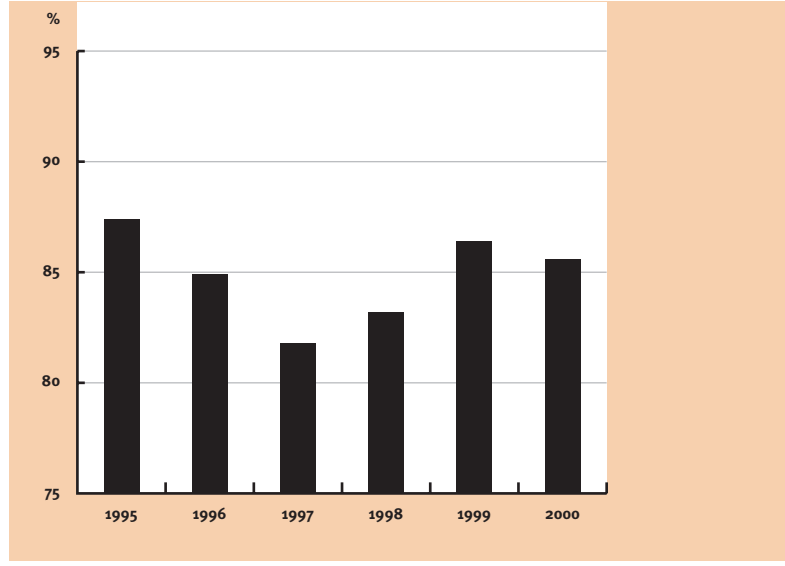
1 Erasmus Universiteit Rotterdam,
Faculteit Economische
Wetenschappen
Burg. Oudlaan 50
3062 PA Rotterdam

2 Erasmus Universiteit Rotterdam,
Faculteit Bedrijfskunde
Burg. Oudlaan 50
3062 PA Rotterdam

Probleem

Vervoer van mensen per trein is het hoofdproduct van NS Reizigers (NSR). Belangrijke aspecten van dit product zijn dat het vervoer veilig, comfortabel, snel en op de gewenste tijden plaatsvindt. De tijdsplanning van dit product is in eerste instantie afgestemd op de capaciteit van de dienstregeling. Elk jaar wordt een dienstregeling gemaakt die aangeeft op welke tijden een klant een trein kan verwachten. Punctualiteit bij aankomst is daarbij een belangrijk succeskenmerk van dit product. NSR onderkent het belang daarvan en houdt daarom diverse prestatiekarakteristieken bij.
De door NSR gehanteerde definitie voor punctualiteit is: het percentage van de reizigerstreinen dat 3 minuten binnen de geplande tijd aankomt op een knooppunt. De knooppunten zijn de 35 grootste stations in Nederland. Deze punctualiteitcijfers worden niet alleen landelijk per jaar bijgehouden, maar per trein in een database opgeslagen, waardoor de cijfers bijvoorbeeld ook per dag, per serie (bijv. de Intercity Den Haag Centraal naar Heerlen) of per knooppunt kunnen worden opgevraagd. Ze kunnen dus zelfs gebruikt worden om een bepaalde trein op een bepaalde dag te volgen. Ook kan een andere grens dan 3 minuten gekozen worden. Internationaal wordt in het algemeen gewerkt met een grens van 5 minuten.

De punctualiteit van de dienstregeling wordt door de NS wekelijks gepubliceerd in het NS-blad 'De Koppeling' [NS, 2000]. Hieruit blijkt dat de punctualiteit van de treinen per week nogal kan verschillen. Verder valt op dat er jaarlijks twee minder goede perioden zijn aan te wijzen (zie figuur 18.2). Ten eerste is er een

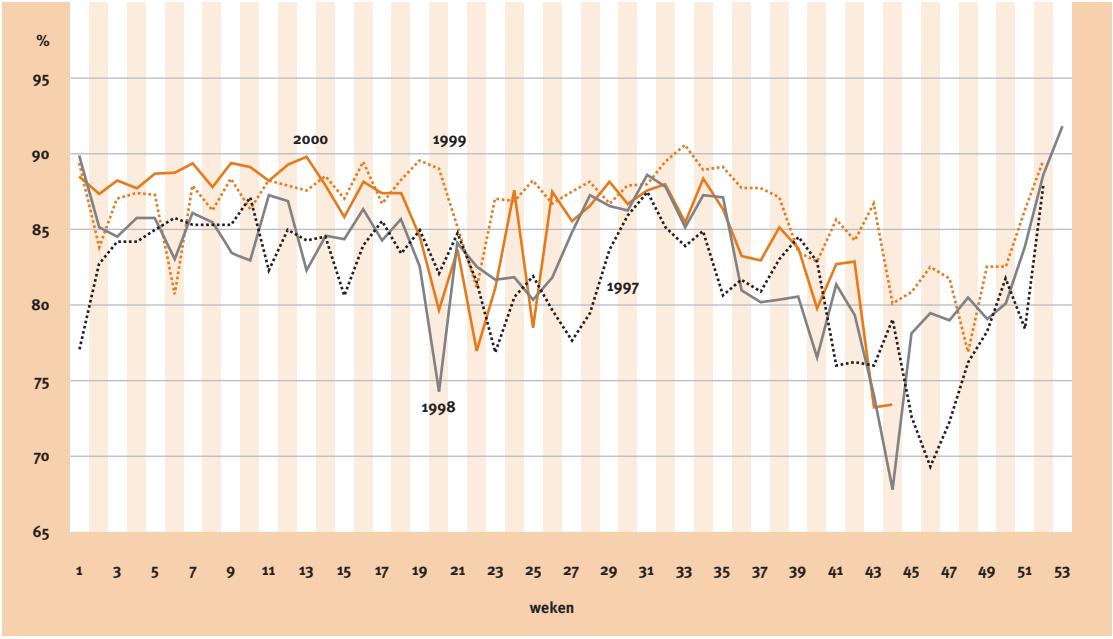


Figuur 18.1
Percentage van de aankomsten 3 minuten binnen de geplande tijd. (2000 tot en met week 44). Bron: [De Koppeling, 2000].

beperkte dip rond week 20, wanneer de nieuwe dienstregeling van kracht wordt. Zowel reizigers als personeel lijken tijd nodig te hebben om aan de nieuwe dienst te wennen. De tweede dip is de herfstdip, die meestal wordt toegekend aan bladeren op de rails en andere weersinvloeden. In januari tot en met maart en in juli en augustus hebben we in het algemeen juist te maken met een bovengemiddelde punctualiteit. Hierdoor is het ook begrijpelijk dat er juist in november 2000 zo'n massale media-aandacht was.

Ook de reizigersorganisatie Rover verzamelt gegevens over de punctualiteit van de dienstregeling. Zij publiceren deze cijfers halfjaarlijks in hun Kwaliteitsthermometer [Rover, 2000]. De cijfers zijn gebaseerd op eigen metingen op de zeven belangrijkste knooppunten gedurende de ochtend- en avondspits. Ondanks het feit dat de metingen op een beperkt aantal dagen zijn gebaseerd, houden ze ongeveer gelijke tred met de cijfers van de NS. Omdat Rover alleen in de spits meet, valt het percentage van Rover ongeveer drie procentpunten lager uit dan dat van de NS.
Er zijn echter tal van andere manieren, waarop de punctualiteit gemeten zou kunnen worden. Een eerlijkere manier zou misschien zijn om het aantal passagiers van de trein te laten meewegen, waardoor een zondagochtendtrein in de Achterhoek niet even zwaar meetelt als de maandagochtendspitstrein van Amsterdam naar Rotterdam. Op dit moment (medio 2000) zijn de databases van de vertragingen en de reizigersaantallen (nog) niet gekoppeld en is zo'n berekening van de punctualiteit moeilijk te realiseren. Een nog verdere verbetering zou kunnen liggen in het doorrekenen van de totale reistijden, waarin ook de

Figuur 18.2
Variatie van de punctualiteit over het jaar. Bron: Bedrijfsbureau Landelijk Coördinatiecentrum Verkeersleiding.



(gemiste) aansluitingen naar voren komen. Hierbij moet gebruik gemaakt worden van matrices waarin de herkomst en de bestemming wordt vermeld. Op dit moment werkt NSR aan een dergelijk model. Wel worden op dit moment al cijfers bijgehouden over het percentage gerealiseerde aansluitingen. Dit percentage ligt rond de 92%, wat ook de streefwaarde van NSR is.

Analyse van vertragingen

Vertragingen kunnen onderverdeeld worden in primaire en secundaire vertragingen. Primaire vertragingen ontstaan door allerlei externe oorzaken, behalve door andere treinen. Secundaire vertragingen worden wel door andere treinen veroorzaakt. Er zijn dus geen secundaire vertragingen zonder primaire vertragingen. Ruwe schattingen geven aan dat wellicht slechts 15% tot 20% van de vertragingen primair is. Dit geeft aan de ene kant een machteloos gevoel: als één trein vertraagd raakt, zijn er gemiddeld meteen nog vijf andere treinen vertraagd. Toch heeft het ook een voordeel. Als er een manier wordt gevonden om primaire vertragingen te laten afnemen, neemt het totaal aantal vertragingen met een factor 6 af.

De belangrijkste oorzaken van vertragingen zijn:
Bij primaire vertragingen:
- defecte seinen, wissels, bruggen, overwegbomen;
- defecte bovenleiding;
- seinen en wissels verkeerd;
- verkeerde of uitblijvende stationsomroep;
- gebrek aan personeel;
- (te) krappe planning (hiertoe gedwongen door beperkte capaciteit);
- tekort aan materieel;
- defect of slecht functionerend materieel;
- reizigers, bijvoorbeeld lange stoptijden bij stations, agressie, enz.;
- ongevallen, weer (harde wind, overvloedige regenval, herfstblad, ijzel, bliksem), brand.

Bij secundaire vertragingen:
- treinen achter elkaar op hetzelfde spoor;
- kruisende bewegingen van treinen, vooral op en rond knooppunten;
- het in stand houden van aansluitingen ondanks vertragingen;
- personeel dat van een vertraagde of uitgevallen trein moet komen.

Al deze vertragingsfactoren kunnen ook opgesplitst worden naar organisatorische en technische oorzaken. Vertragingen door het in stand houden van aansluitingen bijvoorbeeld zouden organisatorisch kunnen worden opgelost door

de aansluitingen te laten varen. De meeste oorzaken zijn echter van technische aard, zoals defect materieel of niet werkende overwegbomen.
Verder moet opgemerkt worden dat het vertragingsleed veel beperkter zou zijn, als de vervoerders de beschikking zouden hebben over een ruimere infrastructuur. Treinen zitten elkaar dan veel minder in de weg en vooral het aantal secundaire vertragingen zal flink kunnen afnemen. Men moet zich hierbij realiseren dat het netwerk van de NS in veel opzichten vrij complex is. Diverse soorten treinen met verschillende snelheden delen niet alleen baanvakken, maar ook beperkte perroncapaciteit op stations. Metrolijnen hebben bijvoorbeeld wel gescheiden infrastructuur en delen meestal geen perrons in stations. Daarnaast kent de NS geen echt naaf-en-spaak ('hub-and-spoke')-netwerk, zoals luchtvaartmaatschappijen waarin er een ontkoppeling is van verbindingen op de centrale naaf. Bij de NS gaan treinen juist door het hele land waardoor vertragingen landelijke effecten kunnen hebben.
Vooral NS Reizigers (NSR) en Railned hebben daarom veel onvervulde wensen op het gebied van de infrastructuur.
Een verdeling van de vertragingen over de verschillende bedrijfsonderdelen is niet gemakkelijk. Men zou namelijk precies moeten nagaan wat een bepaalde 'foute handeling' tot gevolg heeft, en dat is door de complexe samenhang van de treinenloop bijna onmogelijk. Er is op dit moment wel een maatstaf in gebruik bij de NS die de vertragingen en de gevolgen van vertragingen probeert te kwantificeren en aan een verantwoordelijke probeert toe te wijzen. Bij alle bedrijfsonderdelen bestaan er echter grote vraagtekens over deze maatstaf. Betere maatstaven zijn onderzocht, maar zijn tot op heden gestruikeld over de benodigde extra informatie voor de berekening ervan.

De hoofdrolspelers

De NV Nederlandse Spoorwegen zijn een complex netwerk van bedrijfseenheden waarvan alle aandelen in handen zijn van de Nederlandse staat. Sinds 1993 heeft de privatisering van NS de bedrijfsstructuur al menig maal doen veranderen. De situatie in 2001 die van toepassing is op de verantwoordelijkheden met betrekking tot de punctualiteit van de dienstregeling wordt hier nu kort beschreven.
In grote lijnen is de NV Nederlandse Spoorwegen opgesplitst in een NS Groep NV en drie taakorganisaties. Deze drie taakgroepen vallen direct onder het Ministerie van Verkeer en Waterstaat. De minister van dit departement is dus direct voor hun bezigheden verantwoordelijk. De NS Groep heeft een eigen directie als verantwoordelijke instantie.
De drie taakgroepen zijn NS RailInfraBeheer BV (RIB), Railned BV, en NS Verkeersleiding BV (VL). Het RIB moet zorgen voor een goed onderhoud van het

spoor. Dit omvat onder andere wissels, seinen, bovenleidingen en overwegen. Verder valt ook de uitbreiding van het huidige spoornetwerk onder het RIB. Railned heeft twee belangrijke functies, namelijk onderzoek op de lange termijn, maar vooral een ondersteunende functie voor de andere bedrijfsonderdelen en voor het Ministerie. De tweede functie is van directe invloed op de punctualiteit en behelst de toewijzing van rijwegen aan de verschillende gebruikers van het spoor. Als hier te krappe normen worden gehanteerd, is het hele proces veel gevoeliger voor kleine verstoringen. De VL ten slotte geeft sturing aan het gehele proces. Gegeven de planning die voor alle vervoerders, passagiers en vracht wordt aangeleverd, moet de VL zorgen voor een goede doorstroming van het verkeer. Ze is dus verantwoordelijk voor de stand van alle seinen en wissels. Verder moet ze zorgen voor de informatievoorziening op stations en aan het rijdend personeel. Deze laatste taak gaat binnenkort over in handen van NS Reizigers (NSR).
Van de NS Groep hebben slechts twee onderdelen invloed op de punctualiteit van de dienstregeling. Ten eerste is dit natuurlijk NSR. Zij moet zorgen voor het maken van een goed spoorboekje en voor het inplannen van materieel en personeel. Maar meer zichtbaar is zij verantwoordelijk voor het rijden van de passagierstreinen van NS. Daarnaast is Nedtrain (het voormalige NS Materieel) een belangrijke schakel in het vervoersproces. Zij heeft de treinen van NSR (en een aantal andere vervoerders) onder haar hoede en is verantwoordelijk voor het onderhoud en de reparatie van dit materieel.
Naast de NS zijn ook andere vervoerders aanwezig op het Nederlandse spoor. De belangrijkste zijn NoordNed (passagiers in Groningen en Friesland), Syntus (passagiers in Oost-Nederland) en Railion (de grootste vrachtvervoerder, ontstaan uit een fusie tussen NS Cargo en Deutsche Bahn Cargo).

Conclusie

Het product van de NS zoals dat door de consument gezien wordt, is een samenspel van diverse samenwerkende bedrijven, elk met verschillende belangen. Deze samenwerking verloopt niet altijd optimaal met het gevolg dat vertragingen moeilijk beheersbaar zijn.

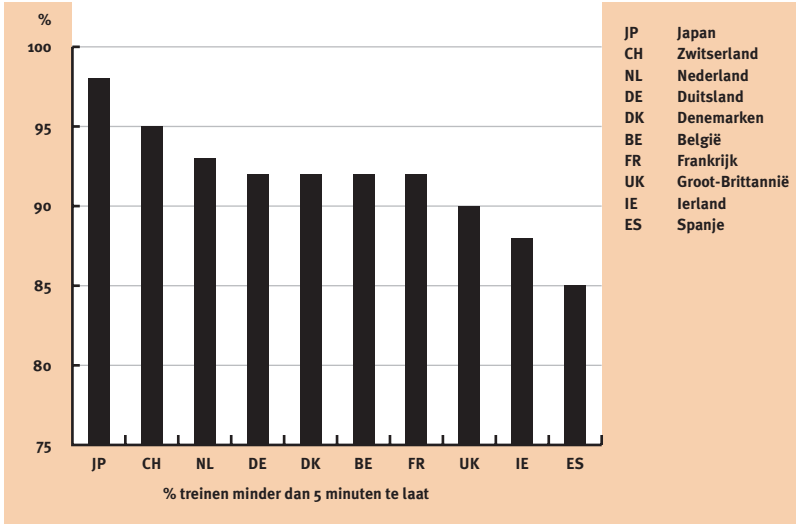
Perceptie publiek over punctualiteit

Is het nu zo dat de vertragingen zijn toegenomen of dat het grote publiek ze erger vindt dan vroeger? Na de piek van 1995 (87,4%) is een duidelijke dip (81,8%) waar te nemen in de punctualiteit van de dienstverlening. Gelukkig is de punctualiteit sindsdien weer enigszins toegenomen. Toch lijkt het of het grote publiek de vertragingen alleen maar ziet toenemen. Een mogelijke verklaring is het feit dat het slechte jaar (1997) de deur tot klagen heeft opengezet.

Verder heeft de combinatie met de toenemende drukte in de treinen een negatieve invloed op de perceptie van de reiziger. Ook kun je misschien wel stellen dat de Nederlander in zijn algemeenheid steeds mondiger wordt. Dit aspect doet zich ook bij onze zuiderburen voor. Ondanks een toegenomen punctualiteit van de Belgische Spoorwegen in 2000, was het aantal klachten bij de ombudsman gestegen [Financieel Economische Tijd, 2001].
De interpretatie van de vertraging wordt overigens nog door vele andere factoren bepaald. Een factor daarbij is het selectief geheugen. Dat iemand twee weken geleden tien minuten vertraging had weet hij nog wel, maar dat hij de acht keer daarna wel op tijd was, is snel vergeten. Ten tweede is de informatievoorziening van grote invloed op de perceptie. Als duidelijk is waarom er vertraging is, hoelang de vertraging ongeveer gaat duren en wat de eventuele alternatieven zijn, is zo'n vertraging heel wat draaglijker. Aan deze informatievoorziening is helaas nog het een en ander te verbeteren [Rover, 2000]. Een derde factor die een rol speelt is dat je eerder geneigd bent negatief over een onderwerp te denken, als veel mensen dat ook doen.

Ter vergelijking

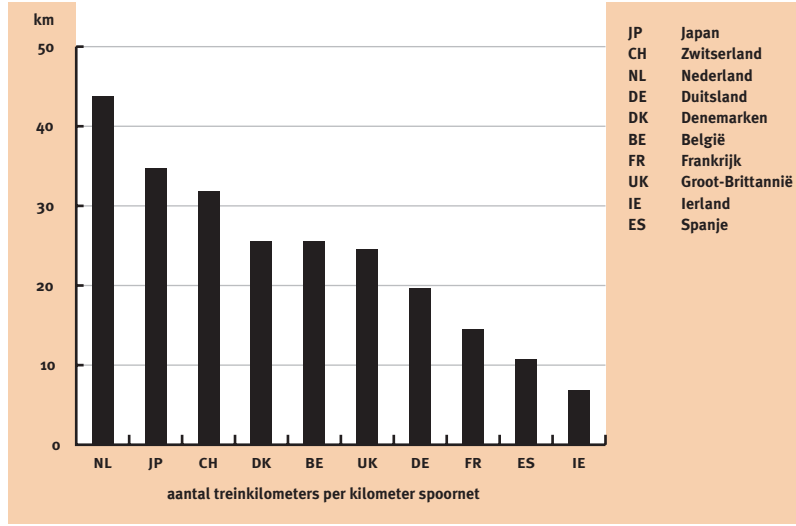
Om het vraagstuk in het juiste daglicht te plaatsen, is het van groot belang om eens te kijken hoe goed het in andere landen gaat. Ook kunnen we eens een vergelijking maken met andere vervoersmiddelen.
Als we de punctualiteit van de Nederlandse reizigerstreinen vergelijken met andere landen, dan blijkt dat Nederland een van de beste scores ter wereld heeft. Alleen Japan en Zwitserland doen het beter. Dit resultaat is des te opvallender als je daarbij ook de drukte op het spoor betrekt. Nederland heeft verreweg het drukste spoorwegnet, wat een optimale punctualiteit alleen maar ingewikkelder maakt.



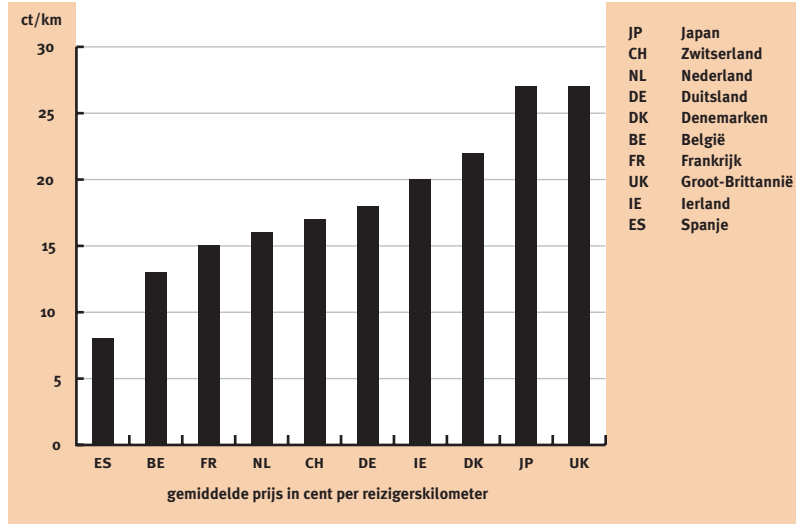
Figuur 18.3
Een vergelijking tussen de punctualiteit van de dienstregeling in verschillende landen. Bron: [De Koppeling, 2000].

Ook wordt vaak gezegd dat het openbaar vervoer in Nederland zo duur is. Als we ook hier weer een vergelijking maken, blijkt opnieuw dat Nederland het goed doet. Verder blijkt dat het relatief slechte Spaanse treinverkeer heel goedkoop is, terwijl men in Japan blijkbaar een hoge prijs betaalt voor het goede product. Ook de tariefsverhogingen in Nederland van de laatste jaren lagen onder het inflatiepeil.

We kunnen het ook eens vergelijken met de perceptie van het file rijden. Dat is ook vervelend, maar daar is niet zo gemakkelijk een schuldige voor aan te wijzen, behalve dan waarom al die andere weggebruikers ook zo nodig nu van A naar B moeten. Een belangrijk element hierbij is dat je bij autorijden zelf keuzen maakt. Vertrek je heel vroeg of laat, dan heb je minder last van files.



Figuur 18.4
Optimaal gebruik van de infrastructuur. Bron: [De Koppeling, 2000].



Figuur 18.5
Vergelijkingen tussen tarieven in verschillende landen. Bron: [De Koppeling, 2000].

Hoelang je er met de auto over doet van Dordrecht naar het centrum van Rotterdam is ook niet in een 'wegboekje' vast te leggen. Files zijn net als het treinverkeer aan toeval onderhevig. Verder zijn autokilometers de afgelopen jaren aanzienlijk duurder geworden dan treinkilometers.

Ten slotte nog een vergelijking tussen de punctualiteit van de dienstregeling van de NS en vliegmaatschappijen. Het US Department of Transportation [US Department of Transportation, 2000] houdt gedetailleerde cijfers over punctualiteit bij van alle in de VS landende en opstijgende vliegtuigen. Zij hanteren daarbij een marge van 15 minuten, waardoor een vliegtuig dat 14 minuten te laat is nog als 'op tijd' wordt meegeteld. Op deze manier komt de Amerikaanse overheid voor oktober 2000 op een aankomstpunctualiteit van 76,2%. Dit percentage ligt niet alleen veel lager dan dat van de spoorwegmaatschappijen, maar laat ook nog een grote mate van 'een beetje te laat zijn' toe. In Europa is het niet veel beter. De Europese Airline Association (AEA) meldde recent dat meer dan 26% van alle vluchten in Europa vertraagd is, hetgeen 1% meer is dan vorig jaar. Het verschil met de NS is echter dat de meeste mensen alleen zo nu en dan vliegen en daardoor vertragingen minder vaak ervaren. Voorts is vliegen voor veel mensen een vakantiebelevenis waardoor vertragingen wel vervelend zijn, maar toch overkomelijk. Ten slotte moet men bij de duur van de vertragingen in acht nemen dat de gemiddelde vlucht ruim langer duurt dan de gemiddelde treinreis. Overigens worden in de luchtvaartwereld de vertragingen voornamelijk veroorzaakt door de versnipperde luchtverkeersleiding en problemen bij luchthavens, en niet zozeer door storingen van materieel en infrastructuur waarvan de spoorwegen last hebben. Ook kan men niet duidelijk een partij als schuldige aanwijzen.

Beheersing van vertragingen

De lage punctualiteit van de dienstregeling in 1997 is gedeeltelijk te wijten aan de grote toename van het aantal passagierstreinen dat jaar. Deze dip was mede aanleiding voor NS om het project 'Bestemming: Klant' in het leven te roepen. Dit project heeft als doel om de kwaliteit en de punctualiteit van de door de NS Reizigers (NSR) verleende diensten te verbeteren. Deze doelstelling wordt nagestreefd door alle NSR-onderdelen erbij te betrekken. Dit project lijkt enig effect te hebben gehad, maar het is nog te vroeg om conclusies te trekken. Vanaf 2001 wordt de punctualiteit van de dienstregeling om nog een reden belangrijk. NSR zal met het Ministerie van Verkeer en Waterstaat een prestatiecontract afsluiten, waarvan het belangrijkste onderdeel een punctualiteit van 88% in 2001 is, oplopend tot 92% in 2005. Aan de hand van dit prestatiecontract zal NSR weer contracten afsluiten met de verschillende andere organisa-

ties binnen de NS. Zo zal van Nedtrain een bepaalde betrouwbaarheid van het materieel worden geëist, en zal met het RIB overeenstemming moeten worden bereikt over de maximale hinder door sein- en wisselstoringen.
Voor een goede aanpak van de punctualiteit is eerst een beter inzicht in de grootste problemen bij vertragingen nodig. Het aanpakken van één enkel aspect kost nu eenmaal erg veel geld dat maar één keer kan worden uitgegeven.

Conclusie

Moeten we treinen complexer of juist simpeler maken? In ieder geval moet de bedrijfszekerheid bij complex functioneren omhoog. Hetzelfde geldt voor de infrastructuur van het spoorwegnet. Het is wel duidelijk dat er meer sporen en infrastructuur bij moeten komen, omdat de bezetting van het spoorwegnet te hoog is.
Ook het beter meten van de kritieke aspecten en een meer wetenschappelijke benadering van het probleem is belangrijk [Vromans, 2001]. Aan de hand van de resultaten van een grondig onderzoek is het wellicht een stuk gemakkelijker om effectief aan de punctualiteit van de dienstregeling te werken. Daarbij moeten we steeds in het achterhoofd houden wat de klant wil. Naast de punctualiteit zijn bijvoorbeeld ook de volle treinen een punt van aandacht voor de klant. Ook de dienstverlening en de informatievoorziening zijn belangrijk. Deze aspecten maken het probleem alleen maar complexer. In deze bijdrage zal hierop niet verder worden ingegaan.

Aanpak punctualiteit

Bij het aanpakken van de punctualiteit is er nog een duidelijke tweedeling tussen kleine vertragingen en grote verstoringen aan te wijzen. De grote verstoringen vanaf ongeveer 15 minuten worden vooral veroorzaakt door defect materieel en door defecten aan de infrastructuur. De oorzaak van deze vertragingen zal niet op korte termijn kunnen worden opgelost. Hiervoor zijn langetermijninvesteringen nodig in het onderhoud van het materieel en in de infrastructuur. Dienstregelingen kunnen ook niet anticiperen op dit soort verstoringen. Deze verstoringen zijn namelijk groter dan de marges en spelingen die je in de dienstregeling kunt opnemen.
Bij deze grote verstoringen zijn naast punctualiteit nog twee andere begrippen relevant. De robuustheid van het systeem is de mate waarin het vervoersproces bloot staat aan verstoringen. Het is een maatstaf voor de mate van invloed van negatieve aspecten op de dienstregeling. Het begrip stabiliteit geeft aan in welke mate het systeem in staat is terug te keren naar de normale staat, nadat een verstoring is verholpen. Dit heeft bij het spoor onder andere te maken met personeel en materieel dat door de verstoring op de verkeerde plek is terechtgekomen. Beide begrippen zijn moeilijk te kwantificeren.
Op de korte termijn zijn de kleine verstoringen veel interessanter. Door spelingen

aan te brengen in het spoorboekje, zullen kleine verstoringen (voor een groot deel) opgaan in deze extra ruimte. NS Reizigers (NSR) hanteert daarom op dit moment al rijtijden die 7% hoger liggen dan wat technisch gezien nodig is. Het is duidelijk dat grotere spelingen de punctualiteit ten goede komen, maar dat de reiziger daar niet op zit te wachten, want dan worden de rijtijden langer. Ook worden stoptijden bij een station langer gepland dan strikt noodzakelijk waardoor een te late aankomst door een korte stop gecompenseerd kan worden, zodat de trein weer op tijd naar het volgende station kan vertrekken.

Maatregelen NS en mogelijke andere oplossingen

Toch moeten we beseffen dat de reiziger klant is van NS Reizigers (NSR). Daarom kunnen we eigenlijk stellen dat NSR de overige bedrijfsonderdelen als onderaannemers zou moeten beschouwen. NSR is verantwoordelijk voor het bedrijfsproces en zou goede prestaties van Nedtrain, Railned, het RIB en de VL moeten afdwingen.
Enige middelen die NSR ter hand neemt of zou kunnen nemen om de doelstelling 'Bestemming: Klant' te realiseren zijn:

a Betrouwbaarheid van rijdend materieel afdwingen (bij Nedtrain).
b Betrouwbaarheid van de infrastructuur afdwingen (bij RIB).
c De bedrijfsvoering veranderen.
d De bedrijfscultuur veranderen.
e Problemen sneller verhelpen.
f Meer spoorcapaciteit afdwingen (bij RIB/Railned).
g 'Invloeden van buiten' beperken.

Alhoewel dit artikel niet geschikt is voor een al te gedetailleerde blik op de hiervoor genoemde punten, zullen deze toch nog enigszins worden uitgewerkt.

a Aangezien Nedtrain een onderdeel is van de NS Groep, zal een grotere betrouwbaarheid van het materieel inhouden dat er meer geld zal moeten worden gereserveerd voor Nedtrain. Op die manier kunnen vaker onderhoud en controle uitgevoerd worden. Ook is het mogelijk om mankementen sneller te verhelpen.
b Het beheer van de infrastructuur is in handen van het RIB, en dus ligt de verantwoording bij de minister. Men zal dus met overtuigende argumenten moeten komen die aangeven dat een groot deel van de vertragingen te wijten is aan het falen van de infrastructuur. Al komen dit soort onregelmatigheden niet zo heel vaak voor, een seinstoring tussen Gouda en Woerden (lees: Den Haag en Rotterdam enerzijds en Utrecht anderzijds) kan van grote invloed zijn op de treinenloop.
c Een verandering van de bedrijfsvoering ligt geheel in handen van NSR zelf en kan op veel zaken betrekking hebben. Enkele voorbeelden worden hier besproken:

– Niet wachten op aansluitingen. Dit lijkt zeer vervelend voor de reiziger, die bij het missen van zijn aansluiting vaak een half uur verliest. Aan de andere kant is het aantal reizigers dat wel al in de trein zit vaak veel groter dan het aantal overstappers, en deze moeten dus wachten op een relatief kleine groep. Ook zal de vertraging zich waarschijnlijk nog verder gaan verspreiden. Een nog veel verdergaande redenering is dat als je maar op tijd vertrekt de aansluitingen vanzelf worden gehaald.
– Productgebonden inzet van het rijdend personeel. Dit houdt in dat personeelsleden meer met hetzelfde werk bezig zijn. Ten eerste is men van mening dat het personeel dan beter kan inspringen op onverwachte situaties. Verder kan deze werkwijze leiden tot meer betrokkenheid bij het werk. Automatisch wordt zo ook het aantal overstappen van conducteurs en machinisten verminderd. Hierdoor wordt de kans kleiner dat een conducteur of machinist een vertraging van de ene trein meeneemt naar een andere trein. Als er dan toch moet worden overgestapt, dan is het goed voor de punctualiteit om deze overstap langer te maken.
– Minder krap plannen van het spoorboekje. De capaciteit van het Nederlandse spoorwegnet is op dit moment zo vol gepland, dat ruimere planning op de meeste plaatsen onmogelijk is zonder treinen te schrappen. Op plaatsen waar eventueel nog wel enige ruimte is, is een verruimende hernieuwde planning vaak alleen mogelijk door het laten vervallen van aansluitingen of het (in grote mate) verruimen van de reistijden. In de zomer van 2001 heeft NSR een aantal treinen geschrapt vanwege tekorten aan materieel en personeel met de bedoeling de punctualiteit van de overgebleven treinen te verbeteren. Hoewel de punctualiteit daarbij is gestegen, is er ook veel kritiek gekomen op dit besluit.

d De bedrijfscultuur veranderen doe je niet van de ene dag op de andere, zeker niet in een bedrijf met 10.000 werknemers verspreid over talloze locaties in het hele land. Een betere motivatie van het personeel en het terugdringen van het ziekteverzuim zijn ook belangrijke elementen. De slechte verstandhouding tussen personeel en directie is dan ook geen goede zaak. Een mogelijkheid die eventueel aanwezig is als de werknemersbonden meewerken is de invoering van prestatieloon. Zeker met behulp van de productgebonden inzet van het personeel zou men de conducteurs en machinisten naar gelang van de punctualiteit in hun gebied kunnen belonen.

e Het sneller verhelpen van problemen kan op verschillende onderdelen betrekking hebben. Zo zouden er afspraken gemaakt kunnen worden met het RIB, waardoor defecten aan de infrastructuur sneller worden verholpen en het treinverkeer sneller weer op gang kan worden gebracht. Ook zou bij grote calamiteiten sneller gereageerd kunnen worden, waardoor er eerder alternatief vervoer beschikbaar komt (nog meer noodscenario's). Ook betere informatie bij vertragingen is nodig. Deze punten dragen niet bij aan de

punctualiteit, maar verbeteren wel de kwaliteit van het spoorwegproduct en de perceptie van het publiek.

f Het afdwingen van meer spoorcapaciteit zal moeten gebeuren bij het Ministerie van Verkeer en Waterstaat dat verantwoordelijk is voor het RIB en daarmee voor de infrastructuur. Hiervoor zal net als voor het onder a. genoemde onderhoud van de infrastructuur moeten worden aangetoond dat een kwalitatief goede bedrijfsvoering niet mogelijk is bij de huidige capaciteiten. Bij spooruitbreidingen gaat het echter over miljarden en realisatie is op korte termijn niet mogelijk.

g Het beperken van de invloeden van buitenaf lijkt een beetje tegenstrijdig. Het weer is inderdaad niet te beïnvloeden, maar daar staat tegenover dat het aantal aanrijdingen op overwegen kan worden beperkt door bijvoorbeeld een betere beveiliging van overwegen of het plaatsen van flitspalen bij deze overwegen. Een veel rigoureuzere aanpak zou zijn om het gehele spoorwegnet af te sluiten van de buitenwereld, zodat ook zelfdoding of koeien op het spoor niet meer mogelijk zijn. Dit is natuurlijk wel erg kostbaar.

Sommige van de genoemde punten hebben betrekking op het voorkomen van vertragingen(b), andere op het voorkomen van verspreiding (zie c. onder niet wachten op aansluitingen), weer andere op beide (zie c. onder minder krap plannen). Ook is de afwikkeling van al ontstane problemen van groot belang (e). Zoals wel blijkt zijn de spoorwegen een complex systeem met een uitgebreide beveiliging, waardoor er maar een kleine schakel hoeft te falen om grote problemen te veroorzaken. Hierdoor is het voor de NS erg moeilijk om grip op de zaak te krijgen. Het is zeer onduidelijk waarop de NS haar aandacht moet vestigen, want het is onmogelijk alle problemen in een keer aan te pakken. Bovendien staat het systeem bloot aan allerlei oorzaken, waaraan NSR, Nedtrain of het RIB niets kunnen doen (blikseminslag, ijzel, aanrijdingen op overwegen).
Ten slotte is ook de directe relatie tussen de klant en het bedrijf van groot belang. Men kan hierbij denken aan een betere klantenservice en of klachtenafhandeling en een vergoedingensysteem bij vertragingen. Dit laatste lijkt alleen mogelijk na invoering van een OV-chipkaart, waarmee kan worden nagegaan wie op welke baanvakken vertraging heeft opgelopen.

Eindconclusies

Voor de NV Nederlandse Spoorwegen (NS) is de punctualiteit van treinen van het grootste belang. Gezien de media-aandacht en publieke reacties, lijkt er weinig goed te gaan bij de NS. Toch rijdt het gros van de treinen keurig op tijd en lijkt de NS het niet echt slechter te doen dan de buitenlandse spoorwegen of de luchtvaartwereld. Het is duidelijk dat perceptie hier een grote rol speelt. Verder

zijn de NS natuurlijk een makkelijk mikpunt van kritiek. Men zou daarom kunnen stellen dat de reacties wat overtrokken zijn, maar percepties hebben nu eenmaal veel invloed, of ze nu terecht zijn of niet. Ze passen ook in de trend dat mensen meer eisen stellen aan hun omgeving en dat geldt evenzeer voor de overheid zelf als voor de NS.

Het laten rijden van treinen is een ingewikkeld proces. Een proces dat relatief erg veilig is, maar heel weinig flexibiliteit kent. Een proces dat voorts niet alleen technisch ingewikkeld is met een hoge gevoeligheid voor storingen, maar ook een proces met veel organisatorische aspecten, zowel in het samenspel tussen diverse bedrijven als in de uitvoering door het personeel. Veel mensen onderschatten de complexiteit van het hele planning- en uitvoeringsproces bij een bedrijf als de NS. Door deze complexiteit is het ook voor de NS zelf moeilijk om met kant-en-klare oplossingen voor het probleem met de punctualiteit van treinen te komen. Veel oplossingen zijn erg duur, hebben een lange realisatietijd en zijn soms ook klantonvriendelijk (bijv. het schrappen van treinen of aansluitingen). Daarnaast staat dit vertragingsprobleem niet los van andere problemen, zoals de volle treinen en de personeelskrapte. Toch zijn de NS hard bezig met het zoeken naar oplossingen. Zowel intern als in samenwerking met verschillende universiteiten wordt intensief onderzoek gedaan. Ook wordt er in de praktijk al hard gewerkt aan verbeteringen, vooral in het kader van het project 'Bestemming: Klant'. Oplossingen moeten hierbij niet alleen in de technische en infrastructurele sfeer gezocht worden, maar ook in de communicatie met de klant, zowel in het algemeen als specifiek bij vertragingen.

Referenties

- De Koppeling. (2000). Weekblad Nederlandse Spoorwegen, nr. 1619, 16 december. Utrecht
- de Volkskrant. (2000). Vertragingen NS lopen nog verder op. 30 november
- Financieel Economische Tijd. (2001). Ombudsman geeft nmbs goede punten; meeste klachten over vertragingen. 14 maart
- Rover. (2000). Kwaliteitsthermometer NS. Zomernummer. Amersfoort
- US Department of Transportation. (2000). Air Travel Consumer Report. October Volume
- Vromans, M.J.C.M. (2001). Punctuality of Railway Systems: Analysis and Improvement. PhD Research Proposal, Faculty of Business Administration, Erasmus University Rotterdam

2

19 Betrouwbaarheid in de mobiele telecommunicatie

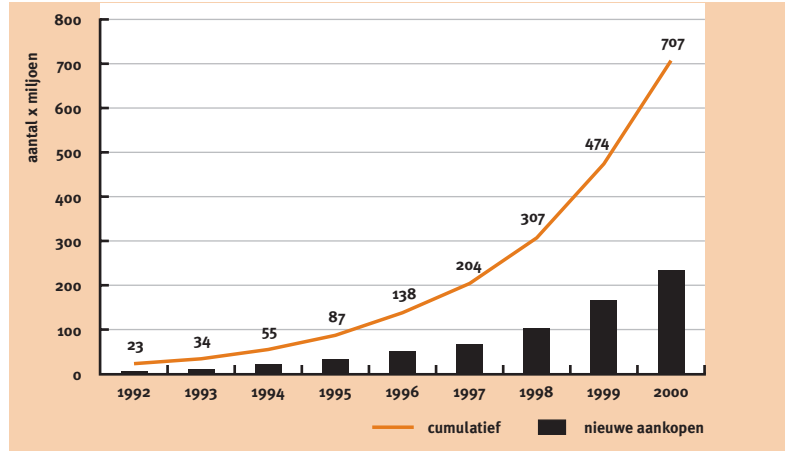
drs.ir. G.J.C. Ransijn [1]

De omvang van mobiele telefonie

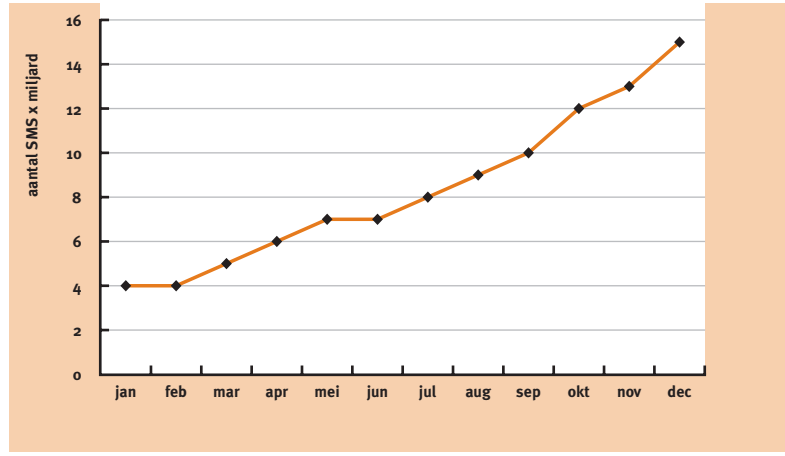
Het aantal mobiele telefoons heeft in het jaar 2000 wereldwijd de 420 miljoen overschreden, aldus Dataquest Inc. Volgens KPMG spendeerde de Nederlandse consument in 2000 gemiddeld 380 euro per persoon aan mobiele telefonie. Dat geld gaat niet alleen op aan mobiele gesprekken. De GSM Association heeft laten weten dat er in december 2000 wereldwijd 15 miljard SMS-tekstberichten over het GSM-netwerk zijn verstuurd. Dit komt neer op een vervijfvoudiging in tekstberichten per maand gedurende het jaar 2000. Men verwacht een toename in 2001 tot een maandelijks aantal van 25 miljard berichten, en een jaartotaal van 200 miljard.

1 CMG Public Sector B.V.,
Afdeling Advanced Technology
Postbus 187
2501 CD Den Haag

Figuur 19.1
Aantal mobiele telefoons wereldwijd (Bron: Dataquest Inc.).



Figuur 19.2
Gebruik SMS-verkeer in 2000 wereldwijd (Bron: GSM Association).



De techniek van mobiel bellen

De mogelijkheden die mobiele telefoons ons bieden zijn inmiddels al zo gewoon dat we er niet bij stilstaan dat het sturen van bijvoorbeeld SMS-berichten nog maar enkele jaren mogelijk is. De gebruikers krijgen zelfs al enige tijd binnenkort te realiseren mogelijkheden getoond die vijftien jaar geleden met een pc nog niet mogelijk waren. Dit zal allemaal tot stand worden gebracht door een branche die met de volgende technologische en organisatorische uitdagingen te maken heeft.

Zenden en ontvangen

Mobiele GSM-telefoons werken doorgaans met draaggolven met een frequentie van 1.800 MHz. Enkele jaren geleden was dit nog doorgaans 900 MHz, vergelijkbaar met een middengolfradio. In heel Nederland zijn er misschien enkele tientallen middengolfzenders, en de ontvangers sturen niets terug. In het mobiele netwerk zijn er in Nederland enkele miljoenen telefoons, die zender èn ontvan-

ger zijn. Al deze gesprekken moeten tegelijk gevoerd kunnen worden, zonder dat ze elkaar storen. Dit wordt niet alleen gerealiseerd door het hele gebied op te delen in kleine cellen, maar ook door slimme software in de telefoon die het zenden alleen activeert als er daadwerkelijk gesproken wordt. Deze software kent ook het onderscheid tussen achtergrondgeluid en de stem van de gebruiker. Bovendien bevat de telefoon ook software die ondanks alle invloeden op het signaal en schaduwsignalen (reflecties van o.a. gebouwen) toch de juiste informatie weet door te geven.

Verplaatsen van de telefoon

Iemand die in de auto zit te bellen zal veel cellen in- en uitrijden. Maar er hoeft geen handmatig contact gezocht te worden met nieuwe zenders. Dit wordt door de software in de mobiele telefoon gedaan. Deze zoekt continu in de 16 nabijgelegen cellen of hiermee inmiddels een sterkere verbinding te krijgen is. Samen met de zenders wordt het gesprek dan doorgegeven zonder dat de gebruiker daarvan iets zou moeten merken.

Identificatie

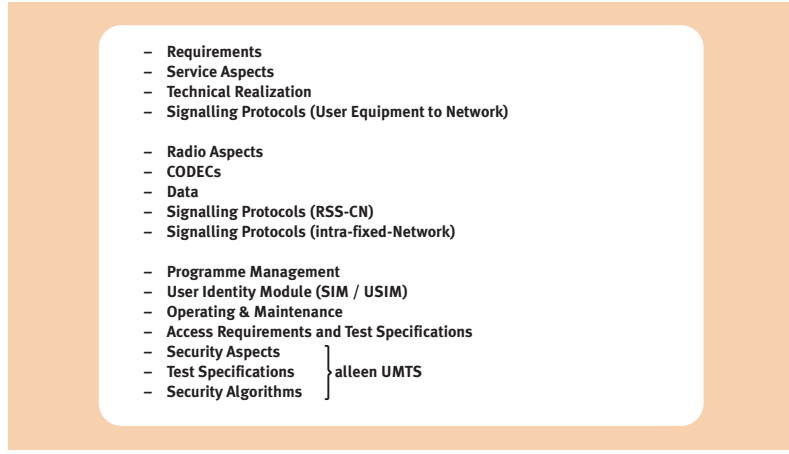
Mobiel bellen is alleen mogelijk als de mobiele gebruiker een unieke identiteit heeft in het mobiele netwerk. Dit is opgelost door zowel de telefoon als de SIM-kaart een uniek nummer te geven dat continu door het netwerk gecontroleerd wordt. Zodoende kan ook de rekening naar de juiste persoon gestuurd worden.

Standaardisatie

Het motto van mobiele telefonie is ‘waar en wanneer dan ook bellen en gebeld worden’. Deze inspanning wordt tot stand gebracht door tientallen operators in diverse landen, duizenden zenders en diverse fabrikanten van mobiele telefoons. Bovendien wordt ieder jaar nieuwe functionaliteit aangeboden zoals SMS, ‘mobile e-mail’, WAP, ‘roaming’ in het buitenland, mobiel betalen. Om dit op verschillende plaatsen te kunnen doen met dezelfde telefoon is het van belang dat netwerken en telefoons elkaar blijven begrijpen. De GSM-standaard wordt van bovenaf opgelegd door ETSI (zie hierna). De VS en Japan hebben zich als overheid bewust niet met de techniek van mobiele telefonie bemoeid, waardoor er in deze landen ook andere resultaten zichtbaar zijn. De meest succesvolle techniek zou door de marktwerking tot een de facto standaard moeten leiden. Inmiddels zijn er in de VS operators die verschillende technische standaarden hanteren die ook nog eens niet compatibel met GSM zijn. Vaak bieden deze technieken echter wel geavanceerde mogelijkheden, zoals NTT DoCoMo grafische mogelijkheden biedt die de WAP-standaard van GSM al lang en breed gepasseerd zijn.

Complexiteit door standaardisatie

In het begin van de jaren tachtig bestond er in Europa een aantal analoge mobiele telefoonnetwerken. Deze waren weliswaar vaak op vergelijkbare techniek gebaseerd (o.a. NMT 450), maar maakten gebruik van frequenties die licht van elkaar verschilden. Hierdoor was het onmogelijk om in bijvoorbeeld Duitsland dezelfde telefoon te gebruiken als in Frankrijk. Deze situatie wordt de eerste generatie van mobiele netwerken genoemd. Om een soortgelijke situatie bij een tweede generatie – die bovendien geheel digitaal moest zijn – te voorkomen, werd in 1982 de Groupe Spéciale Mobile opgericht. Deze groep ontwikkelde het thans bekende Global System for Mobile Communications (GSM). Dit systeem wordt nu wereldwijd door meer dan 100 miljoen mensen in meer dan 130 verschillende landen gebruikt. Het specificatieproces voor GSM (en zijn opvolgers) is in handen gegeven van het in 1988 opgerichte European Telecommunications Standards Institute (ETSI). Dit instituut maakt gebruik van de diensten van meer dan 3.500 experts, en heeft sinds haar oprichting meer dan 4.400 technische documenten geproduceerd. En daar zijn de te verwachten 4.000 documenten voor het jaar 2000 nog niet bij opgeteld.



Figuur 19.3
ETSI-standaardenseries voor GSM en UMTS.

Complexiteit en ketenwerking

Het grootste conceptuele verschil tussen vaste en mobiele telefonie is uiteraard het gebruik van antennes versus het gebruik van kabelverbinding. Deze antennes bestrijken doorgaans in groepjes van vier een gebied variërend van 100 meter tot 35 km, afhankelijk van het aantal obstakels. De antennes in dat gebied worden beheerd door een zogeheten Base Station Controller (BSC) die allerlei taken verricht. Tot deze taken behoort onder andere het reserveren van radiofrequenties – om te voorkomen dat gebruikers elkaar storen, of voor het

overdragen van een gebruiker naar een andere groep antennes – als de gebruiker van het ene naar het andere gebied beweegt, het oproepen van mobiele telefoons, het overzetten van data die via het netwerk tussen de BSC's en andere diensten is binnengekomen naar data die via een antenne te versturen is. BSC's zijn dus een belangrijke schakel in het mobiele verkeer, en vanwege hun functionaliteit en prestaties ook hele dure en complexe apparaten.

Systemen die bedoeld zijn om gespreks- of datacommunicatie te leveren via het mobiele netwerk zullen uiteindelijk met BSC te maken krijgen. Bedrijven die dergelijke systemen leveren worden al snel geconfronteerd met een wereld die aanzienlijk complexer is dan de systemen waaraan hun producten doorgaans gekoppeld worden. De volgende anekdote onderschrijft dit.

Een 'Cell Broadcast System' stelt een gebruiker in staat om alle geabonneerde mobiele gebruikers die zich op dat moment in een bepaald geografisch gebied bevinden dezelfde SMS te sturen. In het najaar van 1999 werd door een Europese mobiele netwerkbeheerder (operator) geconstateerd dat een van de systemen die bedoeld was om 'cell broadcast'-berichten aan haar abonnees te sturen om ogenschijnlijk onverklaarbare redenen vastliep. Dit systeem was al enige tijd in gebruik, en was daarvoor reeds uitvoerig getest. De beschikbaarheid van dit systeem was vooral cruciaal, omdat de operator hiermee informatie over verkeerscongestie en parkeerroutes wilde doorgeven tijdens een internationale beurs over...mobiele telefonie! Wat een demonstratie van een nabije blik in de toekomst had moeten worden dreigde te verzanden in een onplezierige afgang. Haastig opgetrommelde onderhoudstechnici wisten middels symptoombestrijding de show toch nog te redden.
De oorzaak bleek te zitten in een onverwachte interactie tussen een van de BSC's en een systeem dat onderdeel uitmaakte van de koppeling ('system interface') met het cell broadcast-systeem. Deze koppeling was zo ingesteld dat als een BSC niet in staat was om een bericht via een van de antennes te versturen, deze de terugontvangen foutmelding netjes opsloeg in een elektronisch logboek. Hierdoor kon later bij het opstellen van de rekening het aantal bereikte abonnees zo nauwkeurig mogelijk ingeschat worden. Bij het ontwerpen van dit systeem was men echter ervan uitgegaan dat een antenne binnen enkele seconden weer operationeel zou zijn, of anders zou de antenne volledig door de BSC zijn uitgeschakeld. Daarom zou het bericht om de paar seconden weer worden aangeboden aan de BSC, totdat een foutmelding zou worden ontvangen die duidelijk aangaf dat de antenne niet meer zou werken. In werkelijkheid bleek de BSC ook nog allerlei andere scenario's te bevatten, en bleef dus andere typen foutmeldingen terugsturen. Na verloop van tijd raakte het elektronisch logboek vol, en liep het systeem vast. Alleen door het logboek regelmatig te legen kon het systeem nog in de lucht gehouden worden.

Is dit incident op zichzelf staand? Is het slecht een kwestie van beter testen, beter specificeren, of domweg betere systemen leveren? De volgende trends zijn aan te wijzen:

- De markt voor mobiel gespreks- en dataverkeer zal enorm toenemen. Op dit moment is slechts 20% van de wereldpopulatie middels een vast of mobiel netwerk verbonden.
- Standaardisatie en het centraal vastleggen van specificaties is in ieder geval in Europa een succesvolle keuze gezien de verspreiding van GSM en de toename van de dienstverlening van ETSI.
- De mogelijkheden van mobiele diensten zal enorm toenemen, onder andere door de derde generatie van mobiele netwerken (o.a. Universal Mobile Telecommunications System – UMTS) en een nieuwe stroom van snufjes in de mobiele telefoons en andere mobiele apparaatjes.
- Het vaste gedeelte van het mobiele netwerk (servers, intelligente systemen, doorgifte van data, mailboxen, WEB, WAP) krijgt steeds meer producten die met elkaar verbonden moeten zijn om zo de mobiele eindgebruiker een transparante set diensten te kunnen verlenen zonder dat deze met het bestaan van individuele producten lastig gevallen wordt. De eindgebruiker is alleen geïnteresseerd in het eindresultaat van de dienstverlening, en niet in de onderliggende techniek (zie ook deel 3).

Om ook het toekomstige mobiele verkeer betrouwbaar te maken wordt het bedrijfsproces dat de nieuwe producten moet voortbrengen uitgedaagd om:

- Kennis te behouden van de exploderende hoeveelheid technische standaarden die door ETSI geproduceerd worden.
- Bij het koppelen van het mobiele netwerk aan de buiten dit netwerk aanwezige diensten niet alleen rekening te houden met de technische beschrijving van de system interfaces, maar ook met de interactie tussen systemen waarvan het gedrag niet direct duidelijk is (doch mogelijk wel ergens verstopt in de techniek).
- Net als de automobielindustrie steeds betere kwaliteit en steeds meer functionaliteit te leveren in steeds kortere ontwerptrajecten. Dit gaat dan vooral over de exploderende hoeveelheid software die in de nieuwe mobiele telefoons te vinden is, en de diensten in het mobiele netwerk die de mobiele eindgebruiker toegang moet verlenen tot de mobiele diensten.

Omvormen van het bedrijfsproces

Het bedrijfsproces van een leverancier van systemen voor het mobiele netwerk zal omgevormd moeten worden. Dit proces moet namelijk in staat zijn om de onderneming beter in staat te stellen mee te gaan met de eerdergenoemde externe trends, en tegelijkertijd producten voort te brengen die in de markt gepositioneerd kunnen worden met een relatief grote hoeveelheid functionaliteit en tevens een groot aantal kwaliteitsattributen. Bovendien zullen dergelijke producten steeds beter moeten integreren om tezamen een totaaloplossing voor de mobiele netwerkproviders te vormen. Dit betekent dat er steeds meer betrokkenen zijn bij de totstandkoming van een nieuw product, ook wel 'stakeholders' genoemd.
Projecten om systemen voor het mobiele netwerk te maken worden dus steeds grootschaliger en vergen een goede beheersing van het bedrijfsproces. Vooral voor 'software engineering' is het definiëren van geschikte bedrijfsprocessen een vrij jonge tak van sport. Dit heeft alles te maken met de relatief jonge leeftijd van de branche.

Een dergelijk proces zou in ieder geval de volgende deelprocessen moeten bevatten:

- Op directe wijze verzamelen van producteisen. Het product wordt gedefinieerd aan de hand van de directe aanlevering van een belangrijke klant.
- Op indirecte wijze verzamelen van producteisen. Het product wordt gedefinieerd aan de hand van de aanlevering van een verzameling klanten (combinatie van product en markt).
- Wijzigingsbeheer tijdens het productieproces. Nadat een product uit de marktwensen gedefinieerd is, en er een moment geweest is dat deze definitie intern ook is afgestemd ('baseline'), dient het productieproces toch nog in staat te zijn om nieuwe veranderingen door te voeren tot het stadium waarin het product op dat moment reeds ontwikkeld is.
- Wijzigingsbeheer na het productieproces. Het product is reeds geïnstalleerd bij een klant, en opgeleverd aan de afdeling die het product ondersteunt. Wijzigingen aan deze versie van het product dienen nu doorgevoerd te worden tot aan de computerinstallaties bij de klant.
- Ontwerp gebaseerd op haalbaarheid op de markt. Producteigenschappen worden zo snel mogelijk aan de markt getoond om de reacties van de klanten te kunnen bepalen en het ontwerp eventueel bij te stellen. Dit moet mogelijk zijn in diverse stadia van het ontwerp, namelijk bij de productdefinitie, de architectuur of middels een prototype.
- Ontwerp gebaseerd op technische haalbaarheid. Het productieproces moet geschikt zijn om actief in te spelen op het selectief kiezen van productaspecten waaraan een hoog risico verbonden is. Functionaliteit die niet eerder

gecreëerd is zou bijvoorbeeld alvast in een prototype gerealiseerd moeten kunnen worden, indien deze functionaliteit cruciaal is voor het slagen van het product.
- Verificatie van de architectuur tegen de producteisen. Om niet te hoeven wachten tot het productieproces een testbaar product heeft opgeleverd, moet het mogelijk zijn om reeds in het ontwerpproces te kunnen analyseren of de gekozen oplossingen aan de eisen voldoen. Dit kan gedaan worden door het analyseren van de architectuur, de ontwerpdocumenten of de incrementele oplevering van de functionaliteit.
- Verificatie van het gerealiseerde product tegen de producteisen. Dit gedeelte zal voornamelijk bestaan uit module-, systeem- en acceptatietesten.

Bij het realiseren van bovenstaande deelprocessen zal men de volgende uitdagingen moeten aangaan:
Bij het verzamelen van producteisen is het noodzakelijk dat de eisen al direct duidelijk verwoord worden. Een van de meest voorkomende onduidelijkheden heeft bijvoorbeeld te maken met de prestaties van een systeem. Deze worden doorgaans uitgedrukt in een bepaald aantal berichten per seconde dat het systeem kan verwerken. Maar het is dan nog niet duidelijk hoe groot die berichten doorgaans zijn, en onder welke omstandigheden die prestaties behaald moeten worden. Een betere manier is om de functionaliteit uit te drukken in een aantal scenario's die tegelijk plaatsvinden. Dit levert dan meteen de basis voor het testen van het systeem.
Bij het wijzigingsbeheer staat voorop dat na verloop van tijd er nog steeds slechts één representatie van het te bouwen systeem is, ook al is deze een aantal keren gewijzigd (iedereen gaat nog steeds uit van dezelfde versie). Maar daarnaast is er het proces waarbij wijzigingen beoordeeld worden, voordat ze definitief aan de specificaties voor het systeem worden toegevoegd. Zo'n proces is noodzakelijk om degene die de wijziging overweegt ook de consequenties van die wijziging terug te koppelen, niet om de bouwer van het systeem toestemming te vragen voor de wijziging. Het spanningsveld ligt uiteraard in het feit dat de opdrachtgever zo laat mogelijk nog functionaliteit zou willen toevoegen, terwijl hij de prijs voorgeschoteld krijgt in oplevertermijn en mogelijk kwaliteitsattributen van het systeem. Voor de bouwer is het doorgaans moeilijk in te schatten wat die prijs precies is, en moeten er ook andere zaken zoals testbeschrijving, handleiding en detailontwerp aangepast worden. Een eerste benadering was om wijzigingen te groeperen en per groep een gedetailleerde impactanalyse te doen. Dit bleek echter zoveel tijd te vergen dat er zelfs prioriteiten gesteld moesten worden per groep. De les die hieruit geleerd werd is dat het ontwerp in het begin al zodanig opgezet moet worden dat een snelle impactanalyse mogelijk is.
Bij verificatie wordt meestal aan testen gedacht. Op de verschillende manieren

van testen zal in deze case niet worden ingegaan. Testen van software is alleen mogelijk, indien er daadwerkelijk uitvoerbare ('executable') code is gegenereerd. Dat gebeurt pas na het detailontwerp, alhoewel middels incrementele oplevering een deel hiervan in het projectschema naar voren kan worden verschoven. De mogelijkheden hiervoor bij het vervaardigen van nieuwe versies van een bestaand product bleken gelimiteerd tot grafische gebruikersschermen (GUI's) en losstaande modulen. Bovendien kost het aanpassen van de testomgeving meestal net zoveel tijd als het gewoon afbouwen van het systeem. Een andere methode om vroeg in het project te kunnen verifiëren is door middel van het nauwgezet analyseren van het algemene ontwerp en later het detailontwerp. Daarvoor zijn op beide niveaus scenario's beschreven (zie verderop in de case) die op logica en kwantitatieve aspecten worden beoordeeld. Alleen al hierdoor zijn belangrijke missers en 'showstoppers' boven water gekomen die anders vele maanden vertraging hadden opgeleverd, terwijl het ontwerp al op velerlei wijze gebruikt kan worden. Het maken van een dergelijk ontwerp kostte de eerste keer zes à acht weken, maar in volgende versies is alleen aanpassing van het ontwerp nodig.

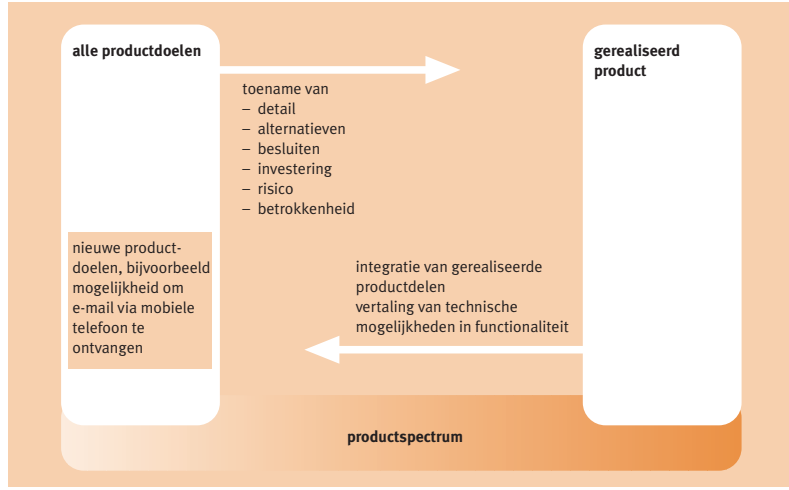
Hoe past dit nu in het uitvoeren van een project? In het volgende deel wordt aangegeven hoe een nieuwe versie van een product vanaf de eerste verzameling van klanteisen doorgevoerd wordt tot aan het product, waarbij de plaats van de deelprocessen is aangegeven.

Omvangrijk computertechniekproject

In figuur 19.4 is aangegeven hoe tijdens de uitvoering van het project een beweging van links naar rechts wordt gemaakt, èn een beweging van rechts naar links, waarbij er groei is in een aantal aspecten die we gemakshalve 'projecthistorie' zullen noemen. In dit geval is een project genomen waarbij een nieuwe versie van een bestaand product moet worden voortgebracht. Terugkijkend op een aantal gerealiseerde projecten blijkt dat de mate van voorbereiding cruciaal is geweest voor het behalen van de projectplanning. Voor een projectleider is het niet altijd even gemakkelijk om het daadwerkelijk bouwen (lees: genereren van softwarecode) uit te stellen, omdat dit vaak een graadmeter van de voortgang is.

Aan de linkerkant van het spectrum zijn alleen aandachtspunten bekend. Dit zijn meestal de zaken die opvallen, dingen die nieuw zijn aan het product ten opzichte van de vorige versie. Men zou deze nieuwe aspecten (functionaliteit, prestaties) met het nieuwe product willen bereiken, waardoor deze als productdoelen aangemerkt kunnen worden.

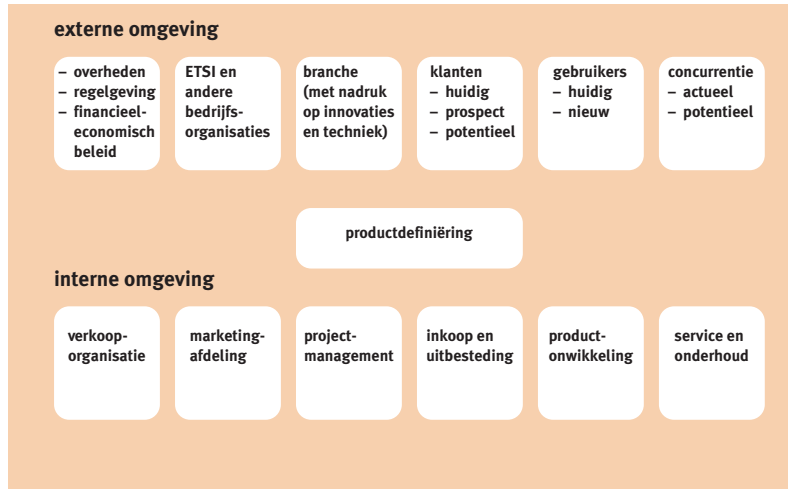
Figuur 19.4
Complexiteit als functie van project-voortgang.



1 De haalbaarheid vanuit technisch of organisatorisch oogpunt is op dat moment nog niet getoetst. Indien een organisatie zo ingericht zou zijn dat bijvoorbeeld de marketingafdeling de productdoelen zou definiëren, zou dat dan voldoende zijn om de ontwikkeling van het nieuwe product in gang te zetten?
Zodra de organisatie met de productdoelen aan de gang gaat, zal er in eerste instantie gekeken worden naar de omvang van het project, en dat hangt weer af van de mate waarin de huidige versie van het product aangepast moet worden (de zogeheten impact). Hoe eerder de impact bekend is, en ook de mate van zekerheid omtrent de impact, hoe minder kans er is op onverwachte tegenvallers.

2 Een impactanalyse op het gehele product (en eigenlijk ook op de organisatie) kan alleen plaatsvinden, indien het gehele product voldoende overzien kan worden, dat wil zeggen voldoende gedocumenteerd is. Indien het product wel in zijn geheel gedocumenteerd is maar alleen op detailniveau, is er dan voldoende tijd voor een goede impactanalyse?
Nadat middels de impactanalyse en een haalbaarheidsstudie voldoende informatie over de omvang en de risico's van het project zijn verkregen, gaat de ontwikkeling van start. Tijdens deze ontwikkeling zal de mate van detail toenemen, en dus zullen ook de alternatieve oplossingen waaruit gekozen moet worden, toenemen.

3 Bij de keuze tussen alternatieve oplossingen zal de volledige consequentie van die keuze pas later blijken, bijvoorbeeld op het integratieniveau (wat is het gevolg voor de betrouwbaarheid van het systeem), of op een verder detailniveau (hoe beïnvloedt de keuze de invoeringsmogelijkheid). Dit zal ertoe leiden dat men een aantal keren van de kant van de invoering van het spectrum moet teruggaan naar de kant van de productdoelen. Ondersteunen de organisatie en de wijze van documenteren en analyseren deze optimalisatie?



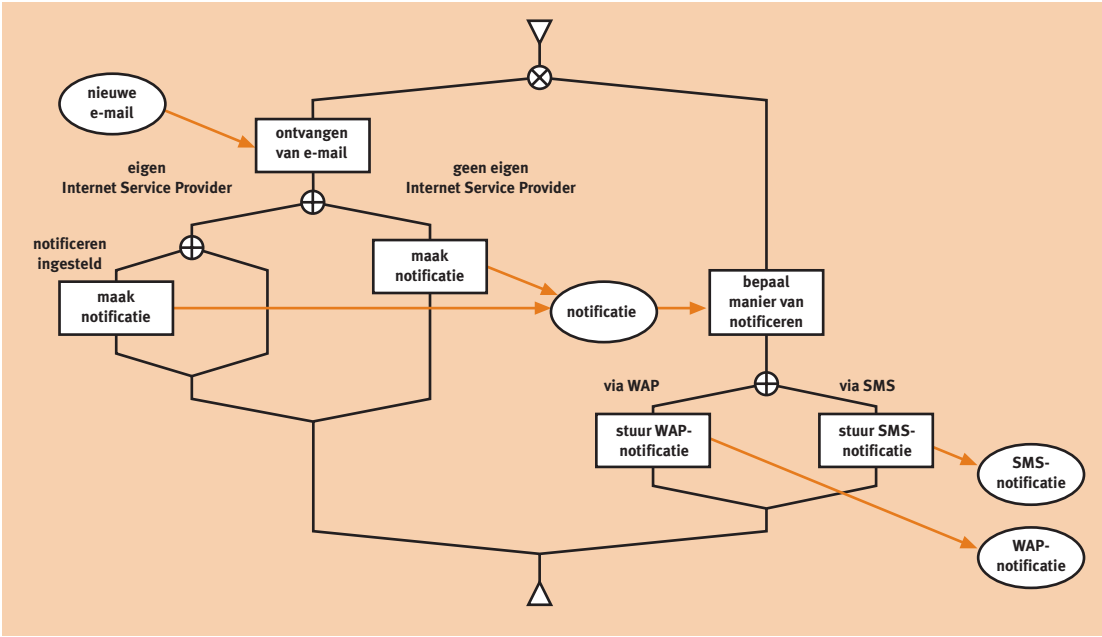
Figuur 19.5
Complexiteit opgelegd vanuit de omgeving.

Alvorens op de gestelde vragen in te gaan, is het goed om eens te kijken hoe de omgeving van dit proces (productdoelen omzetten in een gerealiseerd product) eruit ziet.

De rol van het definiëren van het product is bewust als een centrale rol gekozen. De definitie van het product zal gedurende het maken van de nieuwe versie vele malen aangepast worden. Dit is namelijk afhankelijk van de mate waarin de productdoelen te realiseren zijn.

Ad 1
Voor het toetsen van de haalbaarheid van de productdoelen is tevens nodig:
– De volledige set van productdoelen.
– De volgorde van prioriteit van deze productdoelen.
– De terugkoppeling van de organisatie over de juiste interpretatie van de doelen.
– De omstandigheden waaronder de productdoelen gehaald dienen te worden.

Voorbeeld van een productdoel: “De mobiele gebruiker dient, indien hij dit heeft ingesteld notificatie van nieuwe e-mail via zijn mobiele telefoon te kunnen ontvangen”.
Zodra dit productdoel aan de organisatie zou worden gegeven, ontstaat hopelijk al vrij snel een dialoog, want er is nog een heleboel onduidelijk. Dit zou leiden tot de volgende additionele beschrijving:
“Een gebruiker krijgt een berichtje op zijn mobiele telefoon dat hij een nieuwe e-mail heeft ontvangen. Dit kan zowel een SMS-bericht als een WAP-bericht zijn. Hij moet deze keuze wel ingesteld hebben, en slechts een van beide methoden is mogelijk. Indien de gebruiker geen gebruik maakt van de interservice van de



Figuur 19.6
Complexiteit beheersen door tekenconventies.

netwerkbeheerder maar toch bericht wil ontvangen, dan moet hij doorgifte van nieuwe e-mail bij zijn eigen netwerkbeheerder hebben ingesteld."
Dergelijke verhaaltjes kunnen al vrij snel een behoorlijke omvang gaan aannemen, en toch nog onduidelijkheden bevatten. Een alternatieve methode is weergegeven in figuur 19.6.

Het diagram leest van boven naar beneden. De eerste vertakking geeft een parallel proces aan (x teken). Het systeem ontvangt een e-mail en zoekt uit of de gebruiker een eigen Internet Service Provider (ISP) heeft of niet (het plusteken geeft alternatieve paden aan). Indien de gebruiker notificatie heeft ingesteld, maakt het systeem een notificatiebericht aan dat volgens de rechtertak of via SMS of WAP wordt verstuurd.

Uiteraard zijn er ook andere alternatieven om een dergelijk functioneel diagram te tekenen. Het voordeel van bovenstaande notatiewijze is dat zowel de 'procesflow'-functies als de 'dataflow' is aangeven. Ook is onderscheid gemaakt tussen interne en externe operaties (input van e-mail, output van SMS- of WAP-notificatie).

Ad 2

Stel dat het product wel volledig gedocumenteerd is, maar dat deze documentatie vooral het detailniveau beschrijft. Voor het maken van een impactanalyse moet(en):

- de bedoelde verandering op hetzelfde niveau beschreven zijn als de documentatie;
- de resultaten vertaald kunnen worden naar informatie voor andere partijen, waaronder het management;
- de input van andere partijen ook weer terugvertaald kunnen worden;
- de analyse verhoudingsgewijs een fractie van de bronnen nodig hebben vergeleken met het gehele productproces.

Om die redenen is het nodig dat er voldoende mate van detail is, zoals in het voorbeeld is aangegeven. Maar ook niet teveel detail, zoals detailontwerp of softwarecode. Het op lijn brengen van alle stakeholders gebeurt namelijk veel meer aan de linkerkant van het spectrum. Eventueel corrigeren achteraf vereist dus dat al het werk ervoor ook aangepast moet worden, plus dat er door veel meer detailgegevens gespit moet worden.

Ad 3

Een deel hiervan is al bij ad 2 beantwoord. Maar belangrijk is dat er zowel een productdefinitie aan de linkerkant van het productspectrum bestaat als aan het deel rechts ervan. Indien de verbanden tussen de verschillende niveaus van de productdefinitie goed zijn weergegeven, kan het wijzigen van een detail snel naar een hogere niveaudefinitie getraceerd worden.
Een SMS-bericht heeft een maximumomvang, en een door ETSI gespecificeerd formaat. WAP-berichten zijn echter opgebouwd uit een stroom pakketjes en kunnen dus vele malen langer zijn. Bij de notificatie via SMS stuit men dus op het probleem dat als het oorspronkelijke e-mailbericht meegezonden zou moeten worden, men slechts een klein deel kan sturen. Bij WAP zou die beperking er niet zijn. In de eerste fasen van de ontwikkeling van het product zou men hiermee al rekening kunnen houden. Maar stel dat nu blijkt dat WAP wel degelijk beperkt is, namelijk door de capaciteiten in het netwerk. Dan zou men toch ook aan WAP-berichten beperkingen aan de omvang moeten stellen. Dit is een verandering van de conceptfunctionaliteit die mogelijk ook de beste oplossing voor het probleem is. Zou men alleen een watervalmethode gebruikt hebben, dan zou men allerlei capaciteitsverhogende maatregelen moeten verzinnen om toch aan het oorspronkelijke concept te kunnen voldoen. Nu zijn tenminste partijen als verkoop en marketing betrokken bij het zoeken van de optimale keuze. Zij gebruiken echter het hogere niveaudocument als discussiedocument, omdat daar voor hen de relevantie informatie staat.

Samenvatting

De gebruiker van een mobiele telefoon heeft in korte tijd de beschikking gekregen over een complex stuk techniek. Deze complexiteit komt voort uit de functionaliteit die in de mobiele telefoon zelf zit, maar vooral ook door de integratie van het mobiele netwerk en de mobiele diensten. Bovendien zal de functionaliteit met steeds grotere sprongen toenemen, terwijl de onderliggende complexiteit voor de gebruiker onzichtbaar blijft.
Om de complexiteit te beheersen en betrouwbaar te houden, hebben een aantal Europese landen besloten om van overheidswege de techniek te standaardiseren. Dit heeft geleid tot de oprichting van het European Telecommunications Standards Institute (ETSI) en het volgen hieruit van de GSM- en UMTS-standaarden.
De systemen die binnen het mobiele netwerk te vinden zijn, vormen een onderdeel van een steeds complexere keten waarin naast spraak steeds meer data wordt verstuurd en diensten worden geboden. De mobiele telefoon wordt gebruikt als een terminal die inmiddels meer functionaliteit gaat bieden dan met een pc 15 jaar geleden mogelijk was. Nu komt de functionaliteit echter tot stand via de keten. Betrouwbaarheidseisen liggen echter op het niveau dat men in de telecommunicatiebranche gewend is, en niet op het niveau van de pc.
Deze systemen worden gemaakt door leveranciers van software engineering. De complexiteit, opgelegde standaarden, ketenwerking en geëiste betrouwbaarheid dwingt deze leveranciers tot een ander bedrijfsproces. Bovendien zal dit bedrijfsproces systemen met nog meer functionaliteit in nog kortere tijd moeten gaan leveren.
De complexiteit van het project dat een dergelijk systeem voortbrengt wordt vergroot door de omvang van het product, de omvang van de detaillering van specificatie en integratie, de toenemende interactie met de omgeving en de noodzaak om simultaan met omgevingsbelangen rekening te houden.
Dit bedrijfsproces zal steeds meer aspecten gaan bevatten van ontwikkelingsprocessen in meer traditionele bedrijfstakken waar deze processen reeds volwassen zijn geworden. Een van de manieren om complexiteit te beheersen is het gebruik van processtandaarden, zoals tekenconventies in het specificatietraject.

2

20
Het volledig probabilistisch ontwerp van de stormvloedkering in de Nieuwe Waterweg

prof.dr.ir. H.A.J. de Ridder[1], *ir. J.M. Nederend*[2]

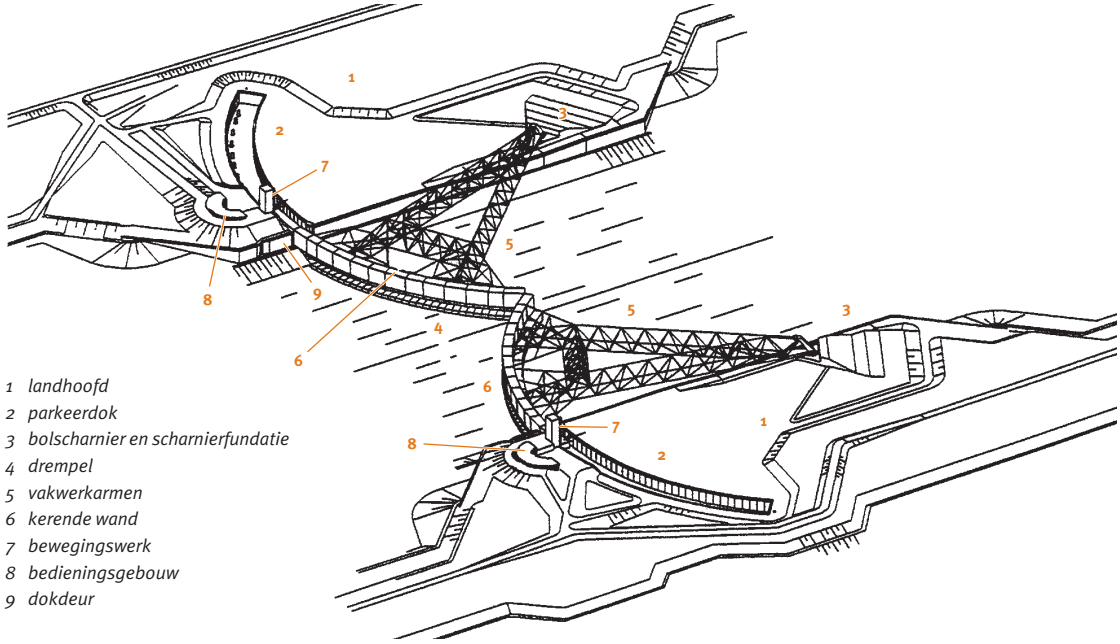
Inleiding

De dijkverhoging van het benedenrivierengebied was het laatste grote project van de Deltawerken. Dat was niet voor niets, omdat het maatschappelijk gezien het meest ingrijpende werk was. Door de noodzaak Rotterdam als grootste haven van de wereld een gegarandeerde open verbinding met de zee te laten behouden, was een omvangrijk dijkverzwaringsprogramma nodig om Zuidwest-Nederland voldoende te beveiligen tegen overstromingen. Deze dijkverzwaringen zouden overigens ten koste gaan van sociaal-culturele en ecologische waarden.

Na een lange periode van groeiende protesten werd een haalbaarheidsstudie gedaan naar een beweegbare stormvloedkering ten westen van Rotterdam in de Nieuwe Waterweg. Met aanvullende werken zou een dergelijke kering ook de vereiste veiligheid kunnen waarborgen. Het bleek dat een stormvloedkering in alle opzichten verkieslijker was dan de voorziene dijkverzwaring. Niet alleen in kosten, maar ook in tijd en in de gevoeligheid voor de zeespiegelrijzing. In 1987 werd een prijsvraag uitgeschreven waarin aannemers werden gevraagd een stormvloedkering te ontwerpen, te bouwen en vijf jaar te onderhouden voor een vaste prijs. De Bouwcombinatie Maeslant Kering (BMK) won de prijsvraag na twee extra ronden en voltooide het werk in 1997.

1 Technische Universiteit Delft,
Faculteit der Civiele Techniek en Geowetenschappen
Postbus 5048
2600 GA Delft

2 Aveco de Bondt bv
Postbus 223
3970 AE Driebergen



Figuur 20.1
Overzicht stormvloedkering Nieuwe Waterweg. Bron: BMK, Rijkswaterstaat.

Ontwikkeling betrouwbaarheidseisen

De veiligheid in het kust- en rivierengebied is gerelateerd aan een toelaatbare kans op overstroming. Deze toelaatbare kans is niet overal dezelfde en is in zekere mate een functie van de potentiële schade voor mens en goed. Ook wordt een dreiging uit zee als ernstiger gezien dan een dreiging uit de grote rivieren. Een dreiging door hoge rivierwaterstanden is immers beter voorspelbaar, waardoor bijvoorbeeld evacuatie een optie is.

Volgens de huidige normen is de toelaatbare overstromingskans voor Rotterdam 1 op de 10.000 jaar en voor Dordrecht 1 op de 2.000 jaar. Als er geen golfoploop en dergelijke zou zijn en de kruinhoogte van (onvoorwaardelijk stabiele) dijken is gelijk aan deze ontwerpwaterstand, dan is de kans op overstromen gelijk aan de hiervoor genoemde waarden. Omdat de werkelijke overstromingskansen nog niet konden worden bepaald, is het begrip Maatgevende Hoog Waterstand (MHW) geïntroduceerd. Onder MHW wordt verstaan de waterstand die behoort bij de toelaatbare overstromingskans die geldt voor de betreffende locatie. Anders gezegd: de MHW van Rotterdam is gelijk aan de waterstand die gemiddeld eenmaal per 10.000 jaar wordt overschreden.

In de praktijk betekent dit dat de kruinhoogte van dijken volgt uit een optelling van (1) MHW, (2) golfoploop, en (3) een waakhoogte. De stormvloedkering heeft als doel de MHW in het achterliggende gebied te verlagen. Hieruit volgt onmid-

dellijk dat de dijken in dit gebied minder hoog kunnen worden. De MHW te Rotterdam was ongeveer 4,80 m+NAP. Met de stormvloedkering wordt gemikt op 3,60 m+NAP. De beoogde verlaging van de MHW te Dordrecht is 0,40 meter.

De vraag is nu een relatie te leggen tussen de gewenste MHW-verlaging en de gewenste betrouwbaarheid (faalkans) van de stormvloedkering. In hoeverre een feilloze kering in staat is een bepaalde MHW-verlaging te bewerkstelligen, is hier niet aan de orde. De volgende formule geeft een indruk van het gewenste faalkansniveau.

P(h › MHW) = P(h › MHW | falen kering) x P(kering faalt) +
+ P(h › MHW | niet falen kering) x P(kering faalt niet)

Hierin is:
P(h › MHW) = kans dat een waterstand h de MHW-waarde overschrijdt
P(kering faalt) = kans dat de kering faalt

De kans op een overschrijding van de gewenste MHW (bijv. 3,60 m+NAP voor Rotterdam) wordt hiermee gekoppeld aan de kans dat de kering faalt. Wanneer de kering zou falen, bestaat er altijd nog een kans dat de waterstand niet boven MHW zal uitkomen. Dit heeft te maken met onder andere een zekere voorspelnauwkeurigheid die maakt dat er vaker wordt gesloten dan strikt noodzakelijk is. De kans dat een waterstand groter dan MHW – gegeven het falen van de kering – optreedt ligt op (met zeespiegelrijzing) 10^{-1} en 10^{-2} per jaar.
Verder wordt even aangenomen dat de kans op een MHW-overschrijding bij een werkende stormvloedkering relatief klein is.

P(h>MHW) ≈ 10^{-1} x P(falen kering) +
(relatief verwaarloosbare term, < 10^{-4} [per jaar])

Hieruit volgt dat:

P(falen kering) ≈ 10^{-3} [per vraag]

Deze formulering geeft enige indruk van de ordegrootte waaraan de faalkans van de stormvloedkering zal moeten voldoen. De werkelijke som is wat ingewikkelder, omdat ook aspecten als voorspelnauwkeurigheid moeten worden meegenomen. Daarbij is gebruik gemaakt van een numerieke probabilistische berekening. Stormen worden gekarakteriseerd door vijf stochasten:

- Stormopzet (m).
- Debiet bij Lobith (m^3/s).
- Stormduur (uur).

– Fase tussen maximumstormopzet en piek van het getij.
– Amplitude van het seiche[3].

Uit deze gegevens zijn vele potentiële stormen te componeren met ieder een kans(je) van voorkomen. Met een hydraulisch model wordt zo'n storm doorgerekend, eenmaal met en eenmaal zonder een keringsoperatie. Als resultaat levert dit – naast vele andere gegevens – per storm een waterstand op bij Rotterdam, enz. De kans dat er inderdaad een keringsoperatie plaatsvindt hangt af van de voorspelnauwkeurigheid en de kans dat de kering niet sluit door allerlei storingen. Je kunt hier nog de kans op niet openen en bezwijken bij optellen, omdat dit ongeveer hetzelfde resultaat oplevert als een niet sluitende kering.

Samengevat levert storm i uit een grote populatie waaruit getrokken wordt twee waterstanden te Rotterdam. De bijbehorende kansen van voorkomen zijn:

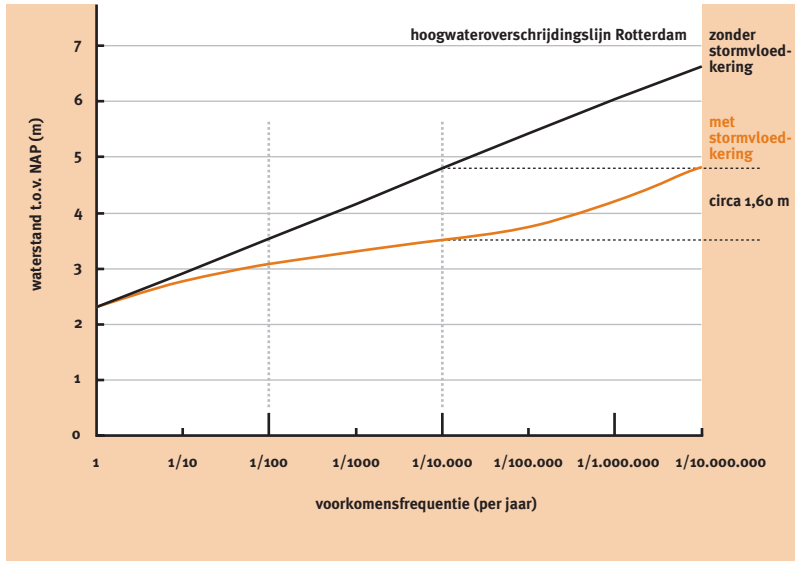
P(hi1) = P(storm i) x P (sluiten | storm i)
P(hi2) = P(storm i) x P (niet sluiten | storm i)

Aldus ontstaat er een matrix van waterstanden en bijbehorende kansen van voorkomen. Door deze op te nemen in een histogram is eenvoudig een overschrijdingsverdeling van de waterstanden te Rotterdam uit te rekenen. Met de kans op niet sluiten kan worden gevarieerd, zodat een beeld ontstaat van deze kans op de MHW. Rijkswaterstaat heeft uit deze beschouwing de toelaatbare kans op niet sluiten afgeleid. Overigens speelt de te bereiken voorspelnauwkeurigheid (van maximumwaterstanden) een zeer belangrijke rol. In figuur 20.2 is de doelstelling van de stormvloedkering grafisch weergegeven.

Ontwikkeling van prestatie-eisen

De Nieuwe Waterweg is een belangrijke toe- en afvoerroute naar de Rotterdamse havenbekkens. De afmetingen van de stormvloedkering volgen daarom voor een belangrijk deel uit de eisen die de scheepvaart stelt. Er is een onbeperkte doorvaarthoogte verlangd bij een vrije doorvaartbreedte van 360 meter. De geëiste waterdiepte bedraagt 17 meter ten opzichte van NAP met opgaande taluds (1:3) naar 10 m-NAP. Uit scheepvaartoverwegingen mag de constructie de stroomsnelheden ter plaatse niet al te veel veranderen. Daarnaast dient vanwege het imago van de Rotterdamse haven de sluitfrequentie zo klein mogelijk te zijn. Het compromis komt uit op een gemiddelde sluitfrequentie van eenmaal per 10 jaar. Met een te verwachten zeespiegelrijzing van

3 Seiches zijn hier lange golven vanuit zee die de eigenschap hebben in havenbekkens te kunnen opslingeren. De periode van de golf ligt tussen circa 10 en 100 minuten. De oorzaak ligt vermoedelijk in meteorologische verschijnselen, al zijn ook zeebevingen niet uit te sluiten.



Figuur 20.2
Doelstelling van de stormvloedkering grafisch weergegeven. Bron: BMK, Rijkswaterstaat.

0,25 meter loopt de sluitfrequentie op naar eenmaal per 5 jaar. Het is wel toegestaan eenmaal per jaar op een vooraf gepland tijdstip een functioneringssluiting uit te voeren.

Om een voldoende waterstandsreductie te bewerkstelligen, dient de kering met voldoende snelheid in en uit de Waterweg te kunnen gebracht. Zowel het openen als het sluiten dient binnen 2,5 uur plaats te vinden. Het sluiten moet onder relatief hoge stroomsnelheden kunnen worden uitgevoerd. De afsluiting hoeft niet volledig te zijn. Een lekoppervlak van orde 100 m^2 is acceptabel; het achterliggende bekken van circa 200 km^2 heeft hiervoor voldoende berging.

De gewenste levensduur bedraagt 100 jaar. Verder mag de constructie de ijs- en slibafvoer slechts in beperkte mate beïnvloeden.

Ontwerp en functioneren stormvloedkering

Het concept en de onderdelen van de kering

De stormvloedkering bestaat uit twee grote sectorvormige stalen deuren. Het cirkeldeel vormt de waterkerende wand en wordt dan ook de kerende wand genoemd. Dit deel bestaat uit holle drijflichamen die met water kunnen worden gevuld. De kerende wand is met vakwerkarmen gekoppeld aan een scharnier. De vakwerkarmen bestaan uit manshoge buizen die de voornamelijk radiale krachten afleiden. Een koppelvakwerk (evenwijdig aan de kerende wand) zorgt ervoor dat tezamen met de kerende wand een ‘hoge’ ligger wordt gevormd die de krachtswerking (en dus het materiaalgebruik) gunstig beïnvloedt.

De vakwerkarmen komen samen in het scharnier dat een bolvormig lichaam is met een diameter van 10 meter. De bol vindt zijn weerstand in de scharnierfundatie. Dit is een op staal gefundeerde betonnen constructie, gevuld met zand en aan de onderzijde voorzien van betonnen 'skirts'. Hiermee wordt voldoende wrijving gemobiliseerd om vooral de horizontale belastingen (tot een orde van 350 MN) te kunnen opnemen. De bol en de kom zijn voorzien van gietijzeren schaaldelen die alleen daar zijn aangebracht waar de krachtswerking dat verlangt. Dit biedt de mogelijkheid om ruimte te creëren voor inspectie en onderhoud van de schaaldelen.

De kerende wand bevindt zich onder normale omstandigheden in een dok, terwijl de vakwerkarmen vrij zijn boven een plateau dat 'droog' op een 2 m+NAP-niveau is gesitueerd. Het dok wordt afgesloten van de Waterweg door een beweegbare dokdeur. Het dok kan worden leeggepompt voor onderhoud en inspectie.
Boven op de kerende wand is een pennenbaan aangebracht. Tevens bevindt zich daar het locomobiel dat de kering horizontaal zal moeten verplaatsen. Het locomobiel heeft zes hydraulische aandrijvingen. Iedere aandrijving kan via een (draaiende) bonkelaar krachten uitoefenen op de pennen van de pennenbaan. Het locomobiel is verbonden via een trekduwstang met een verticale rolwagen. Deze rolwagen kan zich verticaal bewegen tussen de geleidingen van de geleide toren. Op die manier is de locomobiel verticaal vrij en horizontaal gefixeerd (noodzakelijk vanwege de verschillende waterstanden tijdens gebruik). Bij het uit- en invaren van de kerende wand wordt de kering onder de locomobiel weggedraaid.

Het halfronde bedieningsgebouw bevindt zich aan de zeezijde van de kering. Hierin zijn kantoren, werkplaatsen, bedienings- en elektrische ruimten ondergebracht. In het noordelijk bedieningsgebouw bevindt zich een dieselgenerator voor het geval een of beide GEB-aansluitingen zouden uitvallen. Een speciaal aangelegde zinker verzorgt het stroom- en dataverkeer tussen beide zijden van de kering.
Ter weerszijden van de kering zijn in totaal vier waterhoogtemeetopstellingen geplaatst. Het bedienen van de kering is voor een belangrijk deel afhankelijk van de hierin opgestelde meetinstrumenten.

Het keringsproces

In feite kent de kering in de tijd gezien drie fasen (1) rust, (2) inspectie, testen en onderhoud en (3) operationeel gebruik. Op deze plaats wordt alleen de 'standaard' operationele fase behandeld.
De vraag of een keringsoperatie noodzakelijk is hangt af van de voorspelde waterstanden in Rotterdam en Dordrecht. Deze plaatsen fungeren als 'gidsplaatsen'

voor het gehele achterland. Als een zeker alarmpeil wordt overschreden, brengt het Beslis- en Ondersteunend Systeem (BOS) de kering in operationele toestand. Nieuwe voorspellingen worden geanalyseerd om vast te stellen of en wanneer de sluiting nodig is. Enkele uren voor de sluiting wordt de scheepvaart gestremd en de schuiven van de dokdeur geopend, waardoor de waterstand in het dok gelijk wordt aan de waterstand in de Waterweg. Nadat de dokdeuren zijn geopend, wordt gestart met het uitvaren van de kering dat in een half uur kan plaatsvinden.

Volgens een bepaald afzinkscenario worden de kleppen in de kerende wand geopend waardoor de (13) ballastcompartimenten zich vullen. Dit afzinkproces kan worden afgebroken als onverhoopt een negatief verval ontstaat, of als blijkt dat de erosiecapaciteit van het snel stromende water onder de deur onvoldoende is om een gesedimenteerde drempel schoon te spoelen. Op de bodem geland wordt de voorspanning van de kering op de betonnen drempel via een meet- en regelsysteem beheerst. Dit systeem zorgt ervoor dat de fenders[4] niet overbelast raken en de kering zo snel mogelijk na gebruik kan worden opgedreven. Dit laatste is belangrijk, omdat bepaalde natuurverschijnselen een te groot negatief verval kunnen veroorzaken waarvan de resulterende kracht maar in beperkte mate door de scharnierconstructie kan worden opgenomen.

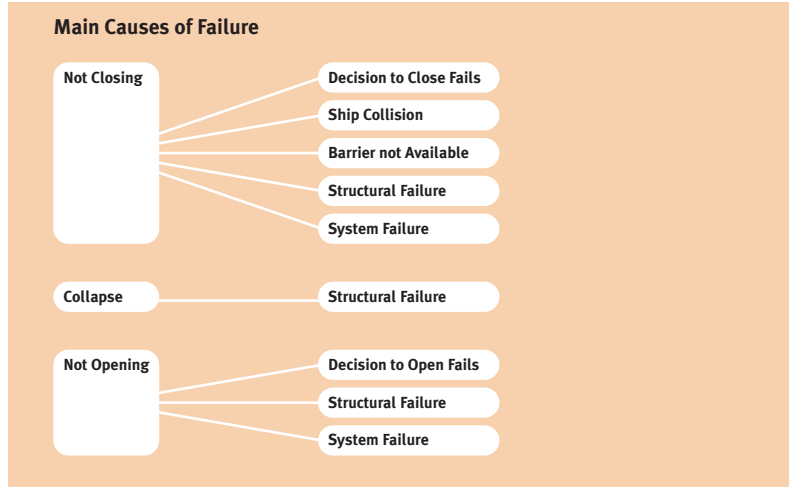
Bij gelijke waterstanden worden de pompen geactiveerd, waarna de kering binnen twee uur wordt opgedreven. Het locomobiel brengt de kering in een half uur terug in het dok.

De volledig probabilistische ontwerpfilosofie

De volledig probabilistische ontwerpfilosofie werd geformuleerd, omdat er een idee was dat op die manier economisch scherp aan de betrouwbaarheidseisen kon worden voldaan. Bovendien had het idee postgevat dat alleen met een dergelijke methode kon worden aangetoond dat daadwerkelijk aan de betrouwbaarheidseisen kon worden voldaan. De centrale faalkanseisen werden ingedeeld naar hoofdonderdelen en -processen en telkens verder onderverdeeld naar lagere schaalniveaus. Deze indeling werd bewerkstelligd met behulp van de drie foutenbomen in figuur 20.3.

De eisen op een hoog niveau boden de mogelijkheid de onderverdeelde eisen zodanig te verdelen dat een min of meer economisch optimum kon worden bereikt. Reeds vanaf de start van het project bleek dat deze mogelijkheid slechts voor een deel kon worden benut. Slechts voor enkele hoofdonderdelen kon de relatie tussen faalkans en kosten (investering) worden afgeleid. Voor de

4 Fenders zijn de schokdempers aan de onderzijde van de kerende wand. Zij bestaan uit vier verticale rubberen cilinders met daaronder een stalen plaat. Het geheel is opgehangen aan zware kettingen. De fenders vangen de golfbelastingen op tijdens landen en opdrijven en bieden een zekere bescherming bij obstakels op de drempel.



Figuur 20.3
Decompositie met behulp van de drie foutenbomen. Bron: BMK, Rijkswaterstaat.

civiele onderdelen (beton) was er een lage gevoeligheid, voor de stalen onderdelen duidelijk meer. De toebedeelde faalkansen voor de civiele onderdelen waren dan ook kleiner (strenger). Binnen het staalwerk is op dezelfde gronden meer faalkans uitgetrokken voor de vakwerkarmen in vergelijking met de kerende wand. De mogelijkheden zijn overigens ook niet volledig uitgenut, omdat het criterium evenwichtigheid (faalkansen niet meer dan een factor 10 tot 100 laten verschillen) gevoelsmatig werd aangehouden.

Voor de E&I-systemen[5] speelde haalbaarheid vaak een rol. Dergelijke systemen behaalden door redundantie een lage (theoretische) faalkans. Er kon een belangrijke optimalisatie in de elektriciteitsvoorziening worden bereikt door een scenarioanalyse. In het (ontwerp)-traject is overigens altijd een ruim reservebudget voor de faalkans aangehouden om tegenvallers (mechanismen, inzichten, optimalisaties) te kunnen opvangen.

Ten aanzien van het aspect betrouwbaarheid werd het ontwerpwerk aangestuurd met behulp van een intuïtieve distributie van toelaatbare faalkansen die met voortschrijdend inzicht werd bijgesteld, al naargelang het gemak waarmee de faalkansen al dan niet werden gehaald. Op deze manier werden de ontwerpers van de onderdelen voorzien van centrale faalkanseisen en mochten zij deze eisen verder distribueren naar de kleinste elementen. Op dat moment leek deze methode op papier haalbaar.

5 E&I-systemen is een verzamelterm voor elektronische en werktuigbouwkundige systemen en instrumentatie.

Evaluatie van de gevolgde probabilistische ontwerpmethode

In de praktijk bleek de voorgestelde werkmethode om met de centrale faalkanseisen om te gaan een pad met positieve en negatieve ervaringen. Dat kwam door een combinatie van factoren:

- De te distribueren faalkansen waren per definitie niet lineair en bleken daardoor niet te verdelen (ze zijn wel te verdelen, maar door niet-lineariteiten en correlaties is het niet zo doorzichtig; in dit proces is eigenlijk de conservatieve bovengrens opgezocht, dus wel veilig maar te duur).
- Er kon tijdens het ontwerpwerk geen beroep gedaan worden op geldende normen voor constructeurs (uiteindelijk is ervoor gekozen via probabilistische methoden de voor constructeurs bekende partiële veiligheidscoëfficiënten en belastinggevallen af te leiden).
- Oversterkte als gevolg van de keuze voor een bepaalde dimensionering kon niet of met veel moeite worden vertaald in extra faalkansruimte.
- De faalkansruimte kon niet altijd op objectieve gronden worden herverdeeld of kostte een bovenmatige ontwerpinspanning.
- De relaties tussen de verschillende hoofdonderdelen, onderdelen, componenten en elementen konden niet adequaat worden meegenomen in het bepalen van de uiteindelijke sterkte.
- De diverse faalmechanismen konden niet op een behoorlijke manier in de faalkansanalyse worden meegenomen.
- De ontwerpmethode ging ten onder in het kleine kansenverhaal voor de kleinste onderdelen. Dit heeft geresulteerd in een zekere oversterkte als gevolg van moleculair probabilisme: hoe kleiner het onderdeel, des te kleiner de toelaatbare kans op falen. Dit werd overigens ook beïnvloed door de schematisering van het systeem. Pas achteraf is een methode ontwikkeld om de kleinste elementen van een seriesysteem op een realistische wijze te definiëren (dus zonder tot een ‘moleculair’ niveau af te dalen).
- Er was vaak weinig statistisch materiaal beschikbaar om de verdelingsfuncties van sterkte en belasting redelijk te toetsen.
- Het bleek niet mogelijk de invloed van veroudering volledig probabilistisch mee te nemen.
- De invloed van de mens (en software) legde een groot (en moeilijk te becijferen) beslag op de totaal beschikbare faalkansruimte.

Op grond van bovenbeschreven problemen werd tijdens het ontwerpproces besloten de volledig probabilistische werkwijze voor enkele constructieve onderdelen te verlaten en over te gaan op een semi-probabilistische benadering. Voor de belastingcombinaties werd in ieder geval wel een volledig probabilistische benadering toegepast. Voor het falen van het systeem werd faalkans-

ruimte toebedeeld aan de hoofdcomponenten. Met die faalkansruimte konden de ontwerpmanagers vrijelijk het ontwerp van de componenten en elementen ter hand nemen.

Conclusies

Het nogal pretentieuze volledig probabilistische ontwerp van de stormvloedkering in de Nieuwe Waterweg is uitgelopen op een interessant leertraject. Dat kwam omdat de betrouwbaarheidseisen zo dominant waren dat gepoogd is het ontwerpproces op een analytische manier alleen daarop te baseren. Iedere ontwerper kreeg als het ware een faalkansruimte toebedeeld waarmee het subsysteem moest worden ontworpen.

Het systeem van toebedeelde faalkansen – de faalkans die in de aanbiedingsfase was afgeleid (uitgerekend) – was op zich niet zo heel slecht. Dan moet het wel gezien worden als een signaleringscriterium. Het ontwerpteam verfijnt en optimaliseert en toetst na verloop van tijd de faalkans. Als de faalkansruimte wordt overschreden, wordt er overlegd met de stafcoördinator faalkansen. Op deze manier wordt ook volgens het 'trial and error'-principe gewerkt, zij het wel op een ingewikkelde manier. Een complex systeem wordt op deze manier toch te complex.

Voorlopig lijkt het het beste om voor het ontwerpwerk van complexe systemen het ontwerpen van onderdelen zoveel mogelijk volgens de geldende normen te doen. Op die manier wordt in ieder geval gebruik gemaakt van langjarige statistiek en de aanwezige ontwerpkennis bij de ontwerpers. Drie zaken zijn van belang. De partiële veiligheidscoëfficiënten en -factoren dienen op probabilistische wijze te worden bepaald. De belastingen op het systeem dienen in ieder geval probabilistisch te worden bepaald. De toetsing op de geëiste faalkans dient op een hoog systeemniveau te worden geverifieerd. Als daarbij blijkt dat de systeembetrouwbaarheid niet voldoende is, moeten die onderdelen die niet sterk genoeg zijn en of voor weinig geld de totale faalkans verkleinen, worden versterkt.

De meeste faalkans ligt bij de mens en de systemen (bedoeld wordt de beslis-, de besturings-, de elektrische en de werktuigbouwkundige systemen). Dit betekent dat meer dan bij de constructieve elementen de faalkans voor een groot deel wordt bepaald door de invulling van opleiding, training, beheer en onderhoud. Deze entiteiten zullen dan ook bepalend zijn voor de duurzaamheid van de faalkans waarop de stormvloedkering is ontworpen.

2

21 Rol overheid bij betrouwbare levering elektriciteit

dr. B.J.M. Ale [1]

De geschiedenis van de elektriciteitsvoorziening in Nederland begint aan het einde van de 19e eeuw in Dordrecht. Een officier uit het leger van de Tsaar begint dan gelijkstroom voor verlichting te leveren met behulp van accu's. Hij verkocht dan ook geen stroom of elektriciteit, hij verkocht licht. De elektriciteitsmaatschappij heette nog lichtmaatschappij en men werd afgerekend op het aantal lampen dat men in huis had.
Pas toen de elektromotor zover was ontwikkeld dat hij kon worden gebruikt, werd elektriciteit ook voor kracht aangewend. Pas toen werd licht elektriciteit. De eerste elektriciteitsmaatschappij was Smit in Slikkeveer. Het was een volledig private onderneming.

1 Dit hoofdstuk is geschreven op persoonlijke titel. Met dank aan N. Ketting.
Rijksinstituut voor Volksgezondheid en Milieu, Laboratorium voor Stralingsonderzoek
Postbus 1
3720 BA Uithoven

Door het toenemende gebruik van elektriciteit voor licht en voor kracht werd elektriciteit steeds belangrijker voor de maatschappij. In de jaren twintig kwamen de overheden dan ook tot de conclusie dat de elektriciteitsmaatschappijen in publieke handen moesten komen. Alle elektriciteitsmaatschappijen werden opgekocht door gemeenten en provincies. Deze maatschappijen werken geheel zelfstandig en de elektriciteitsproductiefabrieken waren niet gekoppeld. Om de transportverliezen te beperken, moest een elektriciteitsfabriek zoveel mogelijk in het midden van het verzorgingsgebied staan, centraal dus. Vandaar dat de elektriciteitsfabrieken centrales worden genoemd. De grote gemeenten hadden ieder hun eigen centrale. De provinciale centrales bedienden de kleine plaatsen en de buitengebieden. De PNEM was de eerste provinciale elektriciteitsmaatschappij.
Langzaam werd de rol die technische en fysische aspecten bij de betrouwbaarheid van de voorziening spelen steeds meer zichtbaar. Om ook bij storingen en onderhoud een ononderbroken levering te kunnen garanderen zou iedere gemeente een tweede centrale nodig hebben, een redundantie dus van 100%, maar niet iedere gemeente beschikte over zo'n reserve, zodat het licht nog wel eens uitging. De centrales waren in de beginjaren overigens niet zo groot: 1,5 kW was al veel.
Als vanzelf rees in gemeenten de vraag of het niet handiger zou zijn de reservecentrale van de naburige gemeente als reserve te gebruiken in plaats van zelf een tweede erbij te plaatsen. In zo'n geval is de redundantie nog maar 50%. Deze notie luidde het begin in van het gekoppeld bedrijf. Hoe groter het gezamenlijk elektriciteitsvermogen, hoe minder redundantie nodig is.
Het beheer van de centrales en van de provinciale koppelnetten was in handen van de provinciale en gemeentelijke bedrijven. Het rijk stond daar buiten. In feite werd de elektriciteitsvoorziening beheerd door de Vereniging van Directeuren van Elektriciteitsbedrijven in Nederland (VDEN). De directeuren waren ambtshalve lid. De VDEN regelde bijna alles: de standaarden, de aansluitingen, de frequentie (50 Hz) en het voltage. Alleen als dit soort zaken netjes waren geregeld, konden de netten immers worden gekoppeld. In het begin (aan het einde van de jaren twintig) ging het dan ook langzaam. Tot aan de Tweede Wereldoorlog bleef het gekoppeld bedrijf meer incident dan regel.
De rijksoverheid sloeg deze ontwikkeling met enige verbazing gade. Echter Nederland is bestuurlijk gezien nog steeds meer een vereniging van provincies dan een staat, met daardoor een relatief zwak landelijk bestuur.Vergunningen voor elektriciteitsbedrijven werden door de provincies en niet door het rijk verleend. Dit spanningsveld tussen gemeenten (VNG, Vereniging van Nederlandse Gemeenten) en provincies (IPO, Interprovinciaal Overleg) enerzijds en het rijk anderzijds bestaat op zeer veel terreinen, en dus ook op het gebied van de elektriciteitsvoorziening.

Begin jaren dertig begint men het ontbreken van enige regelgeving op nationaal gebied als storend te ervaren en wordt er een proces op gang gebracht om een elektriciteitswet tot stand te brengen. Nadat diverse staatscommissies daarop hun krachten hadden beproefd, komt deze wet in 1938 tot stand. Maar hij wordt nimmer in het staatsblad afgedrukt, de provincies zijn namelijk tegen zonder dat overigens ooit duidelijk is geworden wat daarvan de reden is. Die wet is dus nooit van kracht geworden. Alleen het KEMA-keur krijgt echt een wettelijke basis.
Dan volgt de Tweede Wereldoorlog en wordt de infrastructuur nagenoeg volledig verwoest. Na de oorlog wordt de reconstructie krachtig ter hand genomen. Niet door de bedrijven, maar door de VDEN, de vereniging van directeuren die weliswaar ambtshalve, maar niettemin als persoon lid zijn van deze vereniging en samen de bedrijfstak bestuurden.
In 1947 besluit men dat incidenteel gekoppelde bedrijven weliswaar prima werken, maar dat door de koppeling van alle netten in heel Nederland doelmatiger gewerkt kan worden. Een landelijk koppelnet zou tot maximale betrouwbaarheid van de voorziening leiden tegen de laagst mogelijke kosten.
Hoewel de leden van de VDEN het goed met elkaar konden vinden, was het onderlinge vertrouwen weer niet zo groot dat men het er over eens kon worden welk bedrijf bij het tot stand brengen van het landelijke koppelnet het voortouw zou krijgen en welk bedrijf voor de technische uitvoering van het koppelnet zou moeten zorgen.
De bedrijven richtten daarom de SEP, de Samenwerkende Elektriciteitsproductiebedrijven op. De SEP had als taken het realiseren van het landelijke koppelnet en het voeren van het secretariaat van het samenwerkingsverband. De SEP ging aan het werk, ondergeschikt aan de bedrijven en zonder wettelijk kader; de elektriciteitswet was er immers nooit gekomen.

Het gekoppelde bedrijf is sindsdien gegroeid tot de huidige capaciteit. Een totale koppeling van Nederland en België samen: 30 GW in eenheden van ongeveer 500 MW zou kunnen volstaan met een redundantie van ruim 20%. Dit is er echter nooit van gekomen, omdat de daarvoor benodigde 'fusie' van SEP en Electrabel nooit tot stand is gekomen. Als het koppelnet nog uitgebreider zou worden, ontstaan er sturingsproblemen van een andere orde die tot minder efficiëntie leiden.
In 1952 kwam men tot de conclusie dat een Europees koppelnet nog efficiënter zou zijn en de UCPTE werd opgericht: de Union pour la Coordination de la Production et Transportation d'Electricité. Sindsdien zijn alle netten van Denemarken tot Italië gekoppeld en is het grootste gekoppelde net ter wereld tot stand gebracht. Nederland speelde in die ontwikkeling een voortrekkersrol.
Inmiddels was de EGKS (Europese Gemeenschap voor Kolen en Staal) en later de EEG (Europese Economische Gemeenschap) opgericht. In het verdrag van

Rome echter komt energie niet voor en blijft dus een kwestie van subsidiariteit. De lidstaten dienen dat zelf – desgewenst onderling – te regelen.

Met de groei van het koppelnet werd meer mogelijk dan alleen het verhogen van de betrouwbaarheid. Het probleem met elektriciteit is immers dat het niet kan worden opgeslagen. Het moet steeds worden geproduceerd, wanneer het wordt gevraagd. Overdag is de vraag twee maal zo hoog als 's nachts, waardoor de inzet van centrales een relatief slecht rendement heeft. Het is efficiënter een centrale op vollast te laten draaien of af te schakelen. Een groot net heeft ook veel centrales. Daardoor kan men kiezen hoeveel en welke centrales op welk moment worden ingezet. Dit maakt het mogelijk de vraag naar en de productie van elektriciteit grotendeels te ontkoppelen. De centrales hoeven ook niet meer op een centrale plaats te staan. Men kan dus geschikte locaties zoeken, waar brandstoffen en koelwater voorhanden zijn. Het op deze wijze optimaliseren van de plaats waar centrales moeten komen leidt tot een verdere verlaging van de kosten.
Bovendien maken de kosten van brandstof 50 tot 85% van de productiekosten uit, zodat daarmee zo efficiënt mogelijk moet worden omgesprongen. De brandstofkosten variëren sterk per type centrale. Kolen- en kerncentrales zijn qua brandstof het goedkoopste, terwijl gasturbines het duurste zijn. In een gekoppeld net kan men naarmate de vraag toeneemt eerst de goedkope en pas later de duurdere centrales inzetten. Ook dat levert aanzienlijke besparingen op. Bij zo'n wijze van bedrijfsvoering echter verliezen de afzonderlijke bedrijven hun autonomie: immers de efficiëntie van het totale net is bepalend voor de vraag wie wanneer stroom mag produceren. Dit stuitte op veel weerstand bij de VDEN. Immers met een landelijke economische optimalisatie zou de dienst in Arnhem (bij de SEP) worden uitgemaakt en niet meer bij de afzonderlijke bedrijven. De aanpak van de efficiëntie leverde echter zo veel winst op dat men – zij het mokkend – akkoord ging.

In Nederlandse bedrijven was tot de jaren veertig warmtekrachtkoppeling normaal. Tot ver in de jaren vijftig blijft de in de loop van de dag sterk variërende huishoudelijke vraag naar elektriciteit dominant in de openbare voorziening. In die periode ontwikkelt Nederland zich mede als gevolg van de vondst van aardgas van een handels- en landbouwnatie naar een industrienatie met een industrieel pakket dat buitengewoon energie-intensief is, zoals raffinage, chemie, metaal en intensieve land- en tuinbouw.
De toenemende vraag leidde tot de noodzaak meer centrales te bouwen. Als gevolg van het koppelnet was het niet vanzelfsprekend welk bedrijf de centrale mocht bouwen. De VDEN wees centrales aan bedrijven toe. Het Rijk vond het toch minder aangenaam dat deze toewijzing geheel in handen was van een vereniging van provinciale en gemeentelijke bedrijven. Er werd dan ook een conve-

nant tussen het Rijk en de SEP tot stand gebracht, waarin werd afgesproken dat er een elektriciteitsplan zou komen, waarvan de locatie van de centrales onderdeel zou uitmaken. Dit plan behoefde de goedkeuring van de minister van Economische Zaken, maar niet van het parlement.
In de jaren zestig vlakt de groei wat af, zodat er tussen de bedrijven wat grimmiger werd gestreden om de toewijzing van centrales.

Dan dient zich kernenergie aan. Dit leidde ertoe dat de toenmalige minister van Economische Zaken Van Aardenne op grotere eenheden wilde overgaan en de lappendeken van kleine en grote bedrijven geheel wilde vervangen. Dit idee in combinatie met de energiecrisis van de jaren zeventig leidde tot de conclusie dat de elektriciteitsvoorziening van te groot maatschappelijk belang is om het bij een convenant tussen rijk en een verzameling bedrijven te laten. Er moest een elektriciteitswet komen. Daarbij werd aangevoerd dat de op winst beluste elektriciteitsproducenten de prijs van stroom hadden opgedreven, hoewel toen 85% van de opwekkingskosten brandstofkosten waren en het verwijt dus grotendeels onterecht was.
Het Rijk brengt dan een ontwerp van wet voor de landelijke productie en het transport van elektriciteit tot stand: PROTRANS. De VDEN, die een eind aan hun macht zagen komen, kregen echter de Tweede Kamer op hun hand. Daar kwam bij dat de provinciale en gemeentelijke autonomie in het tarievenbeleid verloren zou gaan, wat provincies en de gemeenten veel geld opleverde, en bovendien ook als politiek instrument kon worden gebruikt. Men kon immers op gemeentelijk of provinciaal niveau bepalen of de tarieven zo zouden worden opgezet dat bedrijven ook voor het huishoudelijk gebruik betaalden, of juist omgekeerd.
De langdurige onderhandelingen en besprekingen die daarop volgden, leidden in 1986 tot het besluit PROTRANS te laten varen. Wel werd door de Tweede Kamer een aantal beslissingen genomen:

- Het aantal productiebedrijven wordt teruggebracht tot 3 à 5 bedrijven.
- SEP wordt dirigerend in plaats van coördinerend.
- SEP en de productiebedrijven moeten functioneren als één bedrijf.
- Er komt een beleidsmatige scheiding tussen productie en transport.

Er komt dus niet een productie- en transportbedrijf. In 1989 verschijnt deze regeling in het Staatsblad en is daarmee van kracht. Er komen 4 productiebedrijven.
Dan blijkt dat de scheiding tussen productie en transport een groot nadeel had. Immers, de totale productiecapaciteit was door de efficiëntiemaatregelen van de jaren daarvoor min of meer op het minimum dat nodig was voor een stabiele voorziening. Er was dus de facto geen concurrentie, hetgeen een lage prijs in ieder geval niet garandeerde. Men gaf daarom de SEP de mogelijkheid stroom te importeren, zodat er concurrentie kwam tussen de vier productiebedrijven en

de SEP. Vervolgens gaf men de distributiebedrijven de mogelijkheid om zelf warmtekrachtcentrales tot 50 MW per eenheid te installeren, die eerder in onbruik waren geraakt vanwege de enorme efficiëntie en bedrijfszekerheid van de gekoppelde elektriciteitsopwekking.

In al deze pogingen concurrentie tot stand te brengen had men echter het effect van het Europese koppelnet onderschat. De concurrentie kwam er wel, maar niet tussen Nederlandse bedrijven onderling, maar tussen Nederlandse bedrijven en het buitenland. De gefragmenteerde Nederlandse bedrijven bleken niet opgewassen tegen de veel grotere en daardoor efficiëntere buitenlandse bedrijven. Voor de distributiebedrijven kwam stroom steeds meer als vanzelfsprekend uit kabel en stopcontact, zonder dat men zich voor productieaspecten interesseerde.
De fragmentatie in Nederland nam inmiddels alleen maar toe. De beperking van 50 MW per eenheid voor warmtekrachtkoppeling werd omzeild door de oprichtingen van een 'warmtekracht BV', die voor 98% eigendom was van een distributiebedrijf en voor 2% eigendom van een industrie, die talloze individuele warmtekracht (w/k)-eenheden installeerde. Dit was vooral voor de industriële partner zeer aantrekkelijk. De financiering viel immers buiten de boekhouding en er werd door het Rijk subsidie verleend. Zo werden de subsidies niet gekoppeld aan het rendement, maar uitsluitend aan het geïnstalleerde vermogen, zodat ook grote inefficiënte eenheden subsidiabel zijn. Bij deze w/k-eenheden blijft stroom over die tegen gunstige terugbetaalregelingen aan het net kon worden terugverkocht, waardoor de economische positie van de Nederlandse productiebedrijven verder werd ondergraven.
Ook het elektriciteitsplan droeg in deze omstandigheden bij aan de ondergraving van de positie van de Nederlandse productiebedrijven. Immers, de SEP moest de betrouwbaarheid van de levering voor 20 jaar garanderen, terwijl de doorlooptijd van de bouw van een centrale 10 jaar is. De Nederlandse overheid had inmiddels een deel van haar kaarten op kernenergie gezet en daarvoor 12 locaties aangewezen, waardoor de beste locaties voor de bouw van conventionele centrales niet beschikbaar waren. Zou men centrales op de wel beschikbare plaatsen bouwen, dan zou de elektriciteit daaruit duur zijn ten opzichte van het buitenland. Men wachtte dus met het bouwen van conventionele centrales, totdat de beslissing over de plaats van de kerncentrales zou zijn genomen, waardoor de overige toplocaties zouden vrijkomen. Een beslissing die uiteindelijk nooit zou worden genomen.

Om bij een stijgende vraag en bij het ontbreken van mogelijkheden om op tijd bij te bouwen aan de eis van een gegarandeerde levering van 20 jaar te kunnen voldoen, besluit men stroom in het buitenland te kopen. Vanuit de productiebedrijven gezien is immers het koppelnet een soort stopcontact verbonden met

een virtuele centrale met (schijnbaar) onbeperkte capaciteit. Er wordt een contract met onder andere Frankrijk gesloten.

Met de groei van de (gesubsidieerde) warmtekracht, die buiten het elektriciteitsplan valt, dreigt een overschot aan elektriciteit. SEP kan niet over deze informatie beschikken en die in ieder geval niet al bij de planning gebruiken, waardoor het toekomstig benodigde vermogen niet goed meer kan worden ingeschat. Dat lijkt in eerste instantie goed voor de prijsvorming. Elektriciteit kan dan op een concurrerende markt worden verhandeld. Er ontstaat bij de Europese Commissie een plan om een Europese elektriciteitsmarkt op te richten waar stroom kan worden verhandeld, net als aardbeien of aandelen.
Hoewel deze elektriciteitsbeurs er niet komt, wordt wel een Europese elektriciteitsrichtlijn tot stand gebracht. Bij de totstandkoming daarvan hebben zowel het Europarlement als de Europese Commissie het belang ingezien van het element van nutsvoorziening dat aan elektriciteit hangt en dat elektriciteit daarmee doet verschillen van andere commerciële producten. Dit is mede ingegeven door een arrest van het Europese Hof in Straatsburg in een zaak, waarin een private dienst een nationaal postbedrijf wilde beconcurreren op de winstgevende onderdelen ervan, namelijk de bedrijfspost. Door concurrentie zou het postbedrijf niet meer in staat zijn de winsten uit de bedrijfspost gedeeltelijk aan te wenden om de verliezen die de particuliere postbezorging oplevert te compenseren, waardoor deze dienst zou moeten worden opgeheven. Het Hof bepaalde dat het element van maatschappelijk belang hier diende te prevaleren en dat het betrokken land daarom beperkingen kon opleggen aan de concurrentie.
Voor wat betreft de elektriciteitsvoorziening is dit punt vastgelegd in artikel 21 van de elektriciteitsrichtlijn.

De Nederlandse distributiebedrijven worden inmiddels steeds zelfstandiger en willen concurreren. Electricité de France, een staatsbedrijf, is echter zes keer zo groot als alle elektriciteitsbedrijven tezamen in Nederland. Bovendien is het koppelnet niet voor de handel bedoeld, maar voor het leveren van betrouwbaarheid tegen de minste kosten. Voor handel in elektriciteit is een overcapaciteit aan transportmogelijkheden nodig. Die capaciteit is er niet en met kosten van 1 à 2 miljoen gulden per kilometer en het ontbreken van geschikte trajecten is het onwaarschijnlijk dat die capaciteit er zal komen. Zeker als in aanmerking wordt genomen dat het transporteren van elektriciteit over afstanden groter dan 600 à 800 km duurder is dan het transport van de primaire brandstof.
Niettemin trachten de elektriciteitsproducenten hun krachten te bundelen tegen de grote buitenlanden door het oprichten van een grootschalig productiebedrijf. Hoewel vlak voor Kerstmis 1997 alles in kannen en kruiken leek, is die bundeling uiteindelijk toch niet doorgegaan.

In de nieuwe elektriciteitswet komt productie niet meer voor. De wet gaat uit van de gedachte dat elektriciteit handelswaar is die vrij beschikbaar is. Men is vergeten dat de betrouwbaarheid van de voorziening niet vrij te koop is, en ooit de reden was om de voorziening in overheidshanden te brengen. De wet staat de overheden toe de distributiebedrijven te verkopen. Deze bedrijven zijn wel verplicht iedereen die dat wil van een aansluiting te voorzien, maar betrouwbare levering van elektriciteit is niet verplicht.
Drie van de vier productiebedrijven zijn inmiddels aan buitenlandse bedrijven verkocht. Veel aandeelhouders van distributiebedrijven overwegen hetzelfde te doen. Het toezicht op de sector en vooral de toegang tot de netten is nog niet goed geregeld. Dit is de reden dat de verkoop van de netten aan private partijen nog niet is toegestaan. De Mededingingsautoriteit kan alleen achteraf maatregelen nemen.
Hoewel de minister van Economische Zaken volgens de elektriciteitswet een maximum aan de afleverprijs van elektriciteit kan stellen, kan hij dat in feite niet doen, wanneer de productiebedrijven niet in overheidshanden zijn. Immers, dan worden de distributiebedrijven vermalen tussen de producenten, die de inkoopprijs van de distributiebedrijven kunnen bepalen en de maximumafleverprijs. Dan dreigt faillissement voor het distributiebedrijf, die dan niet meer kan leveren.
In zekere zin keert daarmee de situatie van 1920 terug. De elektriciteitsvoorziening is van zeer groot maatschappelijk belang, maar de private ondernemingen kunnen geen betrouwbare levering meer garanderen.

Zo'n halve eeuw geleden werd de elektriciteitsvoorziening door de overheid uit private handen overgenomen, omdat marktwerking leidde tot lokale optimalisatie in plaats van optimalisatie van de voorziening voor het land als geheel. Vooral de gegarandeerde levering tegen een lage prijs was daarbij in het geding. De teruggave van de elektriciteitsvoorziening aan private handen brengt het risico met zich mee dat de afwegingen van de verschillende marktpartijen leiden tot een landelijk beschouwd suboptimaal systeem waarbij levering niet gegarandeerd is en de prijs niet de laagst mogelijke meer is.

2

22 Betrouwbaarheid en kwaliteit in de gezondheidszorg

dr. M.J. van Duin[1], *mr. A. Oosterlee*[2]

Inleiding

Ongelukken doen zich dagelijks voor. Op de werkplek, in de eigen woonomgeving, in het verkeer en ook in de gezondheidszorg. In dit hoofdstuk worden laatstgenoemde soorten van ongelukken besproken. Grotere incidenten en ongevallen in de gezondheidszorg krijgen op het moment dat ze openbaar worden vaak veel aandacht. Onmiddellijk na dergelijke zaken staan de camera's voor het betreffende ziekenhuis en komen allerlei deskundigen om commentaar te geven. Toch wil dat niet zeggen dat er met de regelmaat van de klok in de media verhalen over dergelijke zaken verschijnen. Integendeel zelfs. Het is zo langzamerhand duidelijk aan het worden dat slechts een zeer klein percentage van dergelijke incidenten uiteindelijk in de openbaarheid komt.

1 Universiteit Leiden, COT Crisis Onderzoek Team
Lange Voorhout 26
2514 EE Den Haag

2 Universiteit Leiden, Leids Universitair Medisch Centrum
Postbus 9600
2300 RC Leiden

Wanneer onderzoek wordt verricht naar ongelukken in de gezondheidszorg, kan een breed scala aan incidenten worden onderscheiden, variërend van een minder geslaagde operatie tot het verstrekken van het verkeerde medicijn. Er wordt wel een onderscheid gemaakt tussen 'overuse, underuse and misuse of the health care system' [Kohn, 1999]. Naast fouten in het medisch handelen of nalaten ervan doen zich ook ongevallen voor in instellingen van de gezondheidszorg die geen of nauwelijks een relatie hebben met medisch handelen. Een patiënt kan uitglijden in de douche van het verzorgingshuis; een verpleegkundige kan zich bezeren aan een injectienaald.

Er zijn veel rapporten en boeken geschreven over medisch handelen en medisch falen. In het kader van dit project willen wij in dit hoofdstuk kort twee cases behandelen waarbij zich problemen voordeden met medische apparatuur. De eerste betreft een computerprogramma dat het gehele logistieke proces van bloedmetingen bewaakt; het tweede gaat over een driewegkraantje. Het is niet vreemd dat juist materiaalfouten en problemen met medische apparatuur in de wereld van de gezondheidszorg tot de verbeelding spreken. Een dergelijk incident kan immers verstrekkende gevolgen hebben.
Hoewel deze twee cases de aanleiding waren voor dit artikel hebben wij ervoor gekozen niet de twee cases centraal te stellen, maar juist het model om dergelijke cases te analyseren. Ook willen we de ontwikkelingen in en de context van de medische sector in kaart brengen.

Twee cases

De hier gepresenteerde cases vormen een compilatie van verschillende op waarheid berustende voorvallen.

Bloedgroepverwisseling

Op dinsdag 14 november 1995 meldt de directeur van ziekenhuis A telefonisch aan de Inspectie voor de Gezondheidszorg (IGZ) dat zich een calamiteit heeft voorgedaan bij een operatie van een 45-jarige vrouw. Vermoedelijk zijn bij de vrouw eenheden erytrocyten van een verkeerde bloedgroep toegediend. Een dag later overlijdt de vrouw. Een strafrechtelijk onderzoek wordt gestart.

Enkele dagen later meldt de organisatie die verantwoordelijk is voor de productie en uitgifte van bloedproducten aan de IGZ dat in twee ziekenhuizen problemen zijn geconstateerd bij het inlezen van de bloedgroepbarcode. Op het scherm van de computer verschijnt een andere bloedgroep dan op het etiket staat gedrukt. De leverancier van het softwaresysteem waarschuwt mede op verzoek van de IGZ alle ziekenhuizen die het zelfde softwaresysteem gebruiken.

Enkele dagen later meldt de leverancier dat het probleem van de barcodes is opgelost en dat al haar klanten een softwarematige oplossing krijgen opgestuurd. Wederom enkele dagen later wordt bekend dat zes maanden voor het incident zich in ziekenhuis B een deels vergelijkbaar voorval voordeed. Hierbij bleek een verwisseling van de bloedgroep te zijn opgetreden, mede omdat de barcodesticker van de ene patiënt op het bloedmonster van een andere patiënt was geplakt. Corrigerende handelingen mochten niet baten. De patiënt overleed.

Inmiddels is duidelijk dat inderdaad verkeerde eenheden erytrocyten (rode bloedcellen) waren toegediend. Er was een verkeerde bloedgroepuitslag in de computer ingevoerd, nadat overigens uit laboratoriumonderzoek wel de juiste bloedgroep was vastgesteld. Het bleek te gaan om een incompatibele bloedgroep. Ook andere routinematige controlemechanismen bleken niet te functioneren. Hoewel de fout al zeer kort na de operatie was ontdekt, leveren de verrichte corrigerende handelingen nadien uiteindelijk geen positief resultaat meer op.

Met een relatief simpele typefout is deze calamiteit tot op zekere hoogte te verklaren. Uiteraard roept deze vergissing enkele achterliggende vragen op die zich primair toespitsen op drie zaken: 1. hoe is het systeem van invoer, controle en dergelijke in het ziekenhuis georganiseerd en in hoeverre was men op de hoogte van dergelijke kwetsbaarheden van het computerinformatiesysteem; 2. waarom corrigeert het computersysteem de gemaakte fout niet automatisch; en 3. wat is de relatie met de gebeurtenis in ziekenhuis B en wat is naar aanleiding hiervan gedaan (geleerd)?

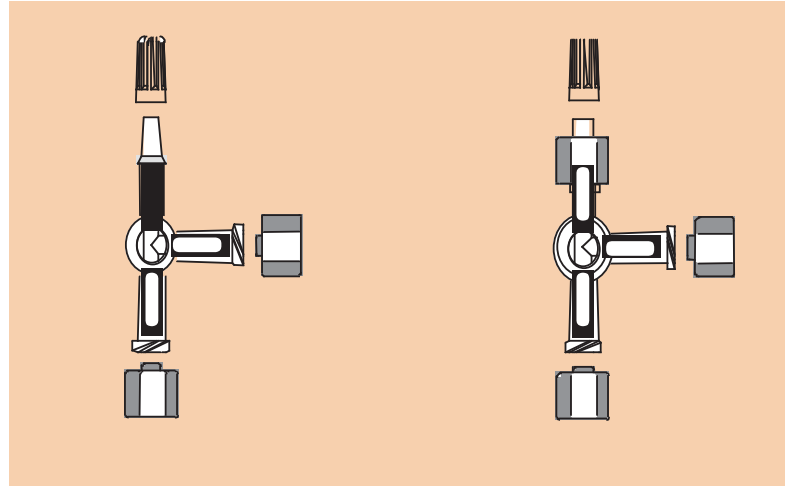
De eerste vraag kan een nader antwoord geven op de loop der gebeurtenissen en bijdragen aan het verkrijgen van een meer compleet beeld. De tweede vraag is uiteraard relevant vanwege het centrale thema van dit project over de rol van techniek, technisch falen en de relatie tussen mens en techniek. De directeur van ziekenhuis A gaf aan het IGZ aan dat het betreffende computerinformatiesysteem zijn medewerkers onvoldoende beschermde tegen menselijke fouten.

De derde vraag gaat in op het thema van eerdere signalen en waarschuwingen en het lerend vermogen. De directeur van ziekenhuis A gaf kort na de calamiteit aan dat het hem verbaasde dat de IGZ, die ook de calamiteit in ziekenhuis B onderzocht, niet heeft gecommuniceerd naar alle ander relevante ziekenhuizen. Wel blijkt dat een medewerker van ziekenhuis B telefonisch contact heeft gehad met een medewerker van ziekenhuis A.

Driewegkraantjes

Als het omgaan met materiaalfouten wordt gezien als maat van de betrouwbaarheid van een technisch systeem, wordt al snel gedacht aan high tech-apparatuur als een pacemaker, radiodiagnostische apparatuur of bijvoorbeeld een beademingsapparaat. De betrouwbaarheid van apparatuur is in belangrijke mate afhankelijk van de wijze waarop de gebruiker met het apparaat omgaat en hoe het in de organisatie wordt ingepast. Dit moge blijken uit de hiernavolgende case over een nieuw geïntroduceerd driewegkraantje voor infuussystemen.

Een driewegkraantje is een kunststof koppelstukje dat buisjes verbindt tussen een infuusnaald die in een patiënt is ingebracht en toe te dienen infuusvloeistoffen. Omdat het koppelstukje dat aan de infuusnaald wordt vastgemaakt zich vertakt in drieën, is het mogelijk om gelijktijdig maximaal drie infuuszakken of pompspuiten aan het kraantje te koppelen. Driewegkraantjes worden vooral gebruikt op plaatsen in het ziekenhuis waar patiënten behandeld worden met verschillende infusen, bijvoorbeeld operatiekamers, intensive care-afdelingen en afdelingen waar kankerpatiënten chemotherapie ontvangen.



Figuur 22.1
Driewegkraantje.

Incidenten

In een periode van een jaar werden aan de Meldingscommissie Incidenten Patiëntenzorg van een ziekenhuis achttien incidenten gemeld over het lekken van infusievloeistof rond driewegkraantjes. Deze commissie is een intern kwaliteitsorgaan van ziekenhuizen, verplicht gesteld door het Staatstoezicht op de Volksgezondheid. Medewerkers uit het ziekenhuis melden op vrijwillige basis incidenten bij patiënten aan deze commissie, zodat de organisatie hiervan kan leren. De meldingen kwamen van zes verschillende afdelingen. Drie van de zes afdelingen bleken afdelingen te zijn waar infusietherapie werd verricht met zeer agressieve middelen tegen kanker (chemotherapie), waardoor niet alleen risi-

co's voor de patiënt maar ook voor het personeel ontstonden. In een enkel geval bleek dat ten gevolge van lekkage te weinig effect van een bepaald toegediend medicament werd gezien. Dit herstelde op het moment dat de lekkage werd gecorrigeerd.

Na signalering van de lekkages werden de defecte kraantjes volgens de in het ziekenhuis geldende richtlijn door de betreffende afdeling aan de Centrale Sterilisatie Dienst gestuurd die verantwoordelijk is voor het verzorgen van eventuele 'recall'-procedures bij geconstateerde defecten aan steriele medische hulpmiddelen. Analyse door deze dienst liet in een aantal gevallen beschadiging van de buitenzijde van de driewegkraantjes zien, maar men vond geen oorzaak. Een recall was (nog) niet aan de orde.

Omdat de melders aangaven dat het om een nieuw type kraan ging, werd door de Meldingscommissie Incidenten Patiëntenzorg nagegaan welke criteria waren gehanteerd bij de keuze voor het nieuwe type driewegkraan en op welke wijze de introductie van het driewegkraantje had plaatsgevonden. Deze kraantjes werden reeds jaren in veel ziekenhuizen in binnen- en buitenland gebruikt. Hierbij waren geen problemen bekend. Dit was onder andere nagevraagd in het landelijk gebruikersoverleg waaraan de meeste ziekenhuizen in Nederland deelnemen.
Alle medewerkers bleken van een speciaal daarvoor aangestelde functionaris instructies te hebben gekregen over de wijze waarop de nieuwe kraantjes dienden te worden gebruikt. Hierbij deden zich geen problemen voor. Wel viel het de gebruikers op dat bij het vastdraaien van infuusslangen op dit type kraantje geen klik werd gevoeld die wel bij het oude type kraantje werd gehoord.

Omdat bij alle afdelingen waar de incidenten zich voordeden ernstig zieke patiënten betrokken waren, bestond bij de Meldingscommissie Incidenten Patiëntenzorg bezorgdheid over de situatie. Na elf maanden werden nog steeds frequent meldingen over de driewegkraantjes ingestuurd. Een herhaalde instructie op de betrokken afdelingen bleek geen effect te hebben, terwijl aan het kraantje zelf geen defect kon worden geconstateerd.

Intensief overleg met de betrokken zorgverleners, inspectie van de werkplekken en simulatie onder laboratoriumomstandigheden brachten ten slotte inzicht in de belangrijkste oorzakelijke factor.

In de praktijk ontvingen de betrokken patiënten regelmatig gelijktijdig meer dan drie verschillende infuusvloeistoffen. Omdat het bij veel van deze patiënten door hun leeftijd en of hun aandoening moeilijk was om infuusnaalden in te brengen, had dit tot gevolg dat op een reeds ingebrachte infuusnaald meer

infuussystemen werden aangesloten dan de driewegkraantjes toelieten. Om dit toch mogelijk te maken werd een tweede kraantje aan het bestaande driewegkraantje gekoppeld. De hierbij gebruikte koppeling bleek instabiel, met lekkage en losschieten tot gevolg.

De door de Centrale Sterilisatie Dienst opgemerkte beschadiging aan de buitenkant van sommige driewegkraantjes kon als volgt worden verklaard. Sommige gebruikers trachtten de infuusslang vast te draaien door een tang te gebruiken, hierbij tevergeefs wachtend op een klik. Door het gebruik van de tang beschadigde het kraantje.
Uiteindelijk nadat zich in een periode van bijna twee jaar in totaal achttien incidenten met het betreffende driewegkraantje hadden voorgedaan werd dit artikel uit het assortiment genomen en vervangen door een kraantje met een klik en door een kranenblok waarop meer dan drie infuussystemen konden worden aangesloten. Ook het Staatstoezicht werd over het betreffende kraantje geïnformeerd.

In de twee daaropvolgende jaren deden zich nog twee incidenten voor. De combinatie van het nieuwe kraantje en het kranenblok lijkt dus in combinatie met de gebruiker betrouwbaarder.

De cases drievoudig beschouwd

Wij bespraken kort twee gebeurtenissen. In deze paragraaf willen wij deze gebeurtenissen behandelen aan de hand van drie te onderscheiden analytische niveaus waarmee oorzaken van gebeurtenissen verklaard kunnen worden. Bij de categorisering maken wij gebruik van een aantal theoretische noties over oorzaken van rampen en de daarbij passende leerprocessen [Van Duin, 1992]. Wij beginnen steeds met het kort uitleggen van het theoretische analyseniveau, vervolgens kijken wij in meer algemene termen naar oorzaken van ongevallen en incidenten en hoe daarmee vooral in een ziekenhuis wordt omgegaan. Vervolgens kijken wij nog specifiek naar de twee cases.

Bij de analyse van de gebeurtenissen hanteren wij een systematische methode waarbij wij een onderscheid aanbrengen in drie niveaus: het niveau van individuen (microniveau); het niveau van de organisatie (mesoniveau) en het niveau van het systeem (macroniveau). Deze drie niveaus helpen ons bij het systematiseren van de factoren die de verstoring of calamiteit verklaren en kunnen tegelijkertijd gehanteerd worden om de lessen en gevolgen van de gebeurtenissen in kaart te brengen. Het leren van fouten wordt ook aan de hand van deze drie niveaus ingevuld.

Het microniveau

Het microniveau heeft betrekking op het maken van fouten en het verklaren van oorzaken van gebeurtenissen op het niveau van individuen. Het betreft het leren op het niveau van individuen. Als iemand een fout maakt, kan hiervan worden geleerd. Men kan anders gaan werken en of aanpassingen (laten) verrichten om vergelijkbare fouten in de toekomst te voorkomen.

Naarmate de fouten meer tot het niveau van het individu zijn te herleiden, is individueel leren belangrijker. Uit de praktijk en uit onderzoek weten wij dat meer routinematig handelen gemiddeld tot minder fouten leidt. Gemiddeld genomen zal een arts die vele tientallen keren dezelfde operatie uitvoert dat beter doen dan de arts die een dergelijke operatie slechts sporadisch verricht. Leren door ervaring is een van de belangrijkste middelen om het aantal fouten te verminderen. Uiteraard kan routinisering wel weer tot gevolg hebben dat de waakzaamheid afneemt.

Op het niveau van individuen vooral in ziekenhuizen vindt op veel afdelingen een zogeheten complicatiebespreking plaats, al dan niet gecombineerd met een necrologiebespreking. Beide besprekingen worden door de wetenschappelijke beroepsverenigingen zelfs als eis gesteld aan het erkennen van een opleiding tot specialist.

De complicatiebespreking heeft als onderwerp het bespreken van ongewenste gebeurtenissen in de patiëntenzorg waarvan het risico op optreden was gewogen, voorafgaand aan de betreffende behandeling of diagnostiek (‘calculated risk’). Het gaat om complicaties die in de literatuur zijn beschreven en die als zodanig bekend mogen worden verondersteld. Er bestaan professionele normfrequenties voor aan behandeling en diagnostiek gerelateerde complicaties. De complicatiebespreking wordt bijgewoond door de specialisten en arts-assistenten van één discipline.
Wanneer een patiënt als gevolg van de complicatie komt te overlijden of wanneer er sprake is van ernstige schadelijke gevolgen, dient dit als incident te worden gemeld aan de Meldingscommissie Incidenten Patiëntenzorg en aan de directie van de instelling. De directie moet dit incident doorgeven aan de IGZ.

De necrologiebespreking heeft een vergelijkbare functie als de complicatiebespreking. De patiënten die overleden zijn worden al dan niet afzonderlijk per specialisme besproken, indien postmortale autopsie (lijkschouwing) heeft plaatsgevonden. Hierdoor wordt de mogelijkheid geboden om te verifiëren of het oordeel van de behandelende arts overeenkomt met de bevindingen tijdens de autopsie. Ook het effect van behandelingen kan worden vastgesteld.

‘To err is human’ zo luidt de heldere titel van een Amerikaans rapport van het Institute of Medicine uit 1999 [Kohn, 1999]. In dit rapport constateren de onderzoekers dat er jaarlijks meer dan 50.000 personen en mogelijk zelfs 100.000 in de VS omkomen als gevolg van medische missers. Voor Nederland zou dat meer dan 1.500 doden per jaar betekenen. Vergissen is menselijk zo is de teneur, maar er zijn wel veel mogelijkheden om dat aantal vergissingen terug te brengen. Tenslotte zijn het geen enkele personen, maar vele duizenden die al deze vergissingen en missers veroorzaken. Uit het onderzoek blijkt dat 40% van deze missers van doen heeft met vergissingen met medicamenten.

Hoewel ongetwijfeld het leeuwendeel van deze fouten is te herleiden tot menselijk falen of nalaten, betekent dat niet dat ook de lessen alleen op het niveau van de afzonderlijke individuen geleerd kunnen worden.

De twee verschillende cases lieten uiteenlopende soorten van menselijk falen zien. Bij de bloeduitgifte begon het met een simpele typefout in het ene ziekenhuis en het plakken van een barcodesticker op het verkeerde buisje in het andere ziekenhuis. Hierna merkten vervolgens verschillende personen in het gehele proces de ontstane discrepantie niet, of merkten deze wel maar gingen er om uiteenlopende redenen vanuit dat de discrepantie reeds was hersteld of opgelost. Mogelijk zou een iets andersoortige veiligheidscultuur – waar afwijkingen min of meer automatisch leiden tot extra controles en ‘checks’ – eerder tot een actievere opstelling hebben geleid.

De case van de driewegkraantjes lijkt vooral verklaard te kunnen worden door individuele gewoonten. Het aan elkaar koppelen van verschillende driewegkraantjes kan worden beschouwd als een verkeerd gebruik van de kraantjes met lekkage als gevolg. Verplegend personeel was gewend te werken met een systeem waarbij een klik de bevestiging gaf dat het kraantje goed was aangesloten. De afwijking van het bekende patroon leidde tot incidenten.
De beide cases zijn niet bij uitstek cases die aanzetten tot leren op het microniveau. De driewegkraantjes zouden worden vervangen door een systeem met een klik en door kranenblokken voor die situaties waarin meer dan drie infuussystemen aan één infuusnaald moesten worden gekoppeld.

Mesoniveau

Het mesoniveau richt zich op het niveau van de organisatie. Ondanks het feit dat veel fouten het gevolg zijn van individuele fouten, betekent dat niet dat het organisatieniveau niet van invloed is op deze fouten. Incidenten die tot dit niveau zijn te herleiden hebben vaak te maken met een gebrekkige communicatiestructuur, tegenstrijdige doelstellingen (snelheid en zorgvuldigheid) of genegeerde signalen.

Als er bij twee vergelijkbare bedrijven bij het ene bedrijf veel verstoringen en fouten worden geconstateerd en bij het ander bedrijf niet of nauwelijks, is er een gerede kans dat een deel van de verklaring op het niveau van de bedrijven gezocht moet worden. Dat betekent dat ook op het niveau van de organisatie verschillende ongevallen en fouten zijn te verklaren. Het ziekenhuis of de fabrikant van het betreffende apparaat of instrument dat faalde beschouwen wij in het kader van deze thematiek als het mesoniveau. Wagenaar deed een vergelijkend onderzoek naar het handelen en de incidenten in verschillende intensive care-afdelingen van ziekenhuizen en constateerde dat organisatorische factoren als een opgeruimde werkomgeving, kwaliteit van onderhoud en interne communicatieprocessen mede bijdroegen aan het verklaren van de verschillen in aantallen incidenten [Wagenaar, 1992].

Op mesoniveau bestaat het door de overheid vereiste systeem van het melden van incidenten. Afdelingen melden incidenten in de patiëntenzorg aan een centrale Meldingscommissie. Daardoor wordt het mogelijk om door middel van een nadere analyse van de calamiteit structurele tekortkomingen in de zorg op het spoor te komen, zodat maatregelen kunnen worden genomen om herhaling te voorkomen.

Sinds 1984 geldt voor ziekenhuizen de door de overheid gestelde verplichting tot het instellen en het functioneren van een Meldingscommissie Incidenten Patiëntenzorg (MIP), voorheen FONA[3]-commissie ('Faults Or Near Accident'). De Inspectie voor de Gezondheidszorg ziet voor het functioneren van deze commissies een kwaliteitsbevorderende rol weggelegd, doordat systematisch na een incident bezien wordt in hoeverre het risico op herhaling kan worden gereduceerd of geëlimineerd. Leren staat voorop. Wanneer een incident of een complicatie heeft geleid tot de dood of een ernstig schadelijk gevolg voor de patiënt, is er sprake van een calamiteit en is de melding aan de Inspectie verplicht.

Hoewel de Inspectie geen voorschriften geeft over de wijze waarop ziekenhuizen invulling moeten geven aan de MIP, wordt wel geaccepteerd dat de effectiviteit van het systeem gebaat is bij het creëren van een veilige omgeving. Hieronder wordt verstaan dat melders niet gestraft moeten worden voor het melden van een incident. Dat zou immers leiden tot niet melden. Niet melden zou in dit verband vervolgens leiden tot niet leren.

In de organisatie van de MIP-commissies bestaan tussen de zorginstellingen enige verschillen, maar de werkwijze is meestal goed vergelijkbaar. Een multidisciplinaire commissie analyseert in chronologische volgorde de toedracht van het incident, waarna het incident wordt gerubriceerd als fout, ongeval of complicatie.

3 Niet alle ziekenhuizen spreken van MIP, deze commissies worden ook wel FONA- of FOBO-commissie genoemd. In dit stuk zal verder worden gesproken over Meldingscommissie Incidenten Patiëntenzorg, afgekort MIP of meldingscommissie. Hiermee worden dan ook de FONA- of FOBO-commissie bedoeld. We spreken dan ook niet over FONA-melding, maar over MIP-melding.

De rubriek fout valt uiteen in de subtyperingen persoonlijke fout, fouten, materiaalfout of organisatiefout. Indien een incident als fout wordt betiteld, wordt door de commissie nagegaan of de door de betrokken afdeling of dienst voorgestelde corrigerende maatregelen adequaat worden geacht. Vooral organisatiefouten leiden vaak tot aanvullende voorstellen door de commissie voor corrigerende maatregelen aan de directie.
De laatste tijd hecht de Inspectie in toenemende mate belang aan inzicht in de effecten van corrigerende maatregelen naar aanleiding van incidenten. In de praktijk blijkt dit vaak moeilijk vast te stellen.

De hiervoor beschreven systematiek kent naast voordelen ook een aantal in het oog springende nadelen. De belangrijkste is dat de incidentenregistratie geen duidelijk inzicht geeft in de omvang van de veiligheidsrisico's. Het is aannemelijk dat in alle zorginstellingen sprake is van een grote onderrapportage van incidenten.

Daarnaast is de wijze waarop incidenten worden geanalyseerd niet geschikt voor analyse van algemene veiligheidsrisico's op een afdeling. Ieder incident wordt uniek gedefinieerd. Er wordt niet naar gemeenschappelijke factoren met andere soortgelijke incidenten gekeken.

Veel medische fouten zijn eenvoudigweg 'georganiseerd'. "Zo waren er op een gegeven moment twintig merken infuuspompen op de markt en had een ziekenhuis vijf of zes merken in gebruik, omdat de ene periode pomp A goedkoop was en in een andere periode pomp B. Elke infuuspomp werkte anders. Bij pomp A betekende stand 1 iets anders dan bij pomp B. Je kunt je voorstellen dat daar ongelukken van zijn gekomen"[4]. Tussen het moment van het voorschrijven van een medicijn door een arts en de uiteindelijke inname van dat medicijn door de patiënt zitten in de regel zo'n 10 tot 13 stappen; handelingen van vaak verschillende personen. Dat maakt het tot een buitengewoon kwetsbaar systeem, "a complex system – a system prone to human and technological failure" [Norton, 2001].

Ook de cases van de bloedtoediening en de driewegkraantjes hebben duidelijk organisatorische aspecten. Bij de case van de bloedtoediening speelt de organisatorische inbedding van het gehele proces een rol. De Inspectie beveelt dan ook aan het bestaande kwaliteitssysteem sterk te verbeteren. Bij de driewegkraantjes roept het mesoniveau vooral vragen op. Hoe kan het dat slechts in enkele afdelingen het legio van de defecten zijn opgetreden? Waarom duurde het zo lang alvorens het ziekenhuis ingreep?
In beide situaties blijkt één aspect essentieel te zijn. Op welk moment (hoe snel) komt naar voren dat er achter een individueel geval structurele aspecten schuil-

4 Citaat van de directeur van het CBO in Intermediair, 9 november 2000, p. 15

gaan. Op welk moment komen de verschillende klachten over de driewegkraantjes bij elkaar en onderkent iemand de bovenindividuele aspecten?

Macroniveau

Het macroniveau richt zich op systemen, zoals in dit geval de gezondheidszorg. De theorie van Perrow [Perrow, 1984] is nauw verbonden met dit analytische niveau. Hoogtechnologische rampen (kernramp, biotechnologie, luchtvaart) zijn welhaast als normaal te beschouwen. De strakke koppelingen in het systeem en de complexiteit ervan maken het erg kwetsbaar. Het spreekt vanzelf dat afwijkingen en gebreken op het microniveau veel gemakkelijker zijn te onderkennen dan op het macroniveau. Het is bijvoorbeeld veel gemakkelijker aan te tonen dat een bepaalde arts relatief veel fouten maakt dan dat bijvoorbeeld het gebrek aan personeel of de overbelasting van verpleegkundigen bijdraagt aan een groter aantal incidenten en problemen in de gezondheidszorg.

Leren op en het beschouwen van het macroniveau kan bijvoorbeeld plaatsvinden door de rol van de IGZ te beschouwen en de wijze waarop landelijke organisaties of fora omgaan met bepaalde kennis over falende systemen.
Naast de reeds beschreven activiteiten van de MIP (verplicht) bestaat er landelijk een vrijwillig systeem van incidentmeldingen. Het belang van deze systemen ligt in de signalerende functie.
Het systeem van melden aan de Inspectie heeft onder andere als functie dat zorginstellingen transparantie kunnen betonen als het om de kwaliteit van zorg gaat. Wel is het zo dat zorginstellingen het melden van ernstige incidenten aan de Inspectie min of meer als een morele verplichting zien. Momenteel zijn er ontwikkelingen aan de gang die het waarschijnlijk maken dat het melden van incidenten aan de Inspectie in de toekomst een meer verplichtend karakter zullen krijgen.

Doordat incidenten worden gemeld is het mogelijk om instellingen, de overheid, de industrie en andere belanghebbenden te informeren, te waarschuwen of te adviseren. Indien er sprake is van grove onkunde of ernstige onzorgvuldigheid, dan is het de taak van de Inspectie om maatregelen te treffen zoals het in gang zetten van een tuchtrechtelijke procedure. In feite draagt de Inspectie in relatie tot de gemelde incidenten een dubbele pet. Enerzijds vervult zij een kwaliteitsbevorderende rol en anderzijds moet zij repressief kunnen optreden bij grove nalatigheid of onkunde. Hoewel deze dubbelrol in de praktijk weinig problemen lijkt te geven, draagt deze constructie risico's met zich mee. Sinds 1995 worden leveranciers van medische hulpmiddelen door de overheid verplicht gesteld om de traceerbaarheid van implantaten te borgen. Bij incidenten waarbij een medisch hulpmiddel in het geding is, dient zowel de Inspectie als de toeleverancier te worden geïnformeerd om zodoende bijvoorbeeld een

adequate recall-procedure tot op het niveau van de individuele patiënt mogelijk te maken.

Aan het begin van de jaren negentig kwamen de ziekenhuizen met de vraag naar de wenselijkheid van een nationale databank van gemelde incidenten. Hiermee zou men kunnen beschikken over een groot aantal meldingen, hetgeen het ontdekken van patronen zou vergemakkelijken en meer mogelijkheden biedt om zich met andere ziekenhuizen te vergelijken.
Nu, anno 2001, bestaat deze landelijke registratie wel, maar leidt vooralsnog een kwijnend bestaan. Enerzijds heeft een wellicht te ambitieuze doelstelling van de registratie ertoe geleid dat veel meer gegevens per incident worden gevraagd dan dat er in veel instellingen worden geregistreerd. Omdat de meldingsbereidheid in instellingen over het algemeen als kritische factor wordt gezien (onderrapportage is standaard), voelen veel instellingen er niet voor om hun medewerkers te verzoeken extra items per melding in te vullen.
In de tweede plaats werden instellingen gevraagd de informatie digitaal aan te leveren in een database. Tot voor kort was het voor instellingen niet mogelijk deze database aan te wenden voor het door de Inspectie voor de Volksgezondheid verplicht gestelde jaarverslag van de Meldingscommissie Incidenten Patiëntenzorg. Dit werd door de gebruikers als een nadeel beschouwd, hetgeen de bereidheid om de database te vullen beperkte.
Recent zijn er nieuwe versies van de databasesoftware beschikbaar gekomen. De eerste geluiden hierover zijn niet optimistisch. Wederom zouden de gebruikers niets met de databasegegevens doen. Om die reden laten grote ziekenhuizen een eigen database bouwen.

De case van de bloedtoediening kent dergelijke aspecten ook. Ook hier speelt de wijze van uitwisseling van kennis een cruciale rol. Of en in hoeverre wordt er op dit niveau vrijwillig of verplicht informatie en kennis uitgewisseld?
Momenteel is er in Nederland betrekkelijk weinig geregeld om het leren op systeemniveau te stimuleren. Er is sprake van onderrapporteren, er is geen verplichting om incidenten en missers te melden. Instellingen hebben de verplichting dergelijke calamiteiten intern te onderzoeken (Klachtwet 1996). De rapporten die afzonderlijke ziekenhuizen indienen, komen met grote vertraging op één centraal punt (IGZ).
Dat maakt dat er nog maar weinig structureel wordt gezocht naar bovenindividuele of bovenorganisatorische fouten en manco's. Zo is er bijvoorbeeld nauwelijks zicht op hoe de huidige grote druk op de gezondheidszorg, de lange wachtlijsten en de tekorten aan personeel van invloed zijn op de omvang en ernst van de individuele en organisatorische fouten.

Wij constateren dat een zo belangrijke sector als de gezondheidszorg op het gebied van de systematische vergaring van informatie over (on)veiligheid en veiligheidscultuur achterligt op sectoren als de procesindustrie en de luchtvaart. Dit is des te opvallender als wij weten dat het aantal calamiteiten in deze sector zoveel malen hoger ligt.

"The health care industry, has reported to be at least 10 years behind other industries in using quality and safety improvement systems. A review of industries that have been successful in improving quality and reducing errors has shown that there are many similarities in their error-reducing cultures." [Norton, 2001].

Uiteraard zijn er veel verklaringen waarom dat zo is. De sector handelt dagelijks over situaties van leven en dood, waarbij dood een veel vanzelfsprekender begrip is dan in andere sectoren. In tegenstelling tot de andere sectoren kunnen hier veel meer personen noodlottige fouten maken, inclusief de patiënten zelf.

Bij vrijwel elke medische handeling is het aantal handelingen en betrokkenen extreem groot. Uiteraard verhoogt dat de kwetsbaarheid en de kans op fouten. Daarnaast is het vaak lastig te bepalen wat goed en fout is; verschillende patiënten reageren vaak heel verschillend op dezelfde behandeling. Dat is wel iets anders dan 'de constante kwaliteit van een Mars' of een 'goed te beheersen chemische productiekolom'. Tenslotte zijn de veroorzakers van veel fouten (de professionals: artsen in maatschappen e.d.) zelf de managers en of verantwoordelijken van het systeem. Daarmee is het belang van een goed inzicht geheel anders. De luchtvaarttyconen en de managers in de petrochemie willen zo goed mogelijk weten wat 'hun personeel' aan fouten heeft begaan. In de wereld van de medici zijn het deels de professionals zelf die de incidenten veroorzaken.

Trends van invloed op de betrouwbaarheid van het technische systeem

Welke trends in de gezondheidszorg zouden in de toekomst van invloed kunnen zijn op de betrouwbaarheid van technische systemen? Er worden in dit kader vier trends genoemd. Het gaat hierbij om de toenemende krapte op de arbeidsmarkt, de toenemende buraucratisering van de gezondheidszorg, de toenemende rol van de technologie in het medisch proces, de trend naar superspecialisatie alsmede de verregaande concentratie van zorginstellingen.

– *Krapte op de arbeidsmarkt*
  In toenemende mate is er sprake van onderproductie in zorginstellingen door een tekort aan medisch en verpleegkundig personeel. De toekomstscenario's voor de middellange termijn zijn somber over de ontwikkeling van dit tekort aan menskracht in de sector. Zo is berekend dat voor vrijwel alle medische specialismen een aanzienlijk tekort (10-30%) aan gekwalificeerde specialisten zal ontstaan. Het tekort aan menskracht zal leiden tot toenemende wachtlijsten (zowel in aantal als in lengte) in de gezondheidszorg.
  Wachtlijsten veroorzaken een toename van de werkdruk bij het personeel in de gezondheidszorg.
  De toegenomen werkdruk zal over een langere periode verhoogd zijn en een potentieel negatieve impuls geven aan de betrouwbaarheid van het medisch systeem. Dit komt voort uit de verwachting dat de toegenomen werkdruk een negatieve invloed zal hebben op de ontwikkeling van kwaliteitssystemen in de gezondheidszorg en op ontwikkelingen van veiligheidskundige aard in de sector.
– *Toenemende rol van de technologie in het medisch proces*
  De gezondheidszorg heeft mede door de vele technische ontwikkelingen van de laatste decennia een stormachtige ontwikkeling doorgemaakt, zowel op het gebied van de diagnostiek als van de behandeling.
  Deze ontwikkeling heeft in het verleden telkens weer geleid tot situaties waarbij sprake was van een negatieve beïnvloeding van het risicobewustzijn onder gezondheidszorgwerkers, doordat een gevoel van schijnzekerheid was ontstaan. Zo kan het in een zorginstelling plaatsen van defibrillatoren (te gebruiken bij acute hartstilstand of ritmestoornis) aan de ene kant leiden tot een gevoel van toegenomen veiligheid bij de medewerkers. Aan de andere kant kan dit gevoel aanleiding zijn voor een te laag risicobewustzijn. Dat kan bij het vervoeren van zieke patiënten leiden tot potentieel gevaarlijke situaties. Dit kan gebeuren als niet alle gezondheidszorgwerkers die ermee in aanraking zouden kunnen komen over de bediening zijn geïnstrueerd, of als voor deze apparatuur geen preventief onderhoud is georganiseerd. Er is geen reden om aan te nemen dat de invloed van nieuwe technologische ontwikkelingen op de gezondheidszorg aan het afnemen is.
– *De trend naar superspecialisatie*
  In de afgelopen decennia is een aantal superspecialisaties door de beroepsverenigingen erkend. Het ziet ernaar uit dat ook in de komende jaren enkele nieuwe officiële aandachtsgebieden zullen worden vastgesteld. Deze ontwikkeling is van belang voor het kunnen waarborgen van de continuïteit van specialistische expertise. Omdat een nagenoeg gelijke hoeveelheid medisch specialisten op een groter aantal medisch specialistische deelgebieden actief is, kan dit vooral in de kleinere gezondheidszorginstellingen een groot probleem vormen. Zo zal bijvoorbeeld het dag en nacht waarborgen van de

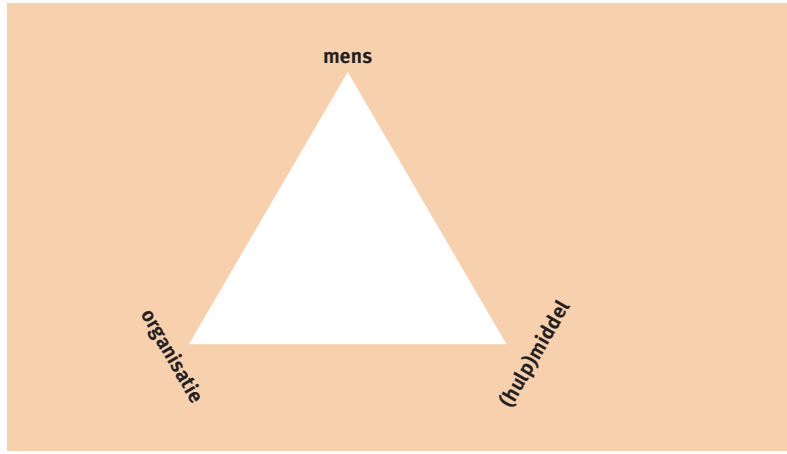
continuïteit van de traumatologische expertise (ongevalchirurgie) in een klein streekziekenhuis een groot probleem vormen. In dat ziekenhuis werken slechts drie chirurgen waarvan er slechts één zich na zijn opleiding tot algemeen chirurg extra heeft bekwaamd in de traumatologie.

– *De concentratie van zorginstellingen*
  Momenteel is er een trend zichtbaar waarbij steeds meer zorginstellingen fusies aangaan met andere zorginstellingen of op zoek zijn naar een geschikte fusiepartner. Als deze tendens wordt voortgezet, bestaat de verwachting dat er in Nederland nog ongeveer 40 zorgorganisaties zullen bestaan. Dit zullen dan conglomeraten van gefuseerde zorginstellingen zijn. Op dit moment zijn er alleen al circa 100 ziekenhuizen voor de intramurale gezondheidszorg.
  Een en ander zal enerzijds tot gevolg hebben dat het nadelige effect van de trend tot superspecialisatie gedeeltelijk of zelfs geheel wordt gecompenseerd. Anderzijds is uit het verleden gebleken dat fusies tussen zorginstellingen en maatschappen lang niet altijd goed verlopen. Het is goed denkbaar dat moeizame fusieprocessen hier en daar een negatieve weerslag op de betrouwbaarheid van het zorgsysteem zullen hebben.

Medische fouten in relatie tot de betrouwbaarheid van het technische systeem

De betrouwbaarheid van technische systemen richt zich primair op de kwaliteit (robuustheid, kwaliteit en dergelijke) van het (hulp)middel; doet het middel datgene wat het zou moeten doen. In dit hoofdstuk beschouwden wij in concreto een driewegkraantje en een computerprogramma ter ondersteuning van het logistieke proces van bloeduitgifte. Wij hebben geprobeerd aan te geven dat in beide gevallen de betrouwbaarheid van het technische systeem eerst en vooral werd bepaald door de handelingsbekwaamheid van individuen enerzijds en de organisatie waarin personen werken en een middel wordt gebruikt anderzijds.

De verschillende cases spelen zich steeds af in de driehoek mens, (hulp)middel en organisatie. De mens behoeft geen nadere toelichting. Het (hulp)middel is het instrument dat de mens gebruikt om een bepaalde werkzaamheid te verrichten. Dat kan een fysiek product zijn als een hamer of een driewegkraantje, maar ook een naslagwerk of een computerprogramma zoals in de case van de bloedtransfusie. De organisatie is het lastigste te duiden. Primair is dat de fysieke context waarin het individu handelt (het laboratorium, het ziekenhuis), maar de organisatie is ook de meer virtuele werkelijkheid van het gehele regelsysteem en de stand van kennis en techniek. Het is ook mogelijk dit laatste deel als de context te zien waarin deze driehoek is geplaatst.



Figuur 22.2
De driehoek mens, (hulp)middel en organisatie.

Individuen maken – uiteraard – fouten. Veel fouten corrigeert men zelf, in sommige gevallen corrigeren anderen en soms corrigeert het systeem (ATB[5]). Daarnaast gaat het in sommige gevallen mis met kleinere of grotere gevolgen. In dit hoofdstuk hebben wij twee voorbeelden behandeld waarin storingen optraden in de driehoek mens, middel en organisatie. Hoewel zo'n klein aantal cases eigenlijk nauwelijks mogelijkheden geeft om tot meer algemene conclusies te komen, willen wij aan het slot toch enkele observaties doen.

Onbetrouwbaar?

Hoewel zich de nodige incidenten voordeden, is de vraag gewettigd of hier nu sprake was van onbetrouwbare hulpmiddelen. Het driewegkraantje functioneerde elders naar tevredenheid. Er was niets 'mis' met het computerprogramma an sich. In beide gevallen zijn er duidelijk verschillende meningen over de mate van betrouwbaarheid van het systeem als zodanig.
In beide gevallen werd het middel onbetrouwbaar door de wijze waarop het door mensen werd gebruikt en door de wijze waarop het middel door de organisatie was geïncorporeerd en geïntroduceerd. Onbetrouwbaarheid van een middel of instrument is dus waarschijnlijk slechts in de context van mens en organisatie te bepalen. Personen maken een middel (on)veilig; een organisatie draagt bij aan het betrouwbare gebruik.
Het is bekend dat de meest onbetrouwbare middelen soms de minste problemen opleveren. Wij spreken dan over de veiligheidsparadox. Onbetrouwbare en onveilige middelen en situaties (de levensgevaarlijke trap of het kruispunt) worden gecompenseerd door de vergrote alertheid van de gebruikers. Andersom leidt grote gepercipieerde veiligheid (kooiconstructie, ABS en airbags) soms tot risicozoekend gedrag.
Om de betrouwbaarheid van (technische) systemen te bepalen kan het dus niet anders dan dat deze betrouwbaarheid in de driehoek wordt getest. Het 'fail-safe'-systeem roept bij sommige personen immers op zijn minst de vraag op

5 ATB is automatische treinbeïnvloeding. Een systeem dat de machinist automatisch corrigeert als hij door een rood sein rijdt.

“hoe zo fail-safe, dat willen wij nog wel eens zien”. Betrouwbaarheid is daarmee ook tijd- en plaatsgebonden. Wat hier en vandaag betrouwbaar is, kan morgen of elders helemaal niet betrouwbaar blijken.

Verhogen van betrouwbaarheid
Daarmee komen wij aan de vraag hoe deze betrouwbaarheid zo goed mogelijk te borgen. Het zal duidelijk zijn dat dan dezelfde driehoek gehanteerd kan worden. In alle stadia van een product van ontwikkeling tot ontwerp, productie en invoering is het nodig steeds de relatie met de organisatie en de mens in ogenschouw te nemen. Betrouwbaarheid wordt in de interactie met mens en organisatie bepaald. Een prima driewegkraantje kan een flop worden, omdat de organisatie onvoldoende onderkent dat de afwijkingen met de voorloper kunnen leiden tot een onjuiste toepassing. Honderd testen vooraf van dat systeem zullen deze discrepantie niet gemakkelijk aan het licht brengen. Bij de introductie van software is dat uiteraard nog veel meer het geval, omdat daar legio mogelijkheden zijn om het systeem suboptimaal te gebruiken, dat wil zeggen bepaalde delen uit te schakelen, enzovoorts.

Organiseren van ‘early warning’
Een derde aspect dat opvalt in de cases is de vroegtijdige signalering. Wanneer en hoe snel kan duidelijk worden dat achter een incidentele verstoring structurele patronen schuilgaan. Achteraf is uiteraard gemakkelijk te bepalen dat bepaalde gebeurtenissen een gemeenschappelijke noemer hebben, maar op het moment zelf is dat anders. Daarbij komen wij niet alleen bij het thema van het melden van incidenten en bijna-incidenten, maar vooral ook bij de wijze waarop informatie wordt geaggregeerd.

Ons valt op dat in de medische wereld het alarmeren, rapporteren, integreren en aggregeren in vergelijking met andere ‘werelden’ (bijv. de procesindustrie, de luchtvaart) nog niet ver ontwikkeld is. Er is enerzijds sprake van een flinke dosis vrijblijvendheid (je moet niet veel) en anderzijds sprake van terughoudendheid. Zowel de professionals op microniveau, de zorginstellingen op mesoniveau als de Inspectie lijken meer te kunnen leren van incidenten. Aan de ene kant bestaat er geen verplichting bij zorginstellingen tot het melden van ernstige incidenten aan de Inspectie IGZ. Er bestaat geen verplicht landelijk registratiesysteem voor het melden van materiaalfouten. Slechts in reactie op in het oog springende incidenten is er voor een heel beperkt gebied een landelijk registratiesysteem (landelijke hartklepregistratie). Daarentegen zijn er wel landelijke ontwikkelingen gaande om het melden van incidenten verplicht te maken.

Referenties

- Duin, M.J. van. (1992). Van rampen leren: een vergelijkend onderzoek naar lessen uit spoorwegongevallen, hotelbranden en industriële ongelukken. Afstudeerscriptie
- Kohn, L.T., J.M. Corrigan, M.S. Donaldson (eds.). (1999). To Err is Human. Building a Safer Health System. Committee on Quality of Health Care in America. Institute of Medicine. National Academy Press, Washington
- Norton, L.L. (2001). Continuing Education – Medical and Medication Errors: A Partial Summary of Reports by the Institute of Medicine and the Quality Interagency Coordination Task Force. Journal of Managed Care Pharmacy 7(1):62-68
- Perrow, C. (1984). Normal Accidents: Living with High Risk Technologies. Basic Books, New York
- Wagenaar, W.A., A.M. Souverijn, P.T.W. Hudson. (1992). Safety Management in Intensive Care Wards. In: B. Wilpert, Th. Ovale (eds.). In Search for Safety. Lawrence Erlbaum Associates, Hove

Bijlage I De werkwijze van de Meldingcommissie Incidenten Patiëntenzorg

Aan de Meldingcommissie dienen door de medewerkers van de instelling incidenten te worden gemeld die zich voordoen in de individuele patiëntenzorg en die tot schade hebben geleid dan wel hadden kunnen leiden.
Meldingen (al dan niet beschreven op het meldingsformulier) bereiken de commissie via de Raad van Bestuur dan wel rechtstreeks via de secretaris.
De melding wordt voor zover mogelijk in de eerstvolgende commissievergadering besproken. Soms bestaat er behoefte aan meer informatie, dan wordt in overleg met de melder aan andere betrokken diensten of afdelingen om commentaar gevraagd. De commissie bekijkt of er preventieve maatregelen mogelijk zijn of dat de door de melder voorgestelde preventieve maatregelen afdoende lijken.
De melding wordt conform de in het reglement gehanteerde definities gerubriceerd. De melder wordt door de commissie geïnformeerd over de rubricering.

De volgende (landelijke) definities worden hierbij gehanteerd:

Fout	handelen in strijd met de in acht te nemen zorgvuldigheid, handelen of nalaten van handelen van een of meer instellingsmedewerkers.
Technische fout/materiaalfout	elke gebeurtenis ontstaan door een defect van de gebruikte apparatuur of materiaal.
Ongeval	elke gebeurtenis, waardoor de patiënt mogelijk schade kan leiden, zonder dat er sprake is van een fout of calculated risk.
Complicatie	elke gebeurtenis, waardoor de patiënt mogelijk schade kan worden toegebracht, die het gevolg is van een van tevoren in aanmerking genomen risico van behandeling of diagnostiek c.q. het afzien daarvan.
Fouten	als er sprake is van meerdere opeenvolgende gebeurtenissen zoals genoemd in fout.
Verkeerde melder	als de melder getuige is van een voorval dat door een andere medewerker gemeld dient te worden.
Organisatiefout	als de gebeurtenis het gevolg is van of kan zijn van procedures en of richtlijnen van de instelling.
Geen rubricering	de melding is niet te rubriceren.

2

23 Vliegtuigafhandeling op luchthavens

drs.ing. K.J. Zwart [1], *dr.ir. T. Goemans* [2], *ing. J.I.H. Oh* [3]

Inleiding

In juli 2000 berichtten de media dat op Schiphol een aanrijding tussen een MD-11 van KLM en een Boeing 747 van Northwest Airlines was voorgevallen. De aanrijding deed zich voor tijdens het van de 'gate' terugduwen van de MD-11. De chauffeur van de 'push back'-truck zette een bocht te vroeg in, waardoor de vleugels van beide vliegtuigen elkaar raakten. Bij de aanrijding raakte de vleugel van de MD-11 zodanig beschadigd dat het toestel voor reparatie naar de hangar moest worden gesleept; de passagiers moesten met een ander toestel worden vervoerd. De chauffeur verklaarde dat hij ten gevolge van de hoge werkdruk gehaast was en daardoor mogelijk niet voldoende zorgvuldig had gehandeld.

1 Inspectie Verkeer en Waterstaat,
Divisie Luchtvaart
Postbus 575
2130 AN Hoofddorp

2 KPMG Consulting
Postbus 29761
2502 LT Den Haag

3 Ministerie van Sociale Zaken en
Werkgelegenheid, Directie Arbo
Postbus 90801
2509 LV Den Haag

Nadere bestudering van de incidentenrapportages van Schiphol leert dat aanrijdingen met vliegtuigen een regelmatig voorkomend verschijnsel zijn. Naast aanrijdingen, waarbij de ontstane schade binnen de toegestane marges blijft, of waarbij de schade al of niet tijdelijk ter plekke kan worden hersteld, vindt in drukke perioden gemiddeld tweemaal per week een aanrijding plaats, die erin resulteert dat het vliegtuig niet meer inzetbaar is voor de voorgenomen vlucht[4]. Meestal betreft het aanrijdingen tussen een vliegtuig en een luchthavenvoertuig, zoals cateringtrucks, gemotoriseerde passagierstrappen, tractors. Dergelijke voorvallen zijn niet direct bedreigend voor een veilige vluchtuitvoering van het betreffende vliegtuig, omdat de schade aan het vliegtuig over het algemeen direct zichtbaar is, waardoor voor aanvang van de vlucht besloten wordt de schade te herstellen of het vliegtuig uit bedrijf te nemen. Wel levert dit soort voorvallen dikwijls onvermijdelijke vertragingen op.

Figuur 23.1
Duidelijk schadegeval. Bron: Christopher.

Figuur 23.2
Een te 'achterlijke' zwaartepuntligging. Bron: Jean Charles Dayot.

4 Informatie ontleend aan de door Schiphol aan de Inspectie Verkeer & Waterstaat (IVW), Divisie Luchtvaart gemelde incidenten.

Bedreigender voor de veiligheid zijn voorvallen, waarvan de gevolgen niet onmiddellijk zichtbaar zijn, bijvoorbeeld fouten bij het beladen of bij het sluiten van deuren en luiken. In januari 1999 raakte een Fokker F-27 tijdens de daling naar de luchthaven op Guernsey in onbalans door een verkeerd geladen partij kranten van 3.000 kg. Het vliegtuig verongelukte. Als op de luchthaven van vertrek de beladingsfout net zo duidelijk zichtbaar was geweest als in figuur 23.2 was er niets gebeurd.

In 1973 verongelukte bij Parijs een DC-10 van een Turkse luchtvaartmaatschappij vlak na de start ten gevolge van een onjuist vergrendelde vrachtdeur. Tijdens de klim op grotere hoogte schoot de vrachtdeur los en ontstond in het vrachtruim de lagere buitenluchtdruk. Omdat de passagierscabine al op druk stond, bezweek de vloer. Onder de vloer liepen de besturingskabels en -leidingen en deze raakten zodanig beschadigd dat het vliegtuig onbestuurbaar werd. Alle inzittenden kwamen bij het ongeluk om. Het ongeluk is een van de meest ernstige uit de luchtvaarthistorie. Onderzoek wees uit dat een potige medewerker van het afhandelingsbedrijf op krachtige wijze de deur had gesloten in de onjuiste veronderstelling dat dat voldoende zou zijn. In de cockpit waren geen indicaties dat de deur niet vergrendeld was. Mede door dit ongeluk beschikken moderne vliegtuigen tegenwoordig over geavanceerde hulpmiddelen, waarmee in de cockpit de configuratie van het vliegtuig afgelezen kan worden, en waarbij de bemanning ook wordt geattendeerd op onjuistheden in die configuratie, zoals niet vergrendelde deuren en luiken. Bovendien dienen grote verkeersvliegtuigen tegenwoordig te zijn voorzien van zogenaamde drukvereffeningsluiken tussen de vloeren.

Het is daarom niet waarschijnlijk dat zo'n ongeluk zich bij moderne vliegtuigen snel zal herhalen. Dat is alléén omdat er een tijdige waarschuwing komt, niet omdat de kans op het verkeerd sluiten van deuren en luiken minder is geworden. Die kans is nog steeds even groot – ook bij moderne vliegtuigen – en het komt dan ook nog regelmatig voor dat er delen van een vliegtuig vallen, omdat ze niet goed zijn vastgezet. Of dat motoren olie verliezen, omdat oliedoppen niet vastzitten. Allemaal voorvallen die voortkomen uit werkzaamheden die op de grond hebben plaatsgevonden.

Betrouwbaarheid van vliegtuigen

De betrouwbaarheid van een vliegtuig wordt bepaald door endogene en exogene factoren. Endogene factoren betreffen de eigenschappen van het vliegtuig zelf, en worden vooral bepaald door het ontwerp, de toegepaste materialen, onderdelen en componenten, het productieproces, de onderhoudsvoorschrif-

ten en de gebruiksprocedures. Exogene factoren hebben betrekking op het daadwerkelijke gebruik van het vliegtuig in de lucht en op de grond, zoals vaardigheid van de bemanning, routeplanning, vluchtprogrammering, verkeersleiding, luchthavenvoorzieningen, uitvoering van onderhoud, belading, brandstofplanning, lengte van omdraaitijden, passagiers.

Op basis van de endogene factoren worden vliegtuigen gecertificeerd, dat wil zeggen luchtwaardig bevonden. Ieder land stelt in principe zijn eigen luchtwaardigheidseisen, maar deze moeten tenminste voldoen aan de eisen die in het Verdrag van Chicago internationaal zijn overeengekomen. Het Verdrag van Chicago is in 1944 totstandgekomen en vormt de basis voor de mondiale ordening van de burgerluchtvaart. De wereldluchtvaartorganisatie ICAO (International Civil Aviation Organization) is belast met de voortdurende actualisering van het Verdrag, waarbij vooral het voortdurend verder ontwikkelen van de in de zogenaamde Annexes vastgelegde normen van belang is. Hierin staat aangegeven wat de minimale eisen zijn waaraan in de burgerluchtvaart moet worden voldaan. De ICAO-verdragslanden hebben zich ertoe verplicht dat zij in eigen land erop zullen toezien dat ook inderdaad aan deze eisen wordt voldaan. Ten aanzien van een aantal luchtvaartaspecten, waaronder luchtwaardigheid heeft een groot aantal Europese luchtvaartautoriteiten zich verenigd in de JAA[5]. Binnen de JAA is per categorie luchtvaartuigen één luchtwaardigheidscode afgesproken in plaats van dat ieder land zijn eigen code heeft. Bovendien is het streven gericht op harmonisatie met de Amerikaanse regelgeving.

De luchtwaardigheidseisen schrijven voor dat vliegtuigen zodanig worden ontworpen dat de sterkte van het vliegtuig berekend is op de maximaal in het vliegtuig voorkomende zware belastingen die op het vliegtuig worden uitgeoefend zonder dat zich fatale scheuren of breuken voordoen. Het ontwerp wordt daarop ook altijd beproefd. Voor vliegtuiginstallaties en -systemen moet worden aangetoond dat een fatale faalkans kleiner is dan eens in de miljard bedrijfsuren. Aangezien dit voor enkelvoudige systemen meestal een onhaalbaar hoge betrouwbaarheidseis is, wordt deze betrouwbaarheid bereikt door het inbouwen van reserves, zoals het meervoudig uitvoeren ('fail-safe') van die installaties of het toepassen van alternatieve back-upsystemen die in geval van falen de functie van het primaire systeem overnemen.
Daarnaast schrijven de luchtwaardigheidseisen voor dat het ontwerp voorzien is van een vlieghandboek met procedures voor de bemanning, een onderhoudshandboek en -programma en een lijst van condities waaraan het vliegtuig minimaal moet voldoen voor een veilige vluchtuitvoering, de zogenaamde Master Minimum Equipment List (MMEL). In deze lijst is aangegeven welke componenten voor kortere of langere tijd buiten werking mogen zijn zonder dat daarmee de veiligheid van de voorgenomen vlucht in gevaar komt. In een aantal gevallen

5 JAA = Joint Aviation Authorities, samenwerkingsverband van 33 Europese luchtvaartautoriteiten, die zich gecommitteerd hebben aan één gezamenlijke set van luchtvaartvoorschriften. Niet inbegrepen zijn voorschriften op het gebied van luchthavens en verkeersleiding. Deze behoren niet tot de competentie van de JAA. Evenmin zijn voorschriften voor toeleveranciers, waaronder vliegtuigafhandelingsbedrijven inbegrepen, omdat de JAA deze niet tot de primaire luchtvaartactoren rekent (n.l. ontwerporganisaties, fabrikanten, luchtvaartmaatschappijen, onderhoudsbedrijven).

zijn er aanvullende operationele instructies opgenomen in deze MMEL die een compensatie vormen voor het buiten bedrijf zijn van bepaalde systemen. Bijvoorbeeld in geval de straalomkeerders buiten werking zijn, mag niet worden geland op korte landingsbanen.

Als het vliegtuig aan de luchtwaardigheidseisen voldoet, wordt het gecertificeerd. Dat gaat in twee stappen, namelijk:

- Eenmalig voor het ontwerp van het vliegtuig via een typecertificaat. De betekenis hiervan is dat via berekeningen en beproevingen is aangetoond dat het ontwerp volledig voldoet aan de in de betreffende code gestelde luchtwaardigheidseisen. Het typecertificaat is onbeperkt geldig op voorwaarde dat geen ontwerpwijzigingen worden ingevoerd. Iedere wijziging moet apart worden gecertificeerd. Het typecertificaat wordt verstrekt door de luchtvaartautoriteit van het land waar de ontwerporganisatie is gevestigd.
- Eenmalig of periodiek voor ieder afzonderlijk vliegtuig dat gebouwd en onderhouden is op basis van het goedgekeurde typeontwerp via een Bewijs van Luchtwaardigheid (BvL). Het BvL wordt verstrekt door de luchtvaartautoriteit van het land waar het vliegtuig is geregistreerd. De geldigheidstermijn van het BvL is afhankelijk van de betreffende luchtvaartautoriteit. In Nederland is het BvL 1 jaar geldig (zweefvliegtuigen 2 jaar). Mits de conditie van het vliegtuig nog met het ontwerp overeenkomt, wordt het BvL op aanvraag verlengd. De geldigheid van het BvL is onafhankelijk gesteld van de onderhoudstoestand van het vliegtuig, dat wil zeggen dat het BvL niet wordt opgeschort op het moment dat het vliegtuig in onderhoud is. Wel moet het vliegtuig na iedere onderhoudsbeurt gebruiksklaar worden verklaard door het onderhoudsbedrijf.

Het gebruik van vliegtuigen

Aan de gebruikskant zijn vele actoren te onderscheiden, n.l.

- luchtvaartmaatschappijen;
- vliegtuigonderhoudsbedrijven;
- luchthavens;
- verkeersleiding;
- vliegtuigafhandelingsbedrijven.

Omdat een goed ontworpen vliegtuig bij verkeerd gebruik een even groot gebruiksrisico kan opleveren als een slecht ontworpen vliegtuig, gelden ook ten aanzien van het gebruik een groot aantal eisen.
Luchtvaartmaatschappijen dienen ervoor te zorgen dat hun vliegtuigen zich in goede conditie bevinden, dat vliegtuigbemanningen voldoende zijn getraind,

dat ze over voldoende personeel en materieel beschikken om de voorgenomen vluchten uit te voeren, enz. Luchtvaartmaatschappijen moeten als het ware aantonen dat de gecertificeerde vliegtuigen bij hen in goede handen zijn. De basiseisen hiervoor zijn in ICAO-verband tot stand gekomen. Tegenwoordig geldt in de meeste Europese landen (de JAA-landen) dat luchtvaartmaatschappijen ook zelflerend vermogen dienen te hebben in de vorm van een goed werkend kwaliteitssysteem. De luchtvaartmaatschappijen in deze landen dienen te voldoen aan de in JAR-OPS[6] gestelde eisen. Wanneer ze hebben aangetoond dat ze voldoen aan de eisen, ontvangt de luchtvaartmaatschappij van de luchtvaartautoriteit een vergunning om verkeersvluchten uit te voeren (in de JAA-landen aangeduid als Air Operator Certificate, AOC).

Voor *vliegtuigonderhoudsbedrijven* geldt dezelfde filosofie als voor luchtvaartmaatschappijen. Zij moeten aantonen voldoende geëquipeerd te zijn om vliegtuigen overeenkomstig de voorschriften te kunnen onderhouden, waarna ze eveneens op basis van een door de luchtvaartautoriteit afgegeven vergunning de werkzaamheden kunnen uitvoeren.

Voor *luchthavens* gelden voorschriften ten aanzien van inrichting en uitrusting (o.a. visuele hulpmiddelen, markeringen, verlichting, rij- en taxibanen en platforms), het ontbreken van obstakels, vogelbestrijding, sneeuw- en ijsbestrijding, hulpverleningsdiensten en rampenplannen. Voorschriften die in ICAO-verband zijn vastgesteld en door nationale overheden in de eigen wetgeving zijn overgenomen. Voor de verkeersleiding zijn eveneens in ICAO-verband voorschriften vastgesteld op het gebied van vakbekwaamheid, navigatie- en communicatieprocedures, radiofrequenties, spraakgebruik, en dergelijke. Nationale overheden zien toe op naleving van deze voorschriften.

Voor *vliegtuigafhandelingsbedrijven*, dat wil zeggen bedrijven die op het platform allerlei werkzaamheden rondom het vliegtuig verrichten (en daarom ook wel grondafhandelingsbedrijven genoemd), zoals belading, catering, schoonmaak, 'boarding' van passagiers en opstelling van het vliegtuig, gelden weinig luchtvaartvoorschriften van overheidswege. Vooral geldt dit voor bedrijven die geen deel uitmaken van een luchtvaartmaatschappij, maar waaraan de luchtvaartmaatschappijen het werk hebben uitbesteed. Het betreft zelfstandige bedrijven die opereren als (onder)aannemer; de verantwoordelijkheid voor de luchtvaartveiligheidsaspecten van hun werkzaamheden berust bij de luchtvaartmaatschappijen. Er is sprake van een relatie tussen opdrachtgever en opdrachtnemer, waarbij de luchtvaartmaatschappijen primair de voorschriften voor de omgang met het vliegtuig bepalen. Daarnaast moeten afhandelaars zich houden aan door de luchthaven bepaalde voorschriften voor orde en veiligheid op het terrein. Nationale overheden hebben via de luchtvaartwetgeving

6 JAR-OPS = Joint Aviation Requirements-Operations. De JAA-regels voor het gebruik van vliegtuigen, zoals vluchtvoorbereiding, vluchtuitvoering, vliegtuiguitrusting (m.n. veiligheidsmiddelen), bemanning, onderhoudsprogramma.

geen directe invloed op afhandelaars met uitzondering van de omgang met gevaarlijke stoffen waarvoor ICAO-richtlijnen gelden. Er bestaat hoofdzakelijk een indirecte relatie tussen overheid en vliegtuigafhandelingsbedrijven, namelijk via de luchtvaartmaatschappijen en de luchthavens. Afhandelingsbedrijven dienen uiteraard wel te voldoen aan de voorschriften die de overheid op het gebied van arbeidsomstandigheden heeft gesteld.

Op het gebied van vliegtuigafhandeling is in 1999 in het kader van de vrije markt een Europese richtlijn van kracht geworden, die erin voorziet dat vliegtuigafhandelingsbedrijven vrije toegang hebben tot de grondafhandelingsmarkt op luchthavens in de EU, de zogenoemde liberaliseringsrichtlijn[7]. De exploitant van de luchthaven heeft wel de mogelijkheid om voorwaarden aan deze toegang te stellen, mits deze relevant, objectief, transparant en niet discriminerend zijn. De richtlijn is vooral bedoeld om gelijke voorwaarden voor vliegtuigafhandelingsbedrijven te scheppen en heeft op bepaalde luchthavens een einde gemaakt aan monopolies op het gebied van vliegtuigafhandeling, onder andere in Madrid en Athene. Op Schiphol was al sprake van verschillende aanbieders van afhandelingsdiensten, maar de richtlijn heeft ook daar tot enige dynamiek op de afhandelingsmarkt geleid door vestiging van nieuwe bedrijven en bedrijfsovernames. Over de effecten van de richtlijn schrijft Dupont in het in 1999 uitgevoerde Kwalitatief Veiligheidsonderzoek Schiphol en Omgeving dat “het proces van het vrijgeven van de markt voor afhandelingsbedrijven niet beheerst heeft plaatsgevonden. Door de druk van de verhevigde concurrentie is de aandacht voor veiligheid in het nauw gekomen.” [DuPont Safety Resources, 1999].

De combinatie van liberalisering en beperkte overheidsinvloed, tezamen met het steeds meer voorkomen van uitbesteding, de toenemende drukte op luchthavens en de kortere omdraaitijden van vliegtuigen leidt tot de vraag welke invloed vliegtuigafhandelingsbedrijven hebben op de betrouwbaarheid, en dan vooral de veiligheid van vliegtuigen.

Het systeem van vliegtuigafhandeling

Vliegtuigafhandeling vindt ‘airside’ plaats binnen de kaders die de luchthavenexploitant daarvoor stelt. De Engelse luchtvaartautoriteit heeft een Airside Safety Management Manual opgesteld dat door veel luchthavens als basis wordt gebruikt voor hun eigen veiligheidshandboek [UK Civil Aviation Authority, 1998]. Hierin staan de vereiste veiligheidskwalificaties voor bedrijven en personen die in het airside-gebied werken. Vliegtuig- of grondafhandeling omvat een groot aantal verschillende activiteiten, waaronder passagiers-, bagage- en vrachtafhandeling, vliegtuigbeweging, vliegtuig-‘servicing’, lijnonderhoud,

7 Richtlijn 96/67/EG van 15 oktober 1996 betreffende de toegang tot de grondafhandelingsmarkt op de luchthavens van de EU.

grondtransport van passagiers en bemanning, en brandstofvoorziening, alsmede de politie- en douaneactiviteiten. Er zijn bedrijven die een scala van diensten aanbieden (meestal op diverse luchthavens in Europa of zelfs wereldwijd) en er zijn bedrijven die gespecialiseerd zijn in één bepaalde dienst. Sommige luchtvaartmaatschappijen doen de afhandeling zelf en beschikken over een eigen grondafhandelingsbedrijf (bijv. KLM Groundservices). Deze zogenoemde zelfafhandelaren kunnen hun diensten ook aan andere luchtvaartmaatschappijen aanbieden.

Tot grondafhandeling wordt ook vluchtafhandeling gerekend. Dit omvat het maken van vluchtplannen, het begeleiden van de vlucht en het opstellen van 'weight and balance sheets' ('load control'). Over het algemeen worden de

Figuur 23.3
Cateringtruck. Bron: ESTEP Special Truck Products BV.

beide eerstgenoemde werkzaamheden verricht door de vliegdiensten van de betreffende luchtvaartmaatschappijen, en de taken voor 'load control' door de afhandelingsbedrijven.

– Een vluchtplan omvat de routebeschrijving, hoogte en snelheid van de vlucht; het vermeldt tevens de uitwijkhavens in geval van noodsituaties en gewijzigde weersomstandigheden op de bestemmingshaven. Het geeft de berekening van de benodigde brandstof met reserve en het bevat ook meteorologische gegevens. Het plan moet worden goedgekeurd door de gezagvoerder van het vliegtuig en ingediend bij de verkeersleiding. Het plan wordt doorgaans opgesteld door 'flight dispatchers'.
– Vluchtbegeleiding is het bewaken ('monitoren') van de vlucht vanaf het moment van vertrek tot aan het moment van aankomst. Voor het geval dat nodig is kan de bemanning op ieder willekeurig moment via de radio contact leggen met de thuisbasis om problemen op te lossen. Dat kan variëren van technische aangelegenheden tot het maken van hotelreserveringen op een uitwijkhaven. Vluchtbegeleiding wordt uitgevoerd door 'operations managers'.
– Het weight and balance sheet dient de gezagvoerder een totaaloverzicht te geven van de massa en de verdeling van de lading om te kunnen beoordelen of de operationele limieten van het vliegtuig niet worden overschreden. Lading wordt gespecificeerd naar passagiers, bagage, vracht, brandstof, en gevaarlijke stoffen. De wijze waarop het vliegtuig wordt beladen is gebaseerd op instructies van de luchtvaartmaatschappij; die instructies zijn per type vliegtuig verschillend. Het weight and balance sheet moet worden ondertekend door degene die de supervisie heeft over de belading van het toestel, de zogenaamde load controller, die daarmee verklaart dat de inhoud van het vliegtuig overeenkomt met het document. Vervolgens dient het weight and balance sheet door de gezagvoerder te worden gecontroleerd en ondertekend. Met de ondertekening van het weight and balance sheet accepteert de gezagvoerder de belading van het vliegtuig voor de voorgenomen vlucht.

Er bestaat een opvallend verschil tussen de VS (en vele andere landen in Noord-, Midden- en Zuid-Amerika) en Europa in de functies van operations manager, flight dispatcher en load controller. In Amerika is voor de uitoefening van deze functies namelijk een overheidsbrevet vereist. In Europa is dat niet het geval. Daar is het brevetteren gedelegeerd aan luchtvaartmaatschappijen.

In IATA[8] hebben grondafhandelaars een internationale (belangen)organisatie, de IATA Ground Handling Council[9], waarvan overigens ook luchtvaartmaatschappijen en luchthavenexploitanten lid kunnen zijn (ca. 400 leden). Deze organisatie heeft een Airport Handling Manual opgesteld en een Standard

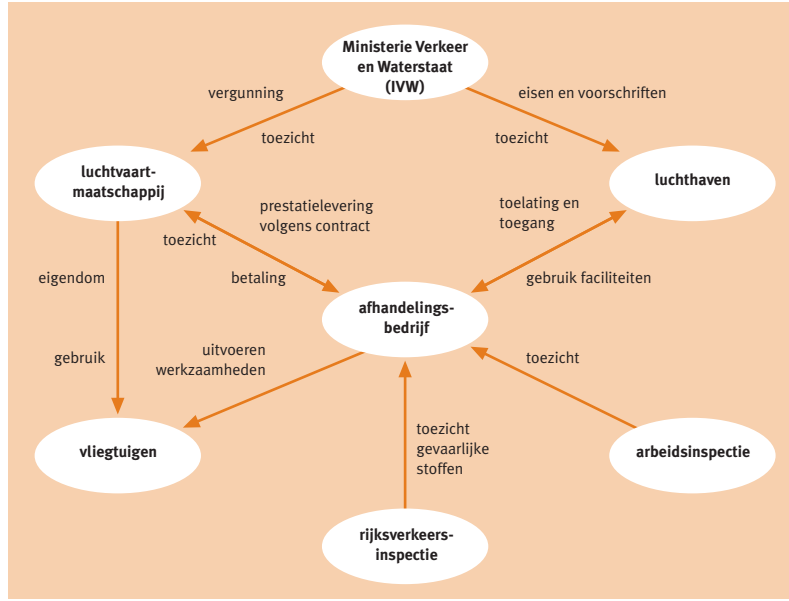
8 IATA = International Air Transport Association (Internationale belangenorganisatie van luchtvaartmaatschappijen).

9 Informatie is te vinden op de website www.iata.org/ighc.

Ground Handling Agreement dat vooral veel wordt toegepast door Europese luchtvaartmaatschappijen. Zoals reeds eerder is vermeld, is het kenmerkend voor het afhandelingsproces dat het (incl. technische controles en lijnonderhoud) geheel plaatsvindt onder verantwoordelijkheid van de luchtvaartmaatschappij. Deze kan ervoor kiezen om het proces in eigen hand te houden (zelfafhandeling) of om het uit te besteden aan een of meer aparte bedrijven. Bij uitbesteding coördineert de grondafhandelaar dus wel bepaalde activiteiten, maar doet dat in opdracht en onder verantwoordelijkheid van de luchtvaartmaatschappij en contractueel geregeld via het eerdergenoemde Ground Handling Agreement. Het opdrachtgeverschap van de luchtvaartmaatschappij komt heel duidelijk tot uiting in de gewoonte bij afhandelingsbedrijven om de passagiersafhandeling uit te voeren in de bedrijfskleding van de betreffende luchtvaartmaatschappij. Passagepersoneel verkleedt zich zodoende verschillende malen per dag.

Figuur 23.4 geeft in een schema de verschillende partijen in het systeem van grondafhandeling en hun onderlinge relaties. Bijlage 2 geeft een overzicht van de afhandelingsbedrijven die momenteel op Schiphol gevestigd zijn.

Wat betreft het kader waarbinnen een afhandelingsbedrijf in Nederland moet werken het volgende. Er is een Regeling Grondafhandeling Luchtvaartterreinen[10], die de minister van Verkeer en Waterstaat de bevoegdheid geeft voor bepaalde categorieën afhandelingsdiensten het aantal verleners te beperken tot niet minder dan twee. Tevens kan de minister criteria vaststellen waaraan dienstverleners moeten voldoen (zoals gezonde financiële positie, voldoende



Figuur 23.4
De verschillende partijen in het systeem van grondafhandeling en hun onderlinge relaties.

10 Regeling van de minister van Verkeer en Waterstaat van 4 februari 1998, nr DGRLD/JBZ/L.98.210058, houdende regels inzake de grondafhandeling luchtvaartterreinen.

verzekeringsdekking, veiligheids- en milieuwaarborgen, adequate arbozorg). Ter concretisering hiervan heeft Schiphol op eigen initiatief een Regeling Afhandeling Schiphol (RAS) opgezet waarin de toelating voor grondafhandelaars is geregeld. In deze regeling stelt Schiphol onder andere als voorwaarden voor toelating dat bedrijven:

- over een gefundeerd businessplan beschikken (d.w.z. klanten hebben);
- over een gedegen veiligheids- en milieuplan beschikken;
- over voldoende financiële draagkracht beschikken;
- gecertificeerd zijn conform ISO 9001:2000 met Schiphol-bijlage. Niet-gecertificeerde bedrijven krijgen na vestiging één jaar de tijd om het certificaat te verkrijgen;
- de IVMS-beleidsverklaring ondertekenen (IVMS = Integraal Veiligheids Management Systeem Schiphol).

Toelating geldt steeds voor een periode van drie jaar.

Een luchthaven kan geen limiet stellen aan het aantal afhandelingsbedrijven dat zich mag vestigen, omdat dit in strijd zou zijn met de liberaliseringsrichtlijn. Londen Heathrow heeft dat in 1998 ondervonden bij een poging maximaal 6 bedrijven voor platform- en bagagediensten en maximaal 9 bedrijven voor vracht toe te laten. Een aantal gebruikers van de luchthaven, waaronder de KLM tekende bezwaar tegen het voornemen aan. De Britse luchtvaartautoriteit (de CAA-UK) toonde weliswaar begrip voor de complexiteit waarvoor de luchthaven zich gesteld ziet, maar oordeelde dat Heathrow onvoldoende aannemelijk kon maken dat een limiet noodzakelijk was en verleende geen toestemming. De CAA-UK was van mening dat Heathrow op grond van de richtlijn voldoende mogelijkheden geboden kreeg om de vestiging van afhandelingsbedrijven op de luchthaven te regelen. Daarom was een limiet overbodig, vond de CAA-UK.

De luchthavenexploitant voorziet in infrastructuur en stelt faciliteiten beschikbaar, waarvan afhandelingsbedrijven gebruik kunnen maken[11]. Zo voorziet Schiphol onder andere in een 400 Hz-voorziening voor energielevering aan stilstaande vliegtuigen, het bagagesysteem, kantoorruimten, incheckbalies, een 'docking'-systeem voor het positioneren van het vliegtuig aan de gate, aviobruggen en afvoer van milieubelastende zaken. Over het gebruik van deze faciliteiten worden met de grondafhandelaars gebruikersovereenkomsten afgesloten. Het beheer en de exploitatie van de vaste brandstofinfrastructuur op Schiphol ligt bij Aircraft Fuel Supply (AFS), een samenwerkingsverband van 11 oliemaatschappijen. AFS levert de kerosine aan drie tankdiensten die deze vervolgens afleveren bij het vliegtuig. Deze tankdiensten worden gerekend tot de grondafhandelingsdiensten, zoals vermeld in Bijlage 1 van de Regeling Grondafhandeling Luchtvaartterreinen.

11 In de VS komt het veel voor dat terminals met bijbehorende voorzieningen eigendom zijn van de luchtvaartmaatschappijen.

Figuur 23.5
Brandstofvoorziening op Schiphol. Bron: Schiphol.

In principe heeft elk grondafhandelingsbedrijf zijn eigen materiaal en wordt er niet aan 'pooling' gedaan. Wel kan het zo zijn dat op een luchthaven een bepaalde dienst slechts door één bedrijf verleend wordt; alle luchtvaartmaatschappijen maken dan van dat bedrijf gebruik. Op Schiphol zijn echter voor alle diensten verschillende leveranciers aanwezig. Op basis van het contract tussen luchtvaartmaatschappij en grondafhandelingsbedrijf kan bepaald zijn dat laatstgenoemde periodiek 'geaudit' wordt. Dit komt echter relatief weinig voor, mede vanwege het grote aantal bestemmingen van veel luchtvaartmaatschappijen. In IACA-verband[12] worden initiatieven ontplooid om dit probleem te ondervangen door poolvorming. Afhandelingsbedrijven worden dan namens de pooldeelnemers geaudit door één luchtvaartmaatschappij in plaats van door elke luchtvaartmaatschappij afzonderlijk. Enkele maatschappijen hanteren al een dergelijke gezamenlijke aanpak voor het auditen van 'de-icing' en tankdiensten. Het verrichten van veiligheidsaudits komt overigens voort uit de eis van JAR-OPS dat een luchtvaartmaatschappij dient te zorgen voor een adequate grondafhandeling op elke bestemming die hij aandoet.

Op grond van de eerder genoemde Regeling Grondafhandeling Luchtvaartterreinen (artikel 8) bestaat op Schiphol een Ground Handling User Committee (SGUC) waarin alle afnemers van afhandelingsdiensten, in casu de luchtvaartmaatschappijen, zijn vertegenwoordigd. Dit overlegorgaan werkt aan gedragscodes en verbeterprogramma's, speciaal gericht op het verbeteren van het veiligheidsbewustzijn. Het SGUC is een door de overheid verplicht orgaan. De verleners van afhandelingsdiensten hebben zich in reactie hierop verenigd in het Schiphol Ground Handling Committee (SGHC) met als doel waar dat nodig is tot samenwerking te komen.

12 IACA = International Air Carrier Association, samenwerkingsverband van 36 luchtvaartmaatschappijen, waaronder Martinair en Transavia.

Voor een gezamenlijke brede aanpak van de veiligheid participeren de bedrijven op Schiphol in IVMS. Deelname in IVMS is nu nog vrijwillig, maar Schiphol wil dit in de toekomst verplicht stellen. Via IVMS worden incidentgegevens uitgewisseld, trends onderzocht en verbeteracties geïnitieerd. IVMS is in principe onafhankelijk, maar de regie is toebedeeld aan Schiphol. Dat wil zeggen dat de coördinatie en het voorzitterschap door Schiphol wordt uitgevoerd. De basis van IVMS wordt gevormd door een centraal incidentendatabestand (OASIS) waarin de incidentmeldingen van de deelnemende bedrijven worden verwerkt. De gegevens in dit bestand zijn vertrouwelijk en alleen toegankelijk voor de deelnemende bedrijven, waarbij die bedrijven in principe alleen toegang hebben tot de door hen zelf gemelde incidenten. Op verzoek kan men echter inzage in meer incidenten krijgen. De gegevens zijn in beperkte mate geanonimiseerd, de gegevens bevatten namelijk geen persoonsnamen. Bedrijfsnamen worden wel vermeld. Het doel van IVMS is vooral de veiligheid te verbeteren, en herhaling van ongevallen en incidenten die hebben plaatsgevonden, te voorkomen. Schiphol brengt hiertoe jaarlijks een niet-openbaar overzicht uit over de gemelde incidenten. Dit overzicht bevat ook conclusies over onderwerpen die aandacht behoeven. Recent is het grote aantal push back-incidenten bijvoorbeeld aanleiding geweest om de push back-procedure te wijzigen. Gezagvoerders kregen via een NOTAM [13] de opdracht om met de push back te beginnen binnen 2 minuten na de klaring hiervoor. De mogelijkheden in IVMS om de betrouwbaarheid van de gegevens te garanderen zijn beperkt. Schiphol controleert regelmatig de meldingsfrequentie van de deelnemende bedrijven. Bij afwijkingen wordt met het betreffende bedrijf contact opgenomen. Meestal loopt in vakantietijd het aantal meldingen sterk terug door de afwezigheid van de verantwoordelijke persoon bij de deelnemende bedrijven.

Ernstige incidenten die op de luchthaven plaatsvinden moeten door Schiphol ook gemeld worden aan de Rijksluchtvaartdienst. Dit betreft ook incidenten waarbij afhandelingsbedrijven zijn betrokken. Schiphol heeft een eigen incidentenbestand, namelijk het Airside Safety Information System. Onderzoek dienaangaande richt zich ook vooral op het voorkomen van herhaling, en niet op het vaststellen van aansprakelijkheid voor schade. Daarvoor dienen alleen rapporten van Luchtvaartpolitie of Marechaussee. Schiphol kent ook een systeem voor anonieme incidentmeldingen, namelijk VOS (Vertrouwenstelefoon Onveilige Situaties). De respons is echter erg laag; er wordt nauwelijks gebruik gemaakt van de mogelijkheid om anoniem te melden. Overwogen wordt daarom hiermee te stoppen. Het Loket Luchtvaartveiligheid van de Handhavingsdienst Luchtvaart (HDL) [14] biedt een mogelijk alternatief.

13 NOTAM= Notice To Airmen, mededelingenblad van de luchtverkeersleiding.

14 De HDL is onderdeel van de Inspectie Verkeer & Waterstaat (IVW), Divisie Luchtvaart.

Bedreigingen

In deze case wordt de betrouwbaarheid van het technische systeem vertaald naar risico's voor mens en vliegtuig. Onder risico's voor het vliegtuig kunnen alle gevaren worden verstaan die het vliegtuig als technisch systeem bedreigen. Beschouwd in relatie tot vliegtuigafhandeling kunnen deze bedreigingen op grond van de incidenten grofweg verdeeld worden in:

- Gevaren die de integriteit van de vliegtuigconstructie bedreigen, zoals aanrijdingen, het niet juist sluiten van deuren.
- Gevaren ten gevolge van het onjuist beladen van het vliegtuig.
- Gevaren die samenhangen met het kleine onderhoud en of het schoonmaken van het vliegtuig, zoals de-icing en het reinigen van de cabine tussen vluchten in.
- Gevaren ten gevolge van het tanken van het vliegtuig.

Onder risico's voor de mens kunnen worden verstaan alle risico's voor passagiers en personeel. Dit zijn dan vooral risico's op het platform. Weliswaar wordt het belangrijkste risico voor passagiers gevormd door het mogelijk neerstorten van het vliegtuig, maar deze bedreiging is identiek aan de bedreigingen voor het vliegtuig en hoeft daarom niet afzonderlijk te worden beschouwd. Op Schiphol en andere grote luchthavens worden passagiers via aviobruggen naar het vliegtuig geleid en hebben geen toegang tot het platform. De risico's hebben dan alleen betrekking op het personeel. De belangrijkste bedreigingen zijn:

- Gevaren die samenhangen met draaiende motoren ('jet-blast') en propellers van vliegtuigen.
- Gevaren die samenhangen met het bedienen van afhandelingsmaterieel, zoals het verliezen van de controle, bekneld raken, of het verkeerd of niet gebruiken van veiligheidsmiddelen.
- Gevaren die samenhangen met het onderlinge verkeer op het platform, zoals het niet in acht nemen van voorrangsregels, botsingen.

Enerzijds hebben de risico's dus betrekking op een veilige vluchtuitvoering en anderzijds op degenen die het werk uitvoeren. In de meeste organisaties wordt over het algemeen een onderscheid tussen deze twee vormen van risico's gemaakt. Het toezicht op de veiligheid van de vluchtuitvoering is vaak toebedeeld aan de kwaliteits- of veiligheidsafdeling van de betreffende luchtvaartmaatschappij. De persoonlijke veiligheid van degenen die het werk uitvoeren heeft een sterke arboinslag en het toezicht daarop is daarom vaak toebedeeld aan een VGM-unit (veiligheid, gezondheid, milieu) in het bedrijf. Het onderscheid tussen de twee soorten risico's wordt gemaakt, omdat gekeken wordt naar de gevolgen van risico's en de daaruit voortvloeiende beschermingsmaat-

regelen. Maatregelen voor persoonlijke bescherming zijn hele andere maatregelen dan die voor de bescherming van het vliegtuig. Kijkend naar het ontstaan van risico's ligt het veel minder voor de hand om dat onderscheid te maken. Gevaren voor verwonding zijn vaak dezelfde als gevaren voor de beschadiging van het vliegtuig. Als een trekkerchauffeur door te weinig rust minder alert is, is hij een gevaar voor zichzelf en voor de vliegtuigen die hij afhandelt.

Uit het voorgaande blijkt dat afhandelingsbedrijven zich bewegen in een werkgebied waar veel mis kan gaan. Het getuigt van goed management om dit punt als uitgangspunt te nemen en de inrichting van de werkprocessen erop te baseren. Risicobeheersing is dus primair op organisatorische leest geschoeid. Incidenten duiden daarom dikwijls op organisatorische tekortkomingen en managementfouten, zoals het niet houden aan voorgeschreven procedures (onwetendheid, tijdsdruk, haast), het inzetten van onvoldoende gekwalificeerde mensen, gebrek aan training en supervisie, werkdruk (ploegendienst, nachtwerk) en onoverzichtelijke werkomstandigheden.

Integriteit van de constructie. Vliegtuigen zijn licht geconstrueerd en daardoor kwetsbaar. Een aanrijding levert al gauw een deuk of een scheur op die tot tijdelijke onbruikbaarheid van het vliegtuig leidt. Zolang dat tijdig wordt gesignaleerd en juist wordt beoordeeld, vormt het geen bedreiging voor de veiligheid. Wel leidt het tot aanzienlijke kosten. Direct omdat een kostbare reparatie moet worden uitgevoerd, en indirect omdat het vliegschema wordt verstoord. Gevaarlijk wordt het als beschadigingen niet worden gemeld of gesignaleerd, of verkeerd worden beoordeeld. Dit is niet ondenkbaar in een drukke werkomgeving, waarin men veelvuldig wordt afgeleid. Ook kan angst voor repercussies een rol spelen. Of wat te denken van een situatie waarin een vliegtuig beschadigd raakt op een locatie waar weinig reparatiefaciliteiten voorhanden zijn. De kans is dan aanwezig dat de ernst van de schade lager wordt ingeschat om in ieder geval de retourvlucht naar de thuisbasis te kunnen maken.

Belading. Ook zonder dat er sprake van schade is, kan door onvolkomenheden in de afhandeling de veiligheid van de vlucht in gevaar komen. De reeds genoemde beladingsfouten zijn daarvan een voorbeeld. Een in 1998 door de Britse luchtvaartautoriteit uitgevoerd onderzoek [CAA-UK, 1998] heeft uitgewezen dat beladingsfouten een regelmatig voorkomend verschijnsel zijn in Groot-Brittannië. De meest voorkomende fout is dat de weight and balance sheets niet correct zijn ingevuld. De formulieren vermelden de hoeveelheid gewicht (passagiers, vracht en brandstof) die zich aan boord bevindt, alsmede hoe die lading is verdeeld over het vliegtuig. Het komt voor dat een late verandering in het gewicht (bijv. toevoeging van een extra vracht) niet wordt gecorrigeerd in het weight and balance sheet. Indien het vliegtuig niet is uitgerust met een eigen weight and

balance systeem, merkt de bemanning de verandering pas direct na de start op als blijkt dat het vliegtuig lastiger te besturen is, of in het ergste geval onbestuurbaar is. Bij moderne vliegtuigen doet zich dit probleem niet voor, omdat die wel over een eigen weight and balance systeem beschikken, waarmee de gezagvoerder een uitstekende controle heeft op het startgewicht en de juiste belading van het vliegtuig. Ook komt het voor dat vergeten wordt de lading te sjorren, waardoor deze gaat schuiven met mogelijke fatale gevolgen voor de zwaartepuntligging van het vliegtuig.

In het aangehaalde onderzoek wordt gebrekkige communicatie tussen vliegtuigbemanning en beladingspersoneel als een belangrijke oorzaak van beladingsfouten gezien. Het in de inleiding genoemde ongeluk met de F-27 die neerstortte door een verkeerd geladen partij kranten, is hiervan een duidelijk voorbeeld. Twee toevallige omstandigheden speelden namelijk een belangrijke rol bij dit ongeluk, namelijk:

– Het vliegtuig bevond zich bij vertrek niet op de luchthaven Gatwick, waar het normaal was gestationeerd. De avond tevoren kon het vliegtuig wegens weersomstandigheden daar niet landen en was uitgeweken naar Luton.
– Men was vergeten de partij kranten in een ander vliegtuig te laden onderweg van Gatwick naar Guernsey.

In eerste instantie was het de bedoeling dat het vliegtuig dat oorspronkelijk de partij kranten had moeten vervoeren zou terugkeren naar Gatwick om de kranten op te halen. Dit vliegtuig kreeg echter kort na de start op Guernsey een technische storing en moest terugkeren. Daarop werd besloten de partij kranten per vrachtauto van Gatwick naar Luton te vervoeren, waarna ze vervolgens door het gereedstaande vliegtuig naar Guernsey konden worden vervoerd. Echter, het beladingspersoneel op Luton was niet bekend met de beladingsinstructies voor een F-27. Ze vroegen de gezagvoerder daarom hoe het vliegtuig beladen diende te worden. Hij beantwoordde die vraag en ging daarna wat drinken. De essentie van de vraag was waarschijnlijk niet goed doorgedrongen tot de gezagvoerder, waardoor hij maar een half antwoord gaf. Hij was de situatie op Gatwick gewend waar het beladingspersoneel de werkzaamheden volledig zelfstandig kon uitvoeren, omdat ze van de hoed en de rand wisten. De gezagvoerder ging er te vanzelfsprekend vanuit dat op Luton dezelfde situatie gold. Dat was helaas niet het geval, met fatale gevolgen.

De-icing en vliegtuigschoonmaak. Ook door fouten bij het schoonmaken en het de-icen kan de veiligheid in gevaar worden gebracht.
Allereerst moet dan worden gedacht aan het sneeuw- en ijsvrij maken van het vliegtuig, in het bijzonder de vleugels en de staartvlakken. Door sneeuw of ijs op de vleugels wordt de luchtstroming rondom de vleugels ernstig verstoord

met als gevolg een sterke reductie van de aërodynamische prestaties van het vliegtuig. Vooral in de start kan dit fataal zijn, omdat te weinig opwaartse kracht (lift) wordt ontwikkeld om te kunnen klimmen. Verschillende vliegtuigen zijn om die reden neergestort. Er zijn technische voorzieningen aangebracht om tijdens de vlucht de vleugels en de staartvlakken van het vliegtuig ijsvrij te houden. Deze voorzieningen werken echter niet bij lage snelheden. Daarom is het noodzakelijk dat de vleugels en staartvlakken voor aanvang van de vlucht worden schoongemaakt. De gezagvoerder moet zich er ook van overtuigen dat deze delen sneeuw- en ijsvrij zijn. Meestal gebeurt dit ook wel, omdat vliegers de gevaren van sneeuw en ijs maar al te goed kennen. Maar het is slechts een van de vele aspecten waaraan een gezagvoerder moet denken. Weliswaar heeft hij de beschikking over een checklist die hem behulpzaam is bij zijn taken, maar effectief heeft hij natuurlijk niet veel tijd om zich ervan te vergewissen dat de vleugels schoon zijn. Bij grote vliegtuigen, zoals de Boeing 747 is het bovendien

Figuur 23.6
De-icing. Bron: KLM Groundservices.

zonder hoogwerker onmogelijk om een goede observatie te doen. In de praktijk zal de gezagvoerder dan blindelings moeten kunnen vertrouwen op de deskundigheid en vaardigheid van het afhandelingsbedrijf, in casu degene die de de-icinginstallatie bedient. Afgezien van de risico's voor de vluchtuitvoering is sneeuw- en ijsbestrijding ook niet zonder gevaar voor het bedienend personeel. Het komt voor dat een vliegtuig al gaat rijden, terwijl dit proces nog niet is afgerond met als gevolg dat de installatie omver wordt getrokken. Recent heeft zo'n ongeluk zich nog in Toronto voorgedaan, waarbij de grondwerktuigkundige zwaar gewond raakte door de val die hij maakte. Drie jaar geleden zijn bij een soortgelijk ongeluk in Montreal 3 mensen om het leven gekomen [Flight Safety Foundation, 1997]. Omdat de gezagvoerder in grote vliegtuigen vanuit zijn positie niet visueel kan waarnemen of het de-icen gebeurd is, wordt vertrouwd op onderlinge radiocommunicatie tussen verkeersleiding, gezagvoerder en grondwerktuigkundige, maar die communicatie is soms gebrekkig.

Een met schoonmaken verbonden risico is ook het tijdelijk afplakken van de statische drukgaatjes om te voorkomen dat zich vuil ophoopt in de gaatjes. Het gevaar hiervan is dat vergeten wordt om voor aanvang van de volgende vlucht het afplakken ongedaan te maken. Primaire vluchtinformatie (vooral snelheid en hoogte) is dan niet meer betrouwbaar. Dit kan desastreus zijn, zoals een ongeluk met een Boeing 757 in de Dominicaanse Republiek in 1998 heeft aangetoond.

Het schoonmaken van ovens aan boord van vliegtuigen gebeurt ook niet altijd even goed. Regelmatig ontvangt de NLA meldingen van ovenbrandjes door aangekoekte etensresten. Deze brandjes zijn niet direct bedreigend voor de vluchtuitvoering, omdat met een brandblusser de brand snel geblust is. Maar indirect zitten er wel risico's aan vast. In de eerste plaats is er een brandblusser minder, die later in de vlucht nog nodig zou kunnen zijn bij een ernstiger brand. En in de tweede plaats kan het oordeelsvermogen van de bemanning worden beïnvloed. Een relatief veel voorkomende incidentmelding betreft namelijk een rook- of brandindicatie in de cabine[15]. Daaraan kunnen velerlei oorzaken ten grondslag liggen, zoals kortsluiting of een haperende airconditioning, maar ook ovenbrandjes. Als ovenbrandjes relatief vaker voorkomen dan andere zaken, neemt de kans op een verkeerde diagnose toe. De oorzaak voor ieder brandgeurtje wordt dan eerst bij de ovens gezocht, hetgeen kostbaar tijdverlies kan opleveren bij het vinden van de werkelijke oorzaak.

15 In 2000 zijn 40 rook- en brandmeldingen in in Nederland geregistreerde vliegtuigen ontvangen (dit komt overeen met 1 melding per 10.000 vluchten). Bron: IVW, Divisie Luchtvaart.

Persoonlijke veiligheid. Uit een studie van de Britse Health & Safety Executive (HSE) uit 1999 [Airports International, 1999] blijkt onder andere dat vliegtuigafhandeling een gevaarlijke sector is om te werken. De HSE constateerde dat in de vliegtuigafhandeling op Britse vliegvelden relatief vijf maal zoveel incidenten plaatsvinden als in de bouw, de sector met het grootste aantal ongelukken in absolute zin. Incidenten werden door de HSE in dit verband gedefinieerd als gebeurtenissen ten gevolge waarvan de betrokken persoon 3 of meer dagen niet in staat was op het werk te verschijnen. Op Schiphol heeft de Arbeidsinspectie het afhandelingsproces onder de loep genomen [Arbeidsinspectie, 1999] en daarbij een aantal zorgwekkende constateringen gedaan. Dagelijks gebeurden er ongelukken met heftrucks, waren er botsingen tussen voertuigen, werden werknemers nauwelijks voldoende getraind of geïnstrueerd om het werk uit te voeren en was er een vuurwerkexplosie tijdens een open dag van een bedrijf.

Omstandigheden

De risico's van grondafhandeling hangen in belangrijke mate samen met de omstandigheden waaronder het werk verricht moet worden, waarbij vooral de inherente procesdynamiek en fluctuaties in de vraag van belang zijn.

Procesdynamiek. Kenmerkend voor vliegtuigafhandeling is dat vaak in zeer korte tijd veel en uiteenlopende activiteiten moeten worden verricht om het vliegtuig gereed te maken voor de volgende vlucht. Een versterkende factor hierbij is dat luchtvaartmaatschappijen een steeds grotere nadruk leggen op een snelle 'turnaround' van hun vliegtuigen, mede in de hand gewerkt door het hanteren van slots door de luchthavens. Ook bij een te late aankomst van een toestel moet alles in het werk gesteld worden om het geplande vertrektijdstip te halen. Dit legt een grote druk op de grondafhandelingsbedrijven om het werk sneller, maar toch veilig uit te voeren. Daar komt nog bij dat veel luchthavens opereren aan de grens van hun capaciteit, waardoor de bestaande infrastructuur – ook voor grondafhandelaars – gaat knellen.

Bovendien zijn vliegtuigen niet altijd even toegankelijk voor afhandelingsactiviteiten. Er is speciaal materieel nodig om ergens bij te kunnen en er moet vaak in kleine ruimten worden gewerkt (zoals in laadruimten). Veelal zijn er verschillende bedrijven bij de afhandeling betrokken, elk met hun eigen materieel en voertuigen (zo'n 30 verschillende) en personeel dat op het juiste moment in actie moet komen. Volgens een betrokkene lijkt het nog het meest op een mierenhoop [Bossenbroek, 1999]. Niet zelden leidt dit in de beperkte ruimte tussen de geparkeerde vliegtuigen en het aankomstgebouw tot congestie. Zeker bij

beperkt licht, slechte weersomstandigheden en met hinder van lawaai en stank vergt het bewegen van typisch gevormde grote stukken in een onoverzichtelijke ruimte grote oplettendheid, waarbij in het bijzonder moet worden opgepast voor draaiende motoren en propellers.

Vanwege de nauw luisterende logistiek van het proces is adequate werkvoorbereiding en planning van uitermate groot belang voor afhandelingsbedrijven. Wegens verschillen in vliegtuigtypen zijn de werkprocessen bij afhandelingsbedrijven typegerelateerd en is er vaak sprake van specialisatie per type. Dit hangt ook samen met de door het bedrijf aan het personeel (vooral load controllers) verstrekte licenties waarin vermeld wordt voor welke vliegtuigtypen de betreffende persoon bevoegd is verklaard. Voor de planning betekent dit een extra afhankelijkheidsfactor. Afhandelingsbedrijven zullen het afhandelingsproces zo proberen te organiseren dat ze zo weinig mogelijk last hebben van dit soort afhankelijkheden om te voorkomen dat het ten koste gaat van de snelheid. Bijvoorbeeld door per gate of per aantal gates een afhandelingsploeg toe te wijzen die voorzien is van alle benodigde apparatuur en typekwalificaties. Een optimaal effect wordt bereikt als het aantal vliegtuigtypen per gate niet al te gevarieerd is.

Vraagfluctuaties. Door verschillen in passagiersaanbod hebben afhandelingsbedrijven het in vakantieperioden drukker dan anders. In de zomermaanden passeren zo'n 4 miljoen passagiers per maand de terminals op Schiphol. In een rustige wintermaand als februari gaat het om zo'n 2,5 miljoen passagiers[16]. Afhandelingsbedrijven vangen de drukte op met de inzet van tijdelijk personeel. Daarnaast geldt dat afhandelingsbedrijven geen grote aantrekkingskracht uitoefenen op werkzoekenden. In sommige sectoren van de luchtvaart resteert nog wel iets van het 'Peter Stuyvesant'-imago, maar in de afhandelingswereld heeft dit imago nooit enige invloed gehad. Gevolg is dat afhandelingsbedrijven zeker in tijden van krapte op de arbeidsmarkt moeite hebben om geschikt personeel te vinden. Tezamen met de toch al aanwezige afhankelijkheid van tijdelijke krachten zorgt dit voor een voortdurend aan verandering onderhevige personeelssamenstelling. Het is dan moeilijk voor deze organisaties om hun kennis en expertise op peil te houden, laat staan te vergroten. Bovendien stimuleert het bedrijven niet om te investeren in uitgebreide samenhangende trainingsprogramma's. Eerder bestaat de neiging zich te beperken tot ad hoc 'on the job'-trainingen van hooguit enkele dagen of alleen tot typetrainingen die nodig zijn voor het verkrijgen van een bedrijfslicentie. Er zijn wel bedrijven met een volwaardig trainingsprogramma, maar dat zijn dan vooral bedrijven die onderdeel zijn van een luchtvaartmaatschappij of van een wereldwijd opererende organisatie.

16 www.schiphol.nl. De genoemde aantallen betreffen juli en augustus 2000 en februari 2001.

Trends

Marktwerking en concurrentie

Voor een grondafhandelaar is een luchtvaartmaatschappij de klant; daar ligt ook de contractuele relatie. Dit komt heel duidelijk tot uiting in het feit dat afhandelingsbedrijven ervoor kiezen om de passagediensten te verrichten in de huisstijlkleding van de klant. In het algemeen trekken de luchtvaartmaatschappijen zich steeds meer terug op de vervoersfunctie en schuiven tegelijk meer taken naar grondafhandelaars. Daardoor komt meer nadruk te liggen op de contracten en de daarbij gestelde expliciete kwaliteitseisen. Deze ontwikkeling wijkt overigens niet af van wat in andere sectoren plaatsvindt. De luchtvaartmaatschappij kan dus kiezen uit verschillende grondafhandelaars en dientengevolge is zijn positie sterker dan vroeger. De toegenomen concurrentie op de grondafhandelingsmarkt leidt enerzijds tot concentratie en anderzijds tot specialisatie. Daarenboven zorgen allianties van luchtvaartmaatschappijen voor wereldwijde behoefte aan dezelfde grondafhandelaar. Dit leidt tot mondiaal werkende afhandelingsbedrijven (dus een bedrijf dat op verschillende luchthavens gevestigd is) die een herkenbare bedrijfsformule nastreven, waardoor de klant overal op de wereld weet wat hij koopt. Toenemende concurrentie betekent echter dat de marges bij grondafhandelaars onder druk staan, hetgeen een voortdurende spanning tussen kwaliteitszorg en kostenbesparing oplevert.

Sinds de Europese Richtlijn van kracht is, is de grondafhandeling op luchthavens in de EU geliberaliseerd (in de VS en Canada was dat al eerder het geval). Elke grondafhandelaar mag zich vestigen, mits hij aan de toelatingseisen voldoet. De toenemende concurrentie die hiervan het gevolg is, kan leiden tot een zekere veiligheidserosie, waarvoor de luchthaven Schiphol zeer beducht is. Als zich ongelukken bij afhandelingsbedrijven voordoen, zal Schiphol daar onmiddellijk de negatieve effecten van ondervinden, omdat bijvoorbeeld de naam van Schiphol eronder te leiden heeft. Er is Schiphol daarom veel aan gelegen een zekere controle over het afhandelingsproces te hebben. Schiphol probeert die controle te krijgen door middel van het invoeren van bepaalde minimumveiligheidseisen, waaraan alle afhandelingsbedrijven moeten voldoen.

Technologie en innovatie

Afhandelingsbedrijven mogen dan in de omstandigheid verkeren dat gebruik kan worden gemaakt van een aantal door de luchthaven beschikbaar gestelde infrastructurele voorzieningen. Voor alle overige voorzieningen moeten ze zelf zorgen. Het betreft dan vooral het rijdend materieel, zoals bagagekarren, tractors, heftrucks, cateringwagens, verrijdbare trappen. In de lucht mogen vliegtuigen er sierlijk en gestroomlijnd uitzien, op de grond zijn het logge en onhandige apparaten om mee te werken, hetgeen lastige en hoge eisen stelt aan ontwerp

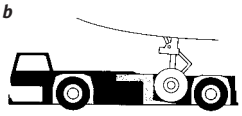
Figuur 23.7
Towbarless tractor. Bron: Goldhofer.

en gebruik van het afhandelingsmaterieel. Vliegtuigen zijn moeilijk toegankelijk. Ze verschillen per type en per model, omvang en vorm leiden gemakkelijk tot beoordelingsfouten, de vleugels zitten in de weg, het landingsgestel vormt een obstakel en ze zijn eenvoudig te beschadigen. Materieel geschikt voor het ene vliegtuig is ongeschikt voor het andere vliegtuig, of slechts te gebruiken onder speciale voorwaarden. Ieder afhandelingsbedrijf heeft zijn eigen materieel dat specifiek geschikt is voor de operaties die het bedrijf uitvoert. Concurrerende bedrijven maken geen gebruik van een gemeenschappelijke pool van materieel.

Figuur 23.8
Schematische weergave van [a] een sleepvoertuig met stang en [b] een towbarless sleepvoertuig. Bron: Goldhofer.

a

b



Technologisch gezien doet het gebruik van karretjes, tractors en trappen nogal verouderd aan in vergelijking tot de beschikbare technologie in vliegtuigoperaties. Wel hebben er natuurlijk voortdurend ontwikkelingen plaatsgevonden om het afhandelingsmaterieel te laten voldoen aan de eisen van de tijd, vooral in verband met grotere en zwaardere vliegtuigen, grotere volumen aan vracht en passagiers en toenemende congestie op de platformen. Zo zijn tractoren in de loop van de tijd steeds krachtiger geworden. De meest recente ontwikkeling is de invoering van de 'towbarless' sleepvoertuigen, waarbij het vliegtuig niet meer via een stang ('towbar') aan een sleepvoertuig wordt gekoppeld, maar

waarbij het neuswiel rechtstreeks op het sleepvoertuig wordt geplaatst. Het sleepvoertuig wordt hierdoor eigenlijk het verlengde van het neuslandingsgestel, waardoor er veel eenvoudiger met het vliegtuig gemanoeuvreerd kan worden. De towbarless tractor biedt belangrijke veiligheidsvoordelen, zoals:

- minder kans op persoonlijke ongelukken, omdat men niet meer in de weer hoeft te zijn met het koppelen van de towbar;
- het verdwijnen van het gevaar van een towbarbreuk, waardoor sleepvoertuig en vliegtuig niet meer ongewenst ontkoppeld kunnen raken (bijv. bij het oversteken van een in gebruik zijnde start- en landingsbaan).

Ook het ijsbestrijdingsmaterieel is in de loop van de tijd steeds geavanceerder geworden, vooral vanuit een toenemende behoefte om onder alle mogelijke weersomstandigheden te kunnen opereren. Luchtvaartmaatschappijen willen betrouwbaarheid garanderen en gaan ervan uit dat passagiers niet zomaar zullen accepteren dat vluchten vanwege het weer worden geannuleerd, of het moet wel heel extreem zijn.

Afgezien van de autonome ontwikkelingen in het afhandelingsmaterieel hebben enkele belangrijke technologische ontwikkelingen in het afhandelingsproces plaatsgevonden. De meeste van deze ontwikkelingen hebben echter op luchthavens plaatsgevonden en niet zozeer bij afhandelingsbedrijven. De belangrijkste ontwikkelingen zijn [McDonald, 1995]:

- Containerisatie van vracht en bagage. Dit heeft de hoeveelheid handelingen die tijdens het afhandelingsproces moeten worden verricht, aanmerkelijk gereduceerd.
- Geautomatiseerde bagageafhandelingssystemen. Grotere volumestromen, langere afstanden die overbrugd moeten worden en kortere overstaptijden noodzaken luchthavens om snellere bagageafhandelingssystemen te introduceren. Deze grotere snelheid kan bereikt worden met behulp van de zogenoemde DCV-technologie (‘Destination Coded Vehicles’), waarbij de bagage via automatisch gestuurde karretjes razendsnel tot aan de bagageruimten op het platform wordt vervoerd. Hoewel de eerste toepassing van deze technologie op de luchthaven van Denver in 1995 op een enorme teleurstelling uitliep (koffers kwamen niet aan op de plaats van bestemming of raakten zoek), wordt het systeem langzamerhand steeds meer toegepast, onder andere ook op Schiphol, waar al enige tijd wordt proefgedraaid met het nieuwe Bagage Afhandelings Systeem (BAS). Met BAS wordt het aantal koffers dat per uur kan worden verwerkt, verhoogd van 3.200 naar 5.400. De technologie is nog volop in ontwikkeling. Verdere versnelling is mogelijk door de bagage rechtstreeks naar de vliegtuigen te transporteren zonder tussenkomst van bagagekarretjes op het platform. In de toekomst kan deze ontwikkeling

worden uitgebreid naar een 'vehicle free ramp', waarbij de hele logistieke voorziening via ondergrondse verbindingen wordt verzorgd en er geen verkeer op het platform meer noodzakelijk is. Hiermee wordt al geëxperimenteerd op de Zweedse luchthaven Stockholm-Arlanda.

Dynamiek

Zoals eerder betoogd is het afhandelingsproces afhankelijk van verschillende factoren die elk aan variaties onderhevig zijn. Hierdoor is het op zichzelf al een dynamisch proces dat een zorgvuldige werkvoorbereiding en planning vereist. Dit jaar zullen bijvoorbeeld op Schiphol in de drukste periode dagelijks tussen de 142.000 en 146.000 passagiers in en uit de vliegtuigen worden geleid en zullen er zo'n 1.200 vliegtuigen worden afgehandeld. Op een rustige dag betreft het ongeveer 73.000 passagiers en 990 vliegtuigen.

Daarnaast staat de afhandelingssector onder invloed van veranderingen die zich in het hedendaagse luchtvaartbestel voordoen. Nu is er sprake van een rijke schakering aan afhandelingsbedrijven qua grootte variërend van gespecialiseerde bedrijven met enkele medewerkers tot wereldwijd opererende bedrijven met honderden vestigingen en duizenden medewerkers. Samenhangend hiermee is er ook een grote verscheidenheid in organisatievormen, besturing en opleidings- en trainingsprogramma's. Hoe deze situatie zich in de toekomst zal ontwikkelen, hangt onder andere af van de invloed van alliantievorming en 'outsourcing' bij luchtvaartmaatschappijen, privatisering van luchthavens en liberalisering van de afhandelingsmarkt. Verschillende scenario's zijn denkbaar, uiteenlopend van verdere diversificatie tot nivellering.

Van alliantievorming valt bijvoorbeeld een nivellerend effect te verwachten. In een alliantie van luchtvaartmaatschappijen is het streven immers gericht op standaardisatie en harmonisatie van het afhandelingsproces, opdat op alle alliantiebestemmingen dezelfde productkwaliteit wordt geleverd. Indien de alliantiepartners verschillende afhandelaars hebben, zal of voor één afhandelaar worden gekozen of de afhandelingsbedrijven zullen nauwer met elkaar gaan samenwerken. Dit zal uiteindelijk resulteren in minder diversificatie. Daarentegen kan van bijvoorbeeld outsourcing een tegengestelde ontwikkeling verwacht worden. Afhandelingsbedrijven zullen zich dan juist van elkaar moeten onderscheiden om de aandacht van luchtvaartmaatschappijen te trekken. Naarmate luchtvaartmaatschappijen zich meer terugtrekken op hun kerntaak (namelijk het vervoeren van passagiers), zullen de verschillen als gevolg van outsourcing nog verder toenemen. In het extreme geval is een luchtvaartmaatschappij niet meer dan een postbusmaatschappij, die geheel afhankelijk is van toeleveranciers.

De wijze waarop de afhandelingssector zich in de toekomst zal ontwikkelen, hangt ook af van de manier waarop luchthavens zich ontwikkelen. Een luchthaven is te beschouwen als een winkelcentrum met de luchtvaartmaatschappijen in de rol van de koper en de afhandelingsbedrijven in de rol van de winkelier. De luchthaven levert slechts de faciliteiten. Een dergelijk 'city'-concept hanteert Schiphol bijvoorbeeld al voor passagiers en omwonenden in de vorm van het Schiphol Plaza. Schiphol heeft ook heel duidelijk het voornemen om dit concept te exporteren in de vorm van deelnemingen in andere luchthavens. Om klanten te trekken heeft Schiphol natuurlijk belang bij een kwalitatief goed aanbod van diensten en om die reden zal Schiphol invloed willen hebben op de bedrijven die zich op de luchthaven vestigen. Selectie en periodieke audits zijn daarbij de instrumenten. Maar aan de andere kant is er toch ook sprake van een functieverruiming. De luchthaven wordt meer dan alleen een voorziening voor het starten en landen van vliegtuigen. De functie van vastgoedexploitant wordt bijvoorbeeld steeds belangrijker, een ontwikkeling die onder invloed van privatisering mogelijk nog sterker zal worden. Wat hiervan op de lange duur de gevolgen zullen zijn voor de afhandelingsprocessen valt moeilijk te voorspellen.

Complexiteit

De complexiteit van een systeem wordt bepaald door het aantal in het systeem aanwezige componenten en het aantal interacties daartussen [Perrow, 1984]. Hoe groter het aantal componenten en het aantal interacties, des te groter het aantal kwetsbaarheden, des te onzekerder de uitkomst en des te groter de complexiteit. Vanwege het aantal actoren en de hoeveelheid invloedrijke factoren is het afhandelingsproces een complex systeem. Dit valt ook af te leiden uit het feit dat er een duidelijke behoefte aan complexiteitsreductie waarneembaar is die zich op verschillende manieren uit. Figuur 23.4 laat zien dat er vier hoofdactoren te onderscheiden zijn:

- Luchtvaartmaatschappijen.
- Grondafhandelaars.
- Luchthaven.
- Toezichthouders.

Met betrekking tot de *relatie luchtvaartmaatschappij-grondafhandelaar* valt te constateren dat het om een relatie tussen opdrachtgever en opdrachtnemer gaat: een grondafhandelaar verleent in opdracht van de luchtvaartmaatschappij een dienst waarvoor een contract wordt gesloten. De kwaliteitseisen waaraan de opdrachtnemer moet voldoen liggen in dat contract vast; de opdrachtgever controleert of aan die eisen wordt voldaan en treft bij geconstateerde gebreken sancties. Als elk contract andere kwaliteitseisen inhoudt, werkt dit voor beide partijen complexiteitsverhogend. Het in allianties opnemen van wereldwijd opererende afhandelingsbedrijven kan worden beschouwd als een

manier om het aantal interacties te beperken, doordat het aantal contractpartners afneemt. Complexiteitsreductie vindt ook plaats door standaardisatie van processen, bijvoorbeeld in de vorm van het Ground Handling Manual en het Ground Handling Agreement (op basis van IATA-afspraken).

De mogelijkheden tot standaardisatie worden echter beperkt door verschillen in vliegtuigtypen en per luchthaven, waardoor afwijkingen van de standaardsituatie altijd zullen voorkomen. Toch loont het de moeite om de diversiteit aan interacties te beperken, waarbij planning en materieelinzet belangrijke instrumenten zijn. Het toewijzen van afhandelingsploegen per gate (of per serie gates) is bijvoorbeeld een manier om het aantal verschillende situaties te limiteren. Het is vergelijkbaar met het zogenoemde 'rondje om de kerk' bij de NS, waar personeel wordt toegewezen aan een bepaald traject. Verder kan de introductie van geavanceerde apparatuur (bijv. het nieuwe bagagesysteem op Schiphol) een bijdrage leveren aan het verminderen van het aantal handelingen dat verricht moet worden, waardoor minder afhankelijkheden ontstaan.

Het toezicht manifesteert zich vooral in de *relaties toezichthouder-luchtvaartmaatschappij en toezichthouder-luchthaven*. De luchtvaartautoriteit stelt regels op over de vliegveiligheid waaraan luchtvaartmaatschappijen moeten voldoen; deze regels werken door in het afhandelingscontract bij de relatie tussen luchtvaartmaatschappij en grondafhandelaar. De inspectie ziet erop toe dat door de luchtvaartmaatschappijen aan de voorschriften wordt voldaan. Voorts stelt de luchtvaartautoriteit regels op over de platformveiligheid; deze regels werken door in de vestigingseisen voor grondafhandelaars op de luchthaven. De inspectie ziet erop toe dat door de luchthaven aan de voorschriften wordt voldaan.

Opvallend is dat de *relatie toezichthouder-grondafhandelaar* zich beperkt tot overheidstoezicht op de naleving van regels over het omgaan met gevaarlijke stoffen en arbeidsomstandigheden bij grondafhandelaars. Waar het vlieg(tuig)veiligheid betreft wordt het toezicht overgelaten aan de luchtvaartmaatschappij en de luchthaven. Er zijn van overheidswege geen veiligheidsvoorschriften voor grondafhandeling (ook niet internationaal vanuit ICAO of JAA). Als elk land dan wel luchthaven zijn eigen voorschriften hanteert, werkt dit voor grondafhandelaars die mondiaal opereren uiteraard complexiteitsverhogend; dit leidt weer tot een roep om uniformering van deze voorschriften. Een pleidooi om de JAA naast regels voor het gebruik van vliegtuigen (JAR-OPS) en voor het onderhoud van vliegtuigen (JAR-145) ook regels voor grondafhandeling te laten opstellen [Schaefers, 2000] staat echter haaks op de opvatting van de JAA dat grondafhandelaars niet tot de primaire luchtvaartactoren worden gerekend. Dergelijke regels zouden de luchtvaartmaatschappijen goed van pas

komen in hun contractuele relaties met grondafhandelaars. Zoals in de paragraaf over het systeem van vliegtuigafhandeling is aangegeven, voeren luchtvaartmaatschappijen wel audits uit, maar in feite ontbreekt de daarbij te hanteren standaard.

Vanuit de toezichthoudende instanties kan globaal aan twee interventies worden gedacht. Ten eerste kan men denken aan middelvoorschriften. Dit is in het algemeen technisch gedetailleerde regelgeving waarin ook voor verdere detaillering verwezen kan worden naar technische normering. Dit wordt vaak toegepast waar de problemen van technische aard zijn. Ten tweede zijn er doelvoorschriften, meer algemeen gestelde regelgeving waarbij het bedrijf vrij gelaten wordt langs welke weg en met welke middelen een doel bereikt wordt. Bij toezicht op deze voorschriften wordt vaak gebruik gemaakt van certificatie. In het algemeen kan gesteld worden dat wanneer de technische veiligheid in het geding is, gebruik gemaakt wordt van technische normering in combinatie met certificatie. Wanneer organisatorische aspecten een rol spelen, wordt vaak alleen certificatie gebruikt .

Met betrekking tot de *relatie luchthaven-grondafhandelaar* valt te constateren dat het hier gaat om een relatie tussen huisbaas en bewoner: een grondafhandelaar mag zich vestigen op de luchthaven, mits hij voldoet aan de huisregels die door de luchthaven zijn opgesteld. De luchthaven controleert of aan die eisen wordt voldaan en treft bij geconstateerde gebreken sancties. Uiteraard kan dit ertoe leiden dat mondiaal opererende grondafhandelaars geconfronteerd worden met toelatingsvoorwaarden die per luchthaven verschillen. Wat Schiphol betreft is in de Regeling Afhandeling Schiphol als voorwaarde voor toelating van grondafhandelaars onder andere opgenomen dat zij gecertificeerd moeten zijn.

Conclusies

In dit essay is een uiteenzetting gegeven over de betrouwbaarheid van het systeem van vliegtuigafhandeling als onderdeel van het totale luchtvaartsysteem. De activiteiten die in het kader van de afhandeling van vliegtuigen op de grond worden verricht zijn de revue gepasseerd en de relaties tussen de belangrijkste actoren zijn besproken. Het systeem is op een aantal punten kwetsbaar en de bedreigingen voor vliegveiligheid en platformveiligheid zijn divers van aard. De ontwikkelingen op dit punt zijn geïllustreerd aan de hand van een aantal gesignaleerde trends:

– De liberalisering van de grondafhandeling op luchthavens in de EU heeft geleid tot toenemende concurrentie tussen oude en nieuwe afhandelings-

bedrijven, waarbij het gevaar van veiligheidserosie op de loer ligt. Hierdoor neemt bij betrokkenen de roep om op grondafhandeling toegespitste regelgeving per luchthaven, per land, dan wel vanuit internationale gremia toe.
- Technologische ontwikkelingen hebben bijgedragen aan een vergroting van de betrouwbaarheid van grondafhandeling en tegelijkertijd een nieuwe afhankelijkheid geïntroduceerd. Op de grond zijn vliegtuigen logge en onhandige apparaten; elk type vergt weer ander afhandelingsmaterieel en terzake kundige mensen. Mede vanwege de korter gewenste turnaround-tijd op een vliegveld worden steeds hogere eisen gesteld aan de afhandelingslogistiek.
- De luchtvaartsector is de afgelopen jaren voortdurend in beweging geweest met als gevolg nieuwe allianties, outsourcing van dienstverlening, privatisering van luchthavens en de hiervoor genoemde liberalisering. De congestie op luchthavens met als direct gevolg verstoring van vluchtschema's heeft ertoe geleid dat de afhandelingstijd voortdurend onder druk staat. Daarbij komt ook nog een aanzienlijke piekbelasting in bepaalde perioden van het jaar.
- De complexiteit in het systeem van grondafhandeling is toegenomen, hetgeen zich uit in een groter aantal componenten (specialisatie via onderaanneming, meer toezichthouders, groter aantal luchtvaartmaatschappijen, enz.) en een groter aantal interacties (meer te bedienen gates, meer (typen) materieel, meer relevante aspecten met bijbehorende regelgeving, meer veiligheidsaudits, enz.).

In het algemeen leiden de gesignaleerde trends tot een toename van de complexiteit in het systeem van grondafhandeling. De strikte planning van het afhandelingsproces vereist dat precies bekend moet zijn welke werkzaamheden moeten worden uitgevoerd, in welke volgorde en door welke mensen, en wat daarbij aan materiaal nodig is. Er is geen ruimte voor afwijkingen in het proces, terwijl die afwijkingen zich natuurlijk toch doorlopend voordoen. Een vliegtuig komt te laat binnen, een sleutelfiguur is ziek en moet vervangen worden, een passagier is zoek, vracht ontbreekt, of materieel raakt onklaar. Die afwijkingen vormen dan de toevallige omstandigheden die het vertrouwen in het normaal feilloos werkende systeem niet langer rechtvaardigen. Vanzelfsprekendheden gelden dan niet meer en het systeem is kwetsbaarder dan men zich realiseert.

De veelheid aan interacties in een complex systeem resulteert erin dat vertrouwen een belangrijke rol gaat spelen. Vertrouwen in technologie, vertrouwen in organisaties en vertrouwen in mensen. In feite is onze samenleving daarop grotendeels gebaseerd. Zonder dat vertrouwen kan samenwerking in ketens, waar een groot aantal partners met elkaar verbonden zijn en elk zijn toegevoegde waarde levert, niet tot bloei komen. Als vliegtuigpassagier is het bijvoorbeeld

ondoenlijk om vooraf na te gaan of het vliegtuig wel luchtwaardig is, of de maatschappij betrouwbaar is en of de bemanning eigenlijk wel geschikt is. De passagier vertrouwt er gemakshalve op dat de bemanning niet met een ondeugdelijk vliegtuig op stap gaat, dat de maatschappij professionele mensen inzet en dat de overheid erop toeziet dat alles volgens de regels gaat. Voor de gezagvoerder van het vliegtuig is het ondoenlijk om alle handelingen van het grondafhandelingspersoneel zelf te controleren; hij vertrouwt er gemakshalve op dat het personeel goed is opgeleid en zich aan de regels houdt. Hij heeft in het algemeen geen andere keus dan het vliegtuig te accepteren op basis van vanzelfsprekendheden.

Beschadiging van het vertrouwen heeft in het algemeen ernstige gevolgen voor het soepel functioneren van de hele keten[17]. Vertrouwen ontstaat echter niet vanzelf, het moet groeien en verdiend worden. Geen enkel systeem zal foutloos werken; dingen gaan ooit kapot en ook de beste mensen maken wel eens fouten. De vele interacties in een complex systeem leiden er bovendien toe dat de uitkomst van systeemprocessen mede afhankelijk wordt van toevallige omstandigheden. Een samenloop van die toevallige omstandigheden blijkt echter dikwijls een onvoorspelbaar effect te hebben, waarbij het gevaarlijk is om uit te gaan van vanzelfsprekendheden. Het ongeluk met de F-27 die neerstortte als gevolg van een verkeerd geladen partij kranten, is daarvoor een goed voorbeeld: een vliegtuig moest wegens slechte weersomstandigheden uitwijken naar een vliegveld waar het normaal niet gestationeerd was en het beladingspersoneel op dat vliegveld was niet bekend met de beladingsinstructies voor dat type vliegtuig, hetgeen de gezagvoerder zich niet realiseerde.

In deze casebeschrijving hebben we de grondafhandeling van vliegtuigen op luchthavens onder de loep genomen als voorbeeld van een technisch systeem waarin de organisatorische kant van de betrouwbaarheidsvraag een belangrijke rol speelt. De relaties tussen de hoofdactoren in het systeem hebben zich door de jaren stap voor stap ontwikkeld naar een hoger niveau van kwaliteitsborging. De nadruk ligt daarbij op de processen die de grootste veiligheidsrisico's geven en op een zodanig systeemontwerp dat bepaalde verstoringen niet tot calamiteiten kunnen leiden. Desondanks doen zich met enige regelmaat incidenten voor die geregistreerd en zorgvuldig onderzocht moeten worden om zicht te krijgen op causaliteiten en trends. Uiteindelijk gaat het steeds om de vraag of het systeem en zijn subsystemen voldoende lerend vermogen hebben om zich te kunnen wapenen tegen oude en nieuwe verstoringen. Alleen dan is vertrouwen in de werking van het systeem gerechtvaardigd.

17 Zie de evaluaties van enkele recente rampen (Enschede, 2000, Volendam, 2001) met als reactie een roep om herstel van het vertrouwen in de overheid.

Referenties

- Airports International. (1999). HSE targets Client Airlines. May. pp22-25
- Arbeidsinspectie. (1999). Project Schiphol. Rapport uitvoering Arbo-beleid in de bedrijven op Schiphol. December
- Bossenbroek, J. How not to Stir up an Ant's Nest, or Balancing Speed with the Need for Safe Practice. (1999). Lezing gehouden op het IIR symposium Ground Operations Safety Management, 14-15 juli
- Data Plus (ref. 98/DP3). (1998). Safety Data Analysis Unit CAA-UK. December
- DuPont Safety Resources (1999). Kwalitatief veiligheidsonderzoek Schiphol en omgeving. november. p62
- Flight Safety Foundation. (1997). Miscommunication leads to three Fatalities during Ground De-icing of Aircraft. Airport Operations Publications. November/December
- http://www.gsetoday.com/NEWS/News-items.htm#febo1-o
- McDonald, N., R. Fuller. (1995). The Management of Safety on the Airport Ramp. In: N. Johnston, N. McDonald, R. Fuller. Aviation Psychology in Practice. Hoofdstuk 4. Avebury Technical. pp68-86
- Perrow, C. (1984). Normal Accidents; Living with High-Risk Technologies. Basic Books, Princeton University Press. pp62-100
- Schaefers, F. (2000). Safety Audit Pooling of Ground Handling at Line Stations. Lezing 12th Annual European Aviation Safety Seminar. Flight Safety Foundation
- UK Civil Aviation Authority. (1998). Airside Safety Management Manual (CAP 642). September

Met dank voor de verstrekte informatie en voor commentaar op de conceptversie aan J.W. Bossenbroek (Dutchport), P.G.C.W. van den Brink (Business Unit Airlines, Schiphol Group), K. Folkeringa (Eurowings), E.R. Galjaard (Products and Procedures, KLM Ground Services), F. Hammecher (Business Unit Airlines, Schiphol Group), F. Schaefers (Quality Assurance, Martinair Operations).

Bijlage 1 Lijst van grondafhandelingsdiensten[1]

1 Administratieve grondafhandeling. Dit omvat:
   a lokale vertegenwoordiging voor luchtvaartmaatschappijen (agenten);
   b toezicht op belading, berichten en telecommunicatie;
   c verwerking, opslag, behandeling en administratie van de vracht;
   d andere door de gebruiker gevraagde administratieve diensten.

2 Passagiersafhandeling. Dit omvat:
   a controle van tickets en reisdocumenten;
   b registratie van bagage;
   c vervoer van bagage tot aan de sorteersystemen;
   d elke andere vorm van assistentie.

3 Bagageafhandeling. Dit omvat:
   a sorteren van bagage in de bagagekelders;
   b beladen en lossen van de transportsystemen tussen vliegtuig en bagagekelders.

4 Vracht- en postafhandeling. Dit omvat:
   a fysieke behandeling ervan;
   b behandeling van bijbehorende documenten;
   c behandeling van douaneformaliteiten, vooral bij vracht;
   d omgang met gevaarlijke stoffen.

5 Platformafhandeling. Dit omvat:
   a het geleiden op de grond van het vliegtuig bij aankomst en bij vertrek, voor zover dit niet door de luchtverkeersleiding wordt verzorgd;
   b assistentie bij het parkeren van het vliegtuig en het verstrekken van de benodigde middelen;
   c de verbindingen tussen het vliegtuig en de dienstverlener op het platform;
   d het beladen en lossen van het vliegtuig, met inbegrip van het verstrekken en inzetten van de benodigde middelen, alsmede het vervoer van bemanning en passagiers tussen het vliegtuig en het luchthavengebouw, alsmede het vervoer van bagage tussen het vliegtuig en het luchthavengebouw;
   e assistentie bij het taxiën van het vliegtuig en verstrekking van de hiervoor benodigde middelen;
   f verplaatsing van het vliegtuig zowel bij aankomst als bij vertrek, de levering en de toepassing van de benodigde middelen;
   g het vervoer, het inladen in en het uitladen uit het vliegtuig van voedsel en dranken.

1 Deze lijst is opgenomen in de Europese Richtlijn.

6 Vliegtuigservicing. Dit omvat:
   a het schoonmaken van de buitenkant en de binnenkant van het vliegtuig, toilet- en waterservice;
   b de klimaatregeling en de verwarming van de cabine, de verwijdering van sneeuw en ijs op het vliegtuig, het ijsvrij maken van het vliegtuig ('de-icing');
   c de inrichting van de cabine met behulp van cabine-inrichting en de opslag van die uitrusting (tapijten, brandblusapparaten, e.d.).
7 Brandstof- en olielevering. Dit omvat:
   a het organiseren en uitvoeren van het vol- en bijtanken van brandstof, met inbegrip van de opslag hiervan, het toezicht op de kwaliteit en kwantiteit van de leveringen;
   b het voltanken met olie en andere vloeistoffen.
8 Lijnonderhoud. Dit omvat:
   a regelmatige handelingen voor de vlucht, waaronder de 'preflight inspection';
   b specifieke door de gebruiker verlangde handelingen;
   c de levering en het beheer van het benodigde onderhoudsmaterieel en de reserveonderdelen;
   d het aanvragen of reserveren van een plaats waar het vliegtuig kan worden geparkeerd en of een hangar om het onderhoud te verrichten.
9 Vluchtafhandeling en administratie van cabinepersoneel. Dit omvat:
   a vluchtvoorbereiding;
   b vluchtbegeleiding;
   c indeling cabinepersoneel (roosters).
10 Grondtransportafhandeling omvat vervoer van passagiers, bemanning, bagage, vracht en post tussen verschillende stationsgebouwen op het luchthaventerrein. Omvat niet het vervoer tussen vliegtuig en luchthavengebouwen.
11 Catering omvat:
   a contacten met de leveranciers en de administratieve verwerking;
   b het opslaan van voedsel, dranken en de voor het bereiden hiervan benodigde hulpmiddelen;
   c het schoonmaken van het toebehoren;
   d het voorbereiden en leveren van het materieel en de voedingsmiddelen.

Bijlage 2 Afhandelingsbedrijven op Schiphol

Generieke bedrijven
KLM (Ground Services)
GlobeGround
Ogden (Menzies)
DutchPort
AviaPartner
Martinair (platform)
CSC-Ned (vracht)
AviaTrading (vracht)
Aero Ground (vracht)

Specifieke bedrijven (catering)
Alpha Flight Services
Gate Gourmet
KLM-Catering
Martinair

Specifieke bedrijven (schoonmaak)
Crombeen
ISS
LAVOS
Rijnstreek
AMS
Air Services
Asito

2

24
Invoering IEC 61508/61511 bij Shell

ing. J.A.M. Wiegerinck [1]

Inleiding

De Europese industrie en dus ook Shell in Europa behoort haar installaties en productieprocessen te beveiligen overeenkomstig de nationale en Europese wetgeving zoals de EC 'Seveso 2'-richtlijn. Tot nu toe hield de overheid zich niet intensief bezig met die aspecten van het handhaven van veiligheid waarbij instrumentele beveiligingssystemen gebruikt worden om de nodige risico's te beperken. Dit zou wel eens kunnen veranderen gezien de gebeurtenissen in Volendam en Enschede. Het NRC schreef op 19 maart 2001 "De burgemeester (Mans) schaarde zich achter het pleidooi van Oosting voor een cultuuromslag, niet alleen in Enschede, maar voor heel Nederland." Volgens Mans betekent dat onder meer een lik-op-stuk-beleid, geen terugtredende, maar een optredende overheid en expliciete aandacht voor veiligheid [NRC, 2001].
De overheid heeft met de nieuwe functionele veiligheidsstandaard IEC [2] 61508/61511 (zie ook hoofdstuk 6, deel 1) een uitstekende standaard in handen om te verifiëren of industrieën met betrekking tot instrumentele beveiligingen aan de intenties van bijvoorbeeld de Seveso 2-richtlijn voldoen. Hierdoor zal de industrie gedwongen worden om ook instrumentele beveiligingen op een traceerbare, verifieerbare en consistente manier te ontwerpen, in bedrijf te stellen en te beheren. Voor nieuwe installaties worden de eerste projecten al volgens deze standaard ontwikkeld.

1 Shell Global Solutions International BV
Postbus 541
2501 CM Den Haag

2 International Electrotechnical Committee.

Instrumentele beveiligingen zijn die beveiligingsfuncties in een proces die worden gerealiseerd met behulp van elektrische, elektronische of programmeerbare elektronische apparaten (instrumenten). De IEC 61508 stelt eisen aan de ontwikkeling, de bouw, het in bedrijf stellen, en het onderhoud van deze instrumentele beveiligingen.
Tot voor kort werden deze beveiligingssystemen gebouwd op basis van ervaring, overlevering ('dit doen we altijd zo'), en een professionele beoordeling van de risico's die met procesvoering verbonden zijn. De systemen werden uitgebreid met additionele functies en instrumenten, wanneer incidenten en ongelukken daartoe aanleiding gaven. Eisen aan de gevoeligheid voor storingen ('fault tolerance') werden vastgesteld op puur kwalitatieve gronden ('Deze meting is erg belangrijk en moet dus 2oo3 ((2 uit 3[3])) worden uitgevoerd.').
Voor test- en inspectie-intervallen werd de algemene praktijk in de industrie aangehouden of bepaald aan de hand van specifieke eisen, zoals die voor op aardgas gestookte installaties gelden. Alhoewel de chemische industrie een behoorlijke reputatie op het gebied van betrouwbaarheid en veiligheid heeft opgebouwd, was het noodzakelijk om de betrouwbaarheid en veiligheid verder te verhogen om met de trends (zoals mondialisering en toenemende kennisintensiteit) te kunnen omgaan.
Met de ontwikkeling en publicatie van deze standaard worden belangrijke hulpmiddelen geboden voor het op meer gestructureerde, rationele en traceerbare gronden bepalen van de eisen die gesteld moeten worden aan instrumentele beveiligingssystemen.

Deze eisen worden niet alleen gesteld aan de instrumenten en systemen die hiervoor nodig zijn, maar – eigenlijk nog belangrijker – aan het ontwerpproces dat aan het stellen van en het voldoen aan de eisen ten grondslag ligt. De IEC 61508 stelt eisen aan het doorlopen van alle levensfasen van de installatie. Het is een universele standaard die van toepassing is op alle sectoren van de industrie, bijvoorbeeld op de spoorwegen, de procesindustrie, de luchtverkeersleiding. De IEC heeft zich tot taak gesteld om afgeleide standaarden uit te brengen die specifiek zullen zijn voor een bepaalde sector. Zo is momenteel de IEC 61511 in voorbereiding voor de procesindustrie. Omdat Shell vooral in de procesindustrie actief is, wordt in dit artikel veelal verwezen naar de 'IEC 61508/61511'.
In Nederland is een bedrijf (nog) niet wettelijk verplicht om zijn instrumentele beveiligingen te ontwerpen en te onderhouden conform de eisen van de IEC 61508/61511. In andere landen zoals in het Verenigd Koninkrijk verwachten de autoriteiten al wel van de industrie dat men aan de IEC/BS 61508 voldoet.

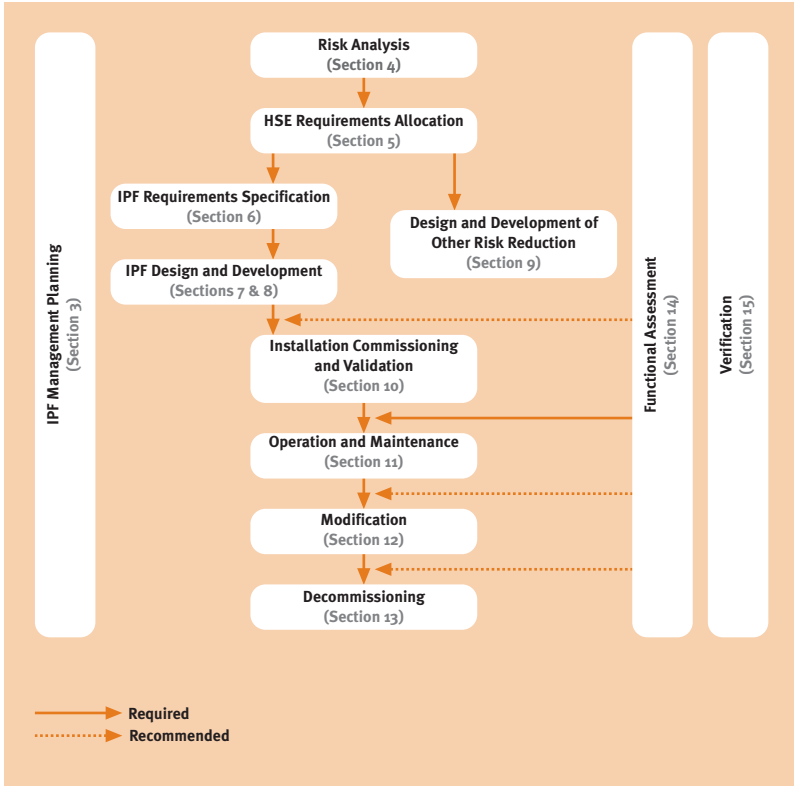
3 2 uit 3 wil zeggen dat er een drievoudige meting wordt gedaan door drie sensoren en twee daarvan moeten een signaal geven.

Intenties en het concept van IEC 61508/61511

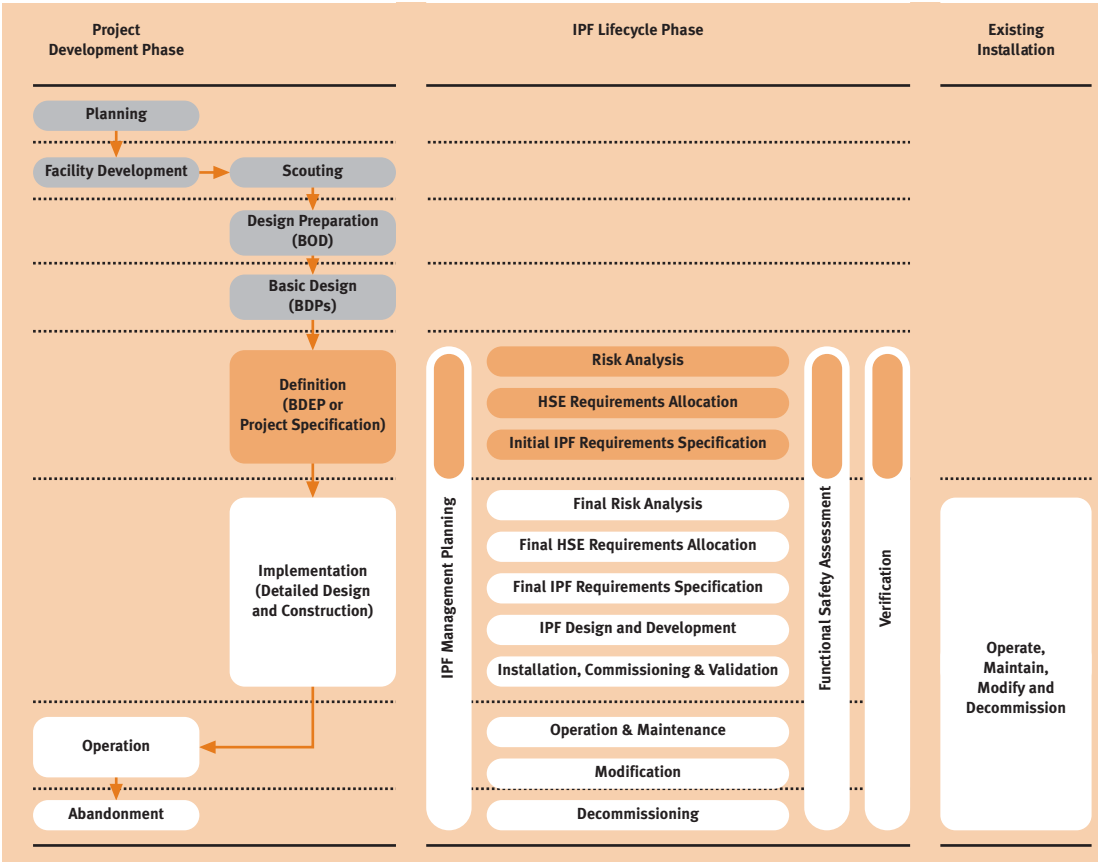
Reeds vele jaren worden elektronische en computergebaseerde instrumenten en systemen toegepast om processen te besturen. Dat geldt in het algemeen ook voor veel niet aan veiligheid gerelateerde toepassingen. Het laatste decennium worden deze systemen echter ook steeds meer toegepast om processen te bewaken en de veiligheid te waarborgen. Bij veiligheid moet hier niet alleen gedacht worden aan de veiligheid van personen in en om de bedrijven en installaties, maar ook van het milieu en aan de instandhouding van de installaties en de procesvoering.

De IEC 61508/61511 geeft normen en richtlijnen voor de veiligheidsaspecten die bij het ontwerp- en onderhoudsproces een rol spelen in het geval elektronische en computergebaseerde instrumenten en systemen worden gebruikt (zie hoofdstuk 6, deel 1).

De standaard is gestructureerd rond een levenscyclusconcept om alle eisen aan ontwerp, onderhoud en wijzigingen aan de installatie en het management daarvan in kaart te brengen. Deze levenscyclus kan van bedrijf tot bedrijf enigszins verschillen en de gebruikers van de standaard kunnen er dus enigszins van afwijken. Shell heeft het levenscyclusmodel van de IEC 61511 overgenomen (zie figuur 24.1).



Figuur 24.1
Levenscyclusmodel dat bij Shell wordt gebruikt. Bron: Shell Global Solutions International BV.

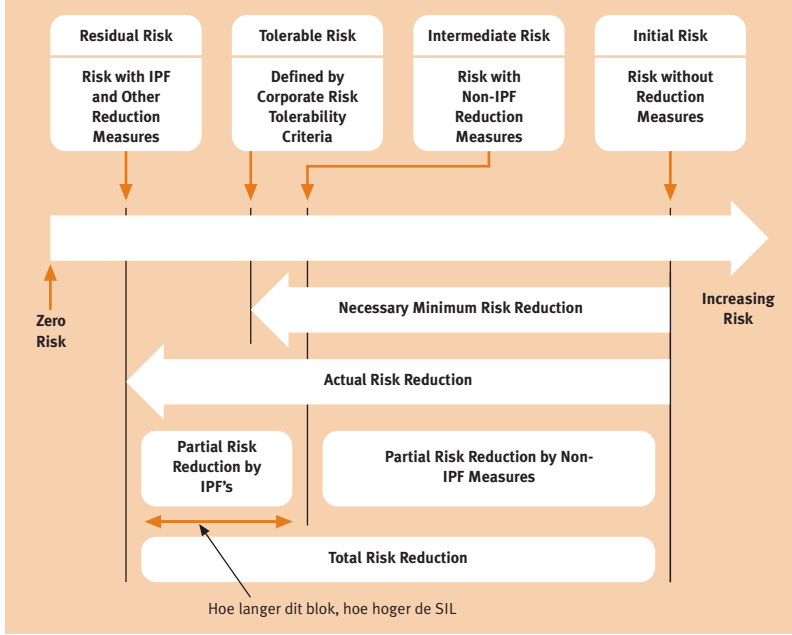


Figuur 24.2
Levenscyclus zoals deze in een nieuwbouwproject gehanteerd zou kunnen worden. Bron: Shell Global Solutions International BV.

Omdat in de meeste projecten het ontwerp in twee fasen wordt uitgevoerd (de projectspecificatiefase en de gedetailleerde ontwerpfase), zijn ook de relevante stappen van het model zoals in figuur 24.2 is weergegeven, opgesplitst.

In de meeste gevallen worden de beveiligingsfuncties niet alleen uitgevoerd met behulp van elektronische of programmeerbare apparaten, maar wordt ook gebruik gemaakt van mechanische, hydraulische of pneumatische technieken. Hoewel de IEC 61508/61511 specifiek betrekking heeft op elektronische en programmeerbare instrumenten, biedt het tevens een basis waarmee de eisen aan andere dan elektronische apparaten kunnen worden geformuleerd. In de praktijk betekent dit dat ook de eisen aan de functionele veiligheid van bijvoorbeeld pneumatisch bediende veiligheidsafsluiters met de IEC 61508/61511 worden geformuleerd.

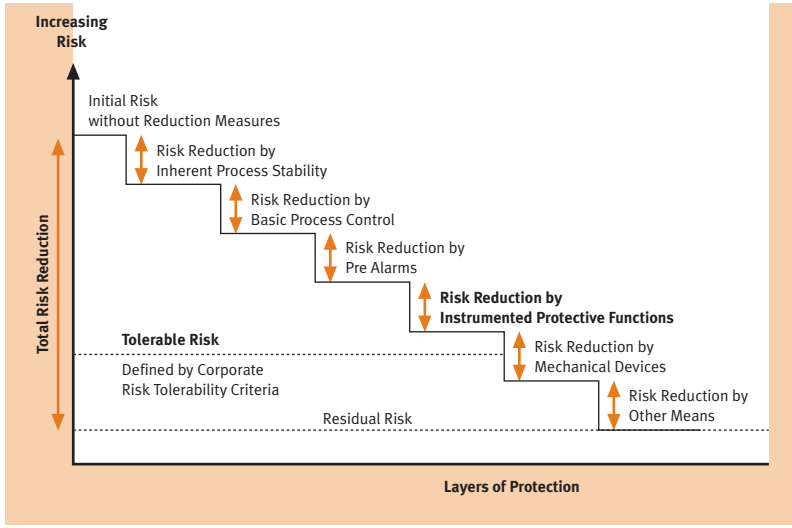
De IEC 61508/61511 gebruikt ‘safety integrity levels’ (SIL) om een gewenste integriteit voor veiligheid te kunnen specificeren (zie hoofdstuk 6, deel 1). De SIL van een beveiligingsfunctie wordt bepaald aan de hand van het risico waartegen moet worden beveiligd, of beter aan de hand van de gewenste risico-



Figuur 24.3
Het concept van risicoreductie. Bron: Shell Global Solutions International BV.

reductie om het initiële risico (het risico dat zou bestaan zonder de functie) tot aanvaardbare proporties terug te brengen. Dit concept van risicoreductie tot aanvaardbare niveaus wordt geïllustreerd in figuur 24.3.

De IEC 61508/61511 stelt een numeriek doel aan de faalkans en aan de storingsgevoeligheid (fault tolerance) van beveiligingsfuncties.
Hoewel de IEC 61508/61511 een groot aantal eisen stelt aan functies waarvan de integriteit is bepaald, stelt de standaard geen eisen aan het restrisico dat nog als aanvaardbaar mag worden beschouwd. Bedrijven of de overheid zullen dus zelf moeten bepalen welke risico's zij nog aanvaardbaar vinden.



Figuur 24.4
Beveiligingslagen ('layers of protection'). Bron: Shell Global Solutions International BV.

Uiteraard vormen de instrumentele beveiligingen slechts een onderdeel van de totale voorzieningen die de risico's van bedrijfsvoering tot een acceptabel niveau moeten terugbrengen. Dit wordt geïllustreerd in figuur 24.4. In deze figuur zijn de maatregelen die tot doel hebben om de gevolgen van een incident te beperken, niet weergegeven. Dat zijn bijvoorbeeld het aanhouden van veilige afstanden tussen installaties, voorzieningen om de verschillende delen van het proces te kunnen isoleren, en systemen om de installatie gecontroleerd van druk te laten, gas- en branddetectie en alarmsystemen, sprinklerinstallaties, een brandvertragende behandeling van staalconstructies en bekabeling, evacuatieplannen, brandweer en eerste hulp.

SIS Safety Management

Voor de Europese procesindustrie is de Seveso 2-richtlijn[4] van de Europese Unie van kracht.
Deze richtlijn houdt onder andere in dat de grotere industrieën ('top tien establishments') een veiligheidsrapport indienen bij de autoriteiten. Dit rapport bevat zowel een paragraaf over het totale veiligheidsmanagementsysteem van het bedrijf als een paragraaf waarin het functioneren en de betrouwbaarheid van de instrumentele beveiligingen worden beschreven. Hierbij worden details verwacht over zowel procesbeveiligingssystemen als over brand- en gasdetectie, en alarmsystemen. Ook het test- en onderhoudsregime moet worden beschreven.
Al met al zou men het beste kunnen voldoen aan de eisen die de IEC 61508/61511 stellen aan het veiligheidsmanagement van instrumentele beveiligingen. Dat zal dan immers automatisch betekenen dat men aan de veiligheidseisen van de Seveso 2-richtlijn voldoet. Dit houdt dan in dat men voor elke fase in de levenscyclus van een instrumenteel beveiligingssysteem de volgende aspecten heeft vastgelegd:

- Gedefinieerde en mogelijke gedelegeerde verantwoordelijkheden.
- Verlangde competenties en mogelijke opleidingsbehoeften.
- Procedures en instructies voor werkzaamheden.
- Procedures voor 'Management of Change' (MoC).
- Procedures voor verificatie en validatie van de resultaten, enzovoorts.

Kortom, 'Wie doet wat, hoe en wanneer, met behulp van wie en wat is daarvoor nodig? Welke eisen worden er gesteld aan vakbekwaamheid en hoe controleren we die zaken?'

4 De richtlijn heeft tot doel om de risico's die complete procesinstallaties voor hun omgeving, het milieu en het personeel met zich meebrengen in kaart te brengen en zo veel mogelijk te beperken.

IEC 61508/61511 bij Shell

Shell heeft de technische functies decentraal georganiseerd. De centrale functies (in Den Haag, Amsterdam en Thornton) hebben een adviserende rol. Groepsmaatschappijen zijn niet verplicht om gebruik te maken van de centrale functies. Deze centrale diensten worden op commerciële basis aangeboden. De Shell-standaarden ('Design and Engineering Practice', DEP) worden aan de groepsmaatschappijen aangeboden via een soort abonnementsysteem. Wanneer een groepsmaatschappij is 'geabonneerd' op de 'DEP's', krijgen ze regelmatig 'updates'. Zo niet, dan moet zo'n maatschappij zijn eigen normen stellen of selecteren uit bestaande internationale standaarden. Zelfs als een groepsmaatschappij is geabonneerd op de DEP's, is er geen verplichting om deze ook in de praktijk te brengen. Dit gebeurt meestal pas, wanneer er sprake is van een nieuw project, omdat de perceptie bestaat dat de DEP's alleen betrekking hebben op het ontwerpen en bouwen van een installatie.

Men kan twee aspecten bij instrumentele beveiligingssystemen onderscheiden:

1 Het ontwerpen en realiseren van een beveiligingssysteem.
2 Het managementproces dat het ontwerpen, realiseren, in bedrijf stellen, onderhouden, en modificeren ondersteunt, zodat de kans op (menselijke) fouten wordt geminimaliseerd.

Voor het ontwerpen en realiseren van deze systemen heeft Shell al sinds 1994 een methode die het bepalen van de SIL, en het implementeren in goede banen leidt. Deze methode 'Instrumented Protective Functions' (IPF) wordt vooral toe-

Figuur 24.5
Het resultaat van het overstromen van een opslagtank met benzine.

gepast tijdens het ontwerpen van nieuwe installaties of wanneer de instrumentatie geheel vervangen wordt. Deze IPF-methode bepaalt niet alleen de SIL, maar stelt de gebruiker ook in staat om de noodzakelijke testintervallen te bepalen. In toenemende mate worden nu echter ook de bestaande installaties geanalyseerd om te verifiëren of de installaties en het onderhoudregime voldoen aan de huidige veiligheidsnormen.

Voor het veiligheidsmanagementproces voor instrumentele beveiligingen is kort geleden een Shell-standaard geschreven die beschrijft hoe dit proces het beste in de bestaande structuren en werkmethoden kan worden uitgevoerd. Daarbij is als voorbeeld het SIS-managementplan gevoegd. Dit plan zal op korte termijn bij de diverse werkmaatschappijen worden geïntroduceerd. Ook is een speciale workshop gepland die deze standaard bij de relevante personen bij een Shell-groepsmaatschappij introduceert. Deze workshop beoogt de gewenste cultuuromslag te initiëren, waarna de groepsmaatschappij de managementprocessen waar nodig zal aanpassen aan de volgende aspecten:

- Organisatie en procedures.
- Verantwoordelijkheden en delegatie van verantwoordelijkheden.
- Leiderschapskwaliteiten van de verantwoordelijke personen.
- Benodigde competenties en training.
- Periodieke verificatie en validatie.
- Vermijden van tegenstrijdige doelstellingen.

Tabel 24.1 geeft de belangrijkste ‘drivers’ en ‘blockers’ voor de introductie van de IEC 61508/61511 bij Shell voor zowel nieuwe projecten als bestaande installaties.

Er wordt gewerkt aan een ‘audit’/’review’-systeem dat de groepsmaatschappijen in staat zal stellen om de integriteit van hun installaties en het bijbehorende onderhouds- en inspectieregime en hun managementprocedures te vergelijken met een benchmark, met andere (Shell en niet-Shell)-bedrijven en met hun eigen prestaties in voorgaande jaren.

Ook bij de Shell-vestigingen in de VS wordt veel nadruk gelegd op veiligheidsmanagement zoals de IEC 61508/61511. Niet alleen omdat Shell een veilige bedrijfsvoering van zijn processen hoog in het vaandel voert, maar ook omdat de Occupational Health & Safety Authority (OSHA) heeft verklaard dat de beste manier om aan de wetgeving op dat gebied te voldoen de ANSI/ISA SP 84.01 is. (Deze standaard is vergelijkbaar met de IEC 61508/61511.)

Tabel 24.1
De belangrijkste 'drivers' en 'blockers' voor de introductie van de IEC 61508/61511 bij Shell voor zowel nieuwe projecten als bestaande installaties.

'Drivers'	'Blockers'
Nieuwe projecten	
Kostenreductie van het instrumentele beveiligingssysteem, vereenvoudiging van het ontwerp	Grote inspanning om de SIL te bepalen van iedere functie
Eisen van autoriteiten	'Process licenser'[5] laat geen wijzigingen toe en werkt niet mee
Goede onderbouwing van het test-regime	Fabrikanten van grote 'packaged unit'[6] werken niet mee
Verbeterde beschikbaarheid van de installatie	Verbeterde veiligheid is niet zichtbaar (op zijn best is het slechts statistiek). Werkelijke faal-kansen van instrumenten zijn slecht bekend.
Bestaande installaties	
Eisen van autoriteiten	Grote inspanning om de SIL van iedere functie te bepalen
Goede onderbouwing van het testregi-me om veiligheid aantoonbaar te ver-beteren	Er is al een testregime. De testintervallen staan onder druk (langer) om kosten te besparen. De verminderde veiligheid bij langere testinterval-len wordt niet onderkend. Afsluiters worden getest volgens 'als het niet kan zoals het moet, moet het maar zoals het kan'.
Verbeterde beschikbaarheid van de installatie	De beschikbaarheid van de installatie moet al slecht zijn, voordat op een gestructureerde manier het probleem wordt aangepakt. Er wor-den ad hoc-oplossingen gezocht en maatregelen genomen.
Een incident dat aanleiding gaf om te twijfelen aan de integriteit van de installatie	Process licenser laat geen wijzigingen toe en werkt niet mee
Een 'audit' of 'review' die duidelijke zwakten in de installaties aantoont	Fabrikanten van grote packaged unit werken niet mee
Mogelijkheid tot uitbesteden van goed gedefinieerde inspectietaken door gecertificeerde monteurs	Verbeterde veiligheid is niet zichtbaar (op zijn best is het slechts statistiek). Werkelijke faal-kansen van instrumenten zijn slecht bekend.
	Er zijn al zoveel eisen waaraan voldaan moet worden. De zaken die direct geld opleveren wor-den het eerst gedaan, zoals Risk Based Inspection en Reliability Centred Maintenance

5 Een 'Process Licenser' is een bedrijf dat het patent heeft op een bepaald petrochemisch proces en licenties uitgeeft aan andere bedrij-ven die dat proces willen gebruiken. De licentieovereenkomst stelt vaak in detail eisen aan de procesregeling en beveiliging.

6 Een 'packaged unit' is een kant-en-klaar geprefabriceerd onderdeel van een fabriek, bijvoorbeeld een complete stoomketel of gasturbine-installatie.

Referenties

– NRC Handelsblad. (2001). Webpagina's. 19 maart

2

25 Helikopters in de offshore-industrie in de Noordzee

dr. G.L. Wackers[1]

De betrouwbaarheid van betrouwbaarheidstechnologieën

> "History arises when the space of possibilities is too large by far for the actual to exhaust the possible."
> *Stuart Kauffman, At home in the Universe (1995)*

Inleiding

In de vroege ochtend van 8 september 1997 stortte een Super Puma helikopter (geregistreerd als LN-OPG) van het Noorse (helikoptertransport)bedrijf Helikopter Service AS ongeveer 200 kilometer uit de kust van Noorwegen in zee. Alle inzittenden (10 passagiers en 2 piloten) kwamen om het leven.

1 Universiteit Maastricht,
Capaciteitsgroep
Maatschappijwetenschap en
Techniek
Postbus 616
6200 MD Maastricht

De helikopters die in de Noordzee voor het personenvervoer naar en tussen olie- en gaswinningsinstallaties worden gebruikt behoren tot de besten ter wereld. De helikopter was uitgerust met een 'Health and Usage Monitoring System' (HUMS) dat bedoeld en ontworpen was om dergelijke fatale ongelukken te voorkomen. HUMS-systemen registreren tijdens iedere vlucht van een toestel vibratiepatronen in motoren, transmissies en rotorsystemen van de helikopter. Veranderingen in die patronen ten gevolge van slijtage of dreigende breuk door metaalmoeheid kunnen met behulp van computersoftware worden opgespoord, zodat tijdig adequate onderhoudsmaatregelen kunnen worden genomen. HUMS is een betrouwbaarheidstechnologie: geïntroduceerd en geïnstalleerd om de betrouwbaarheid (veiligheid, beschikbaarheid) van helikopters te vergroten. HUMS faalde echter in LN-OPG op 8 september.

In dit hoofdstuk zal ik proberen te verklaren waarom HUMS in deze helikopter faalde in zijn vroegdiagnostische functie. In de volgende paragraaf zal ik eerst iets meer zeggen over de omstandigheden en over de directe oorzaak van het ongeluk. Daarna zal ik uitleggen hoe HUMS-systemen werken en met welke verwachtingen de technologie in het begin van de jaren negentig in de offshore-industrie in de Noordzee werd geïntroduceerd. Vervolgens zal ik de ervaringen, processen en mechanismen schetsen die een rol hebben gespeeld rondom de invoering van HUMS bij Helikopter Service AS. Deze processen hebben bijgedragen aan een verhoogde, maar niet tijdig onderkende kwetsbaarheid van het systeem. Ten slotte zal ik proberen aan te geven welke lessen we uit de analyse van dit ongeluk kunnen trekken.

Het ongeluk

LN-OPG, een helikopter van het type Super Puma AS 332L1, was op weg van een helikopterbasis bij Brønnøysund ten noorden van Trondheim in midden Noorwegen naar een nieuwe, drijvende productie-installatie bij het Norne-veld. De Noorse oliemaatschappij Statoil was operateur op Norne. De productiestart van Norne was voorzien op 1 oktober 1997. De bouw van het productieschip had echter ernstige vertraging opgelopen. Statoil besloot in juni 1997 het schip naar het veld te slepen en het ter plaatse af te bouwen, terwijl in de omgeving van het schip de productiebronnen werden geboord. Omdat het voor een normale productiefase berekende aantal bedden op het schip niet toereikend was, moest een aantal arbeiders dagelijks heen en weer pendelen tussen het vaste land en het schip. Zo ook op 8 september 1997.
Na een ongestoorde vlucht bij goede weersomstandigheden met nog ongeveer 5 minuten te gaan meldden de piloten van de helikopter zich af bij de verkeerstoren van het vliegveld van Bodø en meldden zij hun komst bij de radiocentrale

van een boorplatform in de buurt van het Norne-schip. Toen de helikopter na twintig minuten nog niet aangekomen was, werd groot alarm geslagen. Niemand had een SOS-bericht van de helikopter ontvangen. Omdat het exacte tijdstip en de plaats van het ongeluk niet bekend waren, moest een groot zeegebied doorzocht worden. Enkele uren later werden de eerste drijvende wrakstukken gevonden, waaronder een compleet rotorblad van de hoofdrotor. De onderdelen waarmee het blad aan het rotorhoofd bevestigd had gezeten, bleken onbeschadigd te zijn.
In een helikopter is de hoofdrotor niet-redundant uitgevoerd. De rotor wordt dan ook gezien als de achilleshiel van een helikopter, een kwetsbaar punt. Een Super Puma helikopter heeft twee motoren. Elk van die motoren is krachtig genoeg om alleen voor de noodzakelijke aandrijving te zorgen. Zolang de piloten de rotor kunnen besturen, kan een helikopter zelfs bij het uitvallen van beide motoren nog een noodlanding maken, omdat het windmoleneffect ervoor zorgt dat de rotoren blijven draaien. Het verlies van een rotorblad tijdens de vlucht, bijvoorbeeld door het losgaan of –breken van de bouten waarmee het blad aan het rotorhoofd bevestigd is, zou het abrupte karakter van het ongeluk kunnen verklaren.

Nadat het wrak van de helikopter op de zeebodem was gelokaliseerd, werd het enkele dagen later gelicht. Uit inspectie van de motoren bleek dat deze zwaar beschadigd waren. Uit nader technisch onderzoek bleek dat niet het falen van de hoofdrotor de directe oorzaak van het ongeluk was, maar het technisch falen van de verbinding tussen de (holle, cilindrische) aandrijfas van een van de motoren met de as van de hoofdversnellingsbak. Die verbinding bestond uit twee getande manchetten die als sleutel en slot in elkaar grepen en die op de beide uiteinden van de assen waren gemonteerd. Het metaal van de manchet die op de as van de versnellingsbak gemonteerd was (de ‘splined sleeve’) brak als gevolg van metaalmoeheid. Losse fragmenten kwamen in het lumen van de aandrijfas van de motor terecht. Door de enorme centrifugale krachten in deze hoge snelheidsas (de ‘Bendix-shaft’) werd de dunne wand door de losse metaalfragmenten aan stukken gescheurd. De kracht waarmee de losse metaalscherven in de rondte werden geslingerd was zo groot dat de scherven door het warmteschild tussen beide motoren drongen en ook de tweede motor verwoestten. Bovendien drongen scherven door het dak van de cabine van de helikopter en verwoestten de stuurkabels voor de hoofdrotor. De piloten verloren beide motoren èn het vermogen om de rotor te besturen. Daardoor verloren zij ook de mogelijkheid om een noodlanding te maken.

Health and Usage Monitoring Systems

In tegenstelling tot de abruptheid van dergelijke ongevallen ontwikkelt het mechanische probleem dat daaraan ten grondslag ligt zich meestal over langere tijd, langer dan de duur van een gemiddelde vlucht. Als het probleem in een vroeg stadium geïdentificeerd kan worden, is er genoeg tijd om correctieve onderhoudsmaatregelen te treffen. Voor opsporing door middel van visuele inspectie of het testen van onderdelen moet de helikopter aan de grond blijven en gedemonteerd worden. Het vroegdiagnostisch onderzoek zou bij voorkeur aan de vliegende helikopter moeten plaatsvinden. Voor dit doel werden in het laatste decennium van de 20e eeuw bewakingssystemen op helikopters geïnstalleerd die het mogelijk moesten maken een continue registratie van (veranderingen in) vibratiepatronen te koppelen aan de uitvoering van gerichte onderhoudsmaatregelen. Het systeem bewaakte de conditie ('health') van de helikopter en maakte het mogelijk om te 'meten' hoeveel van de gegarandeerde levensduur van onderdelen verbruikt was ('usage').

HUMS kan vergeleken worden met een extern sensorisch zenuwstelsel dat voortdurend de toestand van een helikopter in de gaten houdt door veranderingen in vibratiepatronen op te sporen. Het merendeel van de sensoren zijn vibratiesensoren die bestaan uit een inert lichaampje dat omgeven wordt door piëzo-elektrisch materiaal. Trillingen doen het lichaampje bewegen en die bewegingen doen in het omgevende materiaal elektrische stroompjes ontstaan. Enkele tientallen van die vibratiesensoren zijn verspreid over de motoren, versnellingsbakken, rotoren en romp van de helikopter aangebracht, vooral op die onderdelen die voor de aandrijving van de helikopter en daarmee voor de veiligheid van essentieel belang zijn.[2]

Een centrale data-acquisitie en –verwerkingseenheid registreert de stroompjes die in de vibratiesensoren worden gegenereerd en slaat deze data op een daarvoor geschikte drager op. Na afloop van de vlucht worden deze data overgebracht naar de (grond)computer van de onderhoudsafdeling. Speciaal voor deze toepassingen ontwikkelde computerprogramma's analyseren de aangeleverde data door een groot aantal relevant geachte parameters uit te rekenen en met data van voorgaande vluchten te vergelijken. Zo levert bijvoorbeeld de MRS-parameter (de 'Mean Root Square') informatie op over de totale hoeveelheid energie van een trilling.

Voor relevante parameters zijn in de computerprogramma's overschrijdingswaarden vastgesteld. Wanneer deze waarden overschreden worden, genereert het systeem automatisch een waarschuwing ('alert') die op het scherm getoond of naar de printer gestuurd wordt.

Uit technisch laboratoriumonderzoek en uit ervaringen opgedaan in een jarenlange onderhoudspraktijk zijn de verschillende manieren waarop diverse onderdelen in het aandrijfsysteem van een helikopter kunnen falen goed bekend.

2 Behalve vibratiesensoren maken ook nog enkele andere sensortypen deel uit van HUMS. Deze andere sensoren meten bijvoorbeeld het aantal omwentelingen per tijdseenheid van de motoren en van de rotoren, of zijn gericht op het bewaken van het vlak, waarin de rotoruiteinden zich bewegen ('rotor track and balance' sensors).

Deze faalmodi zijn in de software gemodelleerd. Het HUMS-systeem is daardoor in staat om een dreigend falen van voor de veiligheid van de helikopter essentiële onderdelen te herkennen aan de veranderingen die zij tot stand brengen in de vibratiepatronen die door de sensoren geregistreerd worden. Ieder type falen zet in de vibratiepatronen zijn eigen specifieke 'handtekening'. Het HUMS-systeem waarschuwt niet alleen de onderhoudsmonteurs dat er iets aan de hand is, maar ook wat er aan de hand is en waar het probleem zich bevindt. Samen met de automatisch gegenereerde waarschuwing worden de nummers van specifieke werkkaarten afgedrukt die verwijzen naar de bij dit type helikopter horende onderhoudsklappers. Deze werkkaarten beschrijven gedetailleerd welk nader onderzoek dient plaats te vinden en hoe het probleem verholpen kan worden. HUMS doet niet alleen de (vroege) diagnostiek, maar levert ook aanwijzingen voor de behandeling.
De installatie van HUMS vergroot het vermogen van het systeem om te anticiperen en te reageren op ongewenste gebeurtenissen. De kwetsbaarheid van helikopters voor het 'toevalsfalen' van kritische onderdelen als gevolg van metaalmoeheid is kleiner geworden. Voor piloten en passagiers is de helikopter veiliger geworden. Voor het bedrijf is de beschikbaarheid van de helikopter toegenomen, omdat een continue bewaking met de op HUMS gebaseerde onderhoudsstrategie de organisatie in staat stelt om de tijd die gemoeid is met het testen van onderdelen, met testvluchten en met vervanging van onderdelen terug te dringen. De door de fabrikant gegarandeerde levensduur van onderdelen wordt daardoor optimaler benut (usage). Naast een grotere veiligheid levert HUMS voor het bedrijf een besparing van onderhoudskosten op. HUMS realiseert zowel bedrijfseconomische als veiligheidsdoelen.

Verwachtingen

De verwachtingen ten aanzien van HUMS waren hoog gespannen. Aan de introductie van HUMS in het begin van de jaren negentig gingen enkele decennia van onderzoek en testen vooraf. Het principe van op vibraties gebaseerde bewaking was niet nieuw. De grote afmetingen van het instrumentarium en van de mainframe computers die nodig waren om onvertraagd grote hoeveelheden data te verwerken beperkten de toepassingsmogelijkheden. De enorme toename van de rekencapaciteit die in de jaren zeventig gepaard ging met de miniaturisatie van microprocessoren maakte echter de ontwikkeling mogelijk van kleine en lichte instrumenten die toch met voldoende hoge snelheid grote hoeveelheden data konden opnemen, verwerken en analyseren. Hierdoor kwamen toepassingen in helikopters binnen bereik. Barron schrijft dat de ontwikkeling van 'software suites' voor de analyse van vibratiedata "would allow the whole process of condition monitoring to be carried out automatically, giving a complete service

for measurement, analysis and problem diagnosis followed by a maintenance strategy." [Barron, 1996].

Bristow Helicopters Ltd., een van de producenten van HUMS-systemen, schreef in een HUMS-brochure dat "a recently completed computer study of helicopter accidents and serious incidents has indicated that the cause of 72% of the serious incidents and 55% of accidents in the study were likely to have been detected by the Bristow Health Monitoring System. ... As well as dramatically improving airworthiness of the helicopter the enhanced diagnostics offer considerable reduction in dedicated test flying. Bristow Helicopters are forecasting a reduction in vibration related test flying on their Super Puma fleet by some 78%. ...'[O]n condition' maintenance of major components can now become a reality."

Ook de Britse luchtvaartautoriteiten, de Civil Aviation Authority, ondersteunden de ontwikkeling van HUMS-systemen. De CAA benadrukte dat: "condition monitoring is not a relaxation of maintenance standards or of airworthiness control, it is, in fact, more demanding of both management and engineering capabilities than the traditional preventative maintenance approaches." [CAA, 1990].

De manier waarop HUMS hier gepresenteerd wordt verwijst naar een ideaalbeeld. Deze ideaaltypische representatie genereert een beeld van een technologische ruimte waarin zowel aan dingen als aan mensen specifieke taken, rollen en criteria worden toegeschreven. In dit verhaal zou het beginnende scheurtje in de splined sleeve van LN-OPG een verandering in het vibratiepatroon hebben gegenereerd die door het systeem zou zijn waargenomen, geïnterpreteerd en gecorrigeerd. Dergelijke ideaaltypische representaties van technologieën zijn in onze technologische cultuur invloedrijk en gezaghebbend. Het is het type verhaal waarnaar in eerste reacties na fatale ongelukken vaak verwezen wordt bij de verdeling van causale verbanden en de verantwoordelijkheid tussen mensen en technologie. Het systeem is goed en dus is waarschijnlijk menselijk falen de oorzaak van het ongeluk. De representatie mag dan ideaaltypisch zijn, zij is zeker niet imaginair. We kunnen haar concreet aantreffen in technische literatuur, productinformatie en rapporten van luchtvaartautoriteiten. De ideaaltypische representatie houdt er echter geen rekening mee dat de ontwikkeling en het gebruik van de technologie plaatsvindt in een interactief veld van relaties tussen organisaties en tussen mensen en technologieën in organisaties. Interactieve processen tussen actoren in dat veld dragen in sterke mate bij aan de bepaling van het concrete historische traject dat de ontwikkeling van een technologie zal volgen binnen een grotere 'ruimte van mogelijke ontwikkelingstrajecten'.

Veiligheid helikoptertransport Noordzee

Zowel bij helikopterbedrijven als bij oliemaatschappijen en luchtvaartautoriteiten bestond er in het laatste kwart van de vorige eeuw een grote behoefte om het helikoptertransport in de Noordzee veiliger te maken. Na de ontdekking van de gasbel bij Slochteren kwam de ontwikkeling van olie- en gaswinning in de Noordzee in de loop van de jaren zestig op gang met exploratieboringen. Vanaf het begin van de jaren zeventig vond olie- en gaswinning via productie-installaties plaats. Voor het vervoer van personen naar en tussen installaties werd – en wordt nog steeds – transport met helikopters als de enige reële mogelijkheid gezien. Helemaal van gevaar ontbloot bleek het vliegen van helikopters niet te zijn. In de jaren zeventig vonden in de Noorse sector van de Noordzee enkele ernstige helikopterongelukken plaats waarbij tussen 1967 en 1982 34 mensen het leven verloren [Kårstad, 1983]. Hetzelfde met vergelijkbare cijfers gebeurde in de jaren tachtig in de Britse sector. Na de grote rampen met de Alexander Kielland (1980, 123 doden) en de Piper Alpha (1988, 156 doden) – samen goed voor meer dan 50% – kwam het helikoptertransport in termen van het aantal dodelijke slachtoffers met ongeveer 16% op de tweede plaats. Bovendien eiste het offshore-helikoptertransport tien keer meer levens dan het reguliere vliegverkeer met vliegtuigen met 'vaste vleugels'.

Het HARP-rapport

In 1984 kwam in Groot-Brittannië het Helicopter Airworthiness Requirements Panel (HARP) tot de conclusie dat van de ontwikkeling en invoering van HUMS-systemen een grote bijdrage aan de verbetering van de luchtwaardigheid van helikopters verwacht mocht worden [CAA, 1984]. Dit invloedrijke HARP-rapport werd gevolgd door twee testen met HUMS-systemen met Super Puma helikopters van Bristow Helicopters en met Sikorsky helikopters van British International Helicopters. Bristow Helicopters gaf leiding aan een consortium van bedrijven dat HUMS-systemen voor helikopters ontwikkelde.[3] Een tweede groep bedrijven werd aangevoerd door Stewart Hughes. Beide systemen maakten deel uit van deze testen die in opdracht van de CAA met financiële steun van de Britse overheid en van de in de Britse sector van de Noordzee actieve oliemaatschappijen onder eindverantwoordelijkheid van Bristow werden uitgevoerd. Deze waren gericht op het 'demonstreren' van de technische haalbaarheid van HUMS voor helikopters. Dat wil zeggen dat de testen erop gericht waren om na te gaan met welk van het beschikbare instrumentarium een datastroom van voldoende kwaliteit en stabiliteit verworven kon worden. Het ontwikkelen van 'software suites' voor het analyseren van de data bleek binnen de context van de testen niet mogelijk. De testen gaven derhalve geen uitsluitsel over de vraag of de geteste systemen inderdaad in staat waren om dreigend technisch falen

3 Bristow was een van de grote Britse helikoptertransportbedrijven die in de Noordzee actief waren. Bij Bristow werkte een groep ingenieurs actief aan de integratie en ontwikkeling van bestaand instrumentarium tot voor helikopters bruikbare HUMS-systemen. In de eerste helft van de jaren tachtig werkte Bristow daartoe samen met de Franse producent van Super Puma helikopters, Aerospatiale (nu Eurocopter). In die jaren van expansie in de offshore-industrie was Bristow voornemens om een groot aantal nieuwe helikopters van Aerospatiale af te nemen. Nadat in 1986 de olieprijs dramatisch kelderde en de winstmarges in de offshore-industrie geringer werden, moest Bristow Helicopters afzien van die grote order. Aerospatiale verbrak daarop de samenwerking met Bristow bij de ontwikkeling van HUMS-systemen.

van kritische delen van het aandrijfsysteem van helikopters in een vroeg stadium te diagnosticeren. Het rapport dat de in 1991 afgeronde testen samenvat concludeerde dat: "[v]alidating the effectiveness of the algorithm in detecting failure propagation was beyond the scope of the trial. With the limited flight time exposures it was not anticipated that significant failures would occur – nor did they. For reasons of resourcing and time scales the full suite of diagnostic algorithms planned for embodiment in one of the trial systems was not implemented..." [CAA, 1993].

FDR – Flight Data Recording

In 1990 kondigde de Britse Civil Aviation Authority aan dat vanaf 1991 Flight Data Recorders (FDR) aan boord verplicht zouden worden voor alle in Groot-Brittannië geregistreerde helikopters die in 'vijandige omgevingen' ingezet werden. Vóór 1991 waren helikopters alleen maar uitgerust met een Cockpit Voice Recorder (CVR). Net als CVR moest de installatie van FDR het onderzoek achteraf naar de oorzaken van ongelukken mogelijk maken. De in de spreekwoordelijke zwarte, maar in werkelijkheid oranje (FDR-)doos opgeslagen data zouden niet gebruikt worden voor het optimaliseren van onderhoudsstrategieën. Het instrumentarium dat geïnstalleerd moest worden om de FDR-data te registreren vertoonde echter grote gelijkenis met het instrumentarium dat nodig was voor HUMS (sensoren, een centrale data-acquisitie- en verwerkingseenheid, opslag van data).

Een geïntegreerde oplossing

De consortia van bedrijven die bezig waren met de ontwikkeling van HUMS-systemen zagen in de nieuwe FDR-regelgeving een mogelijkheid om het HUMS-project een sprong voorwaarts te laten maken. Met steun van de in de UK Offshore Operators Association (UKOOA) samenwerkende oliemaatschappijen drongen zij aan op een geïntegreerde oplossing: de integratie van CVR, FDR en HUMS in één systeem. Op die manier konden de cumulatieve ontwikkel- en invoeringskosten van eerst de FDR en enkele jaren later van HUMS gereduceerd worden tot de investeringskosten van één geïntegreerd systeem.
De in de UKOOA samenwerkende oliemaatschappijen introduceerden HUMS samen met de FDR als voorwaarde in de contractonderhandelingen met de Britse helikoptertransportbedrijven. Dit gebeurde in de periode waarin de HUMS-testen net werden afgerond. Deze testen gaven echter geen uitsluitsel over de vraag of de geteste HUMS-systemen de hen toebedachte functie ook daadwerkelijk konden uitvoeren.

Rijping

Het onderzoek naar de 'handtekeningen' die specifieke typen van technisch falen in het vibratiepatroon van helikopters zouden achterlaten, was voornamelijk gebaseerd op laboratoriumtesten. In zogenaamde 'seeded fault tests' werden

aan onderdelen van motoren en versnellingsbakken beschadigingen toegebracht en werd vervolgens nagegaan hoe deze in het geregistreerde vibratiepatroon tot uitdrukking kwamen. Met het opsporen van niet bekende technische problemen in vliegende helikopters was nog heel weinig ervaring opgedaan. Desondanks presenteerden de HUMS-producenten onder leiding van Bristow en Stewart Hughes hun systemen alsof ze al bijna operationeel waren en slechts een korte 'rijpingstijd' nodig hadden. In het productinformatiemateriaal dat Bristow Helicopters in januari 1991 aan potentiële klanten presenteerde voorzag het bedrijf een invoeringstraject dat bestond uit drie fasen.

During Phase I, the diagnostics associated with the advanced transmission vibration analysis ... will be considerably extended and varied ... 6 months of evolution in the diagnostic techniques are envisaged ... the diagnostic suite will mature over a 6 month period from its Phase I standard introduced in February 1991. The basis for the M J Dynamics diagnostics system is intelligent and will trend data self amend as experience is gained.

Phase 2 of the programme in addition to maturing the diagnostic suite and adjusting thresholds will be extending the diagnostic capability in the ground station as new techniques which are already envisaged are applied to the ground station for evaluation. During the later part of Phase 2 a programme will be commenced to look at the capability of on-board processing to give on-board display of parameters in areas where a possibility of propagation rates from detection to failure could be in the order of 5 or less flying hours.

Phase 3, the airborne processing, will then be based on the known probability rates of false alerts and would include an expanded correlation of analysis ... to further reduce false alarm rates. ... The display of values with the alerting of failures to the pilot will be on the basis of valid and extensive ground based analysis. ... In Phase 3 it may also be possible to incorporate an entirely new system of signature diagnosis such as neural networks [Bristow Helicopters, 1991].

Dit invoerings- en rijpingstraject zou 3 tot 4 jaar in beslag nemen.

Resonantie

De bedrijven die deze systemen kochten voldeden daarmee aan de door de CAA-verplicht gestelde FDR-voorwaarde, terwijl zij gaandeweg de vruchten – in termen van verbeterde veiligheid en besparing op onderhoudskosten – konden plukken van steeds betere HUMS-versies. Het zelfvertrouwen van ingenieurs over het realiseren van HUMS resoneerde met de wens van de Britse luchtvaartautoriteiten om via regelgeving de veiligheid van helikoptertransport te verbeteren, en met het vooruitzicht voor HUMS-producenten om de investeringskosten voor het geïntegreerde systeem snel te kunnen terugverdienen.[4] De onrijpe HUMS-systemen liften in 1991 mee op de rug van de invoering van FDR die om geheel andere redenen door de CAA verplicht waren gesteld.

4 De 'markt' bleek kleiner te zijn dan men zich had voorgesteld. Buiten de Noordzee werden HUMS-systemen voor helikopters nergens geïmplementeerd. De eerste grote militaire HUMS-contracten worden nu pas aan het begin van de 21ste eeuw afgesloten. Bristow Helicopters heeft in een periode van economische krapte haar belang in de productie van HUMS in 1993 verkocht.

Noorse fascinatie en frustratie

SINTEF's Helicopter Safety Study

Aan de andere kant van de Noordzee volgden Noorse bedrijven met belangstelling de ontwikkelingen in Groot-Brittannië. Een helikopterongeluk met dodelijke afloop had in de Noorse sector van de Noordzee sinds de jaren zeventig niet meer plaatsgevonden. Dat wil niet zeggen dat de Noren op hun lauweren gingen rusten. Een met financiële steun van oliemaatschappijen (Shell, Statoil) door SINTEF uitgevoerde Helicopter Safety Study concludeerde in 1990 dat het 'dodental' van helikoptertransport in de Noordzee in de loop van 10 tot 15 jaar met 40% teruggebracht zou kunnen worden door middel van R&D-inspanningen, gericht op de verbetering van de technische betrouwbaarheid van helikopters. Aan de ontwikkeling van HUMS-systemen moest daarbij grote prioriteit worden toegekend [Ingstad, 1990].
De conclusies van de SINTEF-studie kwamen overeen met die van het Britse HARP-rapport uit 1984. De studie wees de ontwikkeling van HUMS-systemen aan als een belangrijk domein voor onderzoek en ontwikkeling en hanteerde een tijdshorizon van 10 tot 15 jaar voor het bereiken van een substantieel resultaat. Hier werden technische oplossingen bedoeld die enkele maanden later al door Bristow en Stewart Hughes als (bijna) kant-en-klare technologieën op de markt werden gebracht.

If you don't have it, you don't play!

Oliemaatschappijen die aan beide zijden van de Noordzee actief waren, introduceerden HUMS als een voorwaarde in contractonderhandelingen met Noorse helikoptertransportbedrijven. Helikopter Service AS had op dat moment nog geen heldere strategie over HUMS ontwikkeld. Helikopter Service zag in dat zij aan klanten niet kon garanderen dat steeds met een met HUMS uitgeruste helikopter gevlogen zou worden, tenzij haar hele vloot met die systemen uitgerust zou zijn. Helikopters moesten verspreid over het hele werkterrein van het bedrijf flexibel ingezet kunnen worden. De optie van één helikopter voor één klant was geen realistische mogelijkheid.
In Noorwegen was concurrent Braathens Helikopter het bedrijf dat als eerste via een persbericht aankondigde HUMS-systemen op al haar helikopters te zullen installeren. HUMS werd een factor die mede de concurrentiepositie van een bedrijf bepaalde in een markt waar grote klanten grote contracten afsloten met een relatief klein aantal aanbieders. Bij Helikopter Service duikt al snel in bedrijfsinterne notities de zinsnede 'If you don't have it, you don't play!' op. In de zomer van 1991 besluit het management van Helikopter Service AS tot de installatie van HUMS-systemen in haar helikopters.

Fascinatie voor een nieuwe technologie

De vergelijking van de beide systemen die op de markt waren en de uitwerking van de technische details van het contract werd gedelegeerd aan het Engineering Department van het bedrijf. Net als bij Bristow was er bij Helikopter Service een groep ingenieurs met een fascinerende belangstelling voor vibratiegebaseerde toestandsbewaking. Zij hadden al verschillende keren voor kleine vliegtuigen ontwikkelde apparaten gebruikt, wanneer zich in een van de helikopters hardnekkige problemen voordeden. In het bedrijf waren zij degenen met het best ontwikkelde intuïtieve gevoel voor de trillingseigenschappen van helikopters. Bij de uitwerking van het contract met Stewart Hughes streefden zij ernaar om zoveel mogelijk van de beschikbare functionaliteit in de 'doos' te integreren.[5]

Helikopter Service vloog in 1991 met Super Puma, Boeing en Sikorsky helikopters. Het HUMS-invoeringsbeleid van het bedrijf was erop gericht om één HUMS-systeem te installeren dat compatibel zou zijn voor elk van deze verschillende helikoptertypen. Bovendien was Helikopter Service van plan om op korte termijn enkele nieuwe Super Puma helikopters te kopen bij Eurocopter. Helikopter Service wilde graag dat Eurocopter het Stewart Hughes HUMS-systeem al in deze nieuw te leveren Super Puma helikopters zou integreren, zodat deze systemen ook door de helikopterfabrikant ondersteund zouden worden. In afwachting van de resultaten van de onderhandelingen tussen Eurocopter en Stewart Hughes besloot Helikopter Service in eerste instantie HUMS alleen te installeren op haar Boeing- en Sikorsky-machines.

De installatie zelf werd door de eigen ingenieurs 'in huis' uitgevoerd. Deze HUMS-systemen waren geen 'plug-and-play'-apparaten. Voor elk van de sensoren moest op basis van vibratiemetingen de optimale positie op de helikopter worden gezocht. Met de installatie van het eerste HUMS-systeem op een Sikorsky was dan ook bijna drie maanden gemoeid. De installatie vormde voor de ingenieurs een uitdaging die met grote fascinatie voor de nieuwe technologie en met een dosis professionele trots aangegaan werd, maar tegelijk veel tijd en middelen in beslag nam.

Weerbarstige praktijk

In het invoeringsplan voor HUMS van Helikopter Service was geld vrijgemaakt voor de aankoop en installatie van de 'hardware' van de systemen op bestaande helikopters. Er was echter weinig aandacht besteed aan de manier waarop HUMS ingebouwd zou moeten worden in de bestaande onderhoudsorganisatie van het bedrijf. Welke gevolgen zou de introductie van HUMS hebben voor de eerstelijns onderhoudsmonteurs op de verschillende helikopterbases langs de Noorse kust? De koers van Helikopter Service in deze werd bepaald door de ideaaltypische representatie van de technologie, zoals deze door HUMS-producenten werd gepresenteerd.

5 Een aantal HUMS-subsystemen, zoals rotor track and balance was optioneel.

In de praktijk bleek HUMS veel weerbarstiger. Eerstelijns onderhoudsmonteurs werden frequent geconfronteerd met automatisch gegenereerde, maar valspositieve waarschuwingen. In veel gevallen kon er bij nader onderzoek geen corrigeerbaar probleem gevonden worden. Het gebeurde ook vaak dat de bij de waarschuwingen afgedrukte verwijzingen naar werkkaarten niet klopten. De nummers verwezen naar werkkaarten die betrekking hadden op onderdelen van de helikopter die niets te maken hadden met de componenten die door HUMS werden aangewezen als de plek waar het afwijkende vibratiepatroon ontstond. Daarnaast begonnen ook componenten van het HUMS-systeem zelf gebreken te vertonen. Sensoren gingen kapot en moesten vervangen worden. Vooral het punt waar de vibratiesensor aan het kabeltje vastzat bleek vaak een bron van problemen te zijn. De door Stewart Hughes geleverde doos met kabels, sensoren en apparaten bevatte geen handleiding met procedures voor het onderhoud van HUMS zelf. Het vervangen van sensoren kon niet door iedere eerstelijns onderhoudsmonteur gedaan worden, omdat hiervoor bijzondere vaardigheden en gereedschappen vereist waren.
In een organisatie waarin het handelen in hoge mate door op schrift gestelde procedures en richtlijnen wordt geregeld creëerde de introductie van HUMS een grote mate van onzekerheid. In plaats van besparingen genereerde HUMS extra onderhoudskosten. In plaats van het verbeteren van de beschikbaarheid dreigden problemen met HUMS een reden te worden voor het aan de grond houden van de helikopters. Daar kwam bij dat het streven om met een met alle helikoptertypen compatibel HUMS-systeem te kunnen werken mislukte, toen bleek dat de onderhandelingen tussen Stewart Hughes en Eurocopter niet het gewenste resultaat hadden. Eurocopter ontwikkelde haar eigen versie van het HUMS-systeem. Helikopter Service zag zich genoodzaakt om HUMS-systemen van Stewart Hughes op haar bestaande Super Puma helikopters te installeren, maar kreeg Eurohums als integraal onderdeel van nieuwe Super Puma's meegeleverd. Bovendien kocht Helikopter Service op basis van bedrijfsstrategische motieven haar belangrijkste concurrenten in Noorwegen, Braathens Helikopter en Mørefly. Deze bedrijven kozen in 1991 voor het HUMS-systeem van Bristow. In plaats van met één HUMS-systeem moesten de onderhoudsmonteurs en ingenieurs van Helikopter Service na enkele jaren werken met drie verschillende HUMS-systemen.

Lokale adaptaties en ervaringen

De ingenieurs van de centrale HUMS-afdeling werden in steeds sterkere mate bij deze problemen op de werkvloer van de hangars betrokken. Samen met de monteurs probeerden zij strategieën te ontwikkelen om de ontstane onzekerheid weer te reduceren om het kaf van het koren (dat wil zeggen de valspositieven van de echte problemen) te scheiden. Bij iedere automatisch gegenereerde waarschuwing moest een besluit genomen worden over de vraag of de helikopter

voor zijn volgende vlucht vrijgegeven kon worden. Rasmussen beschrijft dit zoeken naar (lokaal) werkbare oplossingen als een proces van navigeren in een 'werkruimte' waarbij de grenzen van die ruimte door lokale adaptaties geëxploreerd worden [Rasmussen, 1994].
Fascinatie voor de technologie veranderde in frustratie. Maar in die weerbarstige en frustrerende interactie met de technologie ontwikkelde zich na verloop van tijd een praktijk die in ieder geval naar lokale maatstaven werkbare resultaten opleverde. Van die praktijk maakten ook een aantal situaties deel uit waarin HUMS inderdaad in een vroeg stadium technische problemen op het spoor kwam die – indien niet verholpen – dramatische gevolgen gehad zouden kunnen hebben. Mensenlevens werden gered en het verlies van duur materieel werd voorkomen. In probabalistische termen: ondanks zijn geringe specificiteit kon aan HUMS als diagnostisch apparaat een zekere mate van sensitiviteit niet ontzegd worden. Desalniettemin was de betrouwbaarheid van de HUMS-waarschuwingen laag, te laag. Jens Kørte, ingenieur bij Helikopter Service schreef hierover het volgende: "The experience rate of the helicopter being in a critical failure state, given a random alert is typically 1 in 200 alerts, or a fraction of 0.005. This figure can be interpreted as a measure of alert reliability." [Kørte, 2000].

HUMS en (het ontbreken van) Minimal Equipment Lists

In die zichzelf organiserende praktijk[6] rond HUMS werd het al snel duidelijk dat het aan de grond houden van helikopters op basis van technische problemen met HUMS-sensoren absurde gevolgen zou hebben. Dagelijks zou dan een deel van de helikoptervloot aan de grond moeten blijven. Gelet op de hoge benuttingsgraad van de beschikbare capaciteit, zou Helikopter Service haar contractuele verplichtingen ten opzichte van haar klanten niet meer kunnen nakomen. In een bedrijf dat in haar dagelijkse bedrijfsvoering zo sterk aan de regelmatigheidsdwang van de industrie is onderworpen is dat ondenkbaar.
Voor het hanteren van problemen met HUMS-sensoren fungeerde de Minimal Equipment Lists (MELs) als mal in de onderhoudsorganisatie van Helikopter Service. Op deze bestaande en door luchtvaartautoriteiten gelegitimeerde praktijk met het daaraan verbonden niveau van zekerheid en de specifieke distributie van verantwoordelijkheid kon worden teruggevallen bij het zoeken naar pragmatische oplossingen in de nieuwe, door onzekerheid gekenmerkte ruimte die door de introductie van HUMS werd gecreëerd.[7]
Behalve HUMS heeft een helikopter nog wel meer subsystemen die voor de veiligheid niet van doorslaggevend belang zijn. MELs beschrijven welke onderdelen van de helikopter minimaal operationeel moeten zijn, voordat de helikopter mag worden vrijgegeven voor zijn volgende vlucht. Omgekeerd beschrijven MELs ook welke onderdelen defect mogen zijn en hoe lang. Dit betekent dat niet ieder defect meteen gerepareerd hoeft te worden. Als de MEL dat toestaat,

6 Met 'zelforganiserende praktijk' bedoel ik hier dat manieren van het hanteren van problemen ontstaan in de interactie met de technologie en tussen mensen in afwezigheid van door een externe instantie voorgeschreven richtlijnen of procedures.

7 In psychologisch onderzoek naar het gedrag van mensen in crisissituaties wordt een mechanisme beschreven dat 'regressie naar eerst geleerde reacties' ('regression to first learned responses') wordt genoemd. Zie bijvoorbeeld [Weick, 1991]. Het woord regressie heeft negatieve connotaties, maar het mechanisme is vergelijkbaar: een terugvallen op reeds bestaande (geleerde) manieren van doen in situaties van onzekerheid.

kan reparatie uitgesteld worden tot de volgende reguliere onderhoudsbeurt. Het defect wordt dan wel op een lijst gezet die bij iedere helikopter bewaard wordt, een 'deferred defect list'. MELs moeten door de luchtvaartautoriteiten worden goedgekeurd.
Voor de HUMS-systemen die vanaf 1991 aan de bestaande helikoptervloot in de Noordzee werden toegevoegd was er geen MEL. Bij gebrek aan een eigen plaats op de reguliere formulieren werden problemen met HUMS-sensoren op losse briefjes genoteerd. Maar soms ook niet. Omdat er geen MEL was die aangaf binnen welke termijn een bepaalde sensor gerepareerd moest worden, kon zich een praktijk ontwikkelen waarbij defecte sensoren bij 'de eerstvolgende gelegenheid' gerepareerd werden. Voor de relatief jonge basis in Brønnøysund was de eerstvolgende gelegenheid doorgaans de eerstvolgende keer dat een gespecialiseerde monteur met speciaal gereedschap vanuit Stavanger naar het noorden kwam. Dat kon de volgende dag zijn, maar ook de volgende week.
Op 8 september 1997 was een van de HUMS-sensoren in LN-OPG, een Super Puma helikopter die van Mørefly was geweest en die uitgerust was met het iHUMS-systeem van Bristow, al een paar dagen defect. De sensor zou bij de eerstvolgende gelegenheid gerepareerd worden, maar was nog steeds defect toen de helikopter in zee stortte.

Mismanagement?

Helikopter Service AS onderzocht meteen na het ongeval de HUMS-databestanden van voorafgaande vluchten van LN-OPG die op de grondcomputer in Brøynnøysund waren opgeslagen.[8] Helikopter Service ontdekte dat een van de HUMS-sensoren in LN-OPG stuk was. Bovendien ontdekten zij bij handmatige analyse van de data dat een andere sensor een verandering in het vibratiepatroon geregistreerd had die tot uitdrukking kwam in een toename van een van de parameters waarop de analyse van de data is gebaseerd. Voor deze parameter was echter door de producent in de computerprogramma's die voor de analyse gebruikt werden geen overschrijdingswaarde ingesteld. Een automatische waarschuwing werd daarom niet gegenereerd. De trend kon alleen gevonden worden door alle data handmatig op het scherm te brengen. Dat werd in de dagelijkse routine niet gedaan, maar was ook niet vereist.
Omdat de aandacht in de eerste dagen na het ongeluk gericht was op het mogelijke verlies van een rotorblad tijdens de vlucht, werd aan deze HUMS-bevindingen weinig waarde toegekend. Toen na het lichten van de romp van de helikopter bleek dat de motoren ernstig beschadigd waren, kwamen de bevindingen in het middelpunt van de belangstelling te staan.
De sensor die stuk was bleek de sensor te zijn die zich aan de buitenzijde op de plaats bevond waar motor en versnellingsbak met elkaar verbonden zijn. De

8 De drager in de helikopter waarop HUMS-data werden opgeslagen is niet crash- en zeewaterbestendig. De data van de 'ongeluksvlucht' zijn verloren gegaan. Anders dan FDR-data zijn HUMS-data ook niet bedoeld om het onderzoek achteraf mogelijk te maken. Na iedere vlucht worden HUMS-data opgeslagen en geanalyseerd op een grondcomputer. De data van vorige vluchten konden binnen enkele uren na het ongeluk aan een nader onderzoek onderworpen worden. Dit onderzoek hoefde niet te wachten op het lokaliseren en lichten van het wrak.

plaats van deze sensor was zo gekozen om eventuele problemen met de verbinding tussen de aandrijfas van de motor en de as van de versnellingsbak vroegtijdig op het spoor te komen. Het feit dat een andere sensor op dezelfde motor een 'trend' registreerde suggereerde in ieder geval de mogelijkheid dat het ongeluk voorkomen had kunnen worden als die ene sensor wel operationeel was geweest.
Helikopter Service gaf over deze iHUMS-bevindingen meteen openheid van zaken. Deze mededelingen werden in eerste instantie beantwoord door een golf van kritiek en verontwaardiging over het feit dat gevlogen werd met niet-operationele sensors in het iHUMS-systeem. De verleiding is inderdaad groot om de oorzaak van en de verantwoordelijkheid voor het falen van de betrouwbaarheidstechnologie te lokaliseren in het 'mismanagement' van het technisch systeem door de onderhoudsorganisatie van Helikopter Service AS. Het technisch systeem is goed; het onderhoud door mensen en organisaties is blijkbaar niet in orde. Die eerste reacties geven een vrijwaringsbewijs voor de techniek af. Zij geven uitdrukking aan een groot vertrouwen in de betrouwbaarheid van de technologie.

Een nadere analyse van de ontwikkeling, de introductie en de ervaringen met HUMS-systemen voor helikopters laat echter zien dat het goed is om die verleiding te weerstaan. De HUMS-techniek is tien jaar na introductie nog niet goed en nog steeds onbetrouwbaar. Het vliegen met niet volledig operationele systemen is niet ongebruikelijk en is gelegitimeerd in Minimal Equipment Lists. De manier waarop Helikopter Service met de onzekerheid rond de HUMS-technologie omging was geënt op een al bestaande en door luchtvaartautoriteiten gelegitimeerde routine. Sterker nog, de afwijking van een technologisch optimum is in de praktijk noodzakelijk om het (grotere) systeem van helikoptertransport te kunnen laten functioneren met de grote mate van regelmaat[9] die de offshore-industrie en onze moderne, sterk van een regelmatige stroom van energie (en kapitaal) afhankelijke samenleving vereisen.[10]

Drift en kwetsbaarheid van LN-OPG

Drift: verschil tussen protocol en praktijk

Niet iedere afwijking van een (technologisch) optimum heeft meteen gevolgen voor het functioneren van het systeem als geheel. Met andere woorden, een systeem kan zich in een veelheid van toestanden bevinden die verenigbaar zijn met een aanvaardbaar niveau van functioneren. Het systeem is dan wel kwetsbaarder geworden. Het systeem is dus minder goed in staat om te anticiperen of te reageren op, of te herstellen van onverwachte gebeurtenissen. We kunnen dit vergelijken met onze eigen conditie. Wanneer we slecht eten, weinig slapen en

9 In nationale en internationale standaarden over bedrijfsprocessen wordt de term 'regularity' (regelmatigheid) gebruikt. Deze term verwijst naar het vermogen van het 'systeem' om goederen en of diensten op het afgesproken tijdstip te leveren. Een probabalistische formulering van regelmatigheid zou spreken over de kans dat een systeem een dienst x op tijdstip y levert. Regelmatigheid kan statistisch geoperationaliseerd worden in bijvoorbeeld: het percentage treinen of vliegtuigen dat in een bepaalde periode op tijd vertrok. Voor mij is hier echter belangrijker dat het begrip regelmatigheid verwijst naar de continue en onafhankelijke stromen van mensen, goederen, olie en gas, geïnvesteerd kapitaal en winsten waaruit de offshore-industrie als onderdeel van onze geïndustrialiseerde samenleving bestaat.

10 De Britse techniekssocioloog John Law maakt dit argument in een analyse van een ernstig treinongeluk bij Ladbroke Grove in 1999. Zie http://www.comp.lancs.ac.uk/sociology/soc055jl.html

onvoldoende bewegen, gaat onze conditie achteruit. Die slechtere conditie is nog geruime tijd verenigbaar met een aanvaardbaar niveau van functioneren op het werk of thuis. We zijn echter wel kwetsbaarder geworden voor wat medici opportunistische infecties noemen. Door meer te bewegen, meer te slapen en weer gevarieerder te eten kunnen we onze conditie weer verbeteren en neemt ook onze kwetsbaarheid weer af.
We kunnen ons alle mogelijke toestanden waarin een systeem zich kan bevinden als een (abstracte) ruimte voorstellen. Op een bepaald moment bevindt het systeem zich dus ergens in die ruimte van mogelijke toestanden.
Centraal in die ruimte van mogelijke toestanden bevindt zich een punt waarop het systeem zich in een optimale conditie bevindt. Hier voldoet het systeem aan het ideaaltypische beeld dat in de verbeelding van ontwerpers en ingenieurs tot stand kwam. Alle elementen, zowel mensen als dingen presteren conform de functiespecificaties, conform wat we zouden kunnen noemen het protocol.
Een systeem zal zich nooit lang in die optimale toestand bevinden. In de praktijk van het gebruik, door slijtage, door het (normale) kapot gaan van componenten, door lokale adaptaties in onderhoudspraktijken, door incoherenties tussen veiligheids-, productie- en economische doelstellingen, drijft het systeem weg van dat centrale optimum naar de periferie van de ruimte van mogelijke kwetsbaardere toestanden. De richting van deze drift is niet alleen weg van het optimum. Door vervanging van onderdelen of door het veranderen van onderhoudsroutines kan het systeem ook weer terug drijven in de richting van het optimum.
Er zal echter altijd een verschil zijn tussen protocol en praktijk. In de loop van zijn leven legt een systeem binnen die ruimte van mogelijke toestanden een onregelmatig en kronkelig traject af. De omvang en de aard van het verschil tussen protocol en praktijk is niet statisch, maar verandert steeds met de plaats en de richting van de drift.

LN-OPG

Gaandeweg is in de vorige paragrafen een beeld ontstaan over de geschiedenis van LN-OPG, de Super Puma AS 332L1 helikopter die op 8 september 1997 in zee stortte. De helikopter werd gebouwd door de Franse helikopterbouwer Aerospatiale, nu Eurocopter geheten. De helikopter werd gekocht door een klein helikoptertransportbedrijf Mørefly dat enkele jaren een graantje meepikte van de expanderende offshore-industrie. Mørefly installeerde op LN-OPG een iHUMS-systeem van Bristow. Het bedrijf kon de concurrentie met de grote helikopterbedrijven echter niet volhouden en werd door concurrent Helikopter Service opgekocht. Helikopter Service zette de helikopter in voor diverse opdrachten in de gehele Noordzee. In de loop der jaren werden ook concessies verleend en velden tot ontwikkeling gebracht ten noorden van de 62e breedtegraad. Voor het bedienen van die noordelijke velden richt Helikopter Service een nieuwe helikopterbasis in bij Brønnøysund. Als in 1997 Statoil begint met

het bouwen en neerzetten van productie-installaties op het nieuwe Norne-veld dirigeren de logistieke planners van Helikopter Service LN-OPG naar Brønnøysund om ingezet te worden in de pendeldiensten naar het nog af te bouwen Norne-schip.
LN-OPG werd onderworpen aan de preventieve onderhoudsstrategieën die in de helikopterindustrie gebruikelijk zijn. Toen 5.000 vlieguren op de teller stonden, werd LN-OPG helemaal ontmanteld en weer opnieuw opgebouwd waarbij versleten onderdelen werden vervangen en andere grondig gereviseerd. Na die grote beurt was de helikopter weer 'zo goed als nieuw'.[11] Door kleine en grote onderhoudsbeurten werd LN-OPG weer teruggebracht in de richting van de technisch optimale conditie waarvan zij door gebruik, slijtage, belasting door slecht weer en zware lasten, maar ook door het kapot gaan van onderdelen verwijderd was geraakt. Maar ook na een dergelijke grote onderhoudsbeurt verwijdert het systeem zich door het defect raken van componenten weer van het technologisch optimum en kan voor kortere of langere tijd in een toestand van grotere kwetsbaarheid verblijven zonder dat dit tot uitdrukking komt in incidenten of ongevallen die ten grondslag liggen aan veiligheidsstatistieken.

HUMS: verschil tussen protocol en praktijk

HUMS-systemen zijn nooit in de buurt van de plaats die beantwoordt aan de ideaaltypische representatie van de technologie (d.w.z. van het protocol) geweest. Toch heeft HUMS wel enig – op de sensitiviteit van het systeem gebaseerd – anticiperend vermogen aan de onderhoudsorganisatie toegevoegd. Maar HUMS-systemen bleven ook niet lang op die plaats in de ruimte van mogelijke toestanden. Door het stukgaan van sensoren, het breken van kabeltjes, en dergelijke verwijderde het systeem zich steeds weer iets van haar optimale positie. Daardoor verminderde het anticiperend vermogen weer en werd het systeem weer kwetsbaarder. Reparatie van de onderdelen bracht het systeem weer terug in de richting van haar optimale positie. Omdat HUMS niet als veiligheidskritisch systeem werd beschouwd en omdat de (door het systeem gegenereerde) automatische waarschuwingen een geringe betrouwbaarheid hadden en vanwege de regelmatigheidsdruk waaraan de bedrijfsvoering werd blootgesteld, kon het gebeuren dat LN-OPG langere tijd in die kwetsbaardere conditie of positie verbleef.

Conclusie

In dit hoofdstuk ligt de nadruk op een analyse van de concrete processen en mechanismen die geleid hebben tot het falen van HUMS in zijn vroegdiagnostische functie in de helikopter die op 8 september 1997 in zee stortte. Uit deze analyse kunnen we twee algemene conclusies trekken.

11 Een onderhoudsmonteur van Helikopter Service tekende daarbij aan dat wel bedacht moet worden dat "an old hooker will never become a virgin again".

HUMS-systemen werden in het begin van de jaren 1990 prematuur geïntroduceerd in een veld van traditionele economische relaties. Hoewel bij Bristow Helicopters een groep ingenieurs als integratoren van nieuwe HUMS-systemen optraden, werden helikoptertransportbedrijven vooral gezien als 'gebruikers' van de technologie. In de cruciale jaren waarin HUMS geïntroduceerd werd participeerden de helikopterproducenten niet in de ontwikkeling van de technologie. HUMS-systemen van Bristow of Stewart Hughes die op Super Puma helikopters werden geïnstalleerd werden niet door Aerospatiale ondersteund. De kosten voor onderzoek aan onderdelen die naar de fabriek werden gezonden, omdat HUMS aan die onderdelen toegeschreven problemen signaleerde waren voor rekening van het transportbedrijf, als bleek dat geen fabricagefouten werden gevonden. Dergelijke in contracten vastgelegde relaties verhinderden de snelle en vrije uitwisseling van informatie die nodig was om ambigu en moeilijk te duiden HUMS-vibratiepatronen te vergelijken met actuele toestanden in motoren en transmissies. De door Bristow in het vooruitzicht gestelde snelle 'rijping' van de technologie in de loop van drie tot vier jaar heeft daardoor niet of nauwelijks plaatsgevonden. Certificatie van de huidige HUMS-systemen en de praktijk in de huidige economische relaties tussen partijen zullen de ontwikkeling van HUMS alleen nog verder belemmeren.

Complexe producten en systemen als HUMS-systemen worden in toenemende mate ontwikkeld in netwerken van bedrijven en organisaties.[12] In een dergelijk HUMS-netwerk zouden helikoptertransportbedrijven als Helikopter Service een centrale rol moeten spelen. Zij beschikken over een schat aan door HUMS-systemen gegenereerde vibratiepatronen in de databases van hun grondcomputers. Voor de ontwikkeling van HUMS is het van belang dat deze patronen op een systematische wijze aan actuele toestanden van de bewaakte componenten gekoppeld kunnen worden. Helikoptertransportbedrijven moeten dan echter niet langer als 'gebruikers' van de technologie worden gezien, maar (in een netwerk) als ontwikkelaars van de technologie. Dit vereist een grondige herziening van de economische relaties en van de distributie van de kosten tussen betrokken partijen, en van de contracten en contractvormen die daaraan ten grondslag liggen.

De tweede algemene conclusie heeft betrekking op drift in complexe organisaties. Ingenieurs hebben onder de noemer van kwaliteitsbewaking geavanceerde technieken en procedures ontwikkeld om drift in technische productiesystemen te bewaken en te corrigeren. Voor het bewaken van drift in organisaties en de daaruit resulterende kwetsbaarheid van technische systemen zijn nauwelijks instrumenten ontwikkeld. Iedere organisatie, en zeker de organisaties die verantwoordelijk zijn voor het betrouwbaar functioneren van complexe technische systemen zou een reflectieve functie moeten ontwikkelen die gericht is op het continu kritisch ondervragen van de eigen procedures en routines. Een dergelijke functie zou de kwetsbaarheden van de organisatie en van de technische sys-

12 [Hobday, 2000] en [Kash, 2000].

temen in kaart moeten brengen.[13] Deze functie zou ook een belangrijke rol kunnen spelen bij de introductie van nieuwe technologie in een organisatie. Het is van groot belang te onderkennen dat een dergelijke kritische en reflectieve functie iets heel anders is dan het oprichten van een afdeling die moet nagaan of aan wet- en regelgeving en aan kwaliteitsstandaarden voldaan wordt. Het voorbeeld van de Minimal Equipment Lists laat zien dat in de door de luchtvaartautoriteiten geautoriseerde procedures al een compromis tussen veiligheid, productiviteit, regelmatigheid en winstgevendheid is ingebakken. Meer regelgeving of strengere handhaving van bestaande regelgeving hoeft niet noodzakelijkerwijs te leiden tot een grotere betrouwbaarheid van de technische systemen waarvan we zo afhankelijk zijn geworden.

Referenties

- Barron, R. (ed.). (1996). Engineering Condition Monitoring. Practice, Methods and Applications. Longman, Harlow
- Bristow Helicopter Ltd. (1991). Integrated Health and Usage Monitoring System. An Introduction to the Bristow iHUMS system. 25th January. pp5-6
- Brukx, J.F.L.M. (2000). Vulnerability Enhancing Factors and Fatal Accidents. Working paper. Persoonlijke communicatie
- CAA. (1984). Review of Helicopter Airworthiness. Report of the Helicopter Airworthiness Review Panel (HARP) of the Airworthiness Requirements Board, CAP 491. The Civil Aviation Authority, London
- CAA. (1990). Condition Monitored Maintenance, CAP 562, Civil Aircraft Airworthiness, Information and Procedures, Part 1 Airworthiness Procedures. The Civil Aviation Authority, London. Leaflet 1-7:3
- CAA. (1993). CAA Paper 93002. Helicopter Health Monitoring, Operational Trials Review. Civil Aviation Authority, London. p18
- Hobday, M. (2000). Innovation in Complex Products and Systems. Research Policy 29, pp7-8, pp793–804
- Ingstad, O., e.a. (1990). Helicopter Safety Study. Main Report. SINTEF, Trondheim. p3
- Kårstad, O., E. Wulff. (1983). Sikkerhet på sokkelen. Universitetsforlaget, Oslo. p25
- Kash, D.E., R.W. Wycoft. (2000). Patterns of Innovating Complex Technologies: a Framework for Adaptive Network Strategies. Research Policy 29. pp7-8, pp819–831
- Kauffman, S. (1995). At Home in the Universe. Penguin Books, London. p186

13 Brukx spreekt over 'kwetsbaarheidsprofielen' [zie Brukx, 2000].

– Kørte, J., T. Aven. (2000). Health Monitoring or Helicopter – A Framework for Decision Making based on Health Information. In: Cottam, M.P., D.W. Harvey, R.P. Pape, J. Tait, (eds.). Foresight and Precaution. Proceedings of ESREL, SARS and SRA-Europe Annual Conference. Edinburgh, Scotland, United Kingdom. 15-17 May. Volume 2, A.A. Balkema, Rotterdam/Brookfield. pp933–940, pp935
– Rasmussen, J. (1994). Risk Management, Adaptation and Design for Safety. In: Brehmer, B., N.E. Sahlin. Future Risks and Risk Management. Kluwer, Dordrecht. pp1–36
– Weick, K.E. (1991). Vulnerable System: An Analysis of the Tenerife Air Disaster. In: Frost, P.J., e.a. (eds.). Reframing Organizatonal Culture. Sage Publications, London. pp117–130

2

26
Betrouwbaarheid van samenwerkende organisaties

ir. V.A. Wegener[1]

Voorwoord

Uit een brochure van een dienstverlenende ICT-onderneming[2]:

Een onderneming kan bij uitval van bedrijfskritieke operationele systemen zijn hoofdtaak niet langer uitvoeren. Dit kan leiden tot dramatische gevolgen voor de maatschappelijke en persoonlijke veiligheid, of tot materiële dan wel economische schade. Voorbeelden van dergelijke systemen zijn:

- **Systemen waarmee het luchtverkeer wordt gestuurd, zoals Air Traffic Controlsystemen van luchthavens en Eurocontrol.**
- **Systemen waarmee duizenden alarmen per dag à la minuut adequaat moeten worden opgevolgd, zoals bij meldkamers en alarmcentrales.**
- **Systemen die kerncentrales bewaken.**
- **Civiele en militaire command & control systemen, zoals van commandocentrales aan boord van schepen en commandovoeringssystemen te velde, rampenbestrijdingssystemen.**

1 Getronics N.V.
Postbus 652
1000 AR Amsterdam

2 ICT = Informatie & Communicatie Technologie, de overkoepelende term voor alles wat met computertechnologie te maken heeft, inclusief de applicaties en informatie die daarop draaien en bewaard worden.

Typische kenmerken van deze systemen zijn:

- **Zeer hoge betrouwbaarheid en beschikbaarheid van de real time systemen.**
- **Groot aantal menselijke gebruikers van de systemen, 24 uur per dag, 7 dagen per week.**
- **Complexe gedistribueerde ICT-architecturen met veel externe koppelingen.**
- **Complexe achterliggende algoritmen.**

Naast de zeer hoge technische eisen aan deze systemen, worden natuurlijk ook hoge eisen gesteld aan de mensen voor, achter en rond die systemen. De menselijke factor is groot, zowel in de bouw en het beheer van de systemen als in de bediening ervan en de organisaties er om heen.
De ICT-onderneming en al haar personeel moeten zich bewust zijn van het belang van het systeem voor de klant, en de klanten van de klant. De ICT-onderneming moet een echte dienstverlener zijn die de bedrijfsprocessen van zijn klant door en door kent. Wij stellen het belang van de klant voorop en zorgen dat uw bedrijfsvoering door kan gaan. Wij hebben succes als onze klanten succes hebben.

Deze advertentie kenmerkt de tegenwoordige netwerkeconomie. Steeds meer bedrijven zoeken een intensievere samenwerking met elkaar. Een belangrijke oorzaak is de combinatie van de toenemende complexiteit van technische systemen en de afhankelijkheid daarvan – vooral op het gebied van ICT – en de noodzakelijke groei die bedrijven moeten doormaken. Die combinatie maakt dat bedrijven keuzen moeten gaan maken om aan de kwaliteitseisen van efficiëntie en effectiviteit te blijven voldoen. Een van die keuzen is de scheiding tussen kern- en niet-kernvaardigheden en daarmee het laten verrichten van die activiteiten die niet tot de kernvaardigheden van de onderneming behoren. Aanvankelijk had een onderneming alle (kern)vaardigheden in huis om deze aspecten onder controle te houden. Maar om de toenemende complexiteit inzichtelijk te maken en daardoor onder controle te houden, moet de specialisatie in de ontwikkeling van ICT-vaardigheden gerichter worden. En die ontwikkeling was een belangrijke aanzet voor de niet-ICT-ondernemer om onderscheid te maken tussen ICT- en niet-ICT-vaardigheden met alle gevolgen voor het personeel. Dit was onder andere de reden voor de van huis uit niet-ICT-ondernemingen om een samenwerkingsverband aan te gaan met ICT-ondernemingen.
Kenmerk van een samenwerkingsverband is dat wederzijdse bedrijfsactiviteiten op elkaar afgestemd moeten zijn. Samenwerkingsverbanden kennen verschillende toestanden: de relatie tussen klant en leverancier, waarin de klant (ICT)-producten afneemt, tot een strategisch partnerschap waarin beide partijen deelnemen in risicodragende activiteiten.
Dit artikel beschrijft een manier om tot een samenwerkingsrelatie te komen en om die in stand te houden middels een continu verbeterprogramma waarin alle kwaliteitsaspecten (zoals die van betrouwbaarheid) voortdurend aan de orde komen.

Inleiding

De psycholoog Maslow stelde het al vast. Elk individu heeft behoefte zich te ontwikkelen, maar is daarbij afhankelijk van zijn omgeving. Het individu kan niet bestaan zonder de eerste levensbehoefte water, voedsel en zuurstof. Wordt daarin voorzien, dan heeft hij behoefte aan veiligheid en continuïteit. Uiteindelijk zal hij behoefte hebben aan aanzien en dominantie.
Om de theorie van Maslow in het kader van dit artikel te plaatsen: de afhankelijkheid van de omgeving wordt beschouwd als de afhankelijkheid tussen twee of meer individuen waarbij het ene individu de behoefte van de ander vervult. En om dit kader verder te specificeren: we beschouwen dan de afhankelijkheid tussen twee of meer ondernemingen of organisaties. Een organisatie is immers een groep van individuen die een onderlinge afhankelijkheid vertonen.
De afhankelijkheid tussen ondernemingen uit zich dan als een samenwerking tussen die instituten, of anders gezegd homeostase (Van Dale: het bestaan van onderling op elkaar afgestemde bedrijfsprocessen die voor het leven noodzakelijke toestanden constant houden). Een homeostase waarin ieder zijn specialistische rol heeft en daarvoor verantwoordelijk is. En omdat we spreken over (groepen van) individuen speelt het kwaliteitsaspect betrouwbaarheid een belangrijke rol. Dit aspect bepaalt vooral het succes van de samenwerking. In een groep kan de 'betrouwbaarheid' van de samenwerking min of meer worden afgedwongen door bijvoorbeeld een missie en visie op te leggen. De betrouwbaarheid van de samenwerking tussen groepen kan niet afgedwongen worden.

Rollen worden bepaald op basis van vaardigheden. Taken worden toebedeeld aan degenen die dat kunnen. Deze logica vormt de grondslag voor vele strategische keuzen die ondernemingen tegenwoordig maken tussen kern- en niet-kernvaardigheden.
Een auto bestaat uit veel onderdelen die geproduceerd en geleverd worden door verschillende ondernemingen (toeleveranciers) die daarin zijn gespecialiseerd. De automobielonderneming is hun klant en deze heeft de strategische keuze gemaakt om zich te specialiseren in de kernvaardigheden 'assembleren', 'marketen' en 'verkopen'.

De klant kiest ook toeleveranciers die de niet-kernvaardigheden kunnen invullen. Onze vrije markteconomie zorgt echter voor concurrentie onder die toeleveranciers. Indien deze concurrentie groot is, zal de leverancier zich moeten onderscheiden van zijn concurrenten om de leverancierstatus met zijn klant te behouden. In zijn pogingen zich continu te onderscheiden zal de leverancier steeds innovatiever en creatiever worden. Zo kan hij bijvoorbeeld zoals dat genoemd wordt klantgerichter zijn 'water, voedsel en lucht'-product leveren en produceren. Hij zal willen meedenken met zijn klant hoe deze zijn 'water, voed-

sel en lucht'-product tot zich neemt en ook hoe hij die gebruikt, verwerkt tot en met zelfs hoe zijn product door zijn klanten wordt gebruikt.
De leverancier moet daarbij zijn productieproces afstemmen op dat van zijn klant. Vanuit het belang van de klant beschouwd wil deze een betrouwbaar product van zijn toeleverancier ontvangen en wil (dus) weten hoe het 'water, voedsel en lucht'-product geproduceerd wordt. Beide partijen staan toe om in elkaars 'keuken' te kijken. Deze openheid van zaken gebeurt niet van de een op de andere dag. Er moet sympathie en vertrouwen in elkaar opgebouwd worden om dat partnerschap te bereiken. Beide partijen moeten elkaars kwetsbaarheden kennen die de kritieke succesfactoren van het proces bepalen.

Het 'water, voedsel en lucht'-product is echter niet uniek. Dat ligt anders bij het product van de 'T' van ICT. De ontwikkeling in de computertechnologie gaat razendsnel en er is specialistische kennis en kunde voor nodig om de complexiteit het hoofd te kunnen bieden. Aanvankelijk had de organisatie van de klant zelf nog zijn mensen die de complexiteit begrepen. Maar al gauw vereiste dat een meer specifieke kernvaardigheid die niet meer te rijmen viel met de oorspronkelijke kernvaardigheden van die organisatie. De grote afhankelijkheid van ICT vereist dan dat de toeleverancier van die kernvaardigheden zijn bedrijfsprocessen moet afstemmen op die van zijn klant. Zie hier het ontstaan van een partnerschap.

Betrokkenheid bij de klant, een betrouwbaar product leveren, omdat we weten hoe essentieel – zeg maar gerust onmisbaar – onze diensten voor de klant zijn. Zonder energie staat alles stil, loopt alles vast. Zonder energie geen welvaart. Energie staat voor leven, voor bewegen, dus verder komen in het leven. Wij willen samen met onze klanten verder komen. Door een natuurlijke partner in nieuwe energie te zijn. Een partner op wie je kunt bouwen met een traditie van betrouwbaarheid. Een van de grootste en sterkste spelers in Europa. Die positie hebben we verworven door ervaring, een scherpe prijsstelling en een uitgebreide productportfolio. De basis is onderling vertrouwen, een duurzame samenwerking en een gemeenschappelijk belang. Wij zijn een partner die meedenkt, meebeweegt en streeft naar vooruitgang en vernieuwing. Niet als doel, maar als middel. Altijd ten dienste van het klantvoordeel.

De revolutionaire ontwikkelingen in de ICT veroorzaken een versnelling van het proces dat leidt tot een intensieve(re) samenwerking. De toenemende behoefte aan elkaars openheid en meer afhankelijkheid vergen een gestructureerde aanpak. Later in deze bijdrage wordt een model beschreven dat gebruikt kan worden om dit proces stapsgewijs op een betrouwbare manier te begeleiden.
Het model gaat uit van twee ondernemingen die met elkaar een vertrouwensrelatie opbouwen op het gebied van ICT. Deze twee organisaties zijn de zogehe-

ten ICT-onderneming (de leverancier die 'water, voedsel en lucht' produceert) en de niet-ICT-onderneming (de klant die 'water, voedsel en lucht' afneemt). Het model gaat voorts uit van 'toestanden' in de opbouw van vertrouwen in de samenwerking. Dat wil zeggen van een toestand van een samenwerking waarbij de ene onderneming voorziet in de basisbehoefte van de andere (zgn. relatie tussen klant en leverancier). Dat kan leiden tot een toestand van samenwerking tussen twee ondernemingen die 'samen' durven te ondernemen (zgn. 'strategisch partnerschap'). In de termen van Maslow: samen zorgen voor de continuiteit en samen een imago opbouwen.

Wij zijn een partner op het gebied van verpakkingsmaterialen voor alle bedrijven die zich bezighouden met problemen bij het verpakken van agrarische en industriële producten. Onder partner verstaan wij:
- een leverancier van verpakkingsmaterialen;
- een voorraadhoudende groothandel;
- een logistieke organisatie;
- een innovatieve en milieubewuste meedenkende onderneming;
- betrouwbaarheid, hoge servicegraad, klantgerichtheid en prijsbewust handelen.

Trends in ICT

Alvorens het model te beschrijven vatten we de trends op het gebied van ICT in de netwerkeconomie samen aan de hand van enkele statistieken.
Vier trends zijn typerend voor deze tijd en iedere onderneming kampt in meer of mindere mate met problemen die daaruit voortvloeien:
- De afhankelijkheid van ICT-middelen in de bedrijfsactiviteiten neemt toe. Konden organisaties voorheen nog terugvallen op hun oude handmatige activiteiten, tegenwoordig voorzien de vele geautomatiseerde bedrijfsactiviteiten niet meer in een terugval ('fall back')-scenario. Uitval van een ICT-middel kan allerlei stagnaties veroorzaken in het productieproces.
- ICT-middelen worden complexer en duurder in onderhoud. Invoeringen en onderhoud van steeds nieuwe computertechnologieën tezamen met de noodzaak tot het behoud van oude systemen maken de ICT-infrastructuur niet overzichtelijker. De ICT-infrastructuur (de samenhang tussen alle ICT-componenten als pc's, netwerk en 'servers') wordt steeds complexer. Men raakt de greep op de onderhoudskosten kwijt.
- ICT-personeel is moeilijker te werven en ICT-kennis is daardoor niet te behouden. Het onderhoud vergt niet alleen in toenemende mate specialisme van kennis en kunde. Ook het identificeren van de zakelijke mogelijkheden die ICT biedt vereist kundig personeel. Het is algemeen bekend dat de krapte

op de arbeidsmarkt vooral geldt voor dit soort gekwalificeerd ICT-personeel. Voor de niet-ICT-ondernemingen is het dan ook moeilijk om dit soort personeel een adequate carrière aan te bieden. Vandaar dat vele ondernemingen bewust kiezen voor de scheiding tussen kern- en niet-kernactiviteiten.

– Van oorsprong productgerichte ICT-ondernemingen worden meer dienstgericht. ICT-bedrijven zagen nieuwe kansen in het leveren van ICT-diensten naast hun producten, zoals installatie, beheer en onderhoud van de geleverde producten. Maar zij zagen ook kansen in het leveren van bedrijfskundig advies. Zo leveren vooral de grotere ICT-ondernemingen zelfs strategisch advies dat soms niets met de T van ICT te maken heeft. Deze ontwikkeling zorgde voor een professionelere houding van deze bedrijven. Kwaliteitszorg in de dienstverlening is kritischer en moet anders aangepakt worden dan in de productiesector. Een kenmerk van diensten door derden is immers dat zij afgestemd moeten zijn op de bedrijfsactiviteiten van de klant.

De eerste drie trends zijn dus kenmerkend voor bedrijven die ICT primair gebruiken en niet ontwikkelen; we noemen deze bedrijven in dit artikel de niet-ICT-ondernemingen. De vierde trend is kenmerkend voor automatiserings- of ICT-ondernemingen.

Het ligt dan ook voor de hand dat de niet-ICT-onderneming de bewuste strategische keuze maakt om (bepaalde) ICT-activiteiten te laten uitvoeren door een ICT-onderneming (ook wel 'uitbesteding' genoemd). Deze keuze is voornamelijk gebaseerd op de mogelijkheden om de problemen die deze trends met zich meebrengen te kunnen oplossen. Ziehier de totstandkoming van de netwerkeconomie. De vraag naar samenwerkingsrelaties is dan ook groot. Kent u die reclametekst "U de zaken, wij de bijzaken"? En "Wij doen alles waar een ondernemer aan moet, maar niet aan wil denken"?

Formele samenwerkingsrelaties kenmerken zich door het aangaan van contractuele overeenkomsten met afspraken over de dienstverlening in een zogeheten Service Level Agreement (SLA).

De laatste jaren echter hebben dit soort samenwerkingscontracten (vooral met ICT-ondernemingen) zich met moeite of zelfs niet in stand weten te houden.

Enkele statistieken:

– Het bekende onderzoeksbureau Gartner stelde vast dat 45% van de contracten binnen één jaar wordt open- of afgebroken.
– Uit een recent Ernst & Young-onderzoek kwam naar voren dat de verwachtingen te hoog bleken voor meer dan de helft van het aantal ondervraagde niet-ICT-ondernemingen. Zij verwachtten van een 'waar' partnerschap dat de ICT-onderneming professioneel, pro-actief en innovatief moet meedenken met de problemen waarmee de niet-ICT-ondernemingen continu kampen. Zij verwachtten ook dat de ICT-onderneming bereid was om risico's te dragen voor de oplossingen die deze ondernemingen aandroegen.

– Hetzelfde onderzoek gaf voorts aan dat 80% van de niet-ICT-ondernemingen zo ontevreden was dat zij graag hun ICT-dienstverlener zouden willen inruilen.

De gevolgen van de strategische keuze werden dus niet voorzien. Hoe komt dit? De kernoorzaak van het probleem zit in het definiëren van de ICT-activiteiten die uitbesteed moesten worden, en in de vraag wat deze activiteiten moesten opleveren. Het definiëren van activiteiten die losstaan van de bedrijfsprocessen, zoals kantine- of drukkerijactiviteiten is relatief gemakkelijk. Dit geldt ook voor afgebakende ICT-activiteiten als de salarisadministratie of beheeractiviteiten voor systemen die afgeschreven zijn (zgn. sterfhuisconstructies). Het loskoppelen van ICT-activiteiten die betrekking hebben op de ICT-infrastructuur is echter veel ingewikkelder, omdat veel meer afstemming met het bedrijfsproces van de niet-ICT-onderneming moet plaatsvinden. De vraag naar dit soort uitbestedingen is echter groot (vanwege de problemen als gevolg van de voornoemde trends). Het inhuren van ICT-personeel (detachering, 'bodyshopping') wordt als een tijdelijke oplossing gezien vanwege het strategisch belang van deze detacheringsbedrijven om uren te verkopen. De echte ICT-onderneming onderscheidt zich door resultaatgericht ondernemen in een win/win-relatie met zijn klant.
De traditionele relatie tussen klant en leverancier moet veranderen in een relatie van geven en nemen en risico's delen met en door beide partijen. Het tijdperk van het 'uitbesteden van problemen' ('out-so(u)res-ing') is voorbij. De netwerkeconomie moet volwassen worden.

Filosofie van het partnerschapmodel

Samenwerkingsrelaties worden wel 'partnerships' (partnerschap) genoemd, maar andere namen als allianties en joint ventures worden eveneens gehanteerd. Het proces om tot samenwerking te komen wordt ook wel 'outsourcing' en 'outtasking' genoemd, dat wil zeggen het uitbesteden van bepaalde activiteiten aan een onderneming die dit faciliteert aan zogeheten 'Facility Management'-organisaties. Of het uitbesteden van een bedrijfsafdeling die zich wil (of moet) verzelfstandigen. Het model concentreert zich zowel op dit proces als op het in stand houden van de samenwerkingsrelatie. Het beschrijft daarmee een strategie. Hoe het proces of het resultaat daarvan wordt genoemd wordt overgelaten aan de lezer.
De filosofie die achter deze strategie zit is dat stapsgewijs aandacht wordt besteed aan de kwaliteitsaspecten in de samenwerking. Eerst komen de 'voor de hand liggende' aspecten aan de orde die gebaseerd zijn op (het meten van) objectieve kwaliteitsnormen van de routinematige operationele diensten. Elkaars vertrouwen wordt gewonnen wanneer daarin gepresteerd wordt, en dus

wanneer voldaan wordt aan de overeengekomen normen. Geredeneerd vanuit de dienstverlener: zij kapitaliseert op de goodwill die gecreëerd is. Alleen als beide partijen elkaar vertrouwen kunnen ook diensten worden geleverd op tactisch en strategisch niveau. De kwaliteitsaspecten hiervan zijn immers gebaseerd op subjectieve waarden. Des te 'intensiever' de samenwerking, des te complexer de afstemming van (de normen en waarden over) elkaars bedrijfsprocessen met zijn activiteiten en procedures. De theorie van de strategie met de beschreven verbeterdomeinen is ook toe te passen op samenwerking met andere sectoren.

Alhoewel onze werkmiddelen met de dag veranderen, is ons streven naar verzorgd werk en dito kwaliteit onaangetast. Bovendien werken wij bij voorkeur via een partnerschap op lange termijn. Hier volgen enkele redenen waarom klanten ons hun vertrouwen schenken:

- Betrouwbaarheid: alle opdrachten worden stipt volgens de overeengekomen termijnen afgeleverd.
- Kwaliteit: wij hebben een reputatie opgebouwd dankzij onze hoogkwalitatieve dienstverlening aan de klant.
- Technische kennis: onze technische bagage is gegroeid uit jaren van literatuurstudie en interesse voor de sector.
- Een interessante verhouding tussen prijs en kwaliteit: geen verrassingen of aanpassingen achteraf.

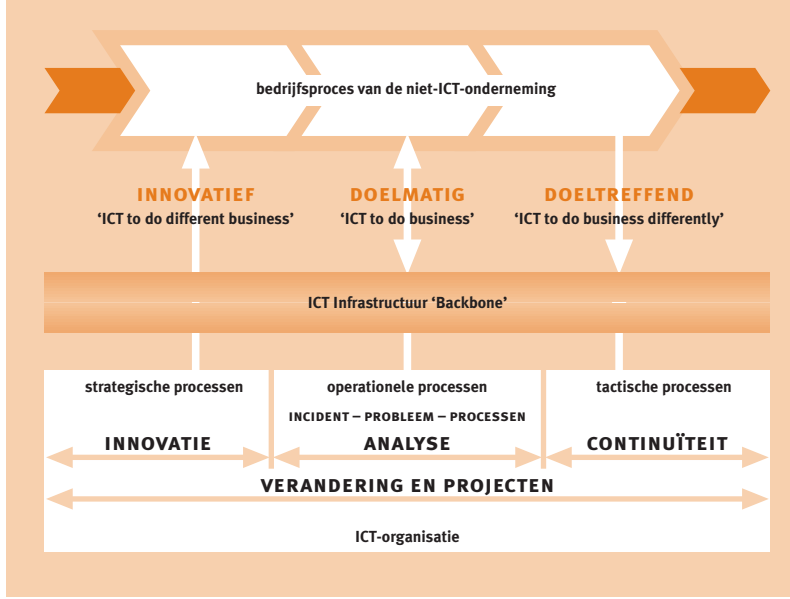
Het samenwerkingsmodel

Figuur 26.1 is een model van een levensvatbaar systeem (Engels: viable system[3]) dat bestaat uit een samenwerkingsrelatie tussen twee partijen. Voor het moment is het niet relevant of deze twee partijen in één onderneming zitten of dat het twee ondernemingen zijn. De ene partij maakt gebruik van ICT om hun product te maken (de niet-ICT-onderneming). De andere partij is verantwoordelijk voor alle kwaliteitsaspecten van de ICT (de ICT-onderneming). Het gaat nu om de samenwerking an sich. Het model symboliseert het continu verbeterprogramma. De toelichting is als volgt:

- De horizontale pijlvormige figuren symboliseren het bedrijfsproces (met zijn processtappen) van de niet-ICT-onderneming.
- Dit bedrijfsproces steunt op de ICT-infrastructuur: het geheel van in de onderneming aanwezige pc's, netwerken en servers met de geïnstalleerde applicaties en de informatie daarop. Dit geheel kan beschouwd worden als de ruggengraat van de niet-ICT-onderneming: de ICT-'backbone'.
- Deze backbone wordt beheerd door de ICT-onderneming. Deze partij ondersteunt het gebruik van deze backbone, dat wil zeggen ondersteunt diegenen die verantwoordelijk zijn voor het bedrijfsproces van de niet-ICT-onderneming.

3 zie [Beer, 1985].

Figuur 26.1
Model voor samenwerking tussen twee partijen.



Tabel 26.1
Beschrijving van de drie domeinen waar verbeteringen geïnitieerd en gerealiseerd worden.

Domein	Kenmerk	(Business)behoefte	Organisatieniveau
Doelmatigheid	'ICT to do business' ('de dingen beter doen')	De noodzaak om (de kosten van) het productieproces te optimaliseren.	Verbeteringen hebben een interne focus en zijn gericht op het operationele niveau van het 'systeem' (ICT- en de niet-ICT onderneming).
Doeltreffendheid	'ICT to do business differently' ('de dingen anders doen')	De noodzaak om het productievolume en of het marktaandeel te vergroten.	Verbeteringen hebben een externe focus en zijn gericht op het tactisch niveau. De uitvoering heeft natuurlijk zijn uitwerking op het operationele niveau.
Innovatie	'ICT to do different business' ('nieuwe dingen doen')	De noodzaak om dankzij ICT kernvaardigheden in te zetten om andere 'dingen te doen'.	Verbeteringen hebben ook een externe focus, maar zijn gericht op het strategische niveau waar de langetermijnkeuzen worden gemaakt. Het tactisch niveau krijgt de opdracht om het operationele niveau daarvoor in te richten.

- De drie verticale pijlen symboliseren drie domeinen waar verbeteringen geïnitieerd (behoeftebepaling) en gerealiseerd worden. Deze verbeteringen zijn gerelateerd aan het organisatorisch niveau. In tabel 26.1 worden deze domeinen beschreven.
- Een algemeen geaccepteerde standaard voor de inrichting van de organisatie beschrijft ITIL[4]. Het model van figuur 26.1 geeft slechts de voornaamste operationele ITIL-processen weer (ook wel helpdeskprocessen) genoemd. Tabel 26.2 geeft aan wat deze processen beogen.
- De organisatie van de ICT-onderneming bestaat uit de volgende managementprocessen:
  - De drie domeinen waar de verbeteringen worden voorgesteld, respectievelijk Analyse, Continuïteit en Innovatie (Analysis, Continuity and Innovation Management).
  - De operationele ICT-ondersteuningsprocessen. Een algemene standaard wordt beschreven door ITIL.
  - Het invoeringsproces Verandering en Projecten (Change and Project Management) dat de verbeterprojecten coördineert. Deze processen zijn cruciaal op elk organisatieniveau, omdat de uitwerkingen deze lagen doorkruisen. Tabel 26.2 definieert deze managementprocessen.

De drie genoemde verbeterprocessen, de operationele ITIL-processen en het invoeringsproces beogen het volgende (zie tabel 26.2 op pagina 316).

Deze zeven processen (waaronder de drie verbeterprocessen) kunnen beschouwd worden als het primaire proces van de ICT-organisatie. De uitwerking naar activiteiten en de beschrijving van de interactie tussen deze processen valt buiten de scope van dit artikel, evenals de uitwerking en de beschrijving van de ondersteunende en managementprocessen waaronder de vele andere ITIL-processen. Zie voor meer informatie[5].
De drie processen die verantwoordelijk zijn voor de drie verbeterdomeinen kennen een tijdshorizon:

- 'Review the past': de verbetervoorstellen uit Analyse hebben een kortetermijnkarakter en kijken als het ware terug op ervaringen van het operationele proces.
- 'Preview the future': de verbetervoorstellen van Continuïteit hebben een middellangetermijnkarakter en geven aan hoe ICT (anders) ingezet kan worden, zodat de niet-ICT-onderneming zijn doelstellingen kan realiseren.
- 'Envision the future': de verbetervoorstellen van Innovatie hebben een langetermijnkarakter en doen uitspraken over (nieuwe) ambities voor de niet-ICT-onderneming.

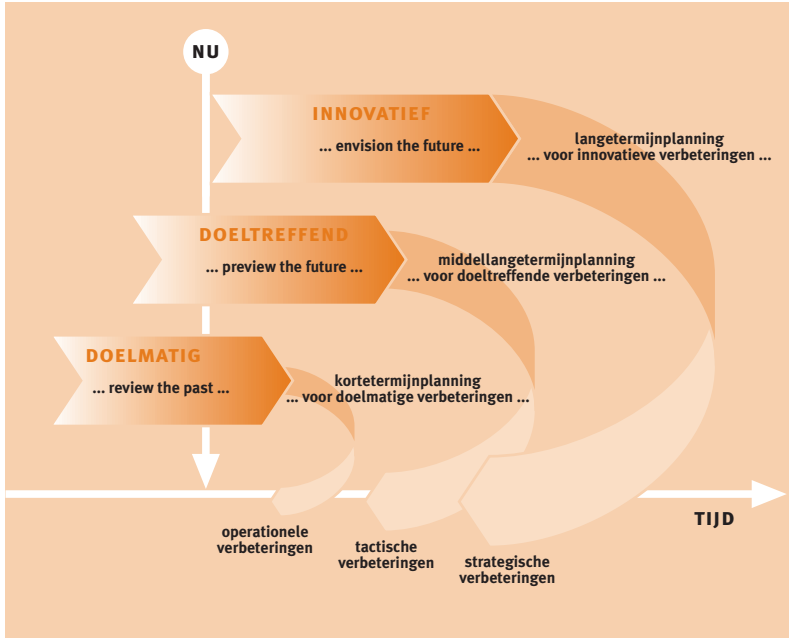
Een en ander is gevisualiseerd in figuur 26.2.

4 ITIL – Information Technology Infrastructure Library. ITIL beschrijft een algemeen geaccepteerde organisatievorm voor een organisatie die de bedrijfsprocessen ondersteunt met ICT. Veel automatiseringsbedrijven hanteren deze methode. Zie ook www.tools2manage-it.com.

5 Het boek 'MKB Groeicertificaat' [Wegener, 2000] geeft een theoretische en praktische uiteenzetting over hoe de primaire, de ondersteunende en de managementprocessen ingericht kunnen worden. Tevens beschrijft het de theorie en de inrichting van de drie verbeterdomeinen daarin. De beschreven methode is certificeerbaar en officieel erkend door de Raad voor Accreditatie.

Organisatieniveau	ICT-proces	Het proces waarin
Operationeel	Incident	het probleem van de gebruiker wordt opgelost. Dit probleem kan veel vormen aannemen. Van een simpele vraag (of klacht) over ICT tot een verzoek tot een ingrijpende verandering van ICT.
	Probleem	het gebruikersprobleem structureel wordt opgelost, indien de oplossing van tijdelijke aard was. Of indien repeterende problemen structureel worden opgelost.
	Operationele processen	de ICT-infrastructuur beschikbaar ('in de lucht') wordt gehouden.
	Analyse	de operationele processen worden geanalyseerd en verbeteringen worden voorgesteld die optimalisaties in de ICT-ondersteuningsprocessen beogen.
Tactisch	Continuïteit	tactische verbeteringen worden voorgesteld die een effectievere ondersteuning beogen van het management van de niet-ICT-onderneming. Hier worden voornamelijk strategische plannen vertaald in ICT-oplossingen en in relatie gebracht met de bestaande infrastructuur.
Strategisch	Innovatie	strategische verbeteringen worden voorgesteld die het management van de niet-ICT-onderneming innovatiever kan maken. Hier worden de strategische plannen ontwikkeld.
Operationeel, tactisch en strategisch	Verandering en Projecten	de voorgestelde wijzigingen in de ICT-infrastructuur en in de organisatie-(procedures) worden beoordeeld en uitgevoerd, eventueel in projectvorm.

Tabel 26.2
Definitie van de management-processen.



Figuur 26.2
De relatie tussen de drie verbeter-processen.

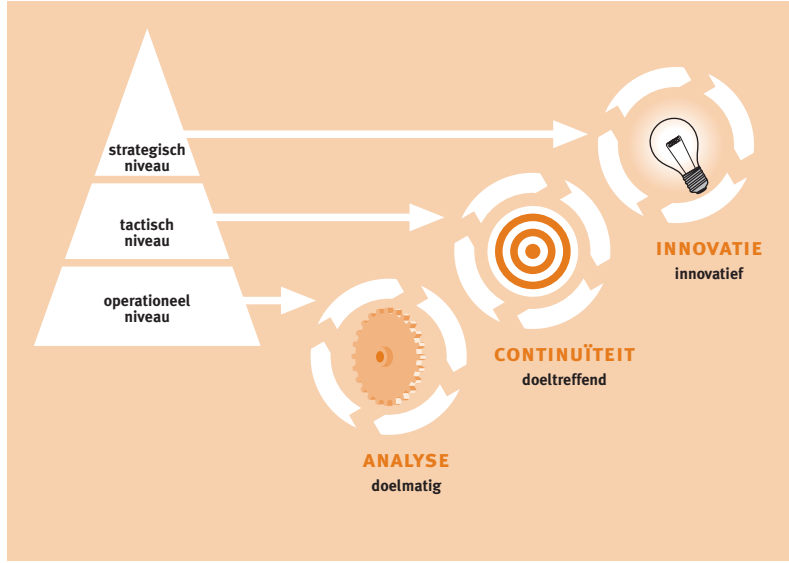
De relaties tussen Analyse en Continuïteit kunnen ook als volgt beschouwd worden. Hiervoor wordt uitgegaan van de eenvoudige economische bedrijfsformule winst is omzet min kosten. Dit betekent dat men de winst wilt maximaliseren voor de niet-ICT-onderneming door de productiekosten zo laag mogelijk te houden en de waarde die de klant 'hecht' aan het product van de niet-ICT-onderneming zo hoog mogelijk te maken. Analyse richt zich op de doelmatigheid van het operationele proces en streeft naar een hogere kwaliteit van het arbeidsproces door de operationele kosten te verlagen, dan wel efficiënter te opereren. Continuïteit richt zich op de doeltreffendheid van het productieproces en streeft naar een hogere kwalitatieve waarde van het product, zodat de omzet wordt verhoogd. Innovatie heeft betrekking op nieuw te ontwikkelen producten.

Elk verbeterproces kenmerkt zich door de cyclus van Deming [6] 'Plan – Do – Check – Act'. Met andere woorden 'continu verbeteren'. Met deze cirkels waarvan Verandering en Projecten dus een essentieel onderdeel uitmaakt, kunnen we de drie verbeterdomeinen in relatie brengen met de bedrijfskolom (zie figuur 26.3 op pagina 318).

De ICT-matrix

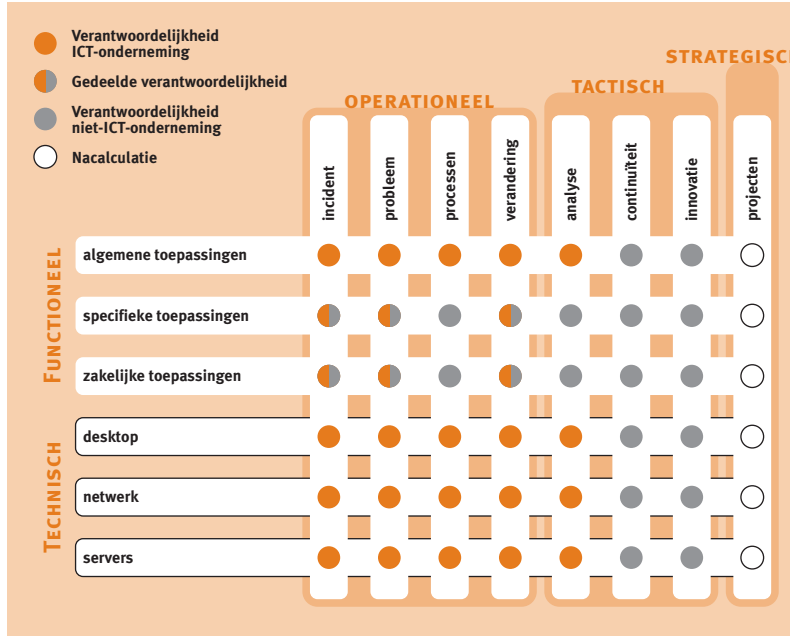
Aan de hand van deze zeven primaire ICT-processen kunnen we de missie van de ICT-organisatie als volgt formuleren 'het doelmatig, doeltreffend en innovatief exploiteren van de ICT-infrastructuur van de niet-ICT-onderneming'.
De inrichting van de ICT-organisatie hangt af van de verschillende partijen die daarin deelnemen. Deze organisatie kan een ICT-afdeling zijn, maar ook een extern ('faciliterend') automatiseringsbedrijf (of een samenwerking van deze twee bedrijven). We gaan nu uit van een samenwerkingsorganisatie tussen de ICT-afdeling van de niet-ICT-onderneming en de ICT-onderneming. De inrichting van deze samenwerkingsorganisatie is sterk afhankelijk van de antwoorden op vragen als 'wie doet wat, wanneer en hoe, welke taken worden overgenomen, hoe moeten die ingevuld worden, enz.' In dit samenwerkingsverband moeten dus afspraken zowel tussen de niet-ICT-onderneming en de ICT-onderneming als tussen deze samenwerkingsorganisatie en de niet-ICT-onderneming die de ICT-middelen gebruikt, gemaakt worden. Het proces van het maken van afspraken kan het beste worden gedaan door middel van een workshop. De verschillende verantwoordelijke personen van beide partijen komen in de eerste plaats overeen hoe elk van de zeven processen eruit ziet om vervolgens per proces overeen te komen wie, wat en wanneer oplevert. Op deze manier wordt duidelijk welke processen of delen van processen 'uitbesteed' worden.
Ook wordt op deze manier duidelijk wie verantwoordelijk is voor elk van de drie verbeterprocessen. Typische afspraken voor die processen liggen in de sfeer

6 Elk proces kent een moment van voorbereiding, actie, bezinning en van het bijstellen van de veranderende omgeving. W. Deming heeft deze wetmatigheid naar bedrijfsprocessen vertaald en koppelt hieraan de begrippen Plan – Do – Check – Act (PDCA). Dit is een repeterend proces in zichzelf. Veel literatuur over kwaliteit in bedrijfsvoering verwijst naar de PDCA-cirkel van Deming. Deming is een beroemde goeroe op het gebied van kwaliteit (zie ook www.deming.org).



Figuur 26.3
De drie verbeterdomeinen per organisatieniveau.

van consultancy 'uren per jaar', van het opleveren van verbetervoorstellen en van het aantal (kwaliteits)audits per periode.
Getronics gebruikt voor het visualiseren van deze afspraken de zogeheten ICT-matrix met horizontaal de processen en verticaal de domeinen waarop deze processen betrekking hebben. Figuur 26.4 beeldt deze matrix op het hoogste niveau af. In diepere niveaus worden de processen uitgewerkt in subprocessen en activiteiten. In elk domein wordt aangegeven wat de niet-ICT-onderneming 'in huis' heeft. De volgorde van de processen in deze matrix is bepaald vanuit

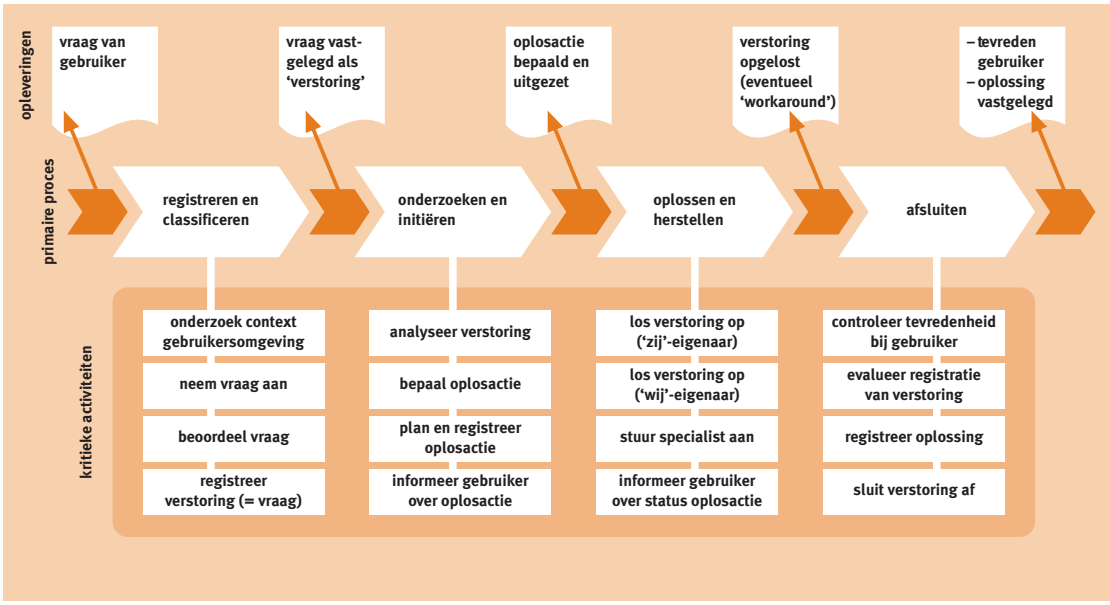


Figuur 26.4
De ICT-matrix voor het visualiseren van de wederzijdse afspraken.

het strategisch belang voor de klant. Eerst komen de re-actieve en routinematige diensten in aanmerking voor het 'uitbesteden', vervolgens worden de drie verbeterprocessen benoemd. De volgorde van de domeinen is bepaald vanuit de perceptie van de gebruiker in de niet-ICT-onderneming. Eerst de 'iconen' op zijn pc die hij activeert om zijn werk te doen, vervolgens de infrastructuur die daar'achter' ligt.

Tevens zullen tijdens de workshop de functionele en technische domeinen tot in detail benoemd moeten worden, zodat er geen onduidelijkheden gaan ontstaan tijdens de processen.
Merk op dat de processen op de 'kruisingen' met een gedeelde verantwoordelijkheid uitgewerkt moeten worden tot op het niveau waarop de verantwoordelijkheden wel toegewezen kunnen worden. Figuur 26.5 is een voorbeeld van een uitwerking van het Incident management in deelprocessen en kritieke activiteiten. De verantwoordelijkheden (en afspraken) van de deelprocessen kunnen op die manier toegewezen worden. En eventueel worden verantwoordelijkheden per kritieke activiteit vastgesteld.
Via deze aanpak van detaillering kan men ook de kosten van de activiteiten bepalen. De ICT-onderneming kan nu immers per activiteit inschatten hoeveel tijd en welke kernvaardigheid nodig is. Dit inzicht in de kosten is een essentieel aspect voor het verkrijgen van wederzijds vertrouwen.
De afspraken worden vervolgens vastgelegd in een document (bijv. een SLA-contract). Dit is een document dat een of twee keer per jaar herzien moet worden (via versiebeheer, ITIL noemt dit SLA-management) via een workshop en of naar aanleiding van verbetervoorstellen of resultaten na verbeterprojecten. Overigens kan dit document een bijlage zijn van een mantelcontract. Dit mantelcontract heeft een 'levensduur' van 3 tot 5 jaar.

Via nieuwe versies wordt het verbeterprogramma tastbaar. Opvolgende versies van het SLA-contract laten een andere kleur stip in de ICT-matrix zien.
Een niet-ICT-onderneming had zijn helpdesk uitbesteed aan een ICT-onderneming. Deze had de verantwoordelijkheid gekregen voor de operationele (ITIL)-processen. Na een jaar samenwerken besloot de niet-ICT-onderneming tot verbeteracties, omdat zij ontevreden was over de dienstverlening. De gebruikers vonden dat hun problemen niet goed werden opgelost, het netwerk viel uit zonder kennisgeving, het management kreeg de indruk dat zij geen waar voor hun geld kregen. Beide partijen hanteerden vervolgens de ICT-matrix om de kwaliteitseisen rondom verantwoordelijkheden te bepalen. Alle ICT-aspecten werden in kaart gebracht en alle matrixprocessen werden besproken. Met de matrix konden concrete (resultaatgerichte) afspraken gemaakt worden. De kostenstructuur was eveneens duidelijk geworden. Het wederzijds vertrouwen was weer terug.



Figuur 26.5
Incident management.

Progressief partnerschapmodel

Zoals met alle afspraken in een samenwerkingsrelatie gaat het om vertrouwen. Dit vertrouwen moet opgebouwd worden. Dit beschrijven we aan de hand van de 'intensiteit' van de samenwerkingsrelatie die we – analoog aan het volwassenheidsmodel van CMM[7] – gedurende vier fasen kunnen kwalificeren. Gedurende elke fase wordt een zekere mate van volwassenheid bereikt door stapsgewijs te werken aan de hiervoor beschreven verbeterdomeinen. De overgang van de ene stap naar de volgende kan bepaald worden aan de hand van toetsingscriteria (CMM spreekt over 'Key Process Areas').

Fase 1: op bestelling georiënteerd ('Order Taking')

De niet-ICT-onderneming plaatst bestellingen voor producten die de toeleverancier of het automatiseringsbedrijf levert. Er kan een voorkeursrelatie met de leverancier ontstaan via bijvoorbeeld een (raam)contract gebaseerd op harde concrete afspraken (normen).

Afspraken over de geleverde producten zijn hard en zijn gebaseerd op normen. Beslissingen over de kwaliteit van de producten hebben een instrumenteel karakter. Men werkt volgens vaste regels en procedures. De toeleverancier denkt in producten en doet zaken (overlegt) met de inkoper of contractmanager van de niet-ICT-onderneming. Wat betreft de zeven ICT-processen komen gedurende deze fase dus slechts die procesactiviteiten in aanmerking voor 'uitbesteding' die te maken hebben met bijvoorbeeld de inkoop.

7 CMM – Capability Maturity Model. Dit model is ontwikkeld door Carnegie Mellon Software Engineering Institute. Het model beschrijft hoe in vijf stappen ('levels') een softwareontwikkelingsorganisatie een volwaardige lerende organisatie kan worden. Zie ook www.sei.cmu.edu.

Fase 2: op diensten georiënteerd ('Service Taking')
De ICT-onderneming levert naast zijn producten ook diensten zoals installatie en reparatie. Dit kan ook geïnterpreteerd worden als de niet-ICT-onderneming heeft een gedeelte van zijn ICT-processen van zijn ICT-afdeling 'uitbesteed'. Dat wil zeggen dat een activiteit die door een externe of derde partij wordt verricht nu als 'dienst' wordt gedefinieerd.
In het begin van deze fase blijft dit gedeelte beperkt tot de routinematige operationele activiteiten. Dat zijn per definitie de activiteiten die voor de niet-ICT-onderneming een relatief laag risico hebben ('volledig onder controle') en worden wel 'commodity'-diensten genoemd. Het kenmerk van deze diensten is dat zij reactief van aard zijn. De klant vraagt en geeft opdracht, de uitvoerder antwoordt en voert de opdracht uit. De opdracht kan ook een onderzoek tot advies behelzen.

Afspraken over de geleverde diensten (en opdrachten) zijn hard en gebaseerd op normen. Beslissingen over de kwaliteits(parameters) hebben een rationeel karakter. Men onderhandelt over de afstemming van de procedures.
Overlegstructuren tussen beide partijen op verschillende 'organisatieniveaus' zijn geformaliseerd. Het contract tussen beide partijen beschrijft een dienst met resultaatgerichte activiteiten.
De ICT-onderneming denkt in processen (diensten) en communiceert met de niet-ICT-onderneming over normen en waarden van de kwaliteit van zijn dienstverlening.
Tegen het einde van deze fase stelt een pro-actieve ICT-onderneming verbeteringen voor die zijn diensten voor de klant efficiënter en eventueel goedkoper maken ('ICT to do business more efficiently'). Hij krijgt immers steeds meer inzicht en ervaring in de 'gebruikers'-problemen van zijn klant. Op de korte termijn echter kan de ICT-onderneming hier dus omzet verliezen, als de klant geen opdracht tot advies heeft afgegeven. De ICT-onderneming krijgt bijvoorbeeld opdracht om snellere pc's of extra geheugens te installeren, maar toont aan dat hiermee de kern van het probleem niet opgelost wordt (De onderneming zou wel met de verkoop kunnen verdienen.).
Wat betreft de zeven ICT-processen komen dus gedurende deze fase slechts de (activiteiten in de) operationele processen in aanmerking voor 'uitbesteding'.

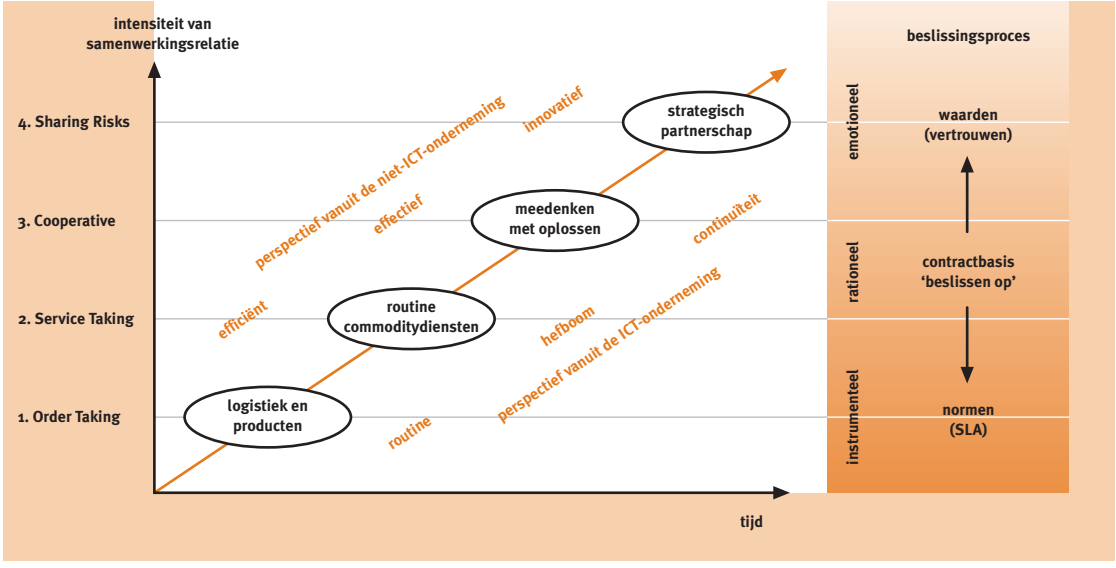
Fase 3: op coöperatie georiënteerd ('Cooperative')
In deze fase levert de ICT-onderneming naast zijn producten en diensten ook onderzoek en advies met het oogmerk 'ICT to do business more effectively'. Dit kan ook geïnterpreteerd worden als de niet-ICT-onderneming heeft nu ook zijn tactische processen uitbesteed.
Met deze diensten krijgt de ICT-onderneming tevens inzicht in de bedrijfsproblemen van de niet-ICT-onderneming. Gedurende fase 3 anticipeert de ICT-onder-

neming op deze problemen en verricht onderzoek ‘zonder opdracht’. De onderneming investeert in tijd en geld, denkt mee met het vinden van professionele oplossingen en stelt verbeteringen voor. De uitvoering van deze verbetervoorstellen heeft invloed op de bedrijfsvoering van de niet-ICT-onderneming in de trant van ‘ICT to do business differently’.
Afspraken over de geleverde diensten worden ‘zachter’. Beslissingen over kwaliteits(parameters) worden genomen, omdat partijen elkaar vertrouwen. Naast het formele overleg worden de werknemers van de ICT-onderneming gezien als werknemers van de niet-ICT-onderneming (lees informeel overleg).
Verbetervoorstellen kunnen leiden tot projecten waarvoor weliswaar concrete afspraken gemaakt worden, bijvoorbeeld over de inzet van deskundigheid en tarieven onder leiding van interim-managers van de ICT-onderneming. Een voorbeeld is de invoering van Internet- of E-commerce-applicaties waardoor de niet-ICT-onderneming op een andere manier zaken doet met zijn klanten en of andere markten aanboort.
Wat betreft de zeven ICT-processen komen gedurende deze fase ook de (activiteiten in de) tactische processen (eerst Analyse en dan Continuïteit) in aanmerking voor ‘uitbesteding’.

Fase 4: op risico’s delen georiënteerd (‘Sharing Risks’)

Op dit ‘hoogste’ niveau wordt het beleid (de strategie) voor de niet-ICT-onderneming ontwikkeld. Door het opgebouwde vertrouwen denkt en beslist de ICT-onderneming hierover mee. Beslissingen hebben een ondernemend (emotioneel) karakter. Een ICT-onderneming met ‘durf’ draagt dan ook de risico’s van de beslissingen, wanneer het projecten betreft waarin ICT een essentiële rol speelt (delen van winst of verlies).

Figuur 26.6
Volwassenheidsmodel voor samenwerkende organisaties van leverancier tot partnerschap.



Dankzij de inzet van ICT is het namelijk mogelijk dat de niet-ICT-onderneming geheel andere producten en of diensten kan gaan leveren. De uitvoering van dit soort verbetervoorstellen kan een enorme invloed hebben op het beleid èn op de bedrijfsvoering van de niet-ICT-onderneming, want het idee is 'ICT to do different business'.
Wat betreft de zeven ICT-processen komen gedurende deze fase ook de (activiteiten in het) strategische proces (Innovatie) in aanmerking voor 'uitbesteding'.
Figuur 26.6 visualiseert deze vier fasen voor samenwerkende organisaties.
Hierin zijn ook de belangen, dan wel perspectieven van beide partijen opgenomen:

- Het belang voor de niet-ICT-onderneming volgt de drie verbeterdomeinen: begin een samenwerkingsrelatie met het uitbesteden van routinematige activiteiten, krijg vertrouwen in de partner en besteedt dan de risicovollere activiteiten uit.
- Voor de ICT-onderneming is het belangrijk dat de continuïteit op de langere termijn moet worden gewaarborgd.

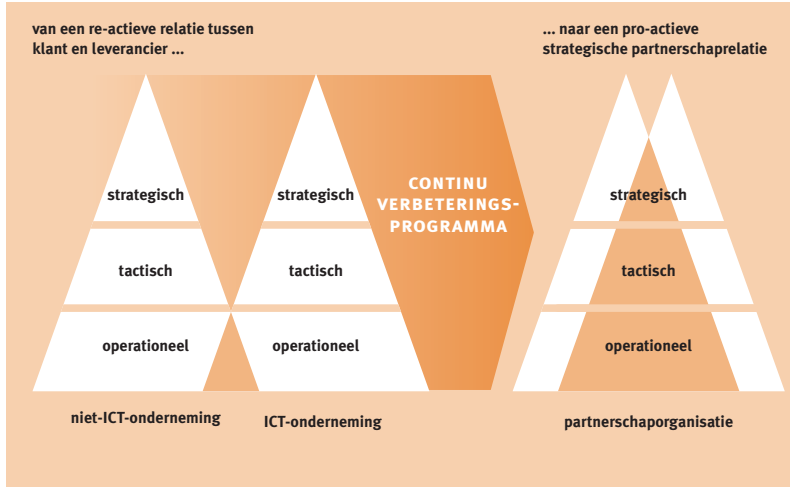
De koppeling tussen dit model en de ICT-matrix wordt zichtbaar door de gekleurde stippen op de kruisingen in deze matrix. De ICT-onderneming krijgt steeds meer verantwoordelijke 'kruisingen'. Tijdens elk tactisch en of strategisch overleg tussen de twee partijen worden de resultaten getoetst aan de criteria per stap, zodat de samenwerkende organisatie naar een hoger ontwikkelingsniveau kan gaan.

Conclusie

Om problemen met de 'netwerkeconomie' het hoofd te bieden, zoeken ondernemingen naar hechtere samenwerkingsvormen met andere ondernemingen.
Dit artikel is ervan uitgegaan dat de niet-ICT-ondernemer in deze zoektocht de bewuste keuze heeft gemaakt om bepaalde ICT-activiteiten uit te besteden.
In figuur 26.7 staat de beschreven strategie samengevat:

- De bedrijfskolom van elke organisatie bestaat uit een strategisch, een tactisch en een operationeel niveau.
- In een beginnende samenwerking is de relatie tussen klant en leverancier reactief: de niet-ICT-onderneming vraagt, de ICT-onderneming levert.
- Middels het continu verbeterprogramma waaraan beide partijen werken, kan deze samenwerking uitgroeien tot een waar strategisch partnerschap. Een nieuwe samenwerkingsorganisatie is een feit.

Voor twee partijen die met elkaar willen samenwerken, is het progressieve partnerschapmodel tezamen met de ICT-matrix een communicatiemiddel om conti-



Figuur 26.7
Van een re-actieve relatie tussen klant en leverancier naar een pro-actieve strategische partnerschap-relatie.

nu de afspraken over alle kwaliteitsaspecten van de afstemming bespreekbaar te houden. Met de ICT-matrix is aangegeven dat de kwaliteitsaspecten niet alleen bepaald worden door de techniek (verticale as). De kwaliteit wordt vooral bepaald door het samenspel van techniek èn processen (horizontale as).
Beide of een van de partners kunnen ook een bewuste keuze maken om in fase 1 of 2 te blijven. Het is namelijk heel goed mogelijk dat een toeleverancier bewust kiest om niet op het strategisch niveau van zijn klant te (onder)handelen. Het beschrevene is verre van uitputtend, maar verdere uitwerking valt buiten de scope van dit artikel.
Natuurlijk zijn er tal van aspecten die van belang zijn en uitgewerkt moeten worden zoals de (communicatie)culturen van beide partijen en de mogelijkheden (en problemen) die geschapen worden om bijvoorbeeld personeel naar de andere partij over te zetten.

Getronics heeft al een groot aantal contracten met 'Nadere Overeenkomsten' die de ICT-matrix bevatten. Regelmatig worden deze NO's herzien tot nieuwere versies. De ervaring heeft geleerd dat de 'versimpelde' weergave van de ITIL-processen in de ICT-matrix een succes is. Op deze manier wordt voorzien in een oplossing tot het continu verbeteren van samenwerkingsrelaties met zijn klanten.

Referenties

- Beer, S. (1985). Diagnosing the System for Organizations. John Wiley & Sons, New York
- Wegener, V.A., G.S.D. Maathuis. (2000). MKB Groeicertificaat. Kluwer Quality Info

2

27 Betrouwbaarheid in de voedingsmiddelenindustrie

dr. R. Cocker[1]

Inleiding

Hygiënische en of aseptische systemen bestaan uit afzonderlijke componenten, machines, meetsystemen, managementsystemen en automatisering. Deze systemen worden gebruikt voor de productie van voedsel, medicijnen, cosmetica, persoonlijke verzorgingsproducten en zelfs water. Deze bijdrage gaat over de rol die de integratie van deze systemen bij de veiligheid van voedsel speelt.

Geschiedenis

In reactie op ernstige incidenten in het verleden, waarbij microbiële en chemische contaminatie is opgetreden, heeft de farmaceutische industrie een uitgebreide structuur geïntroduceerd om de productveiligheid te garanderen. Echter in andere sectoren van de industrie wordt het belang van hygiënisch ontwerp vaak niet ingezien. In 1999 bijvoorbeeld resulteerden onvolkomenheden in de apparatuur en in procedures voor de watervoorziening van zwembaden en gezondheidscentra(!) in Nederland in een gevaarlijke uitbraak van de Legionellaziekte. Veel zwembaden en gezondheidscentra moesten worden gesloten of voor veel geld worden gemoderniseerd.

1 Cocker Consulting and Innovus BV
Bergeendlaan 16
1343 AR Almere

De geschiedenis van de voedselproductie kent veel fouten. Sommige daarvan waren voornamelijk te kostbaar om te herstellen en andere waren catastrofaal. Bijvoorbeeld in de VS alleen al heeft het USDA[2] becijferd dat jaarlijks 76 miljoen infecties door voedsel optreden. Hiervan komen er 300.000 in het ziekenhuis en overlijden er 5.000 per jaar. Een aantal bedrijven zijn failliet gegaan door incidenten waarbij zij aansprakelijk werden gesteld. In 1998 bijvoorbeeld werd Jack-in-the-Box Beef burgers met US$ 58,8 miljoen aan compensatieclaims geconfronteerd, nadat veel personen ziek werden en vier mensen overleden.

Voor het jaar 1999 heeft Kraft Foods becijferd dat 22 miljoen kilo hotdogs en koud vlees voor de Amerikaanse vleesindustrie verloren ging en becijferde een winstvermindering van US$ 27 miljoen die was veroorzaakt door hygiënische fouten. Kraft Foods merkte op dat de incidenten het vertrouwen van de consument konden verminderen en zouden leiden tot verkoopverliezen in de hele bedrijfstak. In Europa alleen al hebben incidenten met besmet dierlijk voedsel, frisdrank, *Escherichia coli HO 157* en BSE substantiële verkoopverliezen, importblokkades en politieke tweedracht veroorzaakt tussen de lidstaten.

Snel veranderende technologieën en processen

Er heeft een snelle revolutie plaatsgevonden in de manier waarop voedsel wordt gemaakt en in de oorsprong van voedselproducten. Al in 1882 vond het eerste transport van bevroren lam plaats van Nieuw-Zeeland naar Groot-Brittannië. Veranderingen zoals inblikken, pasteuriseren en sterilisatie vergrootten de veiligheid, variatie en het assortiment van beschikbaar voedsel, maar gingen vaak ten koste van de kwaliteit van eten en drinken. Met de toegenomen welvaart en de al aanwezige beschikbaarheid van voedsel zijn de consumenteneisen nu hoger. En met het verschijnen van veel nieuwe technologieën worden de grenzen van het onder milde condities bewerken van voedsel steeds verder opgerekt. Tegelijkertijd is er een trend om minder conserveermiddelen toe te voegen en producten te koelen en de houdbaarheid te verbeteren. Dit is om een betere kwaliteit van eten en drinken te verkrijgen samen met meer gemak tegen lagere kosten. Om deze reden zijn relatief nieuwe technologieën als vacuüm-, beschermende atmosfeerverpakking, koken-afkoelen, microfiltratie en hittebehandeling van melk, magnetronverwarming en sterilisatie door gepulseerde hoge spanningen, weerstandsverhitting, hoge druk, intense lichtpulsen en ioniserende straling geïntroduceerd. Een aantal oude voedselconserveringsmethoden als fermentatie van voedsel zijn weer opnieuw 'uitgevonden' in moderne vormen.

De technologie van de detectie en kwantificering van microbiële, chemische en zichtbare (deeltjes)verontreiniging is ook volop in ontwikkeling, in het bijzonder

2 www.nal.usda.gov/fnic

met de introductie van snelle automatiseringstechnieken voor de detectie en metingen van pathogene micro-organismen en complexe organische vergiften als pesticiden en microbiële toxinen.
Ook nieuw is de omslag van de ontwikkelde landen naar massaproductie van kant-en-klaar ('ready-to-eat', RTE) voedsel en gemaksmaaltijden die steeds verder transport vereisen naar het verkooppunt. Dit vereist hogere standaarden van bewaking en controle dan wanneer het voedsel na bereiding meteen zou worden geconsumeerd. Meer en uitgebreidere distributie kan betekenen dat gedistribueerde uitbraken van infecties moeilijker te herkennen en in te dammen zijn, zodat meer grensoverschrijdende meldingen en analysen van ziektepatronen noodzakelijk zijn.
Al deze zaken hebben geleid tot meer aandacht voor het hygiënische en aseptische ontwerp en voor de regulering van de veiligheid van voedsel 'van boerderij tot vork'. Nieuwe reguleringsstandaarden werden overal op de wereld geïntroduceerd voor dierlijk voedsel, verzorging op de boerderij, voedselproductiemachines en integraal riskmanagement. Dit werd mede ondersteund door vrijwillig bijgedragen apparatuur en procedurele standaarden van organisaties als de European Hygienic Equipment Design Group (EHEDG) en in de VS de National Sanitary Foundation (NSF) en de 3-A organisatie.

De rol van het hygiënisch ontwerp

Een belangrijke nadelige factor in het aanleveren van veilig voedsel waren de onvolkomenheden in de standaarden voor hygiënisch ontwerp voor dierverzorging, slachthuizen, voedselproductieapparatuur, productielijnen, fabrieken en geassocieerde systemen. Bijvoorbeeld de introductie (zonder herontwerp) van roestvrijstalen componenten als kleppen en pompen hebben systemen voortgebracht die moeilijk en onnodig duur betrouwbaar te reinigen waren. Dode hoeken waar vuil zich ophoopt en stilstaande zones zijn van weinig invloed op chemische processen; ze kunnen echter fatale gevolgen hebben in voedselproductieprocessen.

De parel van de voedselindustrie: HACCP

Een positieve ontwikkeling is de introductie van het risicomanagementsysteem 'Hazard Analysis and Critical Control Points' (HACCP, spreek uit 'hasup'). Dit is een praktische bewerking van bestaande risicoanalysemethoden als Hazard and Operability Studies (HAZOP) voor voedselproductieprocessen. Het kan in meer of mindere mate het proces van 'Failure Mode Effect Analysis' (FMEA) omvatten. In Europa en in veel rechtstaten in de wereld wordt HACCP gezien als

zo'n krachtig gereedschap dat het een wettelijk vereist systeem voor alle voedselbereiders en toeleveranciers is geworden. De opleidingen en de betrokkenheid van het management hebben echter niet altijd in de pas gelopen met de introductie van wetgeving. Sommige organisaties die verantwoordelijk zijn voor de verzorging en slacht van dieren hebben in het verleden het standpunt ingenomen dat rauw vlees wordt bereid bij de consument thuis. Daar ligt dus de kritieke controlestap. Zij hoeven dus geen actie te ondernemen om het niveau van pathogenen in het vlees te beheersen. De ontdekking van prionziekten die op mensen kunnen worden overgedragen (zoals BSE) heeft een pijnlijke heroverweging geforceerd. De temperatuur die nodig is om prionen te doden is ongeveer 700 °C. Dat betekent dat de belangrijkste plaatsen om prionen te beheersen de boerderij en het slachthuis zijn. Het statement dat veilig voedsel de aandacht eist van 'boerderij tot vork' heeft weer aan kracht gewonnen door BSE. De EU is begonnen met controles in de gehele 'supply chain'.
Standaarden voor de invoering van HACCP variëren enorm. Er zijn incidenten geweest waarbij bedrijven die beweerden HACCP te hebben uitgevoerd ernstige problemen hadden.
Dus zijn er ook ontwikkelingen om de invoering van HACCP, HACCP-trainingen en HACCP-erkennningsorganisaties op dezelfde wijze officieel te erkennen als bij systemen als ISO 9000 en ISO 14000 gebruikelijk is.

Ontwikkeling van een hygiënisch ontwerp als wetenschappelijke en technische discipline

Door de jaren heen hebben commerciële belangen in het bijzonder die van de grote voedingsmiddelenbedrijven de ontwikkeling van systemen en standaarden gestimuleerd die risico's, kosten en de invloed op het milieu kunnen reduceren om veilig voedsel te kunnen leveren voor consumptie. Dit is verbreed en omvat nu ook testinstituten, adviesbureaus, apparatuurleveranciers, opleidingen, overheid en internationale organisaties op het gebied van hygiënisch ontwerp en voedselveiligheidsmanagement. De belangrijkste barrière is echter het gebrek aan mogelijkheden voor een allesomvattende training in hygiënisch ontwerp samen met het probleem om deze kennis te communiceren in bestaande organisaties. Te vaak bijvoorbeeld is de selectie van componenten gebaseerd op 'van horen zeggen' of gewoonte dan op fundamentele kennis en gecontroleerd testen. Een gedeeltelijke verklaring zou kunnen liggen in het feit dat hygiënisch ontwerp een specifieke combinatie van technische, microbiologische en risicomanagementkennis vereist, dat niet in het hoger onderwijs wordt onderwezen. Technici en andere ontwerpers in de voedingsmiddelen-, de farmaceutische en de biotechnologische industrie worden consequent gevraagd om ontwerpen te maken waarvoor hun opleiding ontoereikend is.

Bijdrage professionele organisaties aan veiligheid en betrouwbaarheid

Zoals al vermeld, blijven organisaties als EHEDG, NSF en 3-A voor waardevolle en praktische typecertificaties, ontwerp en procedurele richtlijnen zorgen om de bouwers en gebruikers van hygiënische en aseptische systemen te ondersteunen. Dit proces waarlangs typegecertificeerde componenten beschikbaar komen staat nog in de kinderschoenen. Er is echter duidelijk behoefte aan zulke certificeringen, zoals blijkt uit valse claims die apparatuurleveranciers in hun advertenties zetten. Bijvoorbeeld 'FDA approved', de FDA verstrekt geen certificaten voor apparatuur. Valse claims over EHEDG- en 3-A-certificeringen zijn ook ingediend, waarschijnlijk eerder vanwege slechte communicatie of 'wishful thinking' dan uit opzettelijke misleiding.
Uit ervaringen is duidelijk geworden dat ondanks het bestaan van richtlijnen goede ontwerpen, systemen en componenten vaak op zo'n manier in elkaar worden gezet dat nieuwe gevaren ontstaan, in het bijzonder microbiologische gevaren. Deze gevallen zijn niet alleen een probleem voor de voedingsmiddelenindustrie, het kostte experts veel tijd en moeite om de recente CEN-veiligheidsstandaarden voor biotechnologische apparatuur en processen te schrijven. Integratie van hygiënische systemen blijft een gebied waar echte expertise schaars is. Als resultaat leiden de bouwers, de gebruikers van apparatuur en de consumenten grote verliezen. Veel van de betrokkenen zijn zich er niet van bewust hoeveel zij zouden kunnen besparen, omdat ze geen toegang hebben tot het ontwerpen van kennis en benchmarkinformatie.

Leren van andere veiligheidskritieke industrieën

Iets waar de EHEDG onder andere naar op zoek is is om meer bewustwording te kweken en het gebied van het hygiënisch ontwerp te professionaliseren. Technieken die in andere veiligheidskritieke industrieën worden gebruikt, zoals benchmarking, internationale harmonisering van standaarden, open communicatie en documentatie van incidenten en bijna ongelukken, accreditatie, 'Concurrent Design', en veranderingsmanagement zijn in de regel betrekkelijk onderontwikkeld in de voedingsmiddelenindustrie. Bijvoorbeeld, in andere industrietakken zoals de vliegtuigindustrie worden risicomanagementstudies uitgevoerd samen met waarnemers ('second pair of eyes') die als derde partij optreden om al te optimistische risicocijfers te minimaliseren. Dit gebeurt relatief zelden in de voedingsmiddelenindustrie.

Integratiefouten

Van alle vervuilingen hebben bacteriën de mogelijkheid om zich te vermenigvuldigen, te bewegen en te groeien van de ene plaats naar de andere. Ze kunnen ook toxinen produceren met andere overlevingseigenschappen als hun 'ouder'. Dit laat specifieke ontwerpproblemen zien die niet te vinden zijn bij chemische of deeltjesverontreiniging. Bij de integratie van (traditionele en nieuwe) hygiënische systemen gaat het vaak fout. Integratie is een van de belangrijkste uitdagingen die overblijft om ervoor te zorgen dat de voedselproductie veiliger wordt.

Fouten in de keten van ontwerp, contract, ontwerpverandering, bouw en installatie zijn vaak de oorzaak, zelfs wanneer hygiënische richtlijnen beschikbaar en goed bekend zijn. Dat kan gaan om de volgende zaken.

- Het gebeurt vaak dat leidinggevenden de waarde van een hygiënisch ontwerp in voedselproductiesystemen niet zien. Daarom zijn training, projectfasering, benchmarking en validatie ontoereikend. Het kan bijvoorbeeld gebeuren dat hygiënisch ontwerp en HACCP pas na een incident worden ingezet. Ze worden als dure extra's gezien, omdat systemen die het resultaat van zulke pogingen zijn om het systeem met deze 'hygiënische' extra's uit te breiden complex, duur en onbetrouwbaar zijn.
- Bouwers hebben vaak slechte standaarden op het gebied van hygiëne, meestal omdat ze zich niet bewust van de behoefte aan hygiëne zijn. Als resultaat blijven bijvoorbeeld vet, overblijfselen van schuren, schoonmaakdoekjes, lasstaafjes, pennen, kleding, sigarettenpeuken en knopen achter in de apparatuur. Daar kunnen deze voorwerpen onderdelen kapot maken als kleppen, pakkingen, pompen en lagers. De moeilijkste gevallen hebben een vertraagd effect, waardoor de diagnose moeilijker vast te stellen is.
- Hygiënische apparatuur moet zelfdrainerend zijn om het schoonmaken op de werkplek te vereenvoudigen. In complexe fabrieken en machines moet om hiervan verzekerd te zijn gedurende de ontwerp- en assemblagefase een speciaal subproces worden gestart. Veel ontwerpers zijn daarvan niet op de hoogte.
- De interactie tussen omliggende structuren en de machines wordt niet volledig meegenomen tijdens de ontwerpfase. Open machines bijvoorbeeld worden onder lekkende pijpen geplaatst, of verhinderen pilaren de vrije afvoer uit de machines. Dit vereist dat er 3-D-representaties van de apparatuur en zijn omgeving beschikbaar moeten zijn, en dat is nu nog vaak niet zo.
- Wijzigingen en vervangingen vinden plaats tijdens de bouw of de installatie. Degene die deze wijzigingen aanbrengen realiseren zich vaak niet dat ze een belangrijke en gevaarlijke verandering (met het oog op de hygiëne) in het systeem hebben aangebracht. In sommige gevallen kunnen ze zelfs denken dat ze een verbetering hebben gemaakt.

Andere industrieën zoals de farmaceutische industrie hebben de slecht begeleide ontwerpveranderingen aangemerkt als belangrijkste oorzaak van rampen, vandaar hun belangstelling voor veranderingsmanagement. Dit is echter nog niet aanwezig in de voedingsmiddelenindustrie, behalve waar het onderdeel van de HACCP is (waar het weer verloren kan gaan, als er geen speciale controleprocedure is). Het meest voorkomende probleem is het definiëren van een ontwerpverandering ten opzichte van het onderhoud.
Samenvattend kan men zeggen dat gebeurtenissen van gevaarlijke aanpassingen bestaan uit:

- Fouten bij het bouwen vanaf tekeningen (slechte interpretatie).
- Niet in staat zijn om te bouwen vanaf tekeningen (ontoereikend niveau, onzorgvuldigheid, zelfs sabotage).
- Adaptaties veroorzaakt door onverwachte gebeurtenissen (tekortkomingen, onmogelijke taken).
- Hergebruik van vlees- en slachtafval van runderen (BSE).
- Wijzigingen bedoeld om het ontwerp te verbeteren (nieuwe informatie of ideeën).
- Klantgerichte aanpassingen van standaardmachines (inpakmachines).

– Het vinden van de balans tussen bereiding op de plaats en (voor)bereiding in de fabriek is een proces dat in toenemende mate belangrijk is bij hygiënische betrouwbaarheid. Meestal wordt de voedselapparatuur ter plaatse in elkaar gezet. Dat is moeilijker dan wanneer de apparatuur onder standaard- en geoptimaliseerde productiecondities in elkaar wordt gezet.
– Een direct gerelateerde activiteit op het gebied van integratie is de modularisatie en standaardisatie van functionele subunits van productielijnen en fabrieken. Door het niet kunnen identificeren en gebruiken van de mogelijkheden van modularisatie worden de mogelijkheden van deze functionele subunits om te prefabriceren en te standaardiseren niet benut.
Ontwerp-, verificatie- en validatieprocessen worden steeds opnieuw uitgevonden en de resulterende apparatuur is onnodig complex, groot en minder betrouwbaar.
Een goed voorbeeld is de prefabricatie van grote series van ‘doubleseat mix-proof’[3] kleppen. Functionaliteit die normaal een serie van enkele kleppen verbonden door buizen van verschillende lengte en vorm vereist, kan worden bereikt in een enkel nauwkeurig onderzocht en gevalideerd klepsysteem. Dode ruimten en ’hold up volumes’ worden tot een minimum teruggebracht. Fabricatiestandaarden kunnen heel hoog zijn. Ontwerpers kunnen bibliotheken van functionele modulen bijhouden zodat ze niet steeds het wiel opnieuw hoeven uit te vinden.
– Tijdens de vertaling van de tekeningen naar de werkelijkheid zorgt de ruimtelijke indeling van de onderdelen voor gevaren zoals koude punten en stilstaande zones die nadelig zijn voor thermische behandeling en schoonmaken.

3 Afsluiter met een dubbele afdichting om mengen te voorkomen.

– Verplaatsbare machines kunnen verkeerd worden geplaatst op de specifiek aflopende zelfdrainerende vloeren van een voedingsmiddelenfabriek. Hierdoor worden de zelfdrainerende eigenschappen van de machine teniet-gedaan.
– Componenten kunnen buiten hun specificaties worden gebruikt, in het bijzonder bij procesverandering. Rubberpakkingen bijvoorbeeld kunnen vroegtijdig onveilig worden, als procesingrediënten veranderen of als de sterilisatietemperatuur wordt verhoogd. Ironisch genoeg wordt het verhogen van de sterilisatietemperatuur vaak juist gebruikt om een succesvolle sterilisatie te krijgen van slecht ontworpen apparatuur.
– De mensen die verantwoordelijk zijn voor het bedienen en onderhouden van de apparatuur en de kwaliteitsmanagers zijn niet bij het ontwerpproces betrokken. Dit kan als resultaat onbetrouwbare ontwerpen opleveren, omdat de apparatuur niet eenvoudig kan worden bediend en onderhouden. Er is ook minder betrokkenheid bij deze mensen om de machines goed te laten werken omdat ze zich niet verantwoordelijk voelen (zie ook hoofdstuk 29).
– De documentatie over de installatie, de automatisering, de besturing, het onderhoud en de schoonmaak is niet effectief genoeg om op een hygiënische manier te blijven werken.
– De aanwijzingen voor onderhoud, besturing en schoonmaak van apparatuur zijn niet gevalideerd en ineffectief. In sommige gevallen is dit wellicht het geval, omdat er geen gebruiksaanwijzingen zijn of omdat ze in een verkeerde taal en of vorm zijn opgesteld.
– Geen continuïteit in training en kennis is een probleem voor bouwers en gebruikers. Dit kan variëren van het falen om ontwerpaanpassingen en risicoanalyses te documenteren tot het falen om te leren van terugkoppeling na invoering tot het falen in het vasthouden van kennis als personeel weggaat.
– De werking en performance van de apparatuur is niet getest voor deze in bedrijf is gesteld.

Initiatieven uit de industrie

De EHEDG-stuurgroep (www.EHEDG.org) heeft daarom de vorming van een stuurgroep geautoriseerd om praktische aanwijzingen voor de integratie van hygiënische systemen voor de voedingsmiddelenindustrie aan te geven. Integratielessen en -procedures uit andere bedrijfstakken zijn van grote waarde hierbij.

2

28 Outsourcing in ICT

P.J.M. Poos RE RA[1]

Inleiding

ABZ is een dienstverlenende organisatie op het gebied van ICT in de verzekeringsbranche. De kracht van de organisatie is het efficiënt organiseren van bedrijfsprocessen waarbij verschillende partijen zijn betrokken. De dienstverlening vindt in hoofdzaak plaats op twee gebieden:

- Het verkoop- en distributiedeel (e-Commerce). Dit houdt in dat ABZ een rol vervult in de communicatie tussen de (onafhankelijke) assurantie tussenpersoon en de verschillende Nederlandse verzekeraars. Hiervoor is een protocol ontwikkeld dat een efficiënte communicatie mogelijk maakt tussen door de tussenpersonen afgesloten, dan wel geprolongeerde polissen en de verzekeraar die het risico draagt.
- Schadebehandeling (e-Claims). Vooral op het gebied van autoschade (en in mindere mate voor brand- en letselschade) ondersteunt ABZ het gehele bedrijfsproces rond de schadevaststelling, de opdrachtverstrekking, het expertiseproces en de afwikkeling van de schade. De meest relevante partijen in dit kader zijn de (auto)verzekeraars, de schadeherstelbedrijven en de schade-experts. In hoofdlijnen worden de volgende diensten aangeboden:

1 De auteur was tijdens het project werkzaam bij Ernst & Young EDP Audit. Hij is nu hoofd IT Audit bij SNS Reaal Groep N.V.
Daarnaast is de auteur verbonden aan de vakgroep Bestuurlijke Informatie Verzorging aan de universiteit NIVRA te Nyenrode.

- Een door alle relevante marktpartijen geaccepteerd calculatiemodel (vaststelling schadebedrag) dat een eenduidige bepaling van de omvang van de schade mogelijk maakt.
- De noodzakelijke applicaties en 'workflow' om schadegegevens te kunnen registreren en de calculatie te vervaardigen en het proces verder te kunnen ondersteunen.
- Een database met daarin de voor de calculatie van autoschade benodigde gegevens (vooral onderdelenprijzen en hersteltijden van alle in Nederland verkochte automodellen en bouwjaren).
- Een protocol ter ondersteuning van de gegevensuitwisseling in het schadebehandelingsproces.

Voor beide vormen van dienstverlening is een infrastructuur inclusief besloten netwerk gerealiseerd en is bij ABZ een aantal systemen ontwikkeld om het transactieverkeer te beheersen. Ter indicatie: alleen voor de schadesturing worden per jaar circa 1.100.000 gevallen van autoschade verwerkt, wat ruwweg in 4.500.000 transacties resulteert. Bij ABZ werd veel waarde gehecht aan het in stand houden van het besloten netwerk omwille van de efficiency en de veiligheid. Overigens waren zowel de infrastructuur als het netwerk als dienst ingekocht en dus uitbesteed bij een andere, daarin gespecialiseerde organisatie. Deze zorgt voor de 24-uursbewaking van de diensten. Door de opgebouwde kennis had ABZ in beide vormen van dienstverlening een unieke positie verworven.

Wijzigende omstandigheden

Met de introductie en acceptatie van het Internet heeft het in stand houden van een netwerk als onderscheidende factor sterk aan waarde ingeboet. Eind 1998 is ABZ daarom begonnen zich te heroriënteren op een betere definitie van de toegevoegde waarde van hun dienstverlening. De noodzaak hiertoe werd versterkt door het millenniumprobleem. De technische en applicatieve infrastructuur bleek voor een belangrijk deel niet millenniumbestendig te zijn.

De consensuscultuur, noodzakelijk voor het op één lijn krijgen van de betrokken marktpartijen, was ook doorgedrongen in de eigen bedrijfsprocessen. Hoewel zowel met afnemers als met leveranciers afspraken over de kwaliteit van de dienstverlening waren gemaakt, werden onvoldoende consequenties verbonden aan inbreuken op de overeengekomen dienstverlening. Bovendien bleek uit de heroriëntatie dat de tot dan gevolgde uniforme aanpak niet meer mogelijk was. Steeds meer klanten wensen een aan hun specifieke eisen en wensen aangepaste dienstverlening.

Onder druk van het millenniumprobleem is gedurende 1998 en 1999 alle aandacht uitgegaan naar het oplossen van de technische problemen.

Gekozen richting

ABZ heeft inmiddels besloten zich verder op de kernactiviteiten te concentreren en alle activiteiten die daartoe niet behoren uit te besteden. Hiervoor zijn strategische allianties aangegaan met een aantal leveranciers. Overigens dient dit voor de bestaande partners (verzekeraars, tussenpersonen, schadeherstellers en -experts) geheel transparant te zijn. Uitsluitend de volgende activiteiten zullen nog in eigen beheer worden uitgevoerd:

- Dienstontwikkeling en functioneel beheer.
- Onderhandelingen met marktpartijen over de inrichting en ondersteuning van de bedrijfsprocessen.
- Kennismanagement van de acceptatie- en schadeherstelketens.
- Coördinatie van de ketens. Dit houdt in dat ABZ verantwoordelijk blijft voor de betrouwbaarheid van de volledige dienstverlening.

Bij de acceptatieketen zijn de volgende partijen hierbij betrokken:

- De applicaties voor de assurantietussenpersonen worden aan de tussenpersonen door een beperkt aantal softwarehuizen aangeboden. Deze situatie is niet veranderd.
- De Internetservices en de toegang tot het berichtenverkeer zijn uitbesteed. Dit werd in eigen beheer gedaan door middel van een eigen inbelnetwerk in combinatie met huurlijnen. Het toezicht op de huurlijnen was uitbesteed; de afwikkeling van het berichtenverkeer was weer in eigen hand.
- De ontwikkeling van de protocollen voor het berichtenverkeer is onderdeel van het kennismanagement en blijft in eigen beheer.
- De afwikkeling van de aangeboden polissen alsmede de bouw van de daarvoor benodigde software blijft de verantwoordelijkheid van de verzekeraars.
- Eigen applicaties zoals een ‘business’-portaal komen te draaien bij een ASP (Application Service Provider).

In de schadeketen gaat het om de volgende partners:

- Het aanbieden van programmatuur voor het registreren en calculeren van schade wordt uitbesteed aan een ASP die de benodigde applicaties bouwt en via Internet aanbiedt. Het bouwen van de applicatie werd in eigen beheer gedaan. De applicatie werd aan de afzonderlijke gebruikers gedistribueerd en in veel gevallen onder beheer van ABZ door een derde partij geïnstalleerd.
- De Internetservices voor het berichtenverkeer zijn uitbesteed. (Dit is overigens dezelfde provider als voor de acceptatieketen.) Dit werd in eigen

beheer gedaan door middel van huurlijnen. Het toezicht op de huurlijnen was uitbesteed; afwikkeling van het berichtenverkeer was weer in eigen hand.
- De ontwikkeling van de protocollen voor het berichtenverkeer is onderdeel van het kennismanagement en blijft in eigen beheer.
- Het onderhoud van de database is eveneens onderdeel van het kennismanagement en blijft in eigen beheer.
- De verwerking van de schade blijft de verantwoordelijkheid van de verzekeraar.

Organisatorische verankering

Door de gekozen richting wordt ABZ geconfronteerd met complexiteit op verschillende gebieden.
- *Complexe externe en interne afstemmingsproblemen*. Aan de kant van de klant is er een aantal marktpartijen die voor een deel tegenstrijdige belangen hebben en voor een ander deel concurrenten zijn. Afhankelijk van de wensen van de individuele klanten bestaan hierbij verschillen in dienstverlening in het aangeboden technische systeem (met daarin het netwerk, de hardware, de protocollen, de software, de informatie en de kennis). Aan de kant van de leveranciers worden delen van de dienstverlening uitbesteed. Het betreft hier veel meer de 'harde delen' van het technische systeem (hardware, netwerk en software). Het is hierbij de taak van ABZ als integrator en dienstenexploitant in het geheel om de kwaliteit van het aangeboden technische systeem blijvend te garanderen.
- *Snel veranderende omstandigheden*. De situatie is in geen enkel opzicht stabiel. De technische mogelijkheden veranderen bijzonder snel, de klantwensen wijzigen in de tijd en ook andere omgevingsfactoren zijn aan verandering onderhevig. Strategisch gezien zal ABZ zich zodanig moeten positioneren dat zij blijvend een aantrekkelijke partner voor de aangeboden diensten is. Dit houdt in dat een zodanige structuur van het technische systeem en de daarbij behorende organisatie moet worden gekozen dat op een effectieve en efficiënte wijze op veranderingen kan worden ingespeeld. Op tactisch niveau zal het strategische concept moeten worden vertaald naar concrete oplossingen. Dit houdt in dat op dit niveau afspraken over de uitbesteding van de dienstverlening worden gemaakt. Hierbij zullen tevens de randvoorwaarden moeten worden ingevuld om de kwaliteit van de diensten permanent te kunnen bewaken en bijsturen. Dit speelt zowel voor de diensten die ABZ aan haar klanten levert als voor de diensten die derden leveren.

Externe en interne afstemmingsproblemen

Door de gedeeltelijke overgang van uniforme naar specifieke dienstverlening is er in wezen geen sprake meer van één technisch systeem, maar van verschillende technische systemen. Om het beheer hiervan zo eenvoudig mogelijk te houden, is het klantorderontkoppelpunt zo dicht mogelijk bij de klant gekozen. Daarnaast wordt het systeem niet als één geheel beschouwd, maar als een aantal op verschillende manieren te koppelen componenten. Wanneer specifieke klantwensen niet meer kunnen worden gerealiseerd door het samenvoegen van bestaande componenten zal voor deze klant een afzonderlijke component worden ontwikkeld. Dit maakt het ook mogelijk om de kosten van deze ontwikkeling aan de klant toe te rekenen. Organisatorisch gezien worden de verantwoordelijkheden gescheiden in drie 'lagen'.

Business Line Management

Hier ligt de verantwoordelijkheid voor het concretiseren van de afspraken met de klanten. Bij ABZ is hierin een driedeling gemaakt: 'Schadeafhandeling' (voor zowel Mobiliteit-, Zaak- en Personenschade) en 'Verkoop en Distributie' en 'Risico Management'. Business Line Management houdt in dat met klanten de exacte vorm van de dienstverlening, inclusief de kwaliteitseisen wordt afgesproken. Onderdeel van de afspraken is uiteraard ook de vorm en de inhoud van de rapportering over de daadwerkelijk geleverde diensten. Voor de klant (extern gericht) is dit een verantwoording over de dienstverlening. Intern gezien biedt de rapportering de mogelijkheid om over alle componenten van het systeem heen de totale kwaliteit te bewaken. De Business Lines zijn actief in vijf marktsegmenten: Schadeverzekeringen, Levensverzekeringen, Zorgverzekeringen, Hypotheken en Leasing en Financiering.

Service Line Management

Logistiek gezien vormt het scheidsvlak tussen Business Line Management en Service Line Management het klantorderontkoppelpunt. Service Line Management vertaalt het voorstel van de klant naar de intern leverbare producten. Op deze laag wordt ook de beslissing genomen om eventuele nieuwe componenten te ontwikkelen, dan wel bestaande componenten aan te passen. Hiervoor zijn vier afzonderlijke aandachtsgebieden gedefinieerd: 'Data, Informatie en Kennis Management', 'Netwerk en Communicatie Services', 'Standaards, Certificering en Educatie' en 'Cliënt en Netwerk Applicaties'. Ieder van deze aandachtsgebieden is samengesteld uit verschillende componenten. Zo is de eerdergenoemde database met onderdelenprijzen en hersteltijden één component van het Service Line Managementonderdeel 'Data, Informatie en Kennis Management'.

Component Management

Het grootste deel van het operationeel beheer vindt op deze laag plaats. Hier vindt niet alleen de uiteindelijke vormgeving van de componenten plaats, maar worden ook de beslissingen over het beheer van de componenten genomen. Zowel voor de vormgeving als voor het beheer moeten hierbij 'make or buy'-beslissingen worden genomen. Als de component bijvoorbeeld een applicatie is, moet in eerste instantie een beslissing worden genomen over de bouw. Wordt de applicatie in eigen beheer gebouwd, wordt de bouw uitbesteed òf wordt daarvoor een pakketoplossing aangeschaft? Bij deze keus spelen drie overwegingen een belangrijke rol. Verreweg het belangrijkste hierbij is de vraag in hoeverre de component (en de bijbehorende dienstverlening) behoort tot de kerncompetentie van ABZ. Op de tweede plaats komt de vraag of ABZ voldoende kennis in huis heeft (of in huis wil halen) om de ontwikkeling in eigen beheer uit te voeren. Op de derde plaats (en nauw aan de eerste twee vragen gekoppeld) moet de vraag worden beantwoord in hoeverre op de markt een goede oplossing beschikbaar is.

Ook speelt de vraag of het aan de markt aanbieden van de component in eigen beheer gebeurt of dat het beheer van de component wordt uitbesteed. De afwegingen rondom deze beslissing zijn in wezen dezelfde: behoort het tot de kerncompetentie, is de kennis in huis beschikbaar en zijn er goede alternatieven op de markt aanwezig.

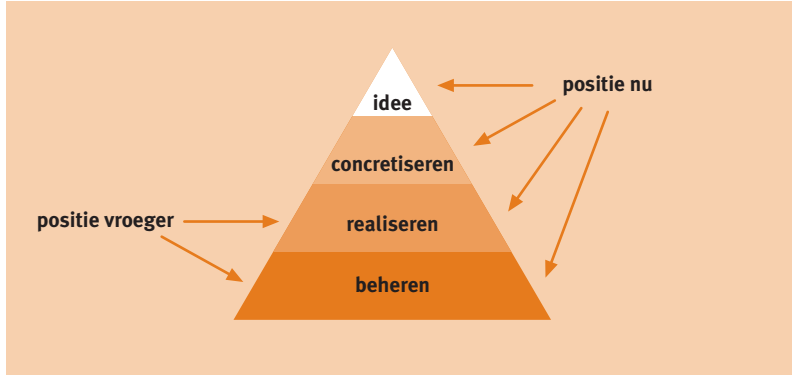
Zo heeft ABZ besloten om de activiteiten voor het bouwen van een applicatie ter ondersteuning van schadeherstellers uit te besteden. Zowel de bouwactiviteit zelf als de ondersteuning van het schadeherstelproces bij het schadeherstelbedrijf wordt niet als kernactiviteit gezien. Hierbij moet overigens wel worden opgemerkt dat het ontwerp van de applicatie (ofwel het inbrengen van kennis rondom het proces) wel in eigen beheer wordt uitgevoerd. Deze applicatie zal door middel van een ASP aan schadeherstellers worden aangeboden. Hiermee is ook de distributie, de opleiding en het onderhoud van de applicatie uitbesteed.

Het beheer van de eerdergenoemde database met onderdelenprijzen en hersteltijden zal niet worden uitbesteed. De kennis die in deze component is opgenomen maakt wèl een belangrijk deel uit van de kerncompetenties van ABZ.

Deze lagenstructuur is direct doorvertaald naar de organisatiestructuur. Het directieteam van ABZ bestaat onder andere uit de volgende functies: de Algemeen directeur, de Directeur Operations (verantwoordelijk voor Service Line Management, projectmanagement en Component Management), de Directeur Marketing en Sales (verantwoordelijk voor onder andere Business Line Management en Accountmanagement), en Finance (hier verder niet behandeld).

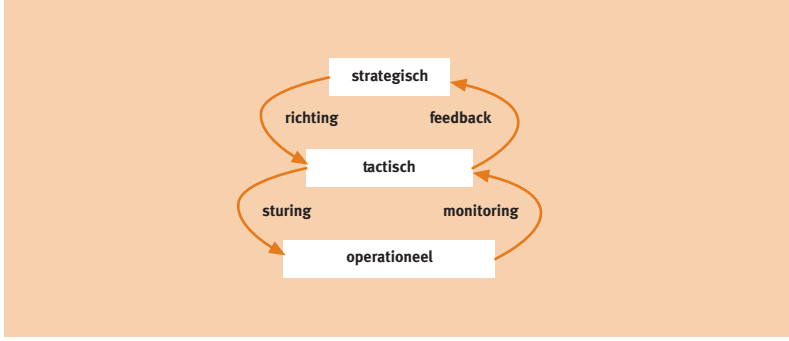
Snel veranderende omstandigheden

Het is niet eenvoudig om een organisatie voor flexibiliteit in te richten (zie figuur 28.1).



Figuur 28.1
Snel veranderende omstandigheden.

Hiervoor is een goede afstemming noodzakelijk tussen de strategische, de tactische en de operationele aansturing. ABZ heeft hierbij gekozen voor een model waarbij op strategisch niveau het beleid wordt bepaald. Het beleid geeft hierbij richting aan de uitwerking van de kortetermijnplannen (tactische aansturing). Deze plannen kunnen de operationele werkzaamheden aansturen. Bij ABZ betreffen deze operationeel plannen zowel bouwactiviteiten van componenten als het beheer van de dienstverlening. Beide soorten activiteiten worden voortdurend bewaakt en bijgestuurd ('monitoring'). De tactische aansturing zorgt voor feedback over eventuele aanpassingen van de strategie bij de realisatie van plannen en het beheer van de dienstverlening (zie figuur 28.2).



Figuur 28.2
Afstemming tussen de verschillende niveaus.

Strategische aansturing

Mede als gevolg van de strategische heroriëntatie heeft ABZ voor een veel meer pro-actieve positie gekozen. Strategisch gezien zal ABZ niet langer reageren op de eisen en wensen van klanten, maar eerder met eigen ideeën komen (latente behoeften) Dit houdt tevens in dat de nadruk van de activiteiten veel meer is komen te liggen op het genereren en concretiseren dan op het realiseren en

beheren ervan. In wezen is dit een verschuiving van de kerncompetenties. Dit verklaart dat ABZ veel meer dan in het verleden bereid is om delen van de dienstverlening uit te besteden.
In deze positionering wordt veel meer vanuit de eigen kracht geredeneerd. Dat betekent dat vanuit de (on)mogelijkheden zoals deze bij het Service Line Management blijken, nieuwe producten en diensten worden ontwikkeld. Het Business Line Management heeft hierbij twee taken. Op de eerste plaats moet worden onderzocht of de klanten van ABZ interesse hebben in de gegenereerde ideeën. Op de tweede plaats moet voeling met de klanten worden onderhouden om eventuele andere eisen en wensen zo snel mogelijk door te spelen. Actief accountmanagement is hierbij belangrijk.

Tactische aansturing

Waar de strategische aansturing vooral is gericht op het genereren van ideeën, is de tactische sturing enerzijds gericht op het concretiseren van de ideeën en anderzijds op het inrichten van het beheer ervan. Dit houdt in dat de make or buy-beslissingen voor een belangrijk deel op dit niveau liggen. Zeker in die gevallen waarbij componenten zijn betrokken die niet tot de kerncompetentie behoren, zal uitbesteding een van de opties zijn.
Beslissingen over de uitbesteding van activiteiten worden door het Component Management genomen. Potentiële leveranciers worden hierbij op een aantal elementen gewogen:

- *Flexibiliteit*. In alle gevallen ligt aan de dienstverlening door de leverancier een Service Level Agreement (SLA) ten grondslag. Hierin is de gewenste dienstverlening beschreven in termen van gewenste en meetbare resultaten. Voor ABZ is echter het belangrijkste beoordelingscriterium de wijze waarop de leverancier reageert op gevallen die niet in het SLA zijn geschreven. Het blijkt in de praktijk niet mogelijk te zijn een zodanig SLA op te stellen dat alle mogelijke scenario's zijn beschreven. De bereidheid om eerder naar de geest dan naar de letter van de overeenkomst te handelen is in een snel veranderende wereld erg belangrijk.
- *Deskundigheid*. Is de leverancier is staat om de gewenste kwaliteit en capaciteit te leveren. Het gaat hierbij niet alleen om het leveren van de juiste mensen, maar veel meer om de bereidheid om creatief mee te denken om de juiste oplossing te realiseren. ABZ levert de ideeën, van een leverancier wordt verwacht dat hij vanuit zijn eigen kerncompetentie weet mee te denken bij het concretiseren van de component.
- *Verhouding tussen prijs en prestatie*. Uiteindelijk zal de component tegen een voldoende concurrerende prijs op de markt moeten worden aangeboden. Dit houdt in dat ook van de leverancier wordt verwacht dat de prijs die hij vraagt voor de ingebrachte flexibiliteit en deskundigheid binnen de heersende marktverhoudingen past.

Operationele aansturing

De operationele aansturing moet ervoor zorgen dat alle mooie strategische en tactische concepten worden geconcretiseerd en gerealiseerd. Aan de klantzijde zal moeten worden bewaakt dat de daar afgesproken serviceniveaus worden gerealiseerd; aan leverancierszijde zal moeten worden vastgesteld dat deze leveren wat is overeengekomen. Uiteindelijk wordt ABZ door haar klanten beoordeeld op basis van de werkelijke dienstverlening. Klanten hebben geen boodschap aan de mededeling dat tekortkomingen in de dienstverlening te wijten zijn aan fouten van een van de leveranciers van ABZ.

De operationele aansturing richt zich daarbij op de volgende elementen:

- *Operationeel beheer*. Voor een belangrijk deel bestaat de dienstverlening van ABZ nog steeds uit het beschikbaar stellen van systemen en databases die via netwerkverbindingen worden aangeboden. Dit houdt in dat de prestaties van de netwerkverbindingen continu zullen moeten worden bewaakt en geregistreerd. Op dit niveau is het zeker voor de klant, maar ook voor ABZ, transparant wie verantwoordelijk is voor het operationeel beheer van de component. Het geheel moet voldoen aan het met de klanten overeengekomen serviceniveau.
- *Incident- en probleemmanagement*. Een belangrijke taak van het operationeel beheer is het tijdig opsporen en afhandelen van incidenten. Dit houdt in dat incidenten snel moeten kunnen worden getraceerd naar de bron en dat ABZ weet wie moet worden aangesproken (zowel intern als extern) over de werking van iedere individuele component. De eigenaar (of beheerder) van deze component is daarmee ook eigenaar van het incident. Ook op dit gebied is het van belang dat eventuele externe beheerders van componenten in staat zijn om creatief mee te denken en minder naar de letter, maar meer naar de geest van de SLA te handelen.
  Het is hierbij de primaire taak van ABZ om de structuur in incidenten op te sporen, zodat onderliggende problemen structureel kunnen worden opgelost.
- *Onderhoud van systemen, databases en infrastructuur*. Aan de hand van probleemanalysen, wensen van klanten, technische ontwikkelingen, wettelijke eisen en tal van andere interne en externe factoren worden de noodzakelijke wijzigingen aan de systemen, databases en infrastructuur gepland. Hierbij zullen waar zinvol nieuwe versies worden nagestreefd om verstoringen in de dienstverlening zoveel mogelijk te vermijden.
- *Ontwikkeling van nieuwe componenten*. Nieuwe componenten moeten worden gebouwd. Ongeacht of dit intern dan wel extern gebeurt, zal voor iedere component een projectplan worden opgesteld. Aan de hand van het projectplan zullen de ontwikkeling en de bouw van de component worden bewaakt.

Voor de operationele aansturing is het vrijwel transparant of delen van de dienstverlening zijn uitbesteed, dan wel in eigen beheer worden uitgevoerd. Uiteraard bestaan er oppervlakkige verschillen in de wijze van aansturing en in de methode van aanpak bij het escaleren van incidenten. Wel moet worden bedacht dat hier een enigszins ideaal beeld wordt geschetst. De werkelijkheid is minder gestructureerd en aanmerkelijk hectischer dan is weergegeven. Bovendien wordt niet ingegaan op de financiële afwikkeling. Van leveranciers wordt verwacht dat zij naar de geest van de SLA handelen. Dat houdt dus ook in dat voor de vergoeding voor deze diensten eerder naar de geest dan naar de letter van de overeenkomst wordt gehandeld.

Conclusie

Wat we kunnen zien is dat wellicht meer dan in het verleden processen over verschillende schakels lopen. In het geval van ABZ is daarbij bewust gekozen voor het uitbesteden van een aantal activiteiten en daarmee schakels toe te voegen. Toch slaagt ABZ erin om de kwaliteit van de dienstverlening aan haar klanten te verhogen. Voor deze schijnbare tegenstelling is een aantal oorzaken aan te wijzen.

Rol als integrator

ABZ blijft zeer nadrukkelijk eindverantwoordelijk voor het totale eindproduct. Zij slaagt hierin, omdat tevens gekozen is voor een rol als integrator. In principe verloopt alle communicatie tussen de beheerders van de verschillende componenten via ABZ. Hiermee is ABZ in staat om de complexiteit van het geheel te beheersen. Omdat een belangrijk deel van het totale systeem is uitbesteed, behoeft ABZ niet de kennis over de complexiteit in de verschillende componenten te hebben (laat staan te beheersen). Dit houdt overigens wel in dat de interfaces tussen de componenten eenduidig moeten zijn beschreven.

Keuze van leveranciers

Het model werkt, omdat ABZ de beheerders en leveranciers van de verschillende componenten zeer zorgvuldig kiest. In een dergelijk concept moeten alle partijen vrijwel blindelings op elkaar kunnen vertrouwen. Het zou teveel inspanning van de operationele aansturing vergen om constant externe partijen te moeten aansturen. Een additionele handicap hierbij is dat de interfaces eenduidig moeten zijn, maar met enige frequentie wijzigen. Dit maakt het belang van een goede leveranciersselectie des te groter.
In een aantal gevallen betreft dit leveranciers die aanmerkelijk groter zijn dan ABZ. Het is hierbij wel van belang dat de leveranciers hun rol accepteren en niet direct met ABZ gaan concurreren.

Eenduidige aansturing

In operationeel beheer wordt in principe geen onderscheid gemaakt tussen interne en externe beheerders. De verschillende componenten worden als het ware als één integraal systeem aangeboden. Elke andere aanpak leidt tot meer complexiteit en minder beheersing van die complexiteit. Relaties met externe partijen worden op strategisch en tactisch niveau uitgewerkt. Op operationeel niveau mag dit verder geen inspanning vergen.

Ten slotte

De beschreven situatie is een momentopname in een snel veranderende omgeving. De informatie voor deze case is voor een belangrijk deel verzameld in het jaar 2000 en geeft dus geen juist beeld van de huidige situatie.

2

29 Nieuw bedrijfsproces bij Unilever Bestfoods Nederland

ing. A.M. van Buren [1]

Achtergrond

Het productiebedrijf van Unilever Bestfoods Nederland aan de Nassaukade in Rotterdam (voorheen Van den Bergh en Jurgens) houdt zich bezig met de productie van margarines en 'spreads'. Het productieproces bestaat in hoofdzaak uit het bereiden van een waterfase en een vet- en of oliefase in een mengafdeling, gevolgd door een emulgeerstap waar water, en vet of olie intensief worden gemengd en gekoeld om een margarine of 'spreadstroom' te verkrijgen die daarna wordt afgevuld in kuipjes, flessen of wikkels. De kuipjes of flessen worden vervolgens gesloten en verpakt in dozen waarna de dozen op pallets worden geplaatst met automatische 'palettisers' (stapelaars). De productie is ingedeeld in lijnen en de fabriek bestaat uit een groot aantal parallelle lijnen. Er werken in totaal circa 200 mensen in de fabriek. Iedere lijn heeft een eigen ploeg die zorgt voor de bediening en het onderhoud.
Het bedrijf is ISO gecertificeerd en heeft gedetailleerde procedures en werkinstructies om de productkwaliteit te borgen.

1 Unilever Research Vlaardingen,
Afdeling Corporate MAST Group
Postbus 114
3130 AC Vlaardingen

De eisen die in dit bedrijf aan de productie worden gesteld, zijn:
- Men streeft naar lage voorraden. Zo ontstaat weinig productbuffer. Men werkt volgens het principe van JIT (Just In Time).
- Er komen steeds meer productvernieuwingen en acties.
- Er is een voortdurende druk om de lijnbezetting (mensuren) te optimaliseren en de kosten te verlagen.
- Er is minder tijd beschikbaar voor onderhoud.

Dit betekent:
- dat er meer productwisselingen en kortere runs nodig zijn. Er is behoefte aan meer flexibiliteit.
- dat de lijnen, het personeel en de bedrijfsprocessen absoluut betrouwbaarder moeten worden.

Om aan deze eisen te voldoen is bij Unilever Bestfoods Nederland Total Productive Maintenance (TPM) geïntroduceerd.
In de volgende paragrafen is beschreven wat TPM in de praktijk voor het bedrijf heeft betekend.

Situatie voor TPM

De fabriek heeft een grote technische dienst (in dag- en ploegendienst) die verantwoordelijk is voor reparatie, onderhoud en smeren. De productie is georganiseerd in 2 afdelingen (een pool van operators, niet lijngebonden) die uitsluitend verantwoordelijk zijn voor de bediening. De productie vindt plaats in een drieploegendienst (3 'shifts'), zodat 24 uur per dag geproduceerd kan worden. De organisatie is hiërarchisch. De productieafdeling kent een managementlaag met een bedrijfsleider en 2 afdelingsleiders. Een laag daaronder staan de ploegchefs, de operators en de monteurs. De technische dienst kent een managementlaag, die bestaat uit een 'Chief Engineer' en 2 afdelingsleiders op het gebied van elektrische installaties en werktuigbouwkunde. Daaronder staan de groepsleiders en de monteurs. De operators en monteurs zijn vrij passief. Alle belangrijke beslissingen worden door leidinggevenden genomen. Wanneer een storing optreedt, belt de operator de technische dienst voor ondersteuning en wacht tot deze dienst de zaak heeft opgelost.
Het management concentreert zich op het terugbrengen van de kosten en een verbetering van de efficiëntie, waarbij zij het initiatief moeten nemen. Waar focus is, worden verbeteringen gehaald, maar de borging is moeilijk. Vaak gaan behaalde verbeteringen weer verloren, onder andere omdat er geen 'ownership' bestaat bij de operators. Verder bestaan er controverses tussen de productie en de technische dienst.

ISO 9001-procedures blijken onvoldoende om verbeteringen in bedrijfsprocessen te borgen. De ISO 9001-borging is vooral een zaak van het management. De operators en de technische dienst worden er niet bij betrokken.
Het blijkt in de praktijk onmogelijk om het bedrijfsrendement structureel te verbeteren. Dit alles heeft geleid tot het plan om de manier waarop de bedrijfsprocessen worden uitgevoerd radicaal te veranderen.

Situatie tijdens TPM

Om als fabriek te overleven is een drastische verhoging van de flexibiliteit en de efficiëntie noodzakelijk. Bij Unilever is in het verleden al ervaring opgedaan met verbeterprocessen, maar meestal hadden deze een ad hoc-karakter, zoals de 'Big Scale Value Analyses' die veel werden toegepast in de jaren tachtig om de efficiëntie te verbeteren en de kosten te reduceren. Het effect hiervan was meestal tijdelijk en de maatregelen hadden geen effect op de cultuur in het bedrijf. Deze keer wordt besloten over te gaan tot een meer drastische maatregel, namelijk de invoering van TPM. Met deze methode zijn elders in Unilever al goede resultaten geboekt.
Voor een algemene beschrijving van TPM wordt verwezen naar de paragraaf over TPM aan het einde van dit hoofdstuk. Hier zijn alleen de praktische maatregelen in en de effecten op de fabriek Van den Bergh en Jurgens kort beschreven.
De fabriek wordt ingedeeld in units met elk 3 vergelijkbare lijnen. De pool van operators vervalt en de operators worden ieder gekoppeld aan een unit. Tevens krijgt iedere unit een technicus die verantwoordelijk voor het onderhoud is.
De gelaagdheid in het management wordt afgeschaft. Er zijn nog maar 2 lagen (leiding en uitvoerenden). De operators worden getraind in elementaire werktuigbouwkunde om eenvoudige reparaties en onderhoudswerkzaamheden zelf te doen of onder begeleiding van de technicus van de unit. De technische dienst ondersteunt de units op het gebied van specialisme, projecten en het onderhoud aan de elektrische installaties.
In december 1997 wordt officieel gestart met TPM. Op een zaterdag wordt door iedereen uit de organisatie (incl. kantoormensen) een start gemaakt met de 'Initial Cleaning' in de gehele fabriek ('kick-off happening').
Het eerste jaar wordt besteed aan training, het weer in de oorspronkelijke staat terugbrengen van apparatuur, leren om verliezen niet te accepteren (een druppel olie is belangrijk als 'lekindicator', niet als vuil). Dit zijn de eerste stappen op weg naar autonoom onderhoud.
De teams aan de lijnen zijn verantwoordelijk voor het goed functioneren en onderhouden van de machines. De teams doen aan teambuilding.
Het eerste jaar is het bedrijfsrendement van de lijnen nog nauwelijks verbeterd. Na ongeveer een jaar begint dit voor het eerst duidelijk structureel te verbete-

Figuur 29.1
Borden bij de lijnen geven de stand van de verliezen aan.

ren. Iedere unit heeft geïnventariseerd waar haar grootste verliezen zitten. Deze verliezen worden aangepakt en zichtbaar gemaakt op borden bij de lijnen (zie figuur 29.1). Doordat verliezen worden geëlimineerd, komt er meer tijd vrij voor andere activiteiten.

Wanneer nu een storing optreedt, neemt de technisch operator het initiatief. In het team kunnen de meeste problemen worden opgelost, alleen voor problemen met de elektrische installaties of het instrumentarium wordt een specialist ingeroepen, maar de technisch operator is eindverantwoordelijke.
In 1999 komt de nadruk steeds meer op verbeteren te liggen. De teams gaan zelf verbeterprocessen starten en dit versnelt het behalen van resultaat. De managementtaken verschuiven naar begeleiden in plaats van leiden. De operators en monteurs nemen meer initiatief en krijgen meer verantwoordelijkheid. Goede prestaties worden extra belicht, records van de lijnen worden gevierd, en ook voor de operators wordt een bedrijfsresultaat- afhankelijke bonus geïntroduceerd.
Ook de veiligheidsaspecten maken deel uit van TPM. Bijna ongelukken (‘near misses’) worden gerapporteerd door de teams en worden met prioriteit opgevolgd.
In 2001 is het bedrijfsrendement met 30% verbeterd ten opzichte van 1995. Ongeplande stops zijn drastisch verminderd, de betrouwbaarheid van de leveringen is hoog, zodat aan de eisen van de huidige ‘Supply Chain’ wordt voldaan (JIT, flexibiliteit, productintroducties).
ISO 9001 speelt een ondergeschikte rol en is alleen nog belangrijk voor sommige aspecten van de formele borging, zoals kwaliteit, calibratie, documentatie.

TPM gaat vooral in verbeteringprocessen veel verder dan ISO 9001.
Het eigendom van de procedures is nu verschoven naar de werkvloer. Wanneer een verbetering wordt doorgevoerd, wordt de betreffende procedure door het verantwoordelijke team aangepast.
De teams maken zelf bedrijfsplannen. Er is een 'georganiseerde autonomie' ontstaan. Operators houden presentaties voor het management. Wanneer de fabriek opgaat voor een klantenaudit of een andere inspectie, voelen de operators zich in dezelfde mate verantwoordelijk als het management. De tegenstelling tussen de technische dienst en de productie vervaagt steeds meer. Het proces van invoering van TPM wordt begeleid door adviseurs van het Japanese Institute of Plant Maintenance.

Samenvatting

rol werknemers	voor invoering TPM	na invoering TPM
operator	bediening	problemen oplossen autonoom onderhoud bediening
monteur	verhelpen van storingen	training van operators specialisme projecten
groepsleider	problemen oplossen, 'brandjes blussen'	begeleiden van teamleden ondernemer
manager	problemen oplossen	begeleiden van teamleden ondernemer

Toekomstvisie

- Het doel is meer perfectie en de opgaande lijn verder voortzetten.
- Men wil 'No Touch-lijnen'[2] ontwikkelen en beginnen met de 'productie met het licht uit'.
- Er komt steeds meer 'Condition Based Maintenance'[3].
- Teams worden echt zelfsturende teams.
- Men wil de werkvloer bij nieuwbouwprojecten ('Early Equipment Management') betrekken.
- TPM zal worden uitgebreid naar de Supply Chain, dat wil zeggen dat leveranciers van apparatuur, grondstoffen en verpakkingsmiddelen aan steeds hogere eisen zullen moeten voldoen. Leveranciers van apparatuur zullen mede verantwoordelijk worden gemaakt voor het behalen van een bepaald bedrijfsrendement. Verder zullen ze worden opgenomen in verbeterteams.

2 productielijn waar tussen geplande stops geen menselijke handelingen nodig zijn.

3 regelmatige meting van parameters die verband hebben met de conditie van de machine (bijv. vibratie, temperatuur, dikte, enz.). Door 'trending' van de meetgegevens is het mogelijk te voorspellen, wanneer de machine zal falen. Dit betekent dat onderhoud of vervanging gepland kan worden in de productieschema's, waardoor falen en ongeplande stops worden voorkomen.

– Het niveau van de medewerkers in het bedrijf moet en gaat steeds verder omhoog. Er is een trend dat het vereiste opleidingsniveau van operators naar MTS en HTS zal gaan.

Figuur 29.2
Mensen maken het verschil bij Unilever Bestfoods Nederland.

Algemene informatie TPM

Definitie

– TPM herstructureert de bedrijfscultuur door verbetering van het personeel en de productieapparatuur.
– TPM creëert een systeem om verliezen aan de lijn te voorkomen en is gericht op het eindproduct. Dit is inclusief systemen om 'zero accidents', 'zero defects' and 'zero failures' te realiseren tijdens de gehele levenscyclus van het productiesysteem.
– TPM wordt toegepast op alle onderdelen, inclusief productie, ontwikkeling en administratie.
– TPM is gebaseerd op de deelname van alle werknemers van het topmanagement tot aan de lijnwerknemers.
– TPM bereikt 'zero losses' door het overlappen van activiteiten van kleine groepen.

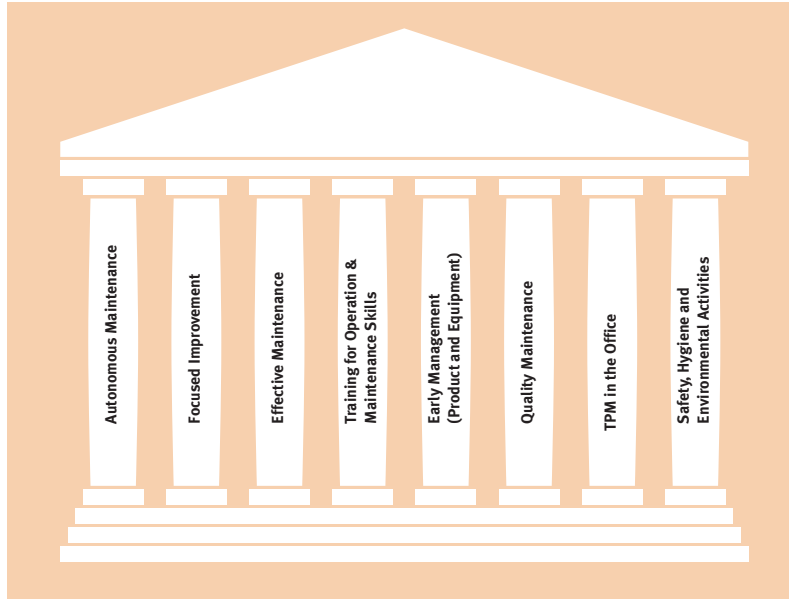
Doel TPM

Het uiteindelijke doel van TPM is een 'zero loss'-werkomgeving te creëren. Om dit te bereiken moeten de verschillende categorieën van verliezen worden geïdentificeerd. De volgende 6 verliescategorieën kunnen worden onderscheiden:

– Apparatuurstoring: verliezen door stilvallen van de lijn of afname van de lijnfunctionaliteit.
– Lijninstelling en of bijstelling: tijdverlies tussen het beëindigen van de originele productie en het op gang brengen van productie na een productverandering.
– Start: verliezen door starten na periodieke stops (na bijv. reparatie, vakantie).
– Kleine stops: verliezen van minder dan 10 minuten (zonder reparatie of vervangen van onderdelen).
– Snelheid: verliezen door een verschil tussen werkelijke snelheid en ontwerpsnelheid.
– Product defect/'rework': productieverlies ten gevolge van productdefect en de noodzaak tot 'rework' (herverwerken van een afgekeurd product).

5S als voorbereiding op TPM

Het is sterk aan te bevelen om eerst een goede werkomgeving te creëren, voordat men met TPM kan beginnen. De introductie van 5S is een goede oefening in teamwerk en teambuilding en wordt gezien als een onderdeel van het programma om zich op TPM voor te bereiden.
De 5S zijn in chronologische volgorde:
– 'Sort' (verwijderen van alle onnodige zaken van de werkvloer).
– 'Set locations and limits' (berg spullen als gereedschap, reserveonderdelen enz. op vaste, gemakkelijk te bereiken plaatsen op).
– 'Shine' and 'Sweep' (schoonmaken).
– 'Standardise' (introduceren van vaste procedures).
– 'Sustain' (vasthouden van het resultaat).



Figuur 29.3
De 8 TPM-pilaren.

De TPM-pilaren

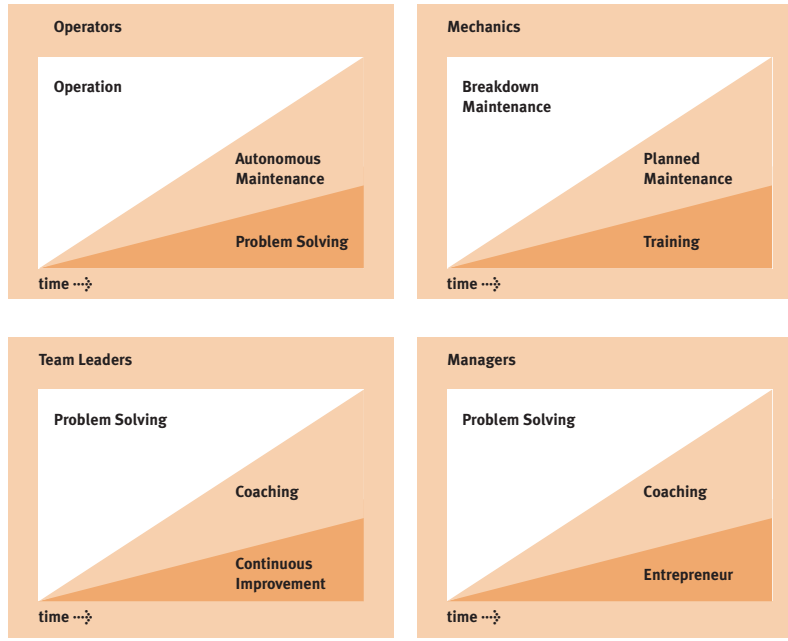
TPM is gebouwd op 8 fundamentele voorwaarden. Dit zijn de 8 TPM-pilaren (zie figuur 29.3). Deze pilaren zijn essentieel voor het succes van TPM.

'Autonomous Maintenance' is 'individually preserving one's own equipment'. Dit betekent dat vanaf de start van TPM de operator zelf verantwoordelijk is voor het normale dagelijkse onderhoud van zijn machines. Zo kunnen de 6 grote verliezen worden voorkomen.
'Focused Improvement' is 'all activities for enhancing production efficiency'. Dit betekent dat alle werknemers continu naar verbetering zoeken en deze verbeteringen proberen in te voeren. Deze methode heet 'focused', omdat het op een bepaald type verlies is gericht. Het is verbetering, omdat het verder gaat dan onderhoud gericht op de basiswerkcondities. Het heeft ook tot doel deze basiscondities en de machineprestatie te verbeteren. Waar Autonomous Maintenance dagelijks uitgevoerd wordt door productiemedewerkers, is Focused Improvement een periodieke teamactiviteit die wordt uitgevoerd door een multidisciplinair team (bediening, onderhoud, ingenieurs, specialisten).
'Planned or Effective Maintenance' is gepland onderhoud door gespecialiseerd onderhoudspersoneel dat kan worden gecombineerd met autonoom onderhoud (Autonomous Maintenance) door operators om verliezen te elimineren en de efficiëntie te verhogen. Vanaf dit moment zijn de taken van het onderhoudspersoneel tweeledig: eerst moeten ze de operators trainen in het autonome onderhoud en daarna het geplande onderhoud. TPM vraagt een grote betrokkenheid en meer kennis van onderhoud van de operator. Daarom is een goed trainingsprogramma nodig (pilaartraining).
'Early Management' richt zich op het ontwerp van het product en de apparatuur en moet ook rekening houden met de geschiktheid van dat ontwerp voor een effectieve en efficiënte manier van produceren (operators en onderhoudsmensen doen mee bij het ontwerp).
'Quality Maintenance' legt de nadruk op de noodzaak van het creëren van een nul-fouten (zero defects)-omgeving. Werknemers stellen continu hun werkprocedures ter discussie en proberen deze te onderhouden. Zoals al eerder vermeld, zoekt TPM naar zero accidents. Om zo'n omgeving te creëren, besteedt men aandacht aan veiligheid, hygiëne en milieuactiviteiten.
'*TPM in the Office'* is bedoeld om de principes van 'zero losses' ook toe te passen buiten de directe productieomgeving.

Veranderende rollen

De invoering van TPM vraagt een andere instelling van de werknemer, zowel op het hoge als op het lage niveau. Natuurlijk moet deze verandering van instelling worden gevolgd door een verandering van rollen. TPM vraagt van zowel de operators, technici, groepsleiders als managers om betrokken te raken bij verschil-

Figuur 29.4
Veranderende rollen door TPM.



lende soorten van activiteiten buiten de normale taken. Dit wordt geïllustreerd in figuur 29.4.

Voor de introductie van TPM was het bedienen van de lijn de taak van de operator. Voor het onderhoud en het oplossen van problemen waren andere mensen verantwoordelijk. TPM vraagt hier om een verandering. Buiten het bedienen van de lijn wordt de operator ook verantwoordelijk voor autonoom onderhoud en het oplossen van problemen aan de lijn. Vergelijkbare veranderingen vinden plaats in de functies van onderhoudstechnici, groepsleiders en managers. De onderhoudstechnicus was in het verleden voornamelijk betrokken bij reparaties van uitgevallen lijnen. Er was bijna geen tijd voor gepland onderhoud. Door het opzetten van kleine teams van operators, onderhoudstechnici (werktuigbouwkundigen en elektrotechnici) met een gezamenlijk doel kan men zich nu bezighouden met het verbeteren van de lijnprestaties. De rol van de onderhoudstechnicus bijvoorbeeld is met TPM veranderd, omdat hij nu ook de operators traint. Daardoor zijn zij in staat autonoom onderhoud te plegen. Zowel de groepsleiders als de managers brachten hun tijd door met het oplossen van problemen van het team of de afdeling waarvoor zij verantwoordelijk waren. Door TPM krijgen zij meer de rol van coach en ondernemer.

De organisatie van TPM

Een kritieke succesfactor bij de invoering van TPM is de manier waarop het georganiseerd wordt. Het moet een omgeving creëren die stimulerend is voor alle werknemers die betrokken zijn bij het werken volgens de principes van TPM.

Een belangrijk middel om de werknemers te motiveren is het werken in kleine groepen. Elke groep heeft een (in)formele leider die een belangrijke rol heeft bij het motiveren van de groep. Om de werkomgeving van de groep te stimuleren, zou het volgende moeten gebeuren:

- Werknemers moeten het belang van hun eigen en andermans werk kennen.
- Er moeten duidelijke doelen zijn, die bij iedereen bekend moeten zijn. Deze doelen moeten in eerste instantie relatief laag zijn gesteld om ontmoediging te voorkomen, wanneer het doel niet wordt bereikt. Deze doelen moeten het liefst door de groep zijn opgesteld.
- Suggesties van de werknemers en of de groep moeten serieus worden behandeld.
- De inzet van de werknemers moet worden beloond.

TPM denkt in groepen in plaats van in individuen, omdat groepen bepaalde voordelen hebben:

- Een groep kan problemen beter identificeren.
- Het werken in groepen stimuleert de creativiteit en de mogelijkheid om te vernieuwen.
- De betrokkenheid van de leden helpt om groepsbeslissingen uit te voeren.
- Een groep kan worden gebruikt als middel om te controleren en om discipline op individuen over te brengen.
- Werken in groepen voorkomt de negatieve gevolgen van grote organisaties, zoals slechte communicatie, hiërarchie en anonimiteit.

De organisatie van het invoeren van TPM bestaat uit groepen die elkaar overlappen. Om een goede communicatie en motivatie te stimuleren maakt de groepsleider van elke groep deel uit van een groep op een hoger niveau.

Een succesvolle introductie van TPM vereist:

- ‘Commitment’ van het topmanagement.
- Zichtbare opname van TPM in de bedrijfsorganisatie.
- Het beschikbaar zijn van meetgegevens over verliezen en efficiency.
- Een goed opgeleide TPM-manager.
- Begeleiding van een professionele adviseur.
- Het doen van pilotactiviteiten.
- Een langetermijnvisie: totale introductie duurt een aantal jaren.

2

30 Veiligheid in de nieuwe spoorwegwet

mr.ir. M.J.P. van der Meulen [1]

Inleiding

Veiligheid is duur. Vooral in een commerciële omgeving kan veiligheid daarom het onderspit delven: het voorkomen van ongevallen is soms duurder dan het betalen van de schade.

Om ervoor te zorgen dat de veiligheid in een commerciële omgeving zoals tegenwoordig het spoorwegverkeer toch voldoende aandacht krijgt, is meer nodig. Een van de mogelijke instrumenten is wetgeving. Wetgeving zorgt ervoor dat alle partijen dezelfde randvoorwaarden voor veiligheid krijgen, zodat ze niet bang hoeven te zijn dat anderen – door minder aan veiligheid te doen – goedkoper zijn. Een nadeel van wetgeving kan wel zijn dat commerciële exploitatie onmogelijk wordt. Deze afweging is per definitie politiek van aard.

Deze case beschrijft hoe de Nederlandse overheid de veiligheid in het voorstel voor de nieuwe Spoorwegwet waarborgt [Spoorwegwet, 2000]. Duidelijk zal worden welke problemen er zijn, welke overwegingen een rol spelen bij de oplossing ervan, en welke keuzen uiteindelijk zijn gemaakt.

1 Simtech
Max Euwelaan 60
3062 MA Rotterdam

Veiligheid in het spoorwegverkeer

Spoorwegwet 1875 en andere regelgeving

De Spoorwegwet 1875 bevat geen bepaling die de veiligheid van de reiziger garandeert. Wel staat de verantwoordelijkheid van de spoorwegonderneming voor de schade door personen of goederen geleden voorop (artikel 1). Ook geeft de wetgever regels waaraan het vervoerssysteem in verband met de veiligheid moet voldoen, zoals artikel 37 'Binnen de afstand van zes meter van een spoorweg geschiedt generlei afgraving.' De minister van Verkeer en Waterstaat kan bestuursdwang toepassen om deze gedragingen af te dwingen (artikel 41).

Speciaal in verband met de HSL (Hogesnelheidslijn) is de Spoorwegwet 1875 op 1 april 1999 gewijzigd. Het nieuwe hoofdstuk IIIA, 'Het Trans-Europese hogesnelheidsspoorwegsysteem', verwoordt de bepalingen in richtlijn 96/48/EG over interoperabiliteit: het mogelijk maken dat treinen in verschillende landen kunnen rijden (zie onder kopje Europese Unie).

Onder de Spoorwegwet 1875 hangt veel regelgeving, en vaak is daarin iets te vinden over veiligheid, bijvoorbeeld de 'Lokaalspoor- en Tramwegwet 1900' en het 'Reglement Dienst Hoofd- en Lokaalspoorwegen 1977'. Verder zijn in het Burgerlijk wetboek, het wetboek van Strafrecht, de wet Personenvervoer en het Besluit Personenvervoer bepalingen over veiligheid te vinden.

Organisatie

De Spoorwegwet 1875 gaat uit van de spoorwegonderneming als één entiteit. Dit is niet meer van deze tijd. We hebben nu te maken met bijvoorbeeld Railinfrabeheer (de beheerder van de infrastructuur), vervoerders van reizigers (NS Reizigers, tot voor kort Lovers, en museumspoorlijnen), vrachtvervoerders (zoals Railion en ATCS), Verkeersleiding, Railned-Capaciteitstoewijzing, Railned-Spoorwegveiligheid.

De relaties tussen de partijen zijn op dit moment voornamelijk privaatrechtelijk van aard. De overheid heeft met enkele partijen contracten op basis waarvan zij hun taken vastlegt en hen financiert. Dit geldt ook voor die partijen die een taak hebben die publiekrechtelijke kenmerken heeft, zoals het garanderen van veiligheid, het verdelen van capaciteit, en de verkeersleiding.

Internationaal verkeer

De spoorwegen zijn bij uitstek een nationale aangelegenheid. Elk land heeft zijn eigen beveiliging, systeem voor stroomafname, procedures, enz. Op dit moment is het niet mogelijk zonder speciale maatregelen met een trein van het ene land naar het andere te rijden. In de loop der tijd zijn er tal van constructies

ontstaan die internationaal verkeer toch mogelijk maken. Nederland doet dit op verschillende manieren. In de eerste plaats via verdragen:

- Het COTIF, het 'Verdrag over Internationaal Vervoer van Treinreizigers en Bagage' van 1980.
- De 'Technische Eenheid der Spoorwegen', over voertuigen en spoorwegen voor het internationale verkeer.
- Verdragen voor grensoverschrijdend verkeer, bijvoorbeeld voor Emmerich-Arnhem, Kaldenkirchen-Venlo, Roosendaal-Essen.

Verder werken de spoorwegmaatschappijen samen in het UIC, de 'Union des Chemins de fer'. De UIC legt bestaande inzichten vast in zogenaamde fiches. Wanneer de spoorwegmaatschappijen zich houden aan deze fiches, leidt dit ook tot een zekere mate van standaardisatie. Elk van deze verdragen gaat in op veiligheid.

Nieuwe ontwikkelingen

De volgende ontwikkelingen maken dat de Spoorwegwet 1875 niet meer voldoet aan de eisen van dit moment.

De Europese Unie

De Europese Unie maakt zich zorgen over het spoorwegverkeer in het algemeen. De grote verschillen in systemen zijn een blokkade voor concurrentie, en een van de doelstellingen is het bevorderen van de onderlinge koppeling en interoperabiliteit van de nationale netwerken, alsmede van de toegang tot deze netwerken (artikel 129B van het EG-verdrag).
Op organisatorisch niveau is richtlijn 91/440/EG van groot belang. Deze regelt de scheiding tussen infrastructuurbeheerders en vervoersmaatschappijen. Deze scheiding is niet terug te vinden in de Spoorwegwet 1875, maar heeft in Nederland feitelijk wel plaatsgevonden.

Op technisch niveau is de richtlijn 96/48/EG 'Richtlijn interoperabiliteit HSL' van belang. De 'Association Européenne pour l'Interoperabilité Ferroviaire' (AEIF) maakt op basis van deze richtlijn normen voor interoperabiliteit van hogesnelheidsspoorwegen, de zogenaamde TSI's (Technical Specifications for Interoperability). Deze bevatten de essentiële eisen waaraan de systemen in de HSL moeten voldoen. Het is een EU-land niet toegestaan meer te verlangen van een buitenlandse trein. Tevens moet men treinen die aan deze eisen voldoen toelaten op het eigen spoorwegnet.

De volgende slag in het internationale speelveld slaat de EU met een richtlijn voor de interoperabiliteit van het conventionele Trans-Europese spoorwegsysteem (nu in de laatste fase van voorbereiding) met een regeling die vergelijkbaar is met die in richtlijn 96/48/EG.

De TSI's zullen vanzelfsprekend ook veel voorschriften bevatten die direct of indirect met veiligheid te maken hebben.

Organisatie

Zoals al eerder is aangegeven, is de organisatie van de spoorwegen in Nederland anders dan in de Spoorwegwet 1875 staat beschreven. De nieuwe spoorwegwet zal in ieder geval recht moeten doen aan de feitelijke situatie met in het achterhoofd de regelgeving van de EU.

Benadering van veiligheid

De Spoorwegwet 1875 en de onderliggende regelgeving schrijven vaak oplossingen voor die de veiligheid moeten verbeteren. Deze aanpak heeft een aantal nadelen. Ten eerste is het vaak zo dat veiligheid op verschillende manieren bereikt kan worden. Zo kan de integriteit van de spoorweg worden gegarandeerd door betere materialen, of door vaker schouwen. Het is niet aan de wetgever dergelijke keuzen te maken.

Ten tweede is vaak onduidelijk aan wie een voorschrift is gericht. Het voorkomen van een ontsporing is een taak van zowel de vervoerder, de infrastructuurbeheerder, als de verkeersleiding. Het is erg complex om door middel van regelgeving hierop in te spelen. Hier speelt de opdeling van de NS in een groot aantal organisaties een sterk complicerende rol.

Trends in het kort

- Internationalisering van het spoorwegverkeer en internationale eisen (ook met betrekking tot veiligheid) maken de autonomie van Nederland kleiner.
- Meer complexiteit door het uiteenvallen van de Nederlandse Spoorwegen in tal van organisaties met een eigen rol stelt andere eisen aan het formuleren van veiligheidseisen.
- De commercialisering zet de veiligheid onder druk. Veiligheid in het spoorwegverkeer is erg duur. De vraag is hoe men de veiligheid in het spoorwegverkeer kan garanderen zonder dat de kosten economisch optimaal gebruik onmogelijk maken.

Het voorstel voor de nieuwe spoorwegwet

Organisatie

Het voorstel voor de nieuwe spoorwegwet gaat uit van één zelfstandig bestuursorgaan (ZBO) dat de publiekrechtelijke taken zal uitvoeren. In een overgangsperiode tot 1 januari 2005 zal deze ZBO bestaan uit Railinfrabeheer, Railned en Verkeersleiding. Dit ZBO moet de voorwaarden scheppen voor een spoorwegnet, waarop vervoerders in concurrentie kunnen opereren.
Duidelijk moet zijn dat het ZBO een groot scala aan activiteiten kent:

- Het beheren van de infrastructuur.
- Het bewaken van de veiligheid.
- Het verdelen van capaciteit.
- Verkeersleiding.

Deze taken kunnen soms conflicteren. Bij het in gebruik stellen van infrastructuur bijvoorbeeld vindt een controle plaats op veiligheidsaspecten. Ook de taak van de verkeersleiding heeft geregeld gevolgen voor de veiligheid, zoals het geven van toestemming om door een 'rood sein' te rijden. Het feit dat het bewaken van de veiligheid de taak van dezelfde organisatie is, brengt het gevaar van belangenverstrengeling met zich mee.

Figuur 30.1
Verkeersleiding, infrastructuur en de Thalys. Bron: Quintus Vosman.

Het garanderen van veiligheid

Het garanderen van veiligheid binnen dit kader van een groot aantal partijen is complex. Dit gebeurt in het voorstel voor de nieuwe spoorwegwet op de volgende manier.

Voor de *vervoerders* worden de procedures die feitelijk al werden toegepast door Railned-Spoorwegveiligheid in de wet vastgelegd. Dit houdt in:

- De vervoerder moet een bedrijfsvergunning hebben. Om hiervoor in aanmerking te komen dient de vervoerder te beschikken over een goede naam, voldoende financiële draagkracht, beroepsbekwaamheid en een verzekering. Het ZBO verleent op aanvraag de bedrijfsvergunning.
- De vervoerder moet een veiligheidsattest bezitten. Om dit te verwerven dient de vervoerder aan te tonen dat hij in staat is veilig gebruik te maken van de spoorweg, onder andere door te beschikken over een veiligheidszorgsysteem. Het ZBO verleent op aanvraag het veiligheidsattest.
- Het voor gebruik bestemde materieel moet aan de eisen voldoen. Gebruik is mogelijk, nadat onder andere de veiligheid van de spoorvoertuigen is getoetst. Het ZBO laat op aanvraag een spoorvoertuig toe tot het verkeer.
- Personen die een veiligheidsfunctie uitoefenen dienen aan bepaalde eisen te voldoen, en dienen een verklaring van hun bevoegdheid bij zich te dragen. Degene onder wiens gezag de veiligheidsfunctie wordt uitgeoefend geeft deze verklaring uit.
- De vervoerder dient capaciteit aan te vragen bij het ZBO. Bij het toekennen ervan wordt onder andere gelet op de veiligheid in relatie tot de toe te kennen capaciteit.

Het ZBO toetst de vervoerder dus op tal van manieren op veiligheid. Hoewel de wetgeving op dit punt sterk is uitgebreid, wordt vooral de bestaande praktijk vastgelegd.

Tussen het ZBO en de overheid bestaat een vrij directe band, onder andere door de financieringsrelatie. Bovendien bestaat het vertrouwen dat het ZBO competent is en vertrouwd kan worden. Om deze reden gelden hier tal van voorwaarden niet, die voor vervoerders wel gelden zoals eisen aan de kredietwaardigheid en het aantonen van beroepsbekwaamheid.

Het meest vergelijkbaar met de positie van de vervoerder is die van de *infrastructuurbeheerder*. Het zou mogelijk zijn deze partij op dezelfde manier te behandelen, dus met een bedrijfsvergunning, een veiligheidsattest, en het 'toelaten' van infrastructuur. Vanwege de nauwe relatie met het ZBO vindt de overheid dit niet noodzakelijk. Uitgangspunt is de competentie van de infrastructuurbeheerder. Wel dient deze 'de risico's van het gebruik en beheer voor de veiligheid van hoofdspoorwegen' te analyseren, en 'passende' maatregelen te nemen om deze risico's afdoende te beheersen' (artikel 16 lid 3, voorstel nieuwe spoorwegwet). Dit komt neer op het afleggen van verantwoording over de veiligheid van de infrastructuur.

De wet stelt beveiliging en Automatische Treinbeïnvloeding boven 40 km per uur verplicht (artikel 7 lid 1, voorstel nieuwe spoorwegwet). Deze maatregelen zijn economisch gezien niet altijd te onderbouwen, omdat de noodzakelijke investeringen hoger kunnen zijn dan de verwachte kosten van ongevallen. In een commerciële omgeving zouden ze dus achterwege kunnen blijven. De Nederlandse overheid wil voorkomen dat bedrijven deze afweging maken en stelt de veiligheidsmaatregelen daarom verplicht.

Voor de taken van het ZBO als bewaker van de veiligheid – bijvoorbeeld het afgeven van het veiligheidsattest, het toelaten van materieel – gelden wel voorschriften, maar deze dienen vooral de rechtszekerheid van de vervoerders. Ze leggen geen veiligheidsvoorschriften op aan het ZBO.

Hetzelfde geldt voor de taak van de *verkeersleiding*. Bij deze taak is het afleggen van verantwoording, vergelijkbaar met die van de infrastructuurbeheerder zeker denkbaar, maar ook daarvan is afgezien.

De taak van het ZBO omvat voorts 'het zorgdragen voor samenhang in de toepassing van veiligheidsvoorschriften en het bevorderen van een samenhangend en doelmatig optreden van diensten, instellingen en bedrijven, in het bijzonder op het terrein van de veiligheid van het spoorwegverkeer' (artikel 73, lid 2a, voorstel nieuwe spoorwegwet).

Conclusie

Het voorstel voor de nieuwe spoorwegwet bevat een raamwerk waarbinnen veilig spoorwegverkeer mogelijk is. De wet sluit beter aan bij de bestaande praktijk die in de loop der tijd wel erg was gaan verschillen van de uitgangspunten van de Spoorwegwet 1875. De wet verwerkt de richtlijnen van de EU over de organisatie en de interoperabiliteit van het internationale spoorwegverkeer.

Het voorstel voor de nieuwe spoorwegwet besteedt uitgebreid aandacht aan de veiligheid. Hij sluit daarbij zoveel mogelijk aan bij de ontwikkelde praktijk. Nieuw zijn de risicoanalyse voor de infrastructuur en de uitbreiding van de taak van het ZBO tot een overkoepelende waakhond voor de veiligheidsaspecten van het spoorwegverkeer.

Toekomstverwachting

Op het moment van schrijven van deze bijdrage zijn er heftige discussies aan de gang over het voorstel van de nieuwe spoorwegwet. Dit was te verwachten. Het is een onderwerp waarover iedereen wel een mening heeft en dat politiek gevoelig ligt. Voorgaande pogingen om de spoorwegwet te vernieuwen zijn om deze reden alle misgelopen. De richtlijnen van de nieuwe wet zijn duidelijk en Nederland dient daaraan op korte termijn te voldoen.

De benadering met betrekking tot veiligheid zoals deze hiervoor is beschreven, ligt bij deze discussies nauwelijks onder vuur. De organisatiestructuur des te meer, en dit kan gevolgen voor de veiligheid hebben. Wordt Railned-Spoorwegveiligheid nu onderdeel van de overheid, wordt het geheel zelfstandig, of wordt het samengevoegd met Railinfrabeheer? Hoe groot wordt de afstand van Railinfrabeheer tot de overheid? Komt Verkeersleiding nu bij Railinfrabeheer of bij NS-Reizigers?

In de nabije toekomst zal duidelijk worden welke antwoorden de politiek op deze vragen geeft.

Referenties

- Spoorwegwet, 1875. Wet van 9 april 1875 tot regeling van de dienst en het gebruik der spoorwegen, en zulks met intrekking der wet van 21 augustus 1859 (Spoorwegwet). Stb. 1875:67
- Lokaalspoor- en Tramwegwet, 1900. Wet van 9 juli 1900, houdende nadere regeling van den dienst en het gebruik van spoorwegen waarop uitsluitend met beperkte snelheid wordt vervoerd. Stb. 1900:118
- Technische Eenheid, 1948. Koninklijk Besluit van 17 november 1948 tot bekendmaking van de gewijzigde tekst der voorschriften getiteld: Technische Eenheid der Spoorwegen. Stb. I 503
- RDHL, 1977. Besluit van 25 januari 1977, houdende vaststelling van een algemeen reglement voor de dienst op de hoofd- en lokaalspoorwegen. Stb. 1977:152
- COTIF, 1980. Organisation des Transports Internationaux Ferroviaires. Verdrag betreffende het internationale spoorwegvervoer, met Protocol en Bijlagen. 9 mei 1980. Trb. 1980:160
- Richtlijn 91/440/EG van de Raad van de Europese Gemeenschappen van 29 juli 1991 betreffende de ontwikkeling van de spoorwegen in de Gemeenschap. PbEG, L237

– Richtlijn 96/48/EG van de Raad van de Europese Unie van 23 juli 1996 betreffende interoperabiliteit van het transeuropees hoge-snelheidsspoorwegsysteem. PbEG, L235
– Aanpassing van de Spoorwegwet in verband met de uitvoering van richtlijn nr. 96/48/EG van de Raad van de Europese Unie van 23 juli 1996 betreffende de interoperabiliteit van het transeuropees hoge-snelheidsspoorwegsysteem (PrEG L 235). Handelingen II 1998/1999, 26351. nrs. 1-2, A
– Voorstel Nieuwe Spoorwegwet, 2000. Nieuwe algemene regels over de aanleg, het beheer, de toegankelijkheid en het gebruik van spoorwegen alsmede over het verkeer over spoorwegen (Spoorwegwet). Tweede Kamer. vergaderjaar 2000-2001, 27482, nrs. 1-2

2

31
Rol cryptografie in de geldautomaatomgeving

ir. G.J.P.M. Wackers [1], *mr. W.H.M. Hafkamp* [2], *G.J. Vergouw* [3]

Inleiding

Dagelijks gebruiken gemiddeld 500.000 mensen in Nederland de ruim 2.700 beschikbare geldautomaten van de Rabobank: pinpasje erin, pincode intikken, het geldbedrag of de saldo-informatie kiezen en dertig seconden later is men voorzien van contant geld of op de hoogte van het saldo. Weinig mensen weten echter hoe complex de omgeving is die schuilgaat achter deze ogenschijnlijk eenvoudige acties.

Het mag duidelijk zijn dat betrouwbaarheid zeer belangrijk is in een geldautomaatomgeving. Net als bij veel andere systemen wordt deze betrouwbaarheid bereikt door een consistent geheel aan maatregelen die zowel technisch, procedureel als organisatorisch zijn. Echter, technische maatregelen kunnen bijdragen aan het uitsluiten van de 'menselijke factor' in een specifieke omgeving: een erg wenselijke eigenschap bij bancaire transacties. Vandaar de belangrijke rol die technische maatregelen spelen bij het waarborgen van de betrouwbaarheid van een geldautomaatomgeving. Er zijn diverse technische maatregelen, waarin cryptografie een prominente rol speelt.

1 Ernst & Young, afdeling EDP Audit
Postbus 100
6200 AC Maastricht

2 Rabobank Nederland, Informatisering Betalingsverkeer
Postbus 17100
3500 HG Utrecht

3 Rabobank ICT, Architectuur
Postbus 17100
3500 HG Utrecht

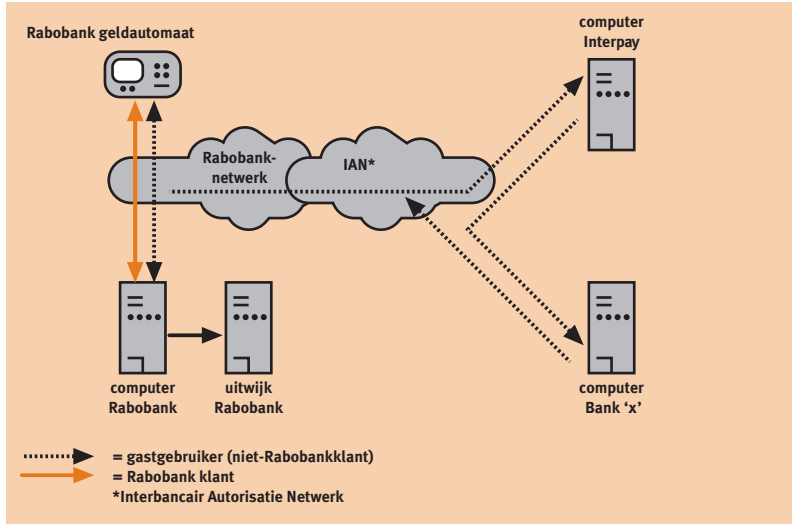
Schets geldautomaatomgeving

De gebruiker ziet alleen maar een scherm, een stevig uitziend toetsenbord met een cijferblok en vier controletoetsen, een gleuf voor de pinpas en een gleuf waaruit de bankbiljetten komen. Het geheel is verankerd in een betonnen muur. Aan de achterkant ziet de geldautomaat er een stuk indrukwekkender uit: het geheel is een machine van ongeveer twee kubieke meter, waarin een stevige kluis is gebouwd naast een grote hoeveelheid elektronica. In de kluis worden de bankbiljetten bewaard. Deze worden er automatisch uit gehaald ter verstrekking aan de klant. De kluis wordt regelmatig bijgevuld en er kunnen verschillende tientallen duizenden guldens in opgeslagen liggen. Boven de kluis bevindt zich een mechanisme, waarin de transacties en de status van de geldautomaat worden geregistreerd. Deze gegevens worden met een speciale printer op papier bijgehouden. Onder het toetsenbord zit een speciaal mechanisme voor het versleutelen van de pincodegegevens. De gleuf waarin de pinpas wordt geschoven is omringd door elektronica voor het lezen van de magneetstrip op de pinpas en voor het bepalen van een aantal essentiële karakteristieken van een geldige pinpas. Ten slotte is er een computer die het geheel coördineert en de overige taken voor zijn rekening neemt, zoals het versturen van berichten. De computer maakt gebruik van een speciale (uitgeklede) versie van het Windows NT besturingssysteem.

Op het moment dat de gebruiker zijn pinpas in de automaat stopt, vindt er een aantal controles plaats die bepalen of de pas wordt geaccepteerd als een geldige pinpas. Vervolgens worden de gegevens op de magneetstrip van de pas ingelezen. Het betreft hier een cijferreeks die informatie verschaft over de eigenaar van de pas en de bijbehorende bankrekening. Daarna wordt de gebruiker gevraagd om de pincode in te toetsen. Met behulp van het speciale mechanisme dat zich meteen onder het toetsenbord bevindt, worden de pincode en de gegevens van de magneetstrip versleuteld.
Daarna worden er twee soorten berichten door de geldautomaat verstuurd. Het eerste bericht gaat over het Local Area Network (LAN) en blijft dus binnen de betreffende bank. Dat zijn berichten over de status van de geldautomaat en het soort transacties. De versleutelde gebruikersgegevens worden niet hiernaartoe gestuurd. Binnen de bank wordt veel gebruik gemaakt van zogenaamde terminalemulatie, waarmee de status van de geldautomaat wordt bijgehouden. Zo weet het bankpersoneel, wanneer de geldautomaat moet worden gevuld of wanneer er een probleem is.
Het tweede bericht gaat over een X.25-netwerk naar de zogenaamde ‘transactiehost’. Bij de transactiehost worden alle aanvragen voor de geldautomaten van de Rabobank verwerkt. Voordat een geldautomaat echter een bericht hiernaartoe kan sturen, zal hij zich moeten authenticeren aan de transactiehost.

Vervolgens worden de versleutelde klantgegevens samen met de opgevraagde informatie voorzien van een Message Authentication Code (MAC) om de integriteit te waarborgen, voordat ze verstuurd worden naar de transactiehost.
De transactiehost decodeert vervolgens het geauthenticeerde vertrouwelijke bericht, controleert de integriteit met behulp van de MAC en bepaalt of aan de aanvraag moet worden voldaan. De transactiehost beschikt daarvoor over alle noodzakelijke klantgegevens. Vervolgens hoeft de transactiehost alleen nog een gecodeerd bericht terug te sturen om te melden of akkoord wordt gegaan met de transactie en wat het (nieuwe) banksaldo is. Of indien er een probleem is een code terug te sturen die aan de geldautomaat vertelt wat het probleem is (overschrijding van de limiet, verkeerde pincode, enz.).
Ook de periodieke verversing van de sleutels die noodzakelijk zijn voor de encryptie (versleutelen) van de klantgegevens wordt door de transactiehost verzorgd. De rol die de transactiehost vervult is dus zeer belangrijk. Daarnaast worden er specifieke beveiligingsmaatregelen gebruikt in deze omgeving. Onder andere kan hierbij gedacht worden aan een volledig identiek uitwijkcentrum en een zeer stabiele en beveiligde computeromgeving (gebaseerd op een Tandem-omgeving met NSK).
Naast de geldautomaten van de Rabobank kan gebruik worden gemaakt van geldautomaten van andere banken in Nederland of in het buitenland. Dit zogenaamde gastgebruik verloopt via Interpay alvorens naar de transactiehost te worden gestuurd. Indien zich een probleem voordoet bij de transactiehost, wordt de transactie helemaal door Interpay overgenomen en afgehandeld. Betalen met behulp van de pinpas in winkels wordt eveneens door Interpay geregeld.

De geldautomaatomgeving van de Rabobank is geschetst in figuur 31.1.



Figuur 31.1
Schets geldautomaatomgeving Rabobank.

Classificatie van risico's

Om de betrouwbaarheid te waarborgen hanteert de Rabobank Groep een classificatiesysteem: het niveau van beveiliging dient in overeenstemming te zijn met de waarde en risico's van het te beveiligen object. Om de waarde eenduidig te specificeren heeft de Rabobank Groep een eigen classificatiemethode ontwikkeld. De classificatie wordt uitgedrukt in de zogenaamde BIV-code. BIV is een afkorting van de drie klassieke kwaliteitscriteria voor informatiebeveiliging: beschikbaarheid, integriteit en vertrouwelijkheid. Elk kwaliteitsaspect kan een waarde hebben van 1 (laag), 2 (middel) of 3 (hoog).

Als voorbeeld worden hier de definities van de drie beschikbaarheidsklassen weergegeven:

- Lage beschikbaarheid. Indien de informatie niet beschikbaar is, worden slechts geringe financiële risico's gelopen.
- Medium beschikbaarheid. Indien de informatie niet beschikbaar is, loopt de organisatie grote financiële risico's.
- Hoge beschikbaarheid. Indien de informatie niet beschikbaar is, loopt de organisatie zeer grote financiële risico's.

Het classificatiemodel kan worden getypeerd als een 'kwalitatief waardenmodel'. Dat wil zeggen de drie waarden geven het niveau ('ernst') van het financiële risico aan, indien het geclassificeerde object in zijn bedoelde functie wordt aangetast. Het risico wordt hierbij niet uitgedrukt in kwantitatieve hoeveelheden, maar in definities als 'zeer groot' tot 'gering'. De belangrijkste reden voor deze keuze is de diversiteit in organisatiegrootte (en daarmee financieel draagvermogen) van de verschillende Rabobank Groepsonderdelen, waardoor één kwantitatief classificatiemodel voor de gehele organisatie niet goed mogelijk is.

Om de BIV-code vast te stellen zijn met behulp van ervaringen uit het verleden diverse vragen ontwikkeld, zoals:

- Zijn gegevens herleidbaar naar cliënten of naar aangesloten banken? (vertrouwelijkheid).
- Wat is de consequentie van onjuiste, onvolledige of niet-tijdige informatie?(integriteit).
- Wat is de toegestane maximale uitvalsduur? (beschikbaarheid).

Bij het vaststellen van de classificatie wordt de verantwoordelijke bij de Rabobank vaak terzijde gestaan door ervaren adviseurs op het gebied van informatiebeveiliging.

Maatregelen ter waarborging van de betrouwbaarheid

Met behulp van de classificatie van risico's kan een consistent stelsel van maatregelen worden gedefinieerd en geïmplementeerd. Het betreft hier zowel technische als organisatorische en procedurele maatregelen.
Voorbeelden van deelgebieden waarop maatregelen worden getroffen zijn onder andere:

- gescheiden ontwikkel-, acceptatie- en productieomgeving.
- functiescheiding (gebruik versus beheer).
- fysieke beveiliging.
- 'change management' (versiebeheer).
- back-up/'recovery'/uitwijk.
- 'monitoring' en 'logging'.
- incidentmanagement/escalatieprocedure.

Verder steunt de Rabobank op bewezen technologie en redundantie om onaangename verrassingen te voorkomen en worden er regelmatig specialisten ingezet voor het uitwerken van complexe deeltaken.

Een van de belangrijkste technieken waarin maatregelen zijn getroffen met betrekking tot de betrouwbaarheid van geldautomaten is de cryptografie.

Cryptografische maatregelen

Cryptografie

Cryptografie betekent volgens Van Dale Groot Woordenboek Der Nederlandse Taal 'kunst om geheimschrift te schrijven'. Het woord is afgeleid van het Griekse woord kruptõ wat 'ik verberg' betekent. De moderne cryptografie biedt echter niet alleen mogelijkheden om de vertrouwelijkheid van gegevens te waarborgen, maar ook de integriteit, de authenticiteit en de onweerlegbaarheid ('non-repudiation') ervan. Dit wordt gerealiseerd door een adequate combinatie van cryptografische bouwstenen.

De Data Encryption Standard (DES)

De sterke punten uit de substitutie- en transpositietechnieken zijn gecombineerd in het welbekende symmetrische DES-algoritme dat in 1977 werd geïntroduceerd. Bij het DES-algoritme wordt de 'klare' tekst verdeeld in blokken van elk acht bytes, die in zestien opeenvolgende ronden worden gepermuteerd (transpositie) en gedeeltelijk vervangen (substitutie). De sleutellengte van DES is 64 bits, waarvan er 56 willekeurig kunnen worden gekozen. De overige 8 posities zijn gereserveerd voor controles op de kwaliteit van de invoer ('parity-check').

Met de huidige moderne rekenmiddelen kan worden gesteld dat de sleutel van 56 bits te klein is om een uitputtende analyse van de sleutelruimte ('brute-force attack') te voorkomen (zie ook tabel 31.1). Het succes van een op DES gebaseerd cryptografisch systeem is daarom sterk afhankelijk van het frequent wijzigen van de sleutel. Opgemerkt wordt dat tegenwoordig veelvuldig gebruik wordt gemaakt van het zogenaamde 'Triple-DES', waarbij het algoritme drie keer met twee of drie verschillende sleutels wordt toegepast. Daarnaast wordt er hard gewerkt aan een nieuwe standaard op het gebied van symmetrische encryptie om DES te vervangen: de 'Advanced Encryption Standard' (AES) waarvoor onlangs een in België ontworpen algoritme genaamd 'Rijndael', is gekozen. AES heeft een variabele sleutellengte van minimaal 128 bits.

vereist budget ($)	**sleutellengte (bits)**				
	40	56	80	112	128
10 K	2 seconden	35 uren	70.000 jaren	10^{14} jaren	10^{19} jaren
100 K	0,2 seconden	3,5 uren	7.000 jaren	10^{13} jaren	10^{18} jaren
1 M	0,02 seconden	21 minuten	700 jaren	10^{12} jaren	10^{17} jaren
10 M	2 milliseconden	2 minuten	70 jaren	10^{11} jaren	10^{16} jaren
100 M	0,2 milliseconden	13 seconden	7 jaren	10^{10} jaren	10^{15} jaren
1 G	0,02 milliseconden	1 seconde	245 dagen	10^{9} jaren	10^{14} jaren

Tabel 31.1
Gemiddelde tijd voor een hardwarematige 'brute-force attack' op een symmetrisch algoritme in 2000.

Rivest, Shamir en Adleman asymmetrische encryptie (RSA)

Bij een symmetrisch algoritme (zoals DES) is het mogelijk om de decryptiesleutel (eenvoudig) af te leiden uit de encryptiesleutel en vice versa. Het voordeel van een symmetrisch algoritme is dat het encryptie- en decryptieproces relatief weinig computertijd kost en daarom veel wordt gebruikt. Vooral is dat zo als encryptie wordt toegepast op grote hoeveelheden data. Bij asymmetrische algoritmen wordt voor de encryptie een andere sleutel gebruikt dan bij de decryptie van het bericht en is de ene sleutel niet (eenvoudig) af te leiden uit de andere sleutel. Elke betrokken partij heeft voor de toepassing hiervan twee sleutels nodig. Deze sleutelparen bestaan uit een geheime sleutel en een openbare sleutel, waardoor deze techniek ook wel het 'public key'-systeem wordt genoemd.

De theorie van asymmetrische algoritmen werd in 1976 door Diffie en Hellman gepresenteerd. Twee jaar later werden de eerste asymmetrische algoritmen ontwikkeld waaronder RSA. Momenteel is RSA de defacto standaard voor asymmetrische algoritmen. RSA staat voor de ontwerpers Rivest, Shamir en Adleman en is in 1978 op de markt gebracht. RSA is relatief trager dan DES (factor duizend) en gebruikt veel langere sleutels (minimaal factor tien). De grootte van de sleutels kan echter eenvoudig aangepast worden en daarmee de betrouwbaarheid

van het algoritme (mits het factorisatieprobleem niet opgelost wordt). RSA is dus uitermate geschikt voor het uitwisselen van (symmetrische) sleutels, die vervolgens gebruikt kunnen worden voor het vercijferen van grote hoeveelheden data.
De betrouwbaarheid van het RSA-algoritme is gebaseerd op de complexiteit van het factorisatieprobleem van het product van twee grote priemgetallen. Zolang de wiskunde niet in staat is om dit probleem efficiënt op te lossen, is RSA zeer betrouwbaar. De snel groeiende rekenkracht van computers kan in het geval van RSA eenvoudig opgevangen worden door het gebruik van langere sleutels (zie ook tabel 31.2).

Tabel 31.2
Enkele wetenswaardigheden met betrekking tot RSA.

De eerste keer dat een 512-bits RSA-getal gefactoriseerd is: 22 augustus 1999.
De benodigde tijd voor het kraken van het 512-bits RSA-getal (met bijna 300 computers): 7,4 maanden.
De benodigde tijd voor een 'brute-force attack' op een 1792-bits RSA-getal [4]: 10^{13} jaren.
De totale levensduur van het universum [5]: 10^{11} jaren.
Het aantal priemgetallen met een lengte tot 512-bits: 10^{151}.
Het aantal atomen in het melkwegstelsel: 10^{67}.
De kans dat twee personen hetzelfde priemgetal kiezen is kleiner dan de kans om de loterij te winnen (mits wordt meegedaan) en dezelfde dag door de bliksem getroffen te worden.
Met behulp van een database van alle priemgetallen, zou theoretisch veel sneller een 'brute-force attack' gepleegd kunnen worden. Het gewicht van een harde schijf met een capaciteit van 1Gb per gram waarop de database met alle priemgetallen tot 512 bits bewaard zou worden, zou echter qua gewicht de natuurkundige Chandrasekharlimiet overtreffen en dus instorten tot een zwart gat, waardoor dit zeker geen praktische oplossing is!

Er vindt momenteel veel wetenschappelijk onderzoek plaats naar nieuwe asymmetrische algoritmen die RSA moeten opvolgen. Sommige zijn net als RSA gebaseerd op het factorisatieprobleem, andere hebben nieuwe uitgangspunten en nieuwe eigenschappen. Zo zijn er tegenwoordig bijvoorbeeld algoritmen die het mogelijk maken om correcte wiskundige operaties uit te voeren op vercijferde data zonder de inhoud van deze data te kennen.

Message Authentication Code

Naast symmetrische en asymmetrische algoritmen is er nog een belangrijke cryptografische bouwsteen: de 'one way'-hashfunctie, ook wel 'Message Digest'-functie genoemd. Deze functie kan op een bericht met een willekeurige lengte toegepast worden met als resultaat een zogenaamde hashwaarde met een vaste lengte. Daarnaast heeft deze functie nog drie specifieke eigenschappen:

4 Met specifieke hardware ter waarde van $100.000 in het jaar 2000.

5 Aangenomen dat het universum gesloten is.

– de hashwaarde van een willekeurig bericht is eenvoudig te bepalen;
– met behulp van een hashwaarde is het moeilijk om een bijbehorend origineel bericht te bepalen;
– het is moeilijk om een tweede bericht te bepalen dat dezelfde hashwaarde oplevert (collisieweerstand).

De meeste hashfuncties leveren een hashwaarde op met een lengte tussen de 64 en 256 bits op. Met de huidige computertechnieken is 64 bits eigenlijk al te klein om collisiegevaar redelijkerwijs uit te sluiten. De meest gebruikte technieken hebben een hashwaarde met een lengte van 128 of 160 bits.
Als basis voor 'one way'-hashfuncties kunnen symmetrische blokalgoritmen (zoals DES) gebruikt worden of asymmetrische algoritmen (zoals RSA). Een ander voorbeeld van een veel gebruikte 'one way'-hashfunctie is Message Digest 5 (MD5).

'One way'-hashfuncties worden voor verschillende doeleinden gebruikt, waaronder:
– het opslaan van wachtwoorden. Alleen de hashwaarde van een wachtwoord wordt bewaard door bijvoorbeeld een besturingssysteem. Telkens als 'authenticatie' plaatsvindt, wordt de hashwaarde van het wachtwoord berekend en vergeleken met de opgeslagen hashwaarde. Op deze manier kunnen wachtwoorden niet achterhaald worden;
– het bewaken van de integriteit van een bericht. Indien een bericht wordt verstuurd samen met de hashwaarde ervan, kan deze laatste gebruikt worden om te garanderen dat het bericht origineel en niet veranderd is, zonder dat het bericht zelf versleuteld is;
– als hulpmiddel voor of zelfs basis van veel protocollen, waaronder digitale handtekeningen.

Indien een hashwaarde wordt gecombineerd met een speciale vorm van een asymmetrisch algoritme (een digitale handtekening), spreekt men over een Message Authentication Code (MAC).

Diverse sleutels

De juiste combinatie van bovenvermelde bouwstenen maakt het mogelijk om een betrouwbare transactie te waarborgen in de geldautomaatomgeving van de Rabobank. Hierbij spelen aspecten als gelaagdheid, functie en wisseling van (cryptografische) sleutels een grote rol. Zo kent de geldautomaatinfrastructuur:
– Opslagsleutels: 'masterkeys' ter bescherming van distributie- en transportsleutels.
– Distributie- en transportsleutels: sleutels voor de bescherming van andere sleutels (bijvoorbeeld werksleutels).

– Werksleutels: sleutels voor specifieke cryptografische bewerkingen, zoals PIN-verificatie en MAC-generatie en -verificatie. Deze sleutels zijn vaak aan beide zijden (transactiehost en geldautomaat) aanwezig, afhankelijk van functionaliteit en opzet. Denk hierbij bijvoorbeeld aan sleutels voor de MAC-generatie.

Opgemerkt dient te worden dat de werkelijke omgeving complexer is dan in de voorgaande paragrafen wordt geschetst.

Trends en toekomstbeeld geldautomaatomgeving

Bij de geldautomaatomgeving zijn diverse trends te herkennen die al besproken zijn in eerdere hoofdstukken van dit boek (zie deel 1). Er is vooral sprake van een toenemende complexiteit en een toenemende behoefte aan integratiecapaciteiten. Toch moet het geheel betrouwbaar en beheersbaar blijven. Hierdoor worden de technische maatregelen in belangrijke mate ondersteund door procedurele en organisatorische maatregelen. Een direct gevolg van deze complexiteit is een opvallend ingewikkelde procedure voor 'change management'.

In de nabije toekomst zal de geldautomaatomgeving onderhevig zijn aan een aantal ingrijpende veranderingen. Zo zal de geldautomaat multifunctioneler worden: nieuwe functionaliteiten zullen beschikbaar komen om gebruikers beter van dienst te kunnen zijn en in te spelen op de nieuwe behoeften van de markt en de consument. Hierbij kan gedacht worden aan transactieoverzichten of het bekijken van aandelenportefeuilles.
Ook de gebruikte techniek zal veranderen. Onder andere kan gedacht worden aan de inzet van het TCP/IP-protocol[6] voor het versturen van de gegevens ter vervanging van het X.25-protocol. De gebruikte encryptiemiddelen zullen eveneens aangepast worden. Hierbij wordt wel rekening gehouden met de inzet van uitsluitend bewezen technologie: de inzet van AES hoeft op korte termijn niet verwacht te worden, wel die van Triple-DES.
Echter, alvorens al deze veranderingen tot de werkelijkheid gaan behoren, wordt de Rabobank met een andere uitdaging geconfronteerd: begin 2002 is de overgang naar de Euro een feit. Alle geldautomaten van de Rabobank zullen daar ook gereed voor zijn.

Indien we de cryptografische hulpmiddelen in de geldautomaatomgeving als zelfstandig technisch systeem benaderen, vallen dezelfde trends te onderkennen: een toenemende complexiteit en een toenemende behoefte aan integratie in bestaande en of nieuwe omgevingen. Wel dient opgemerkt te worden dat de toenemende complexiteit bij cryptografie juist structuur in het geheel brengt en

6 Transmission Control Protocol/Internet Protocol: een (de facto) verzameling 'packet switching' datatransmissieprotocollen voor het verbinden van LAN's, intranetwerken en Internet.

dat door middel van (abstracte) wiskundige modellen eenduidige bewijzen voor de mate van betrouwbaarheid van de techniek te formuleren zijn.
Enerzijds zijn de nieuwe eisen van de elektronische handel een vernieuwde motor voor onderzoek op het gebied van cryptografie, omdat er grootschalig geïnvesteerd wordt in het noodzakelijke onderzoek. Anderzijds is cryptografie daardoor ook sterk onderhevig geworden aan marktgedreven ontwikkelingen. Voor een domein waar het bewijs voor betrouwbaarheid nog altijd sterk afhankelijk is van het aantal succesvolle jaren dat de techniek grootschalig is ingezet, brengt dat toch de nodige tegenstrijdigheid met zich mee.

Literatuur

- Geerts, G., e.a. (1984). Van Dale Groot Woordenboek Der Nederlandse Taal. Van Dale Lexicografie, Utrecht
- Schneier, B. (1996). Applied Cryptography. John Wiley & Sons, New York
- 'Lenstra-Verheul'-tabel. www.cryptosavvy.com/table.htm

2

32
Gebruik risicoanalyse bij beslissingen

ir. E.C.J. Bouwman [1]

Inleiding

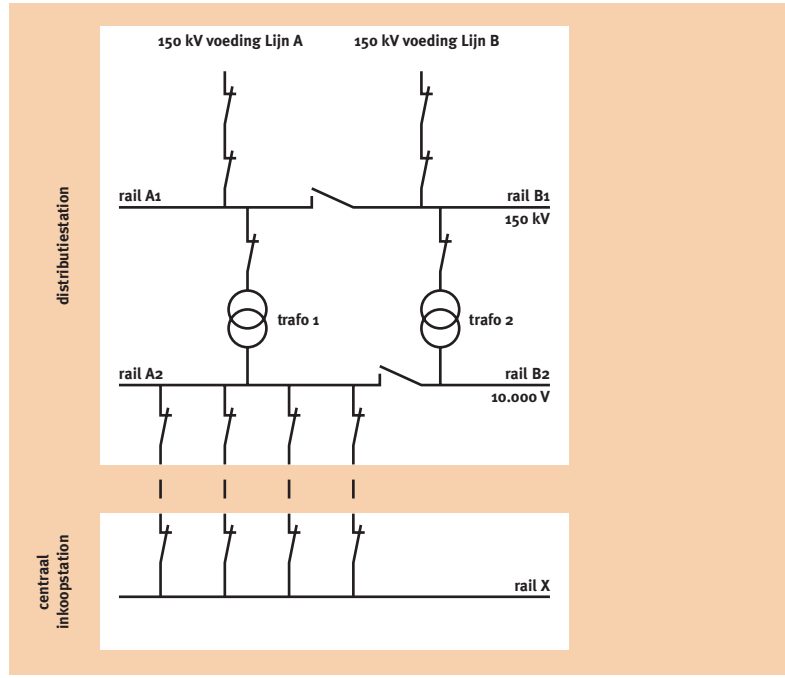
Het bedrijfsleven krijgt in steeds sterkere mate te maken met een vanuit de markt of vanuit de eigen bedrijfsvoering opgelegde verplichting om permanent (24 uur per dag, 365 dagen per jaar) beschikbaar te zijn. Enerzijds wordt van een bedrijf verwacht dat het altijd bereikbaar is. Door de verregaande mondialisering zijn de klanten over de hele wereld verspreid en is een 24-uurservice noodzakelijk voor bijvoorbeeld het uitwisselen van gegevens of het opnemen van orders. Anderzijds leidt de toenemende complexiteit van systemen ertoe dat een afschakeling of uitval direct tot grote gevolgschade leidt. Indien er tijdens de afschakeling al geen gegevens verloren zijn gegaan, kan het uren, zo niet dagen duren om het systeem weer volledig in bedrijf te brengen. Bij grotere gevolgschade voor de klanten zijn zelfs juridische claims te verwachten. Bovendien is het door de toenemende complexiteit en de zich steeds uitbreidende ketenafhankelijkheid moeilijker te achterhalen, waar zich de werkelijke zwakke punten bevinden.

Met deze eisen van een zeer hoge betrouwbaarheid èn een zeer hoge beschikbaarheid dient terdege rekening gehouden te worden bij het ontwerpen van een nieuw systeem. In de hier gepresenteerde case wordt uitgewerkt hoe een relatief eenvoudige risicoanalyse van een productiebedrijf kan helpen bij de keuze van het juiste concept om de energievoorziening uit te breiden.

1 Tijdens het schrijven van dit artikel was de auteur werkzaam bij NRG Arnhem, Afdeling Risk Management & Decision Analysis. Op dit moment werkt hij in een eigen bedrijf, genaamd Delta Pi.
Delta Pi
Postbus 214
6920 AE Duiven

Beschrijving case

In verband met een forse groei van de omzet dient een groot productiebedrijf op relatief korte termijn de productie op haar bedrijfsterrein uit te breiden. Ten gevolge van deze uitbreiding zal de toekomstige behoefte aan elektrisch vermogen ruimschoots het huidige te leveren vermogen overschrijden. Derhalve dient zowel bij het productiebedrijf als bij het elektriciteitsbedrijf een uitbreiding van het te leveren vermogen plaats te vinden. Hiertoe is een aantal mogelijke alternatieven voor de uitbreiding op een rij gezet. Aangezien zelfs een lokale uitval van de elektriciteitsvoorziening bij een van de installaties direct tot grote schade bij het productieproces kan leiden, wil het productiebedrijf de betrouwbaarheid van de verschillende varianten in elektriciteitsvoeding duidelijk een rol laten spelen bij de keuze van de verschillende alternatieven. Om een beter inzicht te krijgen is besloten in drie stappen een analyse uit te voeren om de betrouwbaarheid van de alternatieve varianten vast te leggen. In de eerste stap wordt de betrouwbaarheid van de elektriciteitsvoorziening op het terrein zelf bepaald, uitgaande van een ongestoorde voeding uit het elektriciteitsbedrijf. In de tweede stap wordt de betrouwbaarheid van de bestaande voeding uit het elektriciteitsbedrijf naar het productiebedrijf bepaald. De beide resultaten worden vervolgens met elkaar vergeleken om inzicht te krijgen in de bijdrage van het falen van de eigen systemen ten opzichte van die van het elektriciteitsbedrijf. In de derde en laatste stap wordt de betrouwbaarheid van de drie mogelijke nieuwe varianten bepaald en vergeleken met die in de bestaande situatie.



Figuur 32.1
De aansluitingen van elektriciteit in de bestaande situatie.

In de bestaande situatie zijn alle installaties via transformatoren aangesloten op drie over het terrein lopende ringen met een spanning van 10.000 V. Deze ringen zijn op hun beurt aangesloten op een elektrische voedingsrail in het Centraal Inkoopstation (gebouw CI). Dit gebouw wordt met behulp van vier lijnen gevoed uit het distributiestation A van het elektriciteitsbedrijf.

Analyse ringen op terrein productiebedrijf

Om inzicht te krijgen in de faalkansen op het terrein van het productiebedrijf zijn de drie aanwezige ringen nader in model gebracht. Het model is opgezet vanaf de aansluiting in het inkoopstation CI tot en met de afgaande velden aan de laagspanningskant van de 10 kV/400 V-transformatoren bij de installaties. Voor dit modelleren is gebruik gemaakt van de foutenboomtechniek.

Een foutenboom is een schematische weergave van combinaties van oorzaken die tot een tevoren bepaalde ongewenste gebeurtenis kunnen leiden, de zogenaamde 'topgebeurtenis'. Voor de hoofdmodellen in deze case zijn de volgende twee topgebeurtenissen gedefinieerd:

- **Eén aansluiting van een van de installaties faalt (model 1).**
- **Onvolledige elektriciteitsvoeding uit het elektriciteitsbedrijf naar gebouw CI (model 2, 3).**

Een foutenboom bestaat in principe uit één topgebeurtenis ('top') met daaronder verschillende basisgebeurtenissen ('basic events'). Basisgebeurtenissen beschrijven het falen van een component. De topgebeurtenis volgt logisch uit de combinaties van onderliggende basisgebeurtenissen.
Om een foutenboom op te zetten, wordt uitgegaan van de topgebeurtenis en 'met de vinger' tegen de stroom in door het systeem gelopen. In figuur 32.2 is het falen van de beveiliging de topgebeurtenis. De foutenboom is opgezet door vanaf de beveiliging via de OF-poort en de voelers naar de voeding te lopen. Deze methodiek werkt ook uitstekend bij zeer complexe systemen, zoals bijvoorbeeld kerncentrales met hun zeer grote aantallen componenten.

De basisgebeurtenissen zijn gekoppeld aan de topgebeurtenis via:

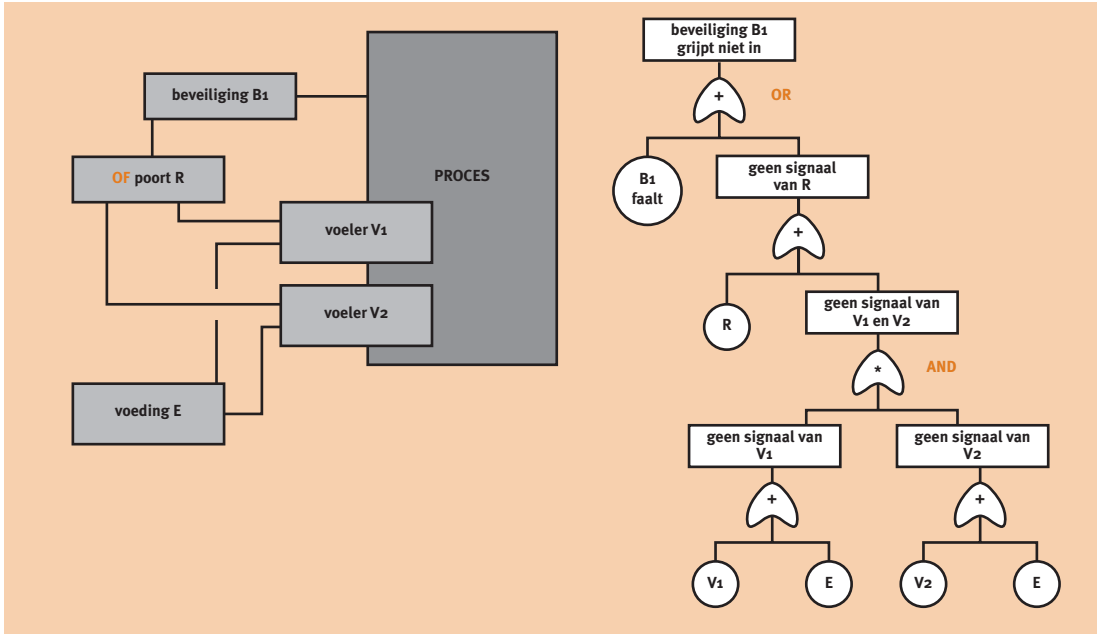
- **EN-poorten ('AND-gates'); deze koppelen de onderliggende gebeurtenissen zodanig dat de uitvoergebeurtenis slechts optreedt als alle invoergebeurtenissen optreden.**
- **OF-poorten ('OR-gates'); deze koppelen onderliggende gebeurtenissen zodanig dat de uitvoergebeurtenis optreedt, indien tenminste een van de invoergebeurtenissen optreedt.**

Voor het bepalen van de verzameling van combinaties van basisgebeurtenissen die nodig en voldoende zijn voor het optreden van de topgebeurtenis ('minimale deelverzameling') wordt de zogenaamde Booleaanse algebra toegepast:

- A AND B = A*B. Indien gebeurtenis A EN gebeurtenis B moeten optreden, is de kans hierop gelijk aan de kans van optreden van gebeurtenis A MAAL de kans van optreden van gebeurtenis B.
- A OR B = A+B. Indien gebeurtenis A OF gebeurtenis B kan optreden, is de kans hierop gelijk aan de kans van optreden van gebeurtenis A PLUS de kans van optreden van gebeurtenis B.
- A AND A = A. Indien gebeurtenis A twee maal moet optreden, is de kans hierop gelijk aan de kans van enkelvoudig optreden van gebeurtenis A.
- A OR A = A. Indien gebeurtenis A twee maal mag optreden, is de kans hierop gelijk aan de kans van enkelvoudig optreden van gebeurtenis A.
- A OR (A AND B) = A. Indien gebeurtenis A OF gebeurtenis A EN B moeten optreden, is de kans hierop gelijk aan de kans van optreden van gebeurtenis A.

De laatste stap in de foutenboomtechniek is het kwantificeren van de minimale deelverzamelingen. Deze geven alle mogelijke combinaties van gebeurtenissen, die kunnen leiden tot het optreden van de topgebeurtenis. Hierbij wordt onderscheid gemaakt naar de orde van de deelverzameling. Een eerste orde deelverzameling bevat slechts één basisgebeurtenis. Deze is al voldoende om de topgebeurtenis te doen optreden; bij een tweede orde deelverzameling dienen twee basisgebeurtenissen op te treden, bij een derde orde deelverzameling drie, enz. Voor meer informatie zie [PATO, 1999; CPR, 1997; NRG].

Figuur 32.2
Foutenboom.



Voor het kwantificeren van de foutenbomen dienen de faalgegevens van de basisgebeurtenissen ingevoerd te worden. Deze faalgegevens bestaan onder andere uit de faalwijze (zekering opent niet als dat gewenst wordt of zekering opent spontaan), de faalfrequentie (component X faalt gemiddeld eens in de Y jaar), de reparatieduur en de testinterval (de component wordt ieder half jaar getest). Op basis van deze gegevens kan zowel de faalfrequentie als het niet-beschikbaar zijn van de topgebeurtenis bepaald worden.
Aangezien bij het productiebedrijf iedere – ook een korte – onderbreking van de elektriciteitsvoeding de bedrijfsvoering verstoort, is het niet beschikbaar zijn voor deze bijdrage minder van belang. Er is dan ook besloten om alleen de faalfrequentie van de topgebeurtenis uit te rekenen om de betrouwbaarheid te bepalen.

Voor het bepalen van de kans op falen is in alle modellen gebruik gemaakt van generieke faaldata uit de industrie en waar mogelijk van statistische gegevens van de elektriciteitslevering.
In tabel 32.1 zijn de gemiddelde resultaten van de analyse van de ringen op het terrein van het productiebedrijf weergegeven. Hierbij is ervan uitgegaan dat de voeding uit het elektriciteitsbedrijf altijd aanwezig is. De faalkans in deze tabel geeft de kans weer dat een van de gebruikers in die bewuste ring geen of onvoldoende voeding krijgt.

Tabel 32.1
Overzicht gemiddelde resultaten ringen op terrein productiebedrijf.

	per ring gemiddeld
faalkans (per uur)	$5{,}1 \cdot 10^{-5}$
faalinterval (jaar)	2
dominante bijdrage 1	zekeringen gebruikers 45%
dominante bijdrage 2	laagspanningsbussen 20%
dominante bijdrage 3	transformatoren 15%

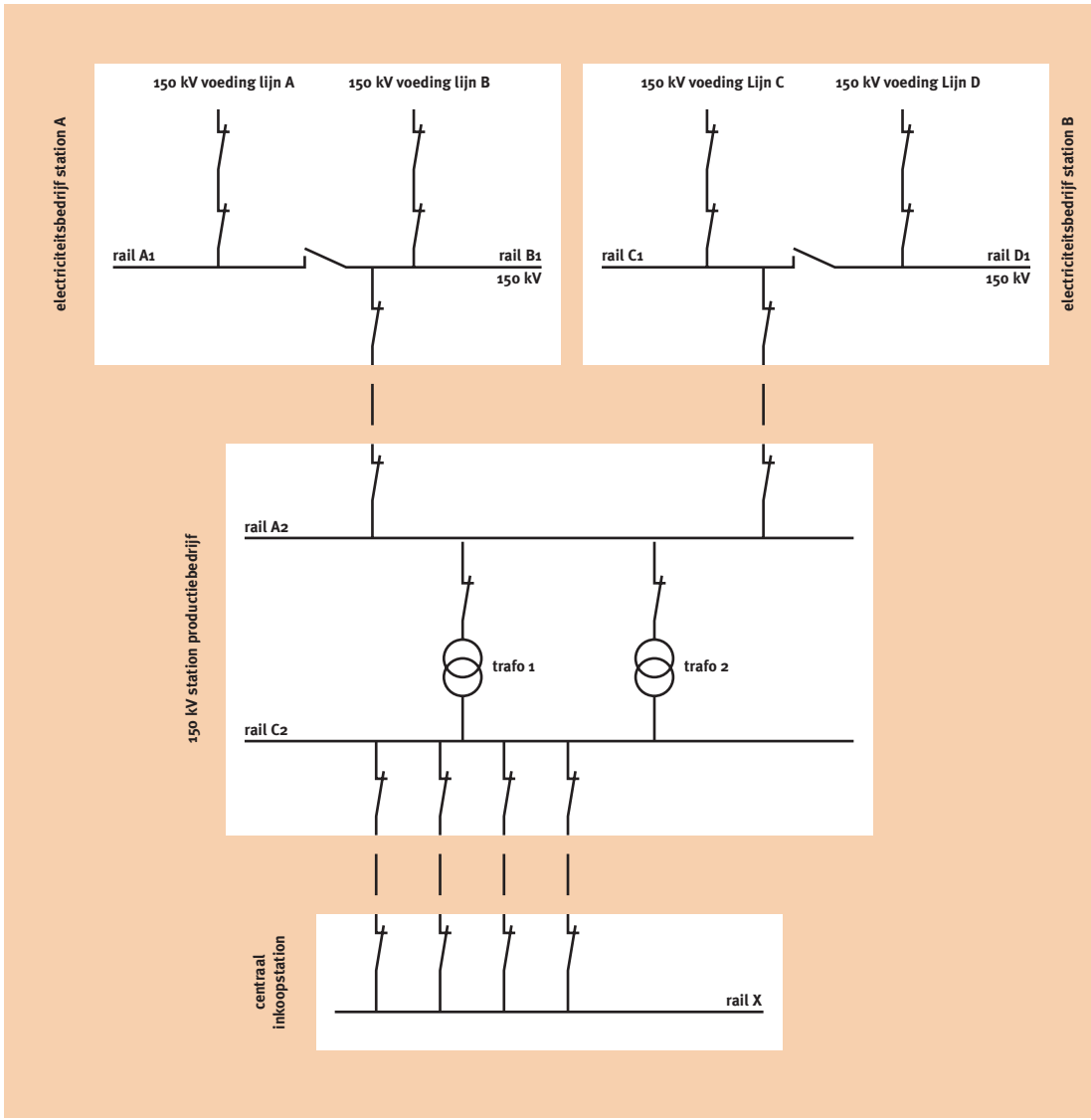
Gemiddeld blijkt zo'n gebeurtenis eens in de 2 à 2,5 jaar voor te komen. Op het hele terrein zal dat gemiddeld iets vaker dan eens per jaar optreden.
Er is niet één enkele component die een duidelijke bijdrage levert aan de faalfrequentie. De grote aantallen componenten bepalen wel duidelijk de uitkomst. Immers indien in een systeem honderd zekeringen zijn opgenomen die ieder eens in de honderd jaar falen, dan wordt de faalfrequentie van het systeem eens per jaar!
Belangrijkste bijdragen aan de faalkans zijn de zekeringen naar de gebruikers, de laagspanningsbussen en de transformatoren. Tussen de ringen onderling werden slechts geringe verschillen gevonden. Deze zijn te verklaren door een enigszins verschillende opbouw en door verschillende aantallen componenten.

Analyse voedingen uit het elektriciteitsbedrijf

Voor het modelleren van de bestaande voeding uit het elektriciteitsbedrijf kon gebruik gemaakt worden van beschikbare informatie. Van de alternatieve voedingen waren slechts principeschetsen beschikbaar. Voor het modelleren van deze alternatieve voedingen kon dus geen gebruik gemaakt worden van gedetailleerde informatie en dienden enige aannamen gedaan te worden over de toekomstige uitvoering. De volgende varianten zijn geanalyseerd:

– *Huidige voeding*. Een transformator in distributiestation A 'voedt in' op een 10.000 V rail. Uit de afgaande velden van deze rail gaan vier ondergrondse kabels naar het inkoopstation CI van het productiebedrijf.

Figuur 32.3
Principeschets van variant 1 van alternatieve elektriciteitsvoeding.



– *Variant 1*. Zowel uit het distributiestation A als uit een tweede distributie station B wordt een ondergrondse 150 kV-kabel aangelegd naar een nieuw te bouwen 150 kV-station op het terrein van de producent. Deze kabels komen samen op een 150 kV-rail. Van daaruit worden twee transformatoren gevoed, die ieder op hun beurt invoeden op een 10.000 kV-rail. Uit de afgaande velden van deze rail gaan vier ondergrondse kabels naar het inkoopstation CI. Deze variant is duur, vooral omdat uit twee inkoopstations kabels naar het productiebedrijf aangelegd dienen te worden, maar naar verwachting zal deze variant veel betrouwbaarder zijn.
– *Variant 2*. Deze variant is identiek aan variant 1 met dien verstande dat beide 150 kV-kabels uit distributiestation A worden getrokken. Aangezien slechts één set kabels aangelegd hoeft te worden, is deze variant goedkoper dan variant 1. De betrouwbaarheid zal naar verwachting iets minder zijn.
– *Variant 3*. Deze variant lijkt veel op de huidige situatie. In het distributiestation A staan nu echter twee transformatoren ter beschikking van de voeding voor het productiebedrijf. Indien gewenst kunnen de vier ondergrondse 10.000 kV-kabels worden uitgebreid. Op het terrein van het productiebedrijf komt een nieuw inkoopstation, waar de 4 kabels op één 10.000 kV-rail samenkomen. Uit de afgaande velden van deze rail gaan vier ondergrondse kabels naar het inkoopstation CI. Aangezien hier de minste nieuwbouw gepleegd hoeft te worden, is dit de goedkoopste variant.

Tabel 32.2
Samenvatting resultaten varianten van alternatieve elektriciteitsvoeding.

De resultaten van de foutenboomanalyse van deze varianten zijn in tabel 32.2 samengevat.

	huidig	**variant 1**	**variant 2**	**variant 3**
faalkans (per uur)	$9{,}9 \cdot 10^{-6}$	$2{,}1 \cdot 10^{-6}$	$2{,}25 \cdot 10^{-6}$	$2{,}4 \cdot 10^{-6}$
faalinterval (jaar)	12	55	50	47
dominante bijdrage 1	falen E-distributienet	falen E-distributienet	falen E-distributienet	falen E-distributienet
	10%	40%	37%	35%
dominante bijdrage 2	falen transformator	rail 150 kV-productiebedrijf	rail 150 kV-productiebedrijf	gemeenschappelijk falen 10 kV-lijnen van distributiestation naar bedrijf
	40%	15%	15%	20%
dominante bijdrage 3	falen 150 kV-systeem	–	gemeenschappelijk falen 150 kV-lijnen van distributiestation naar bedrijf	–
	25%		5%	

De faalkans in deze tabel geeft de kans dat station CI op het terrein van het productiebedrijf geen of onvoldoende voeding krijgt.
Uit de resultaten blijkt dat de kans op falen van de voeding van het elektriciteitsbedrijf in alle varianten aanzienlijk lager is dan de faalkans in de ringen van het productiebedrijf (gemiddeld eens in de 2 jaar). Alle drie de nieuwe varianten geven een aanzienlijke verbetering ten opzichte van de huidige situatie. Variant nummer 1 met voeding van zowel distributiestation A als distributiestation B scoort het beste. Dit wordt vooral veroorzaakt door het feit dat de lijnen van de stations A en B naar het productiebedrijf over volledig gescheiden tracés lopen. In de beide andere varianten lopen alle lijnen over één tracé en dient gemeenschappelijk falen in de analyse betrokken te worden. Variant 3 scoort ten opzichte van variant 2 slechter, vooral als gevolg van het feit dat 10.000 kV-lijnen gemiddeld een hogere faalkans hebben dan 150 kV-lijnen.

Conclusies

In eerste instantie werd verwacht dat de faalkans van variant 1 (elektriciteitsvoeding uit twee onafhankelijke stations) een ruimschoots hogere betrouwbaarheid zou geven dan de andere twee varianten, die slechts uit één distributiestation worden gevoed. De extra hoge aanschafkosten (bijna twee maal hoger) zouden zich dan snel terugverdienen door veel lagere kosten als gevolg van de uitval van productie. Doordat de faalkans van de elektrische systemen relatief klein is ten opzichte van de faalkans van het hele distributienet is deze laatste faalkans dominant. Bovendien is de faalkans van de voedingen van het elektriciteitsbedrijf een orde van grootte kleiner dan die van de elektrische componenten op het terrein van de producent.
Vanuit het oogpunt van faalkansen geredeneerd voldoen alle geanalyseerde nieuwe varianten voor de elektriciteitsvoedingen dan ook even goed. In alle varianten wordt de faalkans bijna 4 maal lager dan die van de huidige voeding. Variant 1 heeft de laagste kans van falen, maar vergeleken met de faalkans van de systemen op het terrein van de producent is de invloed op het totaal klein.

Indien naar de kosten gekeken wordt, dient variant 1 direct af te vallen, omdat de relatief kleine winst in de totale betrouwbaarheid voor variant 1 ten opzichte van de varianten 2 en 3 zeker niet opweegt tegen de extra kosten, die daarmee gemoeid zijn. Daarentegen zijn de verschillen tussen de varianten 2 en 3 niet zo groot dat hieruit snel een eenduidige beslissing getrokken kan worden. Andere overwegingen – hierbij valt bijvoorbeeld te denken aan het niet beschikbaar zijn als gevolg van onderhoud, of de te verwachten levensduur van de componenten – dienen meegenomen worden om een verantwoorde keuze te kunnen maken.

Uit deze bijdrage blijkt dat de betrouwbaarheid van technische systemen met behulp van een risicoanalyse beter in beeld gebracht kan worden. Omdat een goed inzicht in de complexe energievoorziening ontbrak, zou de producent zonder de risicoanalyse gevoelsmatig gekozen hebben voor een variant die wel veel duurder was, maar toch uiteindelijk een te verwaarlozen verbetering van de zo gewenste betrouwbaarheid en beschikbaarheid zou opleveren. Om de betrouwbaarheid en beschikbaarheid daadwerkelijk te verhogen blijkt het voor de hier besproken producent veel beter om extra te investeren in betere of meer redundante voorzieningen in het eigen bedrijf. Bedrijven doen er derhalve goed aan naast de investeringen in een steeds intensievere productontwikkeling ook investeringen te doen om de betrouwbaarheid en de beschikbaarheid van de productielijnen voldoende in de pas te laten lopen.
Alhoewel de risicoanalysetechniek hier is toegepast als assistentie bij de aanschaf van een nieuw systeem, is deze techniek ook uitstekend geschikt om bijvoorbeeld het onderhoud aan bestaande systemen te optimaliseren. Indien immers uit de analyse blijkt dat sommige componenten een dominante bijdrage leveren aan het totale risico, is goed onderhoud aan die componenten van groot belang. Indien uit de risicoanalyse blijkt dat een component slechts van ondergeschikt belang is, kan mogelijk met weinig of geen onderhoud worden volstaan.

In eerste instantie waren de hier besproken analysetechnieken puur gericht op technische systemen. Er is echter gebleken dat ze – weliswaar met enige aanpassingen – ook uitstekend bruikbaar zijn voor de analyse van andere bedrijfskundige processen zoals de administratie en de logistiek. Verdere uitbreiding van deze analysen kan uiteindelijk leiden tot een daadwerkelijke introductie van integraal risicomanagement in de bedrijven.

Literatuur

- Cursus Betrouwbaarheidsanalyse PATO/NRG. (1999). Stichting PATO. Den Haag
- Internet site NRG www.nrg-nl.com/product/riskman
- Methods for Determining and Processing Probabilities. (1997). CPR 12E, second edition. Sdu Publishers

2

33 Herstellen van fouten

drs. L. Kanse, dr. T.W. van der Schaaf [1,2]

Inleiding

De focus bij het management van proces- en productbetrouwbaarheid, veiligheid en kwaliteit lag tot zover voornamelijk op de preventie van fouten. Fouten kunnen immers leiden tot productie- of kwaliteitsverlies, vertraging, schade, letsel, of andere ongewenste gevolgen. In principe voldoende redenen dus om fouten te willen voorkomen.

Om vorm te kunnen geven aan een beleid dat is gericht op de preventie van fouten is voorkennis nodig van de fouten die in een proces kunnen optreden. In de praktijk echter blijkt steeds weer dat niet alle mogelijke fouten kunnen worden voorzien, en dat zelfs niet alle voorziene fouten voorkomen kunnen worden.
Uit dit boek blijkt wel dat er zoveel trends zijn waarmee rekening moet worden gehouden dat niet alle fouten voorkomen kunnen worden. Vooral de megatrends met betrekking tot de toenemende complexiteit en dynamiek laten zien dat fouten kunnen optreden. En in feite zijn het ook niet zozeer de fouten zelf, als wel de negatieve gevolgen van deze fouten die voorkomen zouden moeten worden [Frese, 1991].

1 Technische Universiteit Eindhoven, Faculteit Technologie Management
Postbus 513
5600 MB Eindhoven

2 Deze bijdrage is in een uitgebreidere vorm verschenen in het tijdschrift Gedrag en Organisatie [Kanse, 2000b].

Nadat een fout is opgetreden, is er vaak nog de gelegenheid herstelmaatregelen toe te passen die ervoor zorgen dat de ongewenste gevolgen van de fout geheel of gedeeltelijk voorkomen worden. Vooral het kijken naar de hele keten en de functie van het proces (en niet alleen het systeem zelf; zie ook deel 3) biedt mogelijkheden hiertoe. Dit inzicht vormt de basis voor een additionele alternatieve benadering van het management van proces- en productbetrouwbaarheid, veiligheid en kwaliteit die zich richt op het herstellen van fouten nadat deze hebben plaatsgevonden, maar voordat ze tot ongewenste gevolgen hebben kunnen leiden.

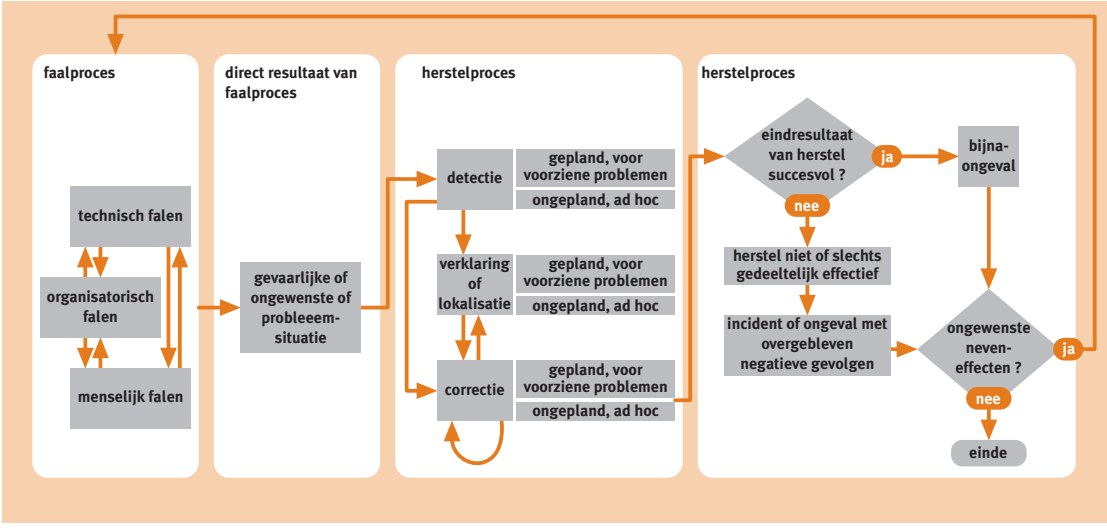
Een voorbeeld ter verduidelijking: een programmeerfout van een softwareontwerper zou kunnen leiden tot storingen bij gebruikers van die software, als de fout niet ontdekt en hersteld wordt, voordat het programma op de markt gebracht wordt. Maar deze storingen bij de gebruiker (ongewenste mogelijke consequentie) kunnen voorkomen worden door bijvoorbeeld het nakijken van de software op programmeerfouten en het testen van de software, voordat deze op de markt gebracht worden. Dit is een meer voor de hand liggende aanpak dan te proberen de programmeerfout zelf te voorkomen.

Het proces van het ontdekken van een fout in combinatie met de analyse van het ontstane probleem en het identificeren en uitvoeren van herstelmaatregelen wordt in deze bijdrage het herstelproces genoemd. Als de herstelacties tijdig en effectief zijn, kunnen we spreken van een bijna-ongeval, waarbij geen negatieve consequenties overblijven. Ook bij heuse ongevallen waarbij dus wel ongewenste gevolgen opgetreden zijn, zoals schade, letsel, productieverlies of -vertraging, kunnen toch herstelacties toegepast zijn. In deze gevallen zijn de herstelacties weliswaar niet geheel succesvol geweest, maar hebben ze wel tot een beperking van de gevolgen bijgedragen.

In het herstelproces spelen vooral mensen een belangrijke rol, omdat deze hun kennis en ervaring op creatieve wijze ad hoc kunnen gebruiken om tot nieuwe oplossingen en tegenmaatregelen te komen voor problemen en fouten die ze niet eerder hebben meegemaakt – iets waar technische systemen (apparaten, installaties) en de door de organisatie geboden voorzieningen (zoals procedureboeken, werkinstructies), op zichzelf minder goed in zijn [Schaaf, 2000]. Uit hoofdstuk 29 blijkt ook dat als het personeel de ruimte krijgt om zelf beslissingen te nemen, de storingen duidelijk afnemen en de herstelperiode wordt verkort. Voor het ontwerpen van systemen waarin deze herstelmogelijkheden voor een menselijke operator optimaal aanwezig zijn, is een belangrijke rol weggelegd voor de hedendaagse technologie en vooral voor ICT [Kontogiannis, 1999; Kanse, 2000b].

Het herstelproces

Een algemeen geaccepteerde onderverdeling van het herstelproces (zie bijvoorbeeld [Schaaf, 1988; Zapf, 1994; Kontogiannis, 1999]) onderscheidt de fasen detectie (van het feit dat een fout is opgetreden, dat er iets mis is), lokalisatie (van de oorzaken van deze fout) en correctie (van de fout door het plannen en toepassen van herstelacties).
Om de functie en werking van een willekeurig herstelproces te verduidelijken is in figuur 33.1 een model van het herstelproces opgenomen.



Figuur 33.1
Model van het herstelproces.

Dit model is een Nederlandstalige versie van het model dat door Kanse en Van der Schaaf is opgesteld op basis van inzichten verkregen in een uitgebreide literatuurstudie en een casestudie [Kanse, 2000b] in de chemische procesindustrie waarbij vijftig zeer uiteenlopende voorvallen met een duidelijke herstelcomponent geanalyseerd zijn.
Figuur 33.1 maakt duidelijk welke functie het herstelproces heeft in gevallen waarin door een willekeurig faalproces (elke mogelijke combinatie van technische en of organisatorische en of menselijke faalfactoren) een gevaarlijke of ongewenste situatie is ontstaan [Schaaf, 1992]. Detectie van deze situatie is altijd de eerst optredende fase van het herstelproces. Hierbij kan het zowel om geplande detectie gaan (als het een voorzien probleem is waarvoor detectiemethoden zijn 'ingebouwd') als om spontane, niet geplande detectie (waarbij geen vast omschreven procedures of hulpmiddelen gebruikt worden). Na de detectiefase kan een onmiddellijke correctieve actie uitgevoerd worden (een 'quick fix'), bijvoorbeeld als dat nodig is vanwege tijdsdruk, of er volgt eerst een lokalisatiefase waarin een verklaring voor het probleem wordt gezocht, voordat correctieve maatregelen gepland en uitgevoerd worden. Ook correcties gericht

op de lange termijn, bijvoorbeeld om herhaling van het probleem te voorkomen of om beter daarop voorbereid te zijn, vallen onder de correctiefase. Herhalingen van de lokalisatie- en correctiefasen, zoals is aangegeven door de pijlen, kunnen voortduren tot het probleem verholpen is of er verder niets gedaan kan worden. Voor de lokalisatie- en correctiefase geldt ook dat hier zowel geplande voorziene acties ondernomen kunnen worden (eventueel zelfs automatisch) als ongeplande acties die op het moment zelf pas bedacht en uitgevoerd worden.

Na afloop van alle herstelacties kan de vraag gesteld worden of het herstelproces succesvol is geweest. Is dat zo, dan is het resultaat van het hele proces (faal- en herstelproces) een bijna-ongeval. Maar in gevallen waar het herstel niet geheel tijdig en of effectief is uitgevoerd, blijven er toch negatieve gevolgen van het oorspronkelijke faalproces over, en is er nog sprake van een incident of ongeval (zij het waarschijnlijk minder ernstig dan het had kunnen zijn). Met betrekking tot de kans op succesvol herstel is vastgesteld dat dit onder andere afhangt van het soort voorafgaande fout [Embrey, 1988]. Herstel van fouten die onbedoeld tijdens een handeling optreden, is bijvoorbeeld waarschijnlijker dan herstel van denk- of redeneerfouten.
Een laatste vraag die in beide gevallen nog gesteld moet worden is of de herstelacties onbedoelde neveneffecten hebben gehad (als het probleem wel verholpen is, maar een nieuw probleem ontstaan is). Als dat het geval is, begint het proces weer van voren af aan, waarbij de onbedoelde neveneffecten het faalproces beïnvloeden.

Als we de hier genoemde inzichten samenvatten, kan gesteld worden dat herstel een belangrijke rol speelt in het functioneren en de prestaties van organisaties en dat er consensus bestaat over de verschillende fasen waaruit het herstelproces is opgebouwd: detectie, verklaring of lokalisatie, en correctie.

Conclusies

Omdat bij het management van betrouwbaarheid, veiligheid en kwaliteit in organisaties niet alle fouten voorzien kunnen worden, en zelfs niet alle voorziene fouten voorkomen kunnen worden, is het ondersteunen van herstel belangrijk als aanvulling op, en niet als alternatief [Keyser, 1995] voor de klassieke benadering waarbij preventie van fouten centraal staat. Gegeven het belang van herstelgedrag, is het voor de ontwerpers van mens/machinesystemen belangrijk rekening te houden met herstelmogelijkheden bij ontwerp en herontwerp. Om menselijke herstelacties optimaal te ondersteunen dient men aandacht te schenken aan de waarneembaarheid, de traceerbaarheid en de omkeerbaar-

heid van fouten en problemen. Hierbij gaat het niet alleen om fouten en problemen die reeds bij het ontwerpen van een systeem met behulp van risicoanalyses te voorzien zijn. Bij voorkeur moeten er ook algemenere voorzieningen getroffen worden die detectie, lokalisatie en correctie van onverwachte problemen mogelijk maken. Daarnaast dient men er rekening mee te houden dat door het te ver doorvoeren van automatisering de mogelijkheden voor de mens om zelf nog in processen in te grijpen te beperkt kunnen worden. Hierdoor raken dus ook de mogelijkheden tot herstel door de mens uitgeput.

Referenties

- Embrey, D.E., D.A. Lucas. (1988). The Nature of Recovery from Error. In: L.H.J. Goossens (ed.). Human Recovery. Proceedings of the COST A1 Seminar on Risk Analysis and Human Error. Delft University of Technology
- Frese, M. (1991). Error Management or Error Prevention: Two Strategies to Deal with Errors in Software Design. In: H.J. Bullinger (ed.). Human Aspects in Computing: Design and Use of Interactive Systems and Work with Terminals. Elsevier Science Publishers, Amsterdam. pp776-782
- Kanse, L., T.W. van der Schaaf. (2000a). Recovery from Failures – Understanding the Positive Role of Human Operators during Incidents. In: D. de Waard, C. Weikert, J. Hoonhout, J. Ramaekers (eds.). Proceedings Human Factors and Ergonomics Society. Europe Chapter Annual Meeting 2000. Maastricht. November 1-3, pp367-379
- Kanse, L., T.W. van der Schaaf. (2000b). Toepassing van ICT bij het herstellen van fouten. Gedrag en Organisatie **6**:360-374
- Keyser, V. de. (1995). Evolution of Ideas Regarding the Prevention of Human Errors. Paper presented at the Man-Machine Systems (MMS '95) Symposium of June 27-29. MIT, Cambridge, MA
- Kontogiannis, T. (1999). User Strategies in Recovering from Errors in Man-Machine Systems. Safety Science **32**:49-68
- Schaaf, T.W. van der. (1988). Critical Incidents and Human Recovery: Some Examples of Research Techniques. In: L.H.J. Goossens (ed.). Human Recovery. Proceedings of the COST A1 Seminar on Risk Analysis and Human Error. Delft University of Technology
- Schaaf, T.W. van der. (1992). Near Miss Reporting in the Chemical Process Industry. PhD thesis. Eindhoven University of Technology
- Schaaf, T.W., van der, L. Kanse. (2000). Errors and Error Recovery. In: P.F. Elzer, R.H. Kluwe, B. Boussoffara (eds.). Human Error and System Design and Management. Springer Verlag, London. pp27-38
- Zapf, D., J.T. Reason. (1994). Introduction: Human Errors and Error Handling. Applied Psychology. An International Review **43** (4):427-432

3

34 Anticiperen op trends

prof.dr.ir. A.C. Brombacher[1]*, dr. M.R. de Graef*

Inleiding

Zoals reeds eerder in dit boek is beschreven is het voorspellen van kwaliteit en bedrijfszekerheid[2] essentieel voor een modern ontwikkelproces. Dit betekent dat bedrijven zich niet alleen dienen te concentreren op het vinden en herstellen van fouten in bedrijfszekerheid, maar ook op het voorspellen en voorkomen van dergelijke problemen. De meeste bedrijven hebben wel vaak zeer goed uitgewerkte procedures over hoe om te gaan met fouten. Het voorkomen van fouten echter is voor veel bedrijven relatief nieuw. Gezien een aantal trends die nader in dit hoofdstuk besproken zullen worden, is juist de combinatie van deze twee factoren essentieel voor het succesvol beheersen van kwaliteit en bedrijfszekerheid. Dit hoofdstuk besteedt daarom aandacht aan de volgende punten:

- Wat zijn recente ontwikkelingen in bedrijfsprocessen en welke invloed hebben zij op kwaliteit en bedrijfszekerheid.
- Wat betekenen kwaliteit en bedrijfszekerheid tegenwoordig vanuit het perspectief van de klant.
- Wat zijn op dit moment de beste voorspellende modellen en zijn deze modellen bruikbaar in de hedendaagse industrie.
- Zo nee, wat zijn de eisen die gesteld kunnen worden aan de ontwikkeling van toekomstige modellen voor kwaliteit en bedrijfszekerheid.

1 Technische Universiteit Eindhoven, Faculteit Technologie Management
Postbus 513
5600 MB Eindhoven

2 Voor de definitie van bedrijfszekerheid zie hoofdstuk 2, deel 1.

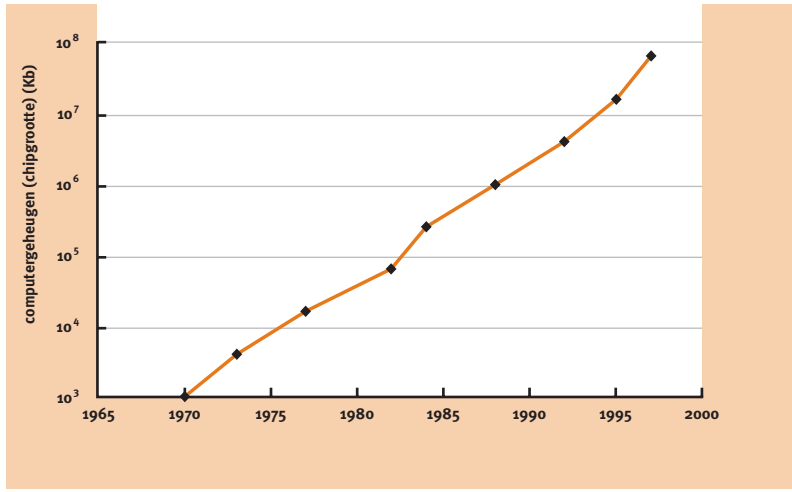
Bedrijfszekerheid: een veranderend perspectief

Bedrijfszekerheid kan niet los gezien worden van een aantal trends die een dominante rol spelen bij de ontwikkeling en de productie van moderne producten. Ook recente veranderingen in de houding van gebruikers ten opzichte van de kwaliteit en daarmee ook de bedrijfszekerheid van producten zijn in dit kader zeker relevant. Al deze zaken zijn de laatste twintig jaar sterk aan verandering onderhevig geweest. De methoden en technieken voor het analyseren en voorspellen van bedrijfszekerheid zijn in deze periode echter conceptueel weinig veranderd. De volgende paragrafen bespreken een aantal belangrijke trends en hun invloed op het concept bedrijfszekerheid. De paragrafen daarna beschrijven een aantal concepten die op een effectieve manier kunnen bijdragen (of dat in de toekomst zouden kunnen doen) aan het beheersen van huidige en toekomstige producten.

Toenemende complexiteit

Een van de factoren die het voorspellen van de bedrijfszekerheid bijzonder lastig maakt is de toenemende complexiteit van producten. Vooral in de elektronica en de daaraan gerelateerde informatietechnologie vond er gedurende de laatste decennia een revolutie plaats. En deze revolutie loopt vandaag de dag nog onverminderd door. De bekende wet van Moore laat zien dat gedurende de afgelopen jaren de complexiteit van belangrijke bouwstenen zoals microprocessors, computergeheugen en andere systemen voor dataopslag en verwerking een constante groei liet zien. Gedurende dezelfde tijd is de prijs van dergelijke bouwstenen nauwelijks veranderd. De prijs van een recente harddisk van 20GB is ongeveer hetzelfde als de prijs van een schijf van 20MB tien jaar geleden. De door deze toegenomen complexiteit verkregen functionaliteit wordt niet alleen gebruikt in de elektrotechniek en de informatica, maar ook ver daarbuiten. Moderne besturingssystemen, zoals die worden gebruikt in de procesindustrie, bij de spoorwegen, in de luchtvaart of bij moderne financiële transacties, zijn nauwelijks denkbaar zonder toepassing van moderne elektronische dataverwerkingssystemen.

Met behulp van deze steeds complexere bouwstenen kunnen bedrijven producten maken met steeds meer mogelijkheden. Om deze producten ook daadwerkelijk op de markt te kunnen afzetten zullen deze bedrijven gebruik moeten maken van zeer korte marktvensters. Brengt iemand een product te laat op de markt, dan betekent dat niet alleen dat dit product dient te concurreren met vergelijkbare producten die reeds eerder op de markt kwamen (voordeel van een hogere marktpenetratie) en met technologisch recentere producten die voor dezelfde prijs meer functionaliteit bieden. Voor veel fabrikanten ontbreekt vaak



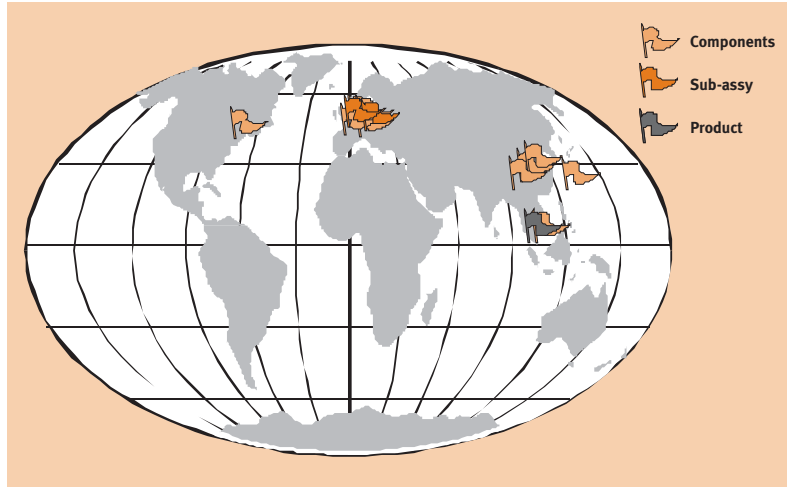
Figuur 34.1
Toenemende complexiteit van producten. Bron: VLSI Research Inc.

ook de tijd om via een vaak tijdrovende test en een validatieprogramma zeker te kunnen stellen dat ook het nieuwe product geen kinderziekten bevat.

Globalisering en segmentering van bedrijfsprocessen

Een tweede trend met een sterke invloed op de bedrijfszekerheid van producten is het effect van de mondiale economie. Veel bedrijven richten zich op hun zogenaamde kerntaken. Dit betekent in de praktijk vaak dat bedrijven die mogelijkheden zien om een deel van hun activiteiten uit te besteden, dit zeker zullen overwegen als het economisch gerechtvaardigd is. Bedrijven kunnen het economisch voordeel van het uitbesteden maximaliseren door globaal te opereren. Vanwege de toegenomen mogelijkheden op het gebied van logistiek en transport (en indirect ook door de miniaturisering) worden dit soort mondiale ketens praktisch mogelijk. Het is op dit moment niet ongebruikelijk dat bijvoorbeeld een geïntegreerde schakeling ontworpen wordt in de VS, wordt geproduceerd in Europa, wordt geassembleerd in Azië, en ingebouwd in een eindproduct in Zuid-Amerika. Hoewel een dergelijk proces op het eerste gezicht tamelijk inefficiënt lijkt, kan het toch economisch zinvol zijn. Voor de hand liggende redenen zouden bijvoorbeeld kunnen zijn dat voor de ene operatie de ene regio beter geschikt is (betere kennis en of infrastructuur), terwijl voor de andere stap een andere regio beter past (loonkosten). In die gevallen waar de logistieke meerkosten niet opwegen tegen regionale economische voordelen zal een dergelijke structuur snel gemeengoed worden. Figuur 34.2 laat het ontwikkelproces van een cd-speler zien met alle daarbij betrokken partijen en hun geografische locatie.

Vergelijkbare situaties gelden voor het ontwerp- en fabricageproces van auto's en vliegtuigen, maar ook voor infrastructurele projecten als havens en vliegvelden. Deze mondiale processen stellen echter niet alleen extra eisen aan logistieke processen, maar ook zoals later in dit hoofdstuk zal worden toegelicht aan



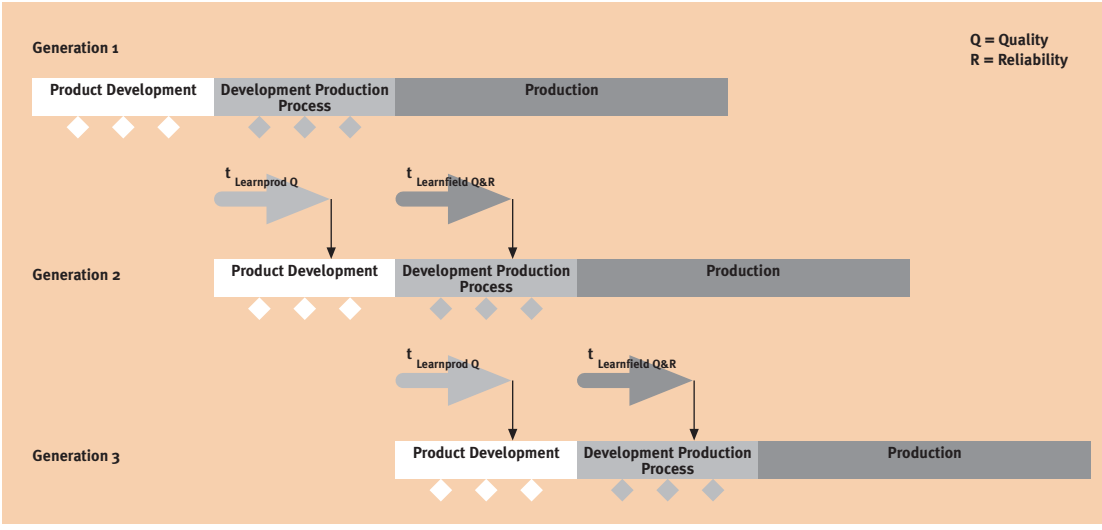
Figuur 34.2
Globalisering van de product-ontwikkeling.

de gekozen structuur voor informatie en communicatie. Er zijn de laatste jaren veel systemen op de markt gekomen die informatiebeheer in bedrijfsprocessen op mondiale schaal mogelijk maken. Voorbeelden zijn financiële systemen en logistieke systemen zoals ERP (Enterprise Resource Planning). Een bijzonder lastig type informatie bij dit soort mondiaal opererende systemen is vooral de informatie over kwaliteit en bedrijfszekerheid. Deze informatie laat zich namelijk bijzonder moeilijk a priori structureren. De werkelijke bedrijfszekerheid van een product is vooral bij sterk innovatieve producten sterk afhankelijk van de uiteindelijke interactie van het eindproduct met de eindgebruiker. Vanwege de grote onvoorspelbaarheid en de vrij geruime tijd die nodig kan zijn om dergelijke informatie te vergaren past dit soort informatie slecht in rigide informatiesystemen. Kleine veranderingen bijvoorbeeld in een lokaal fabricageproces bij een subcontractor kunnen nauwelijks de moeite van het vermelden waard lijken en kunnen vaak niet in een informatieverwerkingssysteem opgenomen worden. Toch is het niet uit te sluiten dat deze ogenschijnlijk kleine veranderingen grote gevolgen hebben voor het eindproduct in het veld. Als een proces in een goed gedefinieerde structuur in één organisatie plaatsvindt, zal de informele communicatie vaak dienen als vangnet voor dergelijke problemen. Bij mondiaal verlopende processen met sterk wissende samenwerkingsverbanden (en daaraan gerelateerde personele wisselingen) is het goed mogelijk dat de opbouw van kennis over en ervaring met kwaliteit en bedrijfszekerheid veel minder of in het geheel niet plaatsvindt. In een dergelijke keten is de verantwoordelijkheid voor de kennis en ervaring op dit gebied immers lastig te bepalen.

De invloed van time to market

Een derde trend met invloed op de kwaliteit en de bedrijfszekerheid heeft te maken met de zeer sterke druk op ‘time to market’ die in veel sectoren gevoeld wordt. Vanwege de eerdergenoemde aanhoudende groei in technologische

mogelijkheden kunnen fabrikanten slechts gebruik maken van smalle tijdvensters. Door de eerdergenoemde mondiale economie spelen ook concurrentieprocessen op wereldwijde schaal. Het bedrijf dat waar ook ter wereld in staat is een nieuw product op het juiste moment op de markt te zetten kan het voor dit product aanwezige tijdvenster dan ook maximaal benutten. Bekende voorbeelden hiervan zijn te vinden in bijvoorbeeld de consumentenelektronica, maar ook in de financiële dienstverlening (elektronisch bankieren), de telecommunicatie (mobiele telefonie) en de procesindustrie (het gebruik van programeerbare elektronische systemen bij procesbesturing of veiligheidsbewaking). In al deze gevallen volgen nieuwe technologische mogelijkheden elkaar met een steeds grotere frequentie op. Hierdoor wordt voor fabrikanten de tijd tussen het beschikbaar komen van een nieuwe technologie en het daadwerkelijk toepassen van deze technologie in nieuwe producten steeds korter. Als gevolg hiervan zien veel bedrijven zich genoodzaakt te zoeken naar alternatieven voor de klassieke vaak sequentiële ontwikkelprocessen.



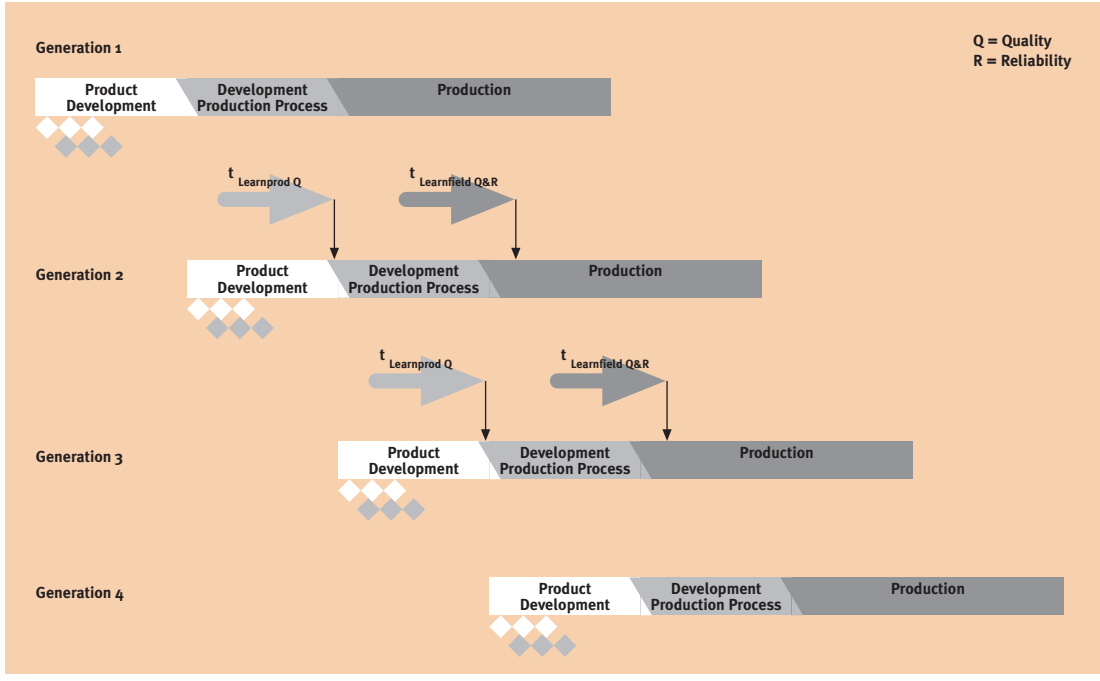
Figuur 34.3
Leren van problemen met bedrijfszekerheid in een klassiek ontwikkelingsproces.

Een van de grootste problemen in een slecht beheerst ontwikkeltraject kan zijn dat een ondeugdelijk of niet uitgerijpt product de productiefase – of erger nog – de markt bereikt. In dit geval moet een fabrikant het productieproces omstellen (met alle kostbare en tijdrovende gevolgen van dien) of moet zelfs een product uit de markt terugroepen. Om te voorkomen dat problemen veroorzaakt in de ene fase doorschuiven naar een volgende fase hebben veel bedrijven in de jaren zeventig en tachtig het ontwikkelproces opgedeeld in functionele blokken, gescheiden door zogenaamde mijlpalen ('milestones'). Voor een dergelijke mijlpaal wordt via uitgebreide verificatie en via testplannen vastgesteld of een product rijp is om verder te gaan naar een volgende fase. Hiermee wordt voorkomen dat bijvoorbeeld problemen die in de ontwikkelfase met een eenvoudige

wijziging te verhelpen waren, onopgemerkt blijven tot de productie of zelfs tot na de marktintroductie met alle kostbare gevolgen van dien.

In het geval dat een fabrikant van tevoren zou weten dat alle zaken die bij een dergelijke mijlpaal naar voren komen al op de een of andere manier afgedekt zouden zijn, zou dit theoretisch een enorm voordeel kunnen geven. Allereerst zouden de vaak zeer kostbare en tijdrovende testen bij een mijlpaal overgeslagen kunnen worden. Een tweede waarschijnlijk nog veel groter voordeel zou daarnaast kunnen zijn dat een aantal activiteiten in de latere fase van het proces alvast zouden kunnen starten op grond van voorinformatie. Als men weet dat een bepaald onderdeel met een lange levertijd (een IC, een spuitgietmal of in een heel andere sector een sluisdeur) toch niet meer wijzigt als gevolg van het testen bij een mijlpaal, kan men dat bewuste onderdeel al in een veel vroegere fase bestellen. Dankzij dit parallel (of 'concurrent') uitvoeren van activiteiten, bereikt men wederom een significante besparing op het totale tijdtraject. Een dergelijk 'Concurrent Engineering'-proces stelt dan ook zeer hoge eisen aan de voorspellende modellen. Op het moment dat men activiteiten onterecht vroegtijdig heeft gestart zal wegens het verder ontbreken van mijlpalen het probleem ook pas zeer laat naar voren komen.

Figuur 34.4
Leren van problemen met bedrijfszekerheid in een modern ontwikkelingsproces.



Het gebruik van dergelijke voorspellende technieken levert echter een interessante paradox op. In een klassiek ontwikkelproces vinden correctieve acties plaats op het moment dat bijvoorbeeld bij een test blijkt dat het product niet

aan de gestelde eisen voldoet. De noodzaak van correctieve acties staat niet ter discussie, omdat men zeker weet dat een probleem ook echt bestaat. De bijbehorende correctieve acties, hoewel vaak zeer kostbaar en verre van efficiënt, zullen worden uitgevoerd en succes daarvan wordt in organisaties zeer gewaardeerd.
Het nemen van preventieve maatregelen om potentiële problemen reeds vroeg in het ontwikkelproces op te lossen levert echter vaak discussies op over de validiteit van de gebruikte voorspellende modellen, de noodzaak om actie te ondernemen en de kans dat een potentieel probleem 'toch wel zal verdwijnen'.
Een speciaal probleem bij het gebruik van voorspellende technieken vormen de problemen met kwaliteit en bedrijfszekerheid. Een zuiver Concurrent Engineering-proces eist dat er reeds in de vroege fasen van een project vergaande kennis bestaat over de uiteindelijke interactie tussen product en gebruiker. En zoals eerder opgemerkt kan de geboden functionaliteit ten gevolge van de hoge innovatiesnelheid in sterke mate verschillen van de functionaliteit van vorige generaties producten. Indien de tijd benodigd voor de validatie van de gebruikte voorspellende modellen voor kwaliteit en bedrijfszekerheid constant zou blijven, betekent dit dat de lessen geleerd in productgeneratie n beschikbaar komen op het moment dat alle beslissingen voor generatie n+1, n+2 en wellicht ook n+3 al genomen zijn. Aangezien de technologische verschillen tussen generatie n en generatie n+3 aanzienlijk kunnen zijn, betekent dit ook dat daarmee de validiteit van de bij generatie n+3 gebruikte voorspellende modellen ter discussie staat.

De veranderende rol van de klant

Om vroeg in het ontwikkelproces een uitspraak te kunnen doen over de kwaliteit en bedrijfszekerheid van een product is het belangrijk om te weten wat deze termen vanuit het perspectief van de klant precies betekenen. Een veel gebruikte definitie voor kwaliteit is [Lewis, 1996]: "The ability of a product to fulfil its intended purpose."
Vergelijkbaar definieert Lewis bedrijfszekerheid als [Lewis, 1996]: "The ability of a product to fulfil its intended purpose for a certain period of time."

Beide definities vertonen een grote gelijkenis. Het enige verschil is het gebruik van de factor 'tijd'. Het probleem ligt bij deze definitie echter vooral in het gebruik van de term 'intended purpose'. Voor een gebruiker van een product kan dit iets geheel anders betekenen dan datgene wat de fabrikant voorzien had. Gezien de eerdergenoemde sterke innovatie is het bovendien vaak bijzonder moeilijk te voorzien hoe een gebruiker op een nieuwe techniek zal reageren. Enerzijds komt dit, omdat het voor hedendaagse producten bijzonder lastig is een 100% dekkende specificatie vast te stellen. En mocht zo'n specificatie bestaan, dan heeft deze voor de klant vaak een beperkte waarde. De waarde

van een product wordt niet alleen bepaald door de specificatie, maar ook door de mate waarin het product in staat is datgene te doen wat de klant van het product verlangt. Dit geldt voor consumentenproducten, maar ook voor professionele producten zoals medische systemen en watersteppers.

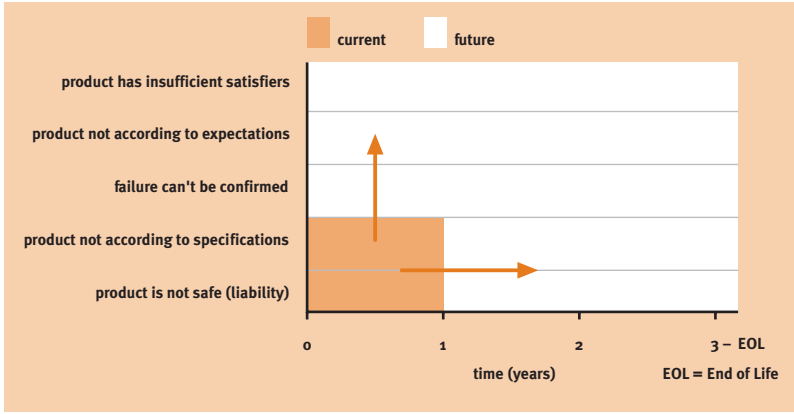
In het algemeen lijkt de houding van klanten namelijk te verschuiven van 'productgericht' naar 'functiegericht' of zelfs 'dienstgericht'. Ook hier treedt een interessante paradox naar voren. Veel moderne zeer complexe producten of systemen verrichten namelijk vanuit het perspectief van de klant relatief simpele functies. Veel klanten beseffen slechts in geringe mate welke technologie nodig is voor het voeren van een simpel telefoongesprek met een GSM-telefoon of om het mogelijk te maken dat een klant met zijn Nederlandse bankpas geld kan opnemen bij een willekeurige geldautomaat in Singapore. Ook de grote hoeveelheid veelal zeer complexe systemen die moeten samenwerken om een vliegtuig van A naar B te brengen ontgaat de meeste reizigers in de meeste gevallen. Men verwacht een bepaalde functie of dienst ongeacht de complexiteit van het onderliggende systeem.
Wat nog veel minder gebruikers (en soms zelfs ontwerpers of beheerders) van dergelijke systemen beseffen is hoe groot de kwetsbaarheid van dergelijke systemen voor bewuste of onbewuste verstoringen ergens in de keten kan zijn. Aangezien de complexiteit en kwetsbaarheid van dergelijke producten (en de achterliggende ketens) bij veel gebruikers voor een groot deel onbekend zijn, is ook te verwachten dat de tolerantie voor problemen laag zal zijn. Zoals ook later in dit hoofdstuk zal worden toegelicht, tolereren gebruikers slechts in beperkte mate fouten in dergelijke systemen. Dit kan bijvoorbeeld geïllustreerd worden aan de hand van de mede onder druk van consumenten gewijzigde garantiebepalingen voor consumentenproducten.

Tabel 34.1
Wijzigingen in productgarantie tussen 1989 en 1999 [Philips, 1989, Philips, 1999].

	1989	**1999**
Warrantee period	6 month – 1 year	3 years
Failures covered	Material defects	Any customer complaints
First line support	Dealer/service organisation	Helpdesks (free phone number)
Logistics	Via service centre 3 years	Replacement at home

Waar in het verleden garantie zich beperkte tot het vervangen van defecte componenten gedurende bijvoorbeeld een jaar, ontstaat er de laatste jaren steeds meer een 'no questions asked policy' waarbij de klant bij elke willekeurige klacht een nieuw product ontvangt of zelfs de aankoopkosten terugkrijgt. Deze uitbreiding in de dekking is ontstaan onder druk van consumentenorganisaties, wetgevers (zie de nieuwe wet op de productaansprakelijkheid) en concurrentie. Voor fabrikanten betekent dit dat een veel verdergaande kennis over achter-

Figuur 34.5
Trends in bedrijfszekerheid in relatie tot klanteneisen.



gronden van klantenklachten vereist is. Men zal in staat moeten zijn ook deze nieuwe klachtenstroom te kennen en te beheersen om onaangename verassingen te voorkomen.

Een factor die het beheersen van juist deze nieuwe aspecten van bedrijfszekerheid aanzienlijk bemoeilijkt is de kwetsbaarheid van veel moderne systemen voor (onverwachte of onbedoelde) externe invloeden. Deze externe invloeden kunnen variëren van klanten die een product op een onvoorziene wijze gebruiken[3] tot opzettelijk of zelfs crimineel misbruik zoals de makers van computervirussen of het optreden van 'hackers'. Zoals aangegeven in hoofdstuk 11 zijn twee belangrijke redenen voor het 'succes' van virussen als 'I love you' het onvoorziene gebruik en of misbruik van de interne adressendatabase van Outlook gecombineerd met de zeer omvangrijke integratie van Internet in de kantoor- en privé-omgeving.

Een en ander betekent dat als men bovenstaande brede en klantgerichte definitie van bedrijfszekerheid hanteert men te maken krijgt met een verschuiving van zuiver productgericht naar de functie of dienst die van een dergelijk product wordt verwacht. Dit betekent dan automatisch dat meer aandacht besteed dient te worden aan het product in interactie met zijn omgeving, waarbij juist de extreme interacties niet vergeten dienen te worden.

Relaties tussen trends en de huidige problemen met bedrijfszekerheid

Bij een nadere analyse van de cases uit deel 2 van dit boek blijkt dat veel van deze cases een nauwe relatie hebben met een of meer van de hiervoor genoemde trends. Tabel 34.2 geeft een overzicht van de relaties tussen de genoemde trends en de problemen (of oplossingen) die in de cases naar voren komen.

3 Bijvoorbeeld het afbreken van antennes in de eerste generatie GSM-telefoons. Niemand had verwacht dat de antenne als handvat gebruikt zou worden.

Tabel 34.2
Verdeling naar de belangrijkste trends van de cases van deel 2.

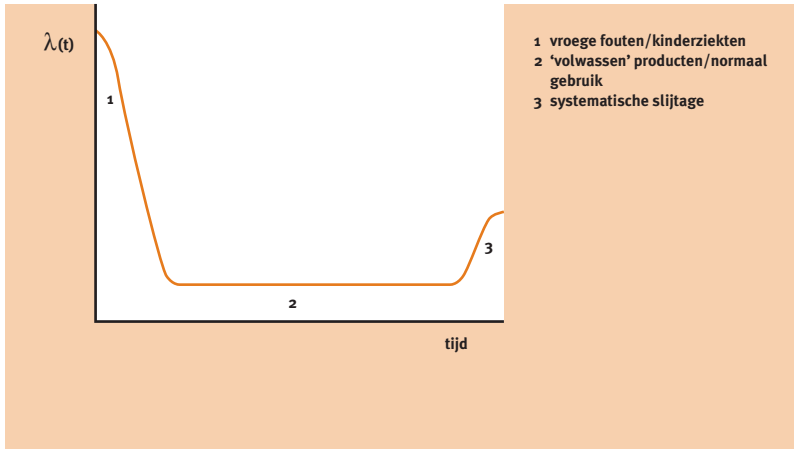
case/hoofdstuk		complexiteit van het product/innovatiegraad	structuur van het bedrijfsproces (gesegmenteerd)	time to market/tijdsdruk	klanteneisen (functional correctness)	klanteneisen (kwetsbaarheid voor externe invloeden)
4	Relatie tussen de diverse bedrijfsprocessen	•			•	•
6	Veiligheid in de procesindustrie	•	•			
10	Informatie- en communicatietechnologie	•	•			•
11	Betrouwbaarheid digitale ruimte		•			•
12	Betrouwbaar ontwerp verkeersvliegtuigen	•	•	•	•	
13	Integraal software testen en de marsmissies	•	•	•	•	
14	Bouwvergunningen tunnels HSL-Zuid		•		•	•
15	Sorteersysteem PTT Post	•		•	•	
16	Verantwoordelijkheid voor ketens in het Internet	•	•			•
17	De betrouwbaarheid van optische disksystemen	•		•		
18	Punctualiteit in het reizigersvervoer per trein	•	•			•
19	Betrouwbaarheid in de mobiele telecommunicatie	•	•	•	•	
20	Probabilistisch ontwerp stormvloedkering	•				•
21	Rol overheid bij betrouwbare levering elektricititeit		•			
22	Betrouwbaarheid en kwaliteit in de gezondheidszorg		•		•	•
23	Vliegtuigafhandeling op luchthavens	•	•	•		
24	Invoering IEC61508/61511 bij Shell		•		•	•
25	Helikopters in de offshore-industrie in de Noordzee	•		•	•	•
26	Betrouwbaarheid van samenwerkende organisaties	•	•			
27	Betrouwbaarheid in de voedingsmiddelenindustrie	•	•			•
28	Outsourcing in ICT	•	•			
29	Nieuw bedrijfsproces bij Unilever Bestfoods (TPM)			•	•	
30	Veiligheid in de nieuwe spoorwegwet	•	•			
31	Rol cryptografie in de geldautomaatomgeving	•			•	•
32	Gebruik risicoanalyse bij beslissingen	•				

De problemen zoals besproken in deel 2, kunnen als volgt samengevat worden:

- De toenemende complexiteit van producten maakt het testen en valideren van producten ook steeds complexer en daarmee ook duurder en tijdrovender.
- De toenemende complexiteit van (mondiale) bedrijfsprocessen met de daaraan gerelateerde eerdergenoemde problemen met informatiestromen en informatieoverdracht bedreigen de kennisopbouw van en de kennisuitwisseling over nieuwe producten en technologieën.
- De sterke druk op time to market vereist echter het gebruik van hoogwaardige voorspellende modellen en technieken.
- Vooral bij sterk innovatieve producten gebruikt in een complexe omgeving of infrastructuur blijft er (als gevolg van eerder onontdekte productproblemen of onverwachte applicatie- of omgevingsaspecten) een grote kans bestaan dat een aantal problemen met bedrijfszekerheid pas in het veld aan het licht zullen komen. Dit maakt de beschikbaarheid van een goed ontwikkeld, snel en efficiënt terugkoppelsysteem noodzakelijk.

De veranderende opvatting over voorspellingen over bedrijfszekerheid

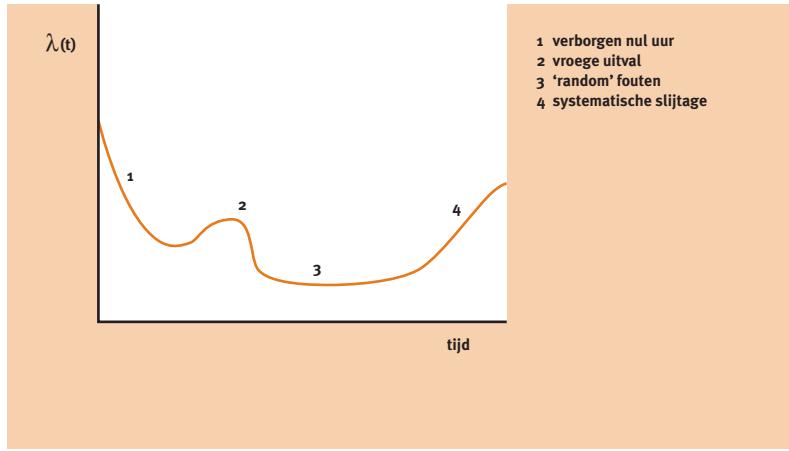
Het gebruik van voorspellende modellen bij bedrijfszekerheidanalyse is niet nieuw. Reeds in 1962 verscheen er naar aanleiding van de rapporten van de AGREE-werkgroep van het Amerikaanse Department of Defense [Coppola, 1984] het bekende Military Handbook 217 [Military Handbook, 1962]. Vooral de militaire industrie had een leidende rol bij de aanpak van problemen met bedrijfszekerheid. Deze aanpak concentreerde zich vooral op componenten die op dat moment de dominante categorie van veldproblemen vormden. De aanpak van dergelijke problemen was in die tijd eenvoudig, maar effectief. Het gedrag van de componenten werd beschreven aan de hand van de welbekende klassieke 'badkuip'curve (zie figuur 34.6 en hoofdstuk 4).



Figuur 34.6
De klassieke badkuipcurve.

De drie fasen in dit model kenmerken zich door de volgende eigenschappen:
- Fase 1: vroege fouten en of kinderziekten als gevolg van ontwerp- of fabricageproblemen.
- Fase 2: 'volwassen' producten gedurende normaal gebruik.
- Fase 3: producten onderhevig aan slijtage.

Voorspellende modellen beperkten zich in die tijd vaak tot fase 2; het praktisch belang van fase 1 en 3 was in die tijd beperkt. Met behulp van strenge testprocedures trachtte men in fase 1 fouten reeds in de fabriek 'uit te testen'. Pas op het moment dat men met enige zekerheid kon vaststellen dat het risico op fouten in fase 1 gering was, werden producten vrijgegeven voor gebruik in het veld. Op het moment dat ondanks onderhoud effecten van slijtage systematisch naar voren kwamen (fase 3) werden producten vervangen door nieuwe producten. In de praktijk betekende dit dat de militaire industrie (maar ook veel bedrijven op andere gebieden) bij de voorspelling bedrijfszekerheidsmodellen hanteerde die zich beperkten tot het gedrag van componenten gedurende fase 2 (constante faalfrequentie).
Hoewel dergelijke voorspellende modellen nog veel gehanteerd worden, roept het toepassen van dergelijke strategieën op moderne producten een aantal vragen op:
- Domineren componenten op dit moment nog het gedrag van producten als het gaat om bedrijfszekerheid?
- Is het op dit moment nog mogelijk om bij sterk innovatieve producten te voldoen aan de stringente testeisen ter voorkoming van problemen in fase 1, gegeven de eerdergenoemde sterke druk op time to market[4]?
- Als dit niet mogelijk is, hoe kan men dan in de praktijk omgaan met problemen in fase 1?



Figuur 34.7
De 'roller coaster'-curve.

4 Op dit moment worden ook in de militaire industrie uitgebreide discussies gevoerd over het toepassen van COTS (Commercially Off The Shelf)-componenten. Men heeft daar de keuze tussen weliswaar grondig geteste MILSPEC-componenten met een betrekkelijk geringe functionaliteit of commerciële componenten met een veel uitgebreidere functionaliteit (en vaak ook een aantrekkelijkere prijs), maar met een veel beperkter test- en validatietraject.

De grote druk op time to market rechtvaardigt in ieder geval een nadere analyse van het eerste gedeelte van de levensduur van producten. Kim Wong [Wong, 1988] kwam reeds is 1988 tot de conclusie dat de 'failure rate'-curve niet uit drie, maar uit vier fasen bestaat.

Het is mogelijk deze vier fasen te beschrijven met behulp van het door de auteur voorgestelde 'Stressor-Susceptibility'-model [Brombacher, 1992; Brombacher, 1993]. Hoewel mathematisch vrij complex, is het mogelijk uit dit model de volgende beschrijvingen voor de vier fasen af te leiden:

- Verborgen nul-uurfouten: subpopulaties van producten die op het tijdstip t=0 niet aan klanteneisen voldoen. De vertraging tussen t=0 en het moment van optreden van een fout ligt hier vooral aan observatie- en of rapportage-vertragingen. De reden dat producten reeds op t=0 fouten kunnen bevatten kan liggen aan het feit dat het product binnen de leveranciersspecificatie valt, maar voor klanten niet acceptabel blijkt te zijn. Redenen voor dit soort fouten kunnen liggen aan onvolledige of vanuit het standpunt van de klant verkeerde specificaties.
- Vroege uitval: subpopulaties van producten die op zeker moment gewerkt hebben, maar als gevolg van producttoleranties of toleranties in gebruik[5] onverwachte (slijtage) fouten vertonen. Dit leidt tot situaties waar subpopulaties van producten frequent falen ver voordat dergelijk gedrag bij de hoofdpopulatie te zien is.
- 'Random' fouten: defecten als gevolg van random gebeurtenissen, hetzij intern in het product hetzij door externe gebeurtenissen waaraan het product wordt blootgesteld. Dergelijke fouten kunnen meestal optreden bij de gehele populatie producten.
- Systematische slijtage: fouten geïnitieerd door inherente slijtagemechanismen in het product. Dergelijke fouten treden over het algemeen op bij de gehele populatie, afhankelijk van leeftijd en gebruiksprofiel van het product.

Als gevolg van eerdergenoemde trends worden op dit moment fase 1 en 2 zeer relevant. Door de korte marktvensters worden producten op de markt gebracht, voordat de fouten in fase 1 en 2 'uitgetest' zijn. Vooral voor sterk innovatieve producten is het ook onwaarschijnlijk dat fase 4 (of zelfs fase 3) bereikt wordt. De kans is groot dat tegen de tijd dat een product dergelijk gedrag gaat vertonen er al betere en of nieuwere producten op de markt zijn die meer functionaliteit tegen lagere kosten bieden.

Het voorspellen van de bedrijfszekerheid zal zich dus steeds meer gaan concentreren op fase 1 en 2 van de 'roller coaster'-curve. Wil men vooral voor deze fasen bedrijfszekerheid succesvol kunnen voorspellen, dan betekent dit dus dat men gedetailleerde kennis dient te hebben over de te verwachten interactie

5 Inclusief het transport van leverancier naar de klant en de installatie van het product bij de klant.

tussen klant en product bij normaal en vooral bij extreem gebruik bij expliciete, maar ook bij impliciete productspecificaties. Bij extreem gebruik volgens impliciete specificaties dient men bijvoorbeeld te denken aan onverwachte (incidentele of opzettelijke) interacties met de omgeving of met andere producten in en buiten de formele specificatie van de leverancier. Het eerdergenoemde I love you-virus is een typisch geval waarbij grote problemen met een product zijn ontstaan in een situatie waarin de formele specificatie niet heeft voorzien.

In het verleden werden problemen wegens impliciete specificaties (of zelfs gebruik buiten specificaties) niet gezien als problemen met bedrijfszekerheid. Omdat zoals eerder vermeld de houding van een klant verschuift van productgericht naar functie- of dienstgericht, is het voor leveranciers steeds minder goed mogelijk om formele productspecificaties te gebruiken als begrenzing van de productkwaliteit.Ten eerste is het gegeven de huidige productcomplexiteit bijzonder lastig om een waterdichte specificatie te schrijven en ten tweede zijn de meeste gebruikers daarin maar ten dele geïnteresseerd. Indien klanten grote problemen hebben met producten buiten de formele specificaties, zal dit voor hen aanleiding zijn hun beklag te doen of een andere leverancier te zoeken.

Oorzaken van moderne problemen met bedrijfszekerheid

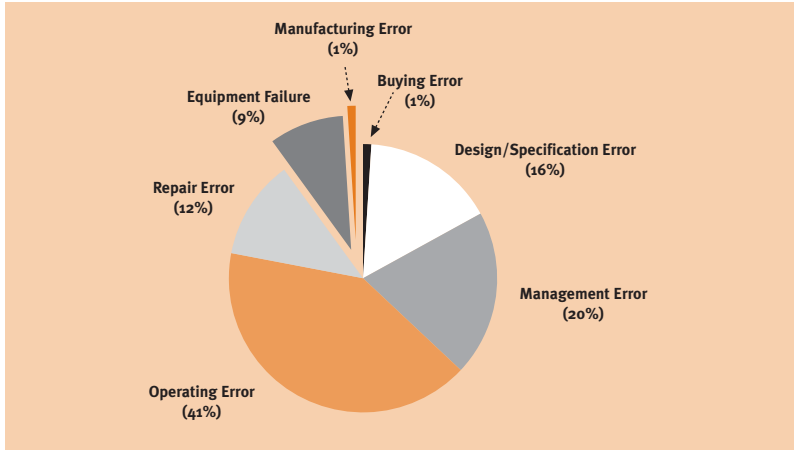
Uit de voorgaande paragrafen valt af te leiden dat in de bedrijfszekerheidstechniek een verschuiving plaatsvindt van aandacht die voornamelijk is gericht op fase 3 en 4 naar aandacht die zich steeds meer concentreert op fase 1 en 2. Om juist ook deze problemen in een hedendaagse bedrijfssituatie te kunnen hanteren is het nodig inzicht te hebben in mogelijke oorzaken van problemen tijdens de levenscyclus van een product. Tabel 34.3 geeft een vereenvoudigd overzicht van de aard van fouten in de verschillende fasen van het roller coaster-model.

Een van de belangrijke achtergronden van de problemen in fase 1 en 2 is dat fabrikanten niet in staat blijken te zijn een product te maken dat aan alle eisen van alle klanten voldoet. Het optreden van fase 1 en 2 kan verklaard worden uit

Tabel 34.3
Overzicht van de aard van fouten in de verschillende fasen van het roller coaster-model.

Phase	Characteristics	Statistical aspects
1	Failures due to mismatch between product functionality and customer use	Main population or subpopulations of products or users
2	Unexpected wear-out of subpopulations of products	Extreme user profiles or extreme product population (weak products)
3	Random failures	Transient often externally induced events resulting in failure of product
4	Systematic wear-out of the main population of product due to inherent end of life characteristics of product	Depending on time or use dependency of failure mechanisms in relation to customer use

het feit dat een aantal producten niet aan de klantenwensen kan voldoen of dat een aantal klanten niet tevreden zijn met wat het product hen te bieden heeft. Dit betekent dat men in het ontwikkelingstraject deze informatie niet ter beschikking heeft of dat deze informatie ergens in het proces verloren is gegaan.
Recent onderzoek, zoals gepubliceerd door Bradley in 1999 [Bradley, 1999] laat duidelijk zien dat een groot aantal van de problemen in recente industriële rampen te maken had met verkeerde informatie of met het ontbreken van informatie ergens in de keten. Slechts 10% van de problemen had volgens Bradley te maken met klassieke technische fouten in de bedrijfszekerheid.



Figuur 34.8
Bedrijfszekerheid in relatie tot bedrijfsprocessen.

Blijkbaar heeft de bedrijfszekerheid van een product niet alleen te maken met de technische structuur van het product, maar ook met de informatiestromen in de bijbehorende bedrijfsprocessen. Het lijkt daarom zinvol meer aandacht te besteden aan de rol van informatie en informatiestromen bij het verder beschouwen van bedrijfszekerheid.

Kwaliteit en betrouwbaarheid van informatie in bedrijfsprocessen

Reeds in 1971 liet Allen in een MIT-studie het belang zien van informatie tijdens de productontwikkeling [Allen, 1971; Allen, 1977]. In 1995 onderstreepten Eisenhardt en Brown in hun boek 'Product Development: Past Research, Present Findings and Future Directions' het grote belang van informatie in moderne productontwikkelprocessen[6]. Onderzoek aan de Technische Universiteit Eindhoven laat zien dat de beschikbaarheid van informatie alleen niet voldoende is voor het voorkomen van problemen met bedrijfszekerheid [Petkova, 1999] . Er kan een aantal redenen zijn om informatie over kwaliteit en bedrijfszekerheid te verzamelen:

6 Als een van de belangrijke redenen om multidisciplinaire teams te introduceren noemen zij: "the use of cross-functional teams increases the amount and the variety of information available" en dat: "the increased information helps the team to catch downstream problems such as manufacturing difficulties or market mismatches before they happen and are generally easier to fix." [Brown, 1995].

– *Meten*: het meest elementaire niveau van informatie over kwaliteit en bedrijfszekerheid heeft vaak te maken met logistiek. Zelfs als er geen plannen bestaan om de bedrijfszekerheid van huidige of toekomstige producten te verbeteren, zal een bedrijf om bedrijfseconomische redenen moeten weten hoeveel reparaties waar plaatsvinden. Hoewel men dit soort reparatieprocessen logistiek uitstekend kan optimaliseren, is er toch sprake van een inherent instabiel proces. Het beste dat men kan doen is de gegeven problemen zo efficiënt mogelijk verhelpen. Op grond van dergelijke informatie is immers nauwelijks af te leiden waarom dergelijke problemen zijn ontstaan en hoe ze zullen doorwerken in toekomstige generaties producten. Toch zijn er veel bedrijven [Petkova, 1999; Brombacher, 2001] – vooral bedrijven die het serviceproces hebben uitbesteed aan derden – die alleen dit soort informatie verzamelen.
– *Beheersen*: Wil men het hiervoor genoemde inherent onbeheerste proces gaan sturen en beheersen, dan dient men de beschikking te hebben over hoogwaardigere informatie. Hoeveel informatie men exact nodig heeft hangt af van een aantal factoren. Wil men een gegeven product kunnen verbeteren, dan dient men ten minste te weten welke producten waarom bij welke klanten falen (zie ook eerdere opmerkingen over fase 1 en 2 van de 'roller coaster-curve). Wil men ook bedrijfskundige achtergronden van problemen met bedrijfszekerheid kunnen aanpakken, dan dient men ook te weten waar zaken zijn fout gelopen in het bedrijfsproces. Vooral dit laatste aspect vereist dat men niet alleen informatie over het product en de klant heeft, maar ook over het ontwerp- en het fabricageproces, en over de informatie-uitwisseling tussen de hierbij betrokken partijen.
– *Preventie*: Als men op grond van eerder verkregen informatie besluit over te gaan tot preventieve maatregelen, dan zal de voorgaande informatie vertaald moeten worden naar (het ontwikkel-, het realisatie- en het gebruiksproces van) toekomstige producten. Dit vereist dat de informatie die is verkregen uit de analyse van eerdere producten van een dusdanige kwaliteit is dat niet alleen correctieve acties mogelijk zijn, maar dat de informatie ook op een zodanig abstractieniveau gebruikt kan worden dat deze kennis vroeg in het ontwikkelproces van toekomstige producten preventief toegepast kan worden.

Verschillende bedrijven kunnen verschillende redenen hebben om aan bedrijfszekerheid te werken. Bedrijven met een lage graad van innovatie waar bedrijfszekerheid een beperkte rol speelt, kunnen zich beperken tot het meten van bedrijfszekerheid en het optimaliseren van het bijbehorende logistieke serviceproces. Op het moment dat de kwaliteitskosten een grotere rol gaan spelen of wanneer de graad van innovatie dusdanig is dat het praktisch niet of nauwelijks meer mogelijk is klassieke kwaliteitsborging toe te passen, wordt het belangrijk

om op technisch en bedrijfskundig niveau in detail naar de oorzaken van problemen te gaan kijken. Wil men gedreven door een grote druk op time to market de kostbare (in tijd en geld) iteraties laat in het ontwerpproces voorkomen, dan dient men over dusdanige methoden en technieken te beschikken die een vroegtijdige voorspelling en optimalisatie van bedrijfszekerheid mogelijk maken. Een en ander stelt echter steeds hogere eisen aan de kwaliteit van de in het bedrijfsproces gehanteerde informatie.

Nieuwe eisen aan voorspellende methoden voor bedrijfszekerheid

Uit het voorgaande valt een aantal conclusies te trekken:

- In moderne tijdgedreven ontwikkelprocessen moeten zaken als kwaliteit en bedrijfszekerheid zo vroeg mogelijk meegenomen worden. Problemen die later opduiken kunnen voor een onaanvaardbaar grote vertraging zorgen.
- Dit vereist de beschikbaarheid van krachtige voorspellende modellen met een bewezen hoge correlatie met de dominante klassen van veldfouten.
- Hierbij is het onvoldoende de analyse te concentreren op het technische systeem alleen. De genoemde voorspellende modellen dienen ook effecten van (informatiepropagatie in) bedrijfsprocessen mee te nemen.
- Veld- (en productie)data dienen met dit doel snel en efficiënt vertaald te kunnen worden in hoogwaardige informatie die gebruikt kan worden bij een risicovoorspelling (en reductie) van toekomstige producten.
- Bij sterk innovatieve producten is het hierbij belangrijk dat ook fase 1 en 2 van de roller coaster-curve expliciet meegenomen kunnen worden.
- Voorspelling van fase 1 en 2 vereist een grondige (statistische) kennis van extremen in het product en in het productgebruik bij de klant.
- Het is hierbij belangrijk dat de voorspellingen zich niet beperken tot de expliciete specificaties zoals gedefinieerd door de leverancier, maar ook de vaak impliciete wensen van de klant meenemen.

De volgende paragrafen gaan nader in op een aantal van de genoemde eisen. Een belangrijke nadruk ligt hierbij op de rol van informatie en informatiepropagatie. Zowel de tijd die nodig is om (veld)gegevens om te zetten in informatie van voldoende kwaliteit als de tijd en de structuur die nodig is om dergelijke informatie in een organisatie efficiënt te verspreiden en te verwerken is hierbij belangrijk. Daarom wordt hier vooral de rol van informatie en de manier waarop de kwaliteit van deze informatie gebruikt kan worden als maatlat voor de volwassenheid van bedrijfsprocessen belicht.

Bedrijfszekerheid van producten in relatie tot de kwaliteit van bedrijfsprocessen

Uit het voorgaande is af te leiden dat een modern bedrijfsproces in regeltechnische termen eigenlijk 'pre-control' of vooruitkoppeling eist. Ter wille van een efficiënte bedrijfsvoering wil men potentiële risico's en problemen identificeren voor ze daadwerkelijk optreden. Dit vereist in het ideale geval een model van zowel het product als van het daaraan gerelateerde bedrijfsproces. Idealiter is een dergelijk model niet alleen in staat een accurate voorspelling uit te voeren, maar biedt ook inzicht in de stuur- of controleparameters waarmee men het product vroegtijdig kan optimaliseren. Hiermee zou het ontwerpen van een product op bedrijfszekerheid tot een (wiskundig) optimalisatieprobleem in de vroege fasen van de productontwikkeling worden. Er is een aantal redenen aan te geven waarom het onwaarschijnlijk is dat een dergelijk model op korte termijn gerealiseerd zal worden:

– *Gebrek aan stabiliteit van de huidige bedrijfsprocessen*. Zoals reeds eerder gemeld is het vakgebied van de productontwikkeling zeer dynamisch. De snelheid waarmee technologie, bedrijfsprocessen en klantengedrag veranderen is zodanig dat een voorspellend model dat al deze factoren op een praktisch bruikbare manier meeneemt waarschijnlijk verouderd is, voordat het uitontwikkeld is.
– *De complexiteit van menselijk handelen*. Hoewel veel bedrijven onvoorspelbaarheid trachten te reduceren met behulp van gestandaardiseerde procedures en werkmethoden, blijft productontwikkeling een proces waarin de menselijke creativiteit en inventiviteit een essentiële rol spelen. Sommige van deze activiteiten kunnen een onverwacht positieve invloed op de bedrijfszekerheid van een product hebben (herstelgedrag en improvisatievermogen bij onverwachte problemen), terwijl andere factoren een negatief effect kunnen hebben (menselijke fouten). Het maken van een voorspellende methode voor dit gedrag en de invloed van dit gedrag op de bedrijfszekerheid van het uit dit proces voortvloeiende product in een omgeving die juist in sterke mate van dit onvoorspelbare gedrag afhankelijk is, lijkt voorlopig nog niet mogelijk.

Dit betekent echter niet dat het onmogelijk is bedrijfszekerheid binnen de huidige industriële randvoorwaarden te beheersen. Aangezien niet alles voorspeld kan worden, wordt het interessant naast de eerdergenoemde voorspellende vaardigheden te kijken naar het 'leervermogen' van organisaties. Onder de gegeven randvoorwaarden lijkt het niet uit te sluiten dat problemen optreden. Het competitief vermogen van bedrijven wordt mede bepaald, wanneer bedrijven problemen waarnemen en hoe snel ze in staat zijn deze problemen op te lossen. Een maatlat voor het vermogen van bedrijven om bedrijfszekerheid te kunnen beheersen zou daarom uit twee elementen kunnen bestaan:

– *Voorspellend vermogen*: in hoeverre is een bedrijf in staat toekomstige problemen te voorspellen en adequate acties te definiëren en in te voeren.
– *Correctief vermogen of leervermogen*: hoe effectief is een bedrijf in staat toch nog optredende problemen te detecteren, te analyseren en te verhelpen in huidige en toekomstige producten.

Wil men bedrijven kunnen analyseren op deze twee aspecten, dan vereist dat mogelijkheden om deze aspecten op een eenduidige wijze in kaart te brengen en vervolgens via een analysemodel te kunnen vergelijken. De volgende paragrafen presenteren een (aanzet voor een) model dat potentieel gebruikt kan worden als 'Reliability Management Performance Indicator'. Hoewel de eerste ervaringen met dit model zeker veelbelovend zijn, zullen de afsluitende paragrafen van dit deel laten zien dat nog meer substantieel onderzoek nodig is om dit model in een breed scala van (huidige en toekomstige) bedrijfsprocessen succesvol en eenduidig te kunnen inzetten.

De rol van informatie en informatiestromen in bedrijfsprocessen

Het analyseren van het 'voorspellend vermogen' van bedrijfsprocessen is een inherent lastig probleem. In een industriële omgeving betekent 'perfect voorspellend vermogen' dat men de beschikking heeft over zeer goede voorspellende modellen en in staat is deze modellen op de juiste manier toe te passen. Het opstellen en valideren van dergelijke modellen vereist vooral in fase 1 en 2 een grondige toetsing aan de ervaringen van (combinaties van) voldoende extreme producten en extreme gebruikers. De economische consequenties van een dergelijk experiment zouden echter aanzienlijk kunnen zijn. Wil men een dergelijk model kunnen valideren, dan moet men ook kijken of voorspelde risico's ook daadwerkelijk optreden. Veel fabrikanten zullen er daarom voor kiezen om niet het model te valideren, maar om het potentiële risico te vermijden. Als gevolg hiervan zullen veel voorspellende modellen inherent een hoge graad van onzekerheid bevatten. Het is de vraag echter of dit een bezwaar is. Ook perfecte modellen die toepasbaar zijn in de producten van vandaag hebben waarschijnlijk morgen als gevolg van de eerdergenoemde trends een beperkte waarde. Een alternatief zou daarom kunnen zijn niet alleen te kijken naar het voorspellend vermogen van een bedrijf, maar vooral naar het lerend vermogen. Uit de voorgaande paragrafen is het mogelijk de volgende karakteristieken van 'leervermogen' af te leiden:

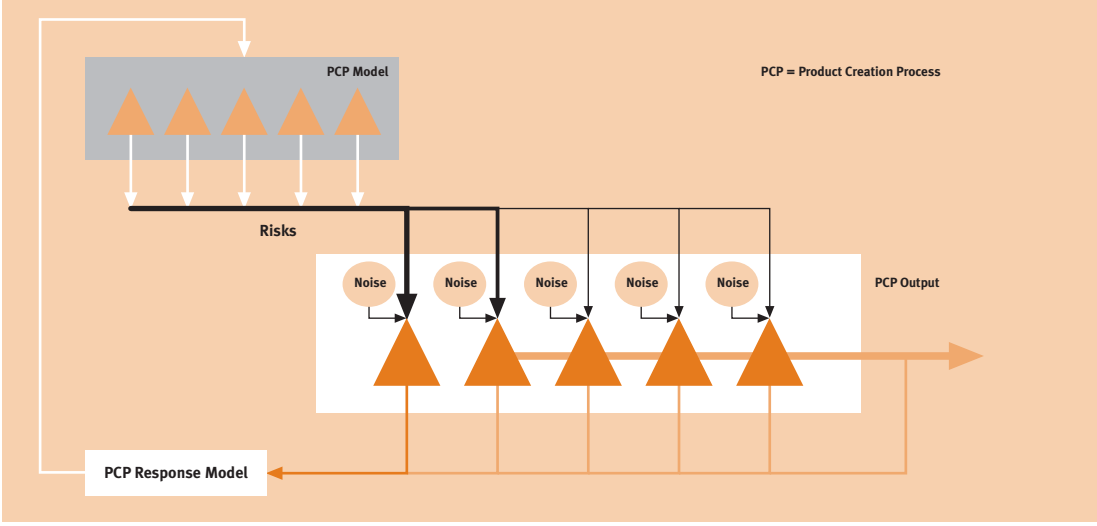
– Snelheid: wat is de tijd die een bedrijf nodig heeft om een nieuwe onverwachte gebeurtenis in het veld te detecteren.
– Kwaliteit: wat is de kwaliteit van de informatie die het bedrijf uit deze gebeurtenis kan extraheren.
– Verspreiding ('deployment'): hoe efficiënt is de verspreiding van informatie naar de relevante actoren in een bedrijfsproces.

Deze aanpak vertoont een sterke gelijkenis met technieken die in de regeltechniek worden gebruikt. Daar is het gangbaar systemen te karakteriseren aan de hand van hun impulsrespons: de responsie van een systeem op een zekere afwijking of verstoring, zoals in dit geval een onverwacht veldprobleem. De resulterende informatiestroom vertoont een sterke gelijkenis met een regelkring uit de klassieke regeltechniek. Een belangrijk verschil met de klassieke regeltechniek vormt de aandacht voor de kwaliteit van de informatie. In de regeltechniek gaat men er vanuit dat de relevante informatie wordt gebruikt bij het besturen van systemen. Bij het analyseren van kwaliteit en bedrijfszekerheid hoeft dit laatste gegeven eerdere opmerkingen beslist niet altijd het geval te zijn. Daarom gebruikt de auteur naast het eerdergenoemde informatiestroommodel ook een kwaliteitsindex voor deze informatie. Met behulp van de zogenaamde Maturity Index on Reliability (MIR) [Brombacher, 1999; Lu, 1999] wordt gekeken of de kwaliteitsinformatie:

- juist gemeten wordt (MIR-niveau 1: how much);
- de juiste actoren in het proces bereikt worden (MIR-niveau 2: where);
- de informatie bevat om de juiste 'root' cause van een probleem met kwaliteit of bedrijfszekerheid te analyseren (MIR-niveau 3: why);
- zodanig gestructureerd is dat herhaling van fouten voorkomen wordt (MIR-niveau 4: what to do).

Deze vier MIR-niveaus worden samen met de analyse van de eerdergenoemde informatiestromen gebruikt om de structuur die een bedrijf gebruikt bij het beheersen van kwaliteit en bedrijfszekerheid te analyseren. Tevens kan de structuur van een aldus verkregen MIR-model worden gebruikt om te analyseren of de gebruikte kwaliteitsstructuur past bij de eisen die zijn opgelegd door het ontwerpproces.

Figuur 34.9
Analyse van productontwikkelingsprocessen via responsiemodellen.



In deel 1 is reeds een voorbeeld gegeven van een dergelijke MIR-case (zie hoofdstuk 5, deel 1). Als een dergelijke case nu geanalyseerd wordt op de aspecten voorspellend vermogen en leervermogen, dan blijkt dat men vrij duidelijk kan aangeven welke problemen in een dergelijk proces te verwachten zijn. Een dergelijk proces kent een groot aantal formeel gedefinieerde kwaliteitsactiviteiten (voorbeelden: FMEA, diverse kwaliteitstesten, simulaties en dergelijke), maar deze activiteiten maken slechts zeer beperkt deel uit van regelkringen. De kans dat daarmee nieuwe klassen van problemen (als gevolg van nieuwe technologie, nieuwe klanteneisen e.d.) opgespoord worden is daarmee uiterst gering. In het proces behandeld in genoemd hoofdstuk in deel 1, bestaan er slechts twee operationele regelkringen: systemen waar afwijkingen in het verwachte productgedrag op de een of andere manier worden teruggevoerd in het ontwikkelproces. De resultaten van veel andere activiteiten worden niet in het verdere proces gebruikt. Productoptimalisatie van kwaliteit en bedrijfszekerheid vindt vrijwel geheel in het natraject (productie) plaats met alle nadelige gevolgen (tijd, kosten) van dien. Een iets verdergaande analyse laat weliswaar een groot aantal mijlpalen zien die echter geen deel uitmaken van actieve regelkringen. Ook kan men per mijlpaal een groot aantal testen terugvinden, maar de resultaten hiervan worden als gevolg van tijdsdruk nauwelijks gebruikt. Als echter gekeken wordt naar de eisen die aan het hier geschetste proces gesteld worden, dan blijkt dat het hier gaat om een proces met een zeer grote druk op time to market en een zeer hoge graad van innovatie. Met andere woorden: een proces dat sterke gelijkenis vertoont met het eerder geschetste model van Concurrent Engineering. Verder onderzoek leert dat dit bedrijf tracht Concurrent Engineering in te voeren (minder mijlpalen, vroege productoptimalisatie, enz.), maar op het gebied van kwaliteit en bedrijfszekerheid lukt dit niet. Het wegvallen van mijlpalen heeft slechts een nadelig effect; er vindt daardoor ook minder borging tegen bekende problemen plaats. De vereiste 'voorspellende modellen' voor kwaliteit en bedrijfszekerheid worden door dit bedrijf niet ontwikkeld. Er is geen capaciteit beschikbaar om de vereiste data te extraheren uit problemen in het natraject en om te zetten in informatie die bruikbaar is in het voortraject[7] van huidige en toekomstige producten.

Bedrijfszekerheid van toekomstige producten: een eerste verkenning

Het voorspellen van bedrijfszekerheid is op dit moment zeker niet eenvoudig en wordt er in de toekomst onder invloed van de eerdergenoemde trends waarschijnlijk ook niet eenvoudiger op. Er zal een aanzienlijke hoeveelheid onderzoek nodig zijn om oplossingen voor de eerder geschetste problemen te vinden. Het onderzoek op dit gebied zou zich hierbij kunnen concentreren op twee onderzoekslijnen:

7 Een voorzichtige schatting leert dat de kosten van de hiervoor vereiste capaciteit een fractie zijn van de daadwerkelijke kosten die nu besteed worden aan correctieve acties in het natraject.

– Het ontwikkelen van krachtige voorspellende methoden en technieken, inzetbaar in de vroege fasen van toekomstige bedrijfsprocessen.
– Het ontwikkelen van modellen voor het snel, efficiënt en adequaat leren van (onverwachte) veldproblemen.

Onderzoek naar voorspellende methoden en technieken

In toekomstige bedrijfsprocessen zal er door de sterk toenemende complexiteit van producten, de tijdsdruk en de veranderingssnelheid een steeds verdergaande ontkoppeling plaatsvinden tussen beslissing en invoering. Ter wille van een efficiënte bedrijfsvoering moeten beslissingen reeds vroegtijdig genomen kunnen worden op grond van beperkte informatie en krachtige voorspellende modellen. Dergelijke modellen zullen altijd in staat moeten zijn met het aspect risico en onzekerheid te werken; ze zijn immers vaak gebaseerd op ervaringen met andere, slechts ten dele vergelijkbare producten en gebruikers. De voorspellende modellen dienen zich hierbij niet alleen te beperken tot technische risico's, maar dienen ook rekening te houden met (onzekerheden in) bedrijfsprocessen en de daarbij behorende informatiestromen.

Tot op zekere hoogte zijn er al methoden en technieken beschikbaar. Instrumenten als Quality Function Deployment (QFD), Failure Mode and Effect Analysis (FMEA) en de foutenboomanalyse (FTA) zijn juist voor dit doel ontwikkeld. Als deze methoden gevoed worden met nauwkeurige informatie, zijn ze zeker bruikbaar, soms zelfs vroeg in bedrijfsprocessen bij de voorspelling van risico's. Zoals Lu [Lu, 2002] in haar proefschrift laat zien, zijn dergelijke instrumenten echter niet goed in staat om te gaan met onzekere informatie. En zoals zij in hetzelfde proefschrift laat zien is informatie juist in de vroege fasen van moderne bedrijfsprocessen vaak inherent onzeker. Daarom zal er nog een aanzienlijke hoeveelheid onderzoek nodig zijn naar methoden en technieken die op een verantwoorde wijze met onzekere informatie kunnen omgaan.

Onderzoek naar informatiestromen en leerprocessen

Naast het onderzoek naar voorspellende technieken zal er ook een aanzienlijke hoeveelheid onderzoek nodig zijn naar (de behandeling van) fouten die wel optreden. Gegeven de eerdergenoemde trends is het niet waarschijnlijk dat er volledig dekkende voorspellende methoden op korte termijn ter beschikking zullen komen. Daarom zal het voor het bedrijfsleven steeds meer nodig zijn om ook snelle en adequate leersystemen (en de daarbij behorende informatie-infrastructuur) te installeren. Leersystemen dienen daarbij aan de volgende criteria te voldoen:

– *Detectie*: een eerste vereiste bij het analyseren van onverwachte problemen is 'het kunnen detecteren van problemen'. Hierbij kan men allereerst denken aan reactieve methoden zoals data mining en 'near miss analysis'. Hiermee

kan men onverwachte patronen trachten op te sporen die zouden kunnen wijzen op onverwacht product- of klantengedrag. Men kan hierbij ook denken aan meer proactieve methoden zoals 'reliability testing'. Omdat naar alle waarschijnlijkheid fase 1 en 2 van de roller coaster-curve steeds relevanter gaan worden, betekent dit dat men in veel gevallen niet meer kijkt naar 'het' product in relatie tot 'de' klant, maar zich vooral steeds meer richt op mogelijke interacties tussen extreme producten en extreme gebruikers. Hoewel de kosten van dergelijke analysen hoger zullen zijn dan de tot op heden gebruikte technieken, kan men juist door dit soort experimenten reeds vroegtijdig zaken op het spoor komen die anders pas in het veld gevonden zouden worden met alle nadelige gevolgen (kosten, tijd) van dien.

– *Allocatie en informatieverspreiding*: de tweede stap bij het inrichten van een efficiënt leer- en regelsysteem voor bedrijfszekerheid is het opzetten van mechanismen voor de allocatie van de betrokken actoren en de verspreiding van (hoogwaardige) informatie naar deze actoren. Vaak worden dergelijke informatiestructuren beperkt tot datgene wat nodig is om een acuut probleem op te lossen. In veel gevallen wordt er minder gekeken naar de oorzaken van problemen en de mensen die invloed daarop kunnen uitoefenen. Wil men echter problemen bij de bron kunnen aanpakken en in huidige en toekomstige producten kunnen voorkomen, dan zal men het gehele bedrijfsproces en alle daarin optredende actoren moeten kunnen meenemen. Eigen onderzoek laat zien [Brombacher, 1999] dat daar waar informatiestromen organisatorische of geografische grenzen overschrijden er veel vertraging en verlies (in de kwaliteit) van informatie optreedt. De genoemde informatiestroommodellen kunnen niet alleen helpen bij het analyseren van oorzaken van bedrijfskundige problemen in bedrijfsprocessen (zie ook [Bradley, 1999]), maar kunnen ook behulpzaam zijn bij het nemen van beslissingen zoals wanneer men bijvoorbeeld het beste bepaalde activiteiten kan uitbesteden aan derden. In het geval van een volwassen en stabiel proces met goed gedefinieerde interfaces zal uitbesteden veel eerder een optie zijn dan in situaties waar gerekend moet worden met een hoge graad van onzekerheid als gevolg van bijvoorbeeld technische innovaties, of in het geval van onbekende klanten, van klantenwensen of klanteneisen.
– *Analyse*: een derde stap bij het opzetten van leersystemen is het invoeren van analysestructuren om een grondige analyse van optredende problemen met kwaliteit of bedrijfszekerheid mogelijk te maken. In veel bedrijven was dit in zoverre het om technische analysen gaat de taak van kwaliteitsafdelingen of serviceorganisaties. Veel bedrijven hebben dergelijke kwaliteitsafdelingen gedecentraliseerd of het servicewerk uitbesteed aan derden. Vooral een grondige analyse van de bedrijfskundige problemen werd en wordt in veel gevallen alleen uitgevoerd bij het optreden van een calamiteit. Het beperken (tot calamiteiten), het uitbesteden en decentraliseren van dergelijke

activiteiten heeft in veel gevallen geleid tot een minder structurele kennisopbouw in bedrijven, terwijl de eerdergenoemde trends juist vragen om een snellere en betere kennisinfrastructuur. Onvoldoende infrastructuur op dit gebied leidt dan ook vaak tot situaties waarin problemen zich blijven voordoen (met alle consequenties wat betreft tijd en kosten), terwijl de organisatie zich daarvan nauwelijks bewust is. Het opzetten van een kennisinfrastructuur die voldoende slagvaardig is om ook in de huidige situatie op een adequate manier te kunnen omgaan met bedrijfszekerheid zal echter nog een aanzienlijke investering in onderzoek vragen.

– *Beheersing en sturing*: voorlopig zal nog een aanzienlijke hoeveelheid onderzoek nodig zijn om de prestaties in het ontwikkelen, vervaardigen en in stand houden van bedrijfszekere producten van producten en hun onderliggende bedrijfsprocessen op adequate wijze te kunnen analyseren. Dat geldt juist in een situatie van sterke innovatie, grote tijdsdruk, mondiaal verlopende bedrijfsprocessen en toenemende klanteneisen. Op het moment dat modellen, methoden en instrumenten beschikbaar komen die zich baseren op een combinatie van continue, snelle en effectieve kennisopbouw (leren) in combinatie met een vertaling van deze kennis naar nieuwe producten (voorspelling) is de verwachting dat bedrijven bedrijfszekerheid in toenemende mate niet zien als iets dat hen overkomt, maar als een proces dat in vergaande mate te beheersen en te sturen is.

De rol van onderwijs bij het ontwikkelen van toekomstige bedrijfszekere systemen

De eerdergenoemde ontwikkelingen zullen een grote invloed hebben op het beroep ‘Quality en Reliability Engineer’. In het verleden concentreerde dit vakgebied zich vooral op de statistische analyse van componenten in het veld en de fysische achtergronden van de daar optredende fouten. Ook nu nog zijn zeer veel mensen in deze gebieden actief en gegeven de sterk toegenomen betrouwbaarheid van componenten met zeer veel succes. De nieuwe eisen aan bedrijfszekerheid betekenen dat daarnaast een nieuw type Reliability Engineers nodig is. Eisen aan deze toekomstige professionals zijn:

– Men moet kennis hebben van het ontwerp en de besturing van moderne bedrijfsprocessen en zich daarbij niet beperken tot kennis van slechts een deel van de keten (zoals productie).
– Men moet voldoende productkennis hebben om inzicht te hebben in het ontstaan van normale, maar ook extreme en of afwijkende producten gedurende het ontwerp- en realisatieproces.
– Men moet voldoende inzicht hebben in het gedrag van klanten om rekening te kunnen houden met de expliciete, maar ook de impliciete eisen die moderne klanten aan producten stellen.

Een probleem dat hier bij optreedt is dat veel klassieke technische opleidingen een sterk monodisciplinaire inslag hebben. Het zal voor veel opleidingsinstituten een uitdaging zijn om naast deze monodisciplinaire ingenieurs ook mensen op te leiden die:

- een grondige kennis hebben van de klassieke technische disciplines om daarmee tot voldoende inzicht in producten te komen;
- een grondige kennis hebben van de statistiek om op snelle en efficiënte wijze velddata te kunnen omzetten in informatie over mogelijke (combinaties van) extreme producten en gebruikers;
- een grondige kennis hebben van de psychologie om de interactie tussen technisch product en de door de klant verlangde functie of dienst te kunnen begrijpen.

Het invoeren van een dergelijk programma zou kunnen leiden tot een nieuwe generatie 'Professional Reliability Engineers': mensen die in staat zijn op verantwoorde wijze om te gaan met het ontwikkelen en in stand houden van toekomstige producten, juist in een markt waarin de dynamiek van technologie, bedrijfsprocessen en markt de enige constante factor zal zijn.

Referenties

- Allen, T.J. (1971). Communications, Technology Transfer and the Role of Technical Gatekeeper. R&D Management
- Allen, T.J. (1977). Managing the Flow of Technology. MIT Press
- Bradley, W. (1999). Analysis of Industrial Accidents. Symposium 'The Reliability Challenge'. Finn Jensen Consultancy. London
- Brombacher, A.C. (1992). Reliability by Design. John Wiley & Sons. Chichester
- Brombacher, A.C., D.C.L. van Geest, O.E. Herrmann. (1993). Simulation, a Tool for Designing in Reliability. Quality and Reliability Engineering International. Special Issue on the ESREL Conference
- Brombacher, A.C. (1999). MIR: Covering Non-Technical Aspects of IEC61508 Reliability Certification. Reliability Engineering and System Safety. Elsevier
- Brombacher, A.C., A.J.M. Huijben, S. Molenaar. (2001). Why do Quality and Reliability Feedback Loops not always Work in Practice; a Case Study. Accepted for Publication in Reliability Engineering and System Safety. Elsevier
- Coppola, A. (1984). Reliability Engineering of Electronic Equipment: a Historical Perspective. IEEE Transactions on Reliability. September
- Lewis, E.E. (1996). Introduction to Reliability Engineering. John Wiley & Sons

- Lu, Y., H.T. Loh, Y. Ibrahim, P.C. Sander, A.C. Brombacher. (1999). Reliability in a Time Driven Product Development Process. Quality and Reliability Engineering International
- Lu, Y. (2002). Analysis of Reliability Problems in Fast Product Development Processes. PhD Thesis. Eindhoven University of Technology
- Military Handbook Reliability Prediction of Electronic Equipment (MIL-HDBK-217). (1962). United States Navy
- Petkova, V.T., P.C. Sander, A.C. Brombacher. (1999). The Role of the Service Centre in Improvement Processes. Quality and Reliability Engineering International
- Wong, K.L. (1988). Off the Bathtub onto the Roller-Coaster Curve. Proceedings Annual Reliability and Maintainability Symposium. IEEE

Organisatie van de studie

Deze publicatie is tot stand gekomen met de actieve medewerking van tientallen deskundigen. STT is veel dank verschuldigd aan al degenen die belangeloos veel tijd en energie aan dit project hebben besteed. Een stuurgroep werd gevormd om de juiste invalshoek te vinden en het inhoudelijke gehalte van de studie te bewaken. De werkgroepleden hebben als auteur of als deelnemer in de verschillende discussie- en commentaarronden in belangrijke mate aan de inhoud van deze publicatie bijgedragen. Behalve de werkgroepleden hebben ook externe auteurs een bijdrage geschreven.

Stuurgroep

dr. B.J.M. Ale	Rijksinstituut voor Volksgezondheid en Milieu (RIVM), Bilthoven
prof.dr.ir. A.C. Brombacher *(voorzitter)*	Technische Universiteit Eindhoven, Faculteit Technologie Management
dr.ir. J.F.L.M. Brukx	Syntelligens, Zwijndrecht
ir. A.J.M. Huijben	Philips Medical Systems, Eindhoven
ir. M.A. Kentie	Unilever Research Vlaardingen
drs. F.J.G. van de Linde	STT, Den Haag (tot 1-9-2000)
ir. R.W. van Otterloo	NRG Arnhem
dr. T.W. van der Schaaf	Technische Universiteit Eindhoven, Faculteit Technologie Management
ing. R.Th.E. Spiker	Yokogawa Industrial Safety Systems B.V., Apeldoorn
drs. E.P.C. van Utteren	Philips Research, Eindhoven (tot 1-2-2000)
ir. J.H. van der Veen	STT, Den Haag (vanaf 1-9-2000)
G.J. Vergouw	Rabobank ICT, Utrecht
dr.ir. C. de Wijs	CMG Public Sector B.V., Den Haag

Werkgroep Techniek

ir. R.J. Baarda	IQUIP Informatica B.V., Diemen
ir. R.D. Boers	Inspectie Verkeer en Waterstaat, Hoofddorp
ir. E.C.J. Bouwman	Delta PI, Duiven
dr. R. Cocker	Cocker Consulting and Innovus BV, Almere
dr. H.L.M. Lelieveld	Unilever Research Vlaardingen
ir. H.A.M. Luiijf	TNO Fysisch en Elektronisch Laboratorium, Den Haag
prof.dr. S.B. Luitjens	Philips Research, Eindhoven
mr.ir. M.J.P. van der Meulen	Simtech, Rotterdam
G.J. Vergouw *(voorzitter)*	Rabobank ICT, Utrecht
prof.drs.ir. J.K. Vrijling	Technische Universiteit Delft
ir. G.J.P.M. Wackers	Ernst & Young, Maastricht
ir. M.N.J.H. Wijnands	Holland Railconsult BV, Utrecht

Werkgroep Bedrijfsprocessen

ing. A.M. van Buren	Unilever Research Vlaardingen
ir. J.A.M. ten Dam	PTT Post B.V., Den Haag
prof.dr. R. Dekker	Erasmus Universiteit Rotterdam, Faculteit Economische Wetenschappen
P. Dieleman	Roccade, Apeldoorn
ir. A.J.M. Huijben *(voorzitter)*	Philips Medical Systems, Eindhoven
drs. A. Jonk	Het Expertisecentrum, Den Haag
ing. H. Paans	Du Pont de Nemours (Nederland) B.V., Dordrecht
P.J.M. Poos RE RA	SNS Reaal Groep N.V., 's Hertogenbosch
drs.ir. G.J.C. Ransijn	CMG Public Sector B.V., Den Haag
prof.dr.ir. H.A.J. de Ridder	Technische Universiteit Delft, Faculteit der Civiele Techniek en Geowetenschappen

Werkgroep Organisatie

dr. L.J. Bellamy	Ingenieurs/adviesbureau Save, Apeldoorn
dr.ir. J.F.L.M. Brukx *(voorzitter)*	Syntelligens, Zwijndrecht
dr. M.J. van Duin	Universiteit Leiden, COT Crisis Onderzoek Team, Den Haag
dr.ir. T. Goemans	KPMG Consulting, Den Haag
ing. J.I.H. Oh	Ministerie van Sociale Zaken en Werkgelegenheid, Directie Arbo, Den Haag
mr. A. Oosterlee	Universiteit Leiden, Leids Universitair Medisch Centrum, Leiden
dr. G.L. Wackers	Universiteit Maastricht, Capaciteitsgroep Maatschappijwetenschap en Techniek
ir. V.A. Wegener	Getronics N.V., Amsterdam
drs.ing. K.J. Zwart	Inspectie Verkeer en Waterstaat, Divisie Luchtvaart, Hoofddorp

Externe auteurs

mr. W.H.M. Hafkamp	Rabobank Nederland, Informatisering Betalingsverkeer, Utrecht
drs. L. Kanse	Technische Universiteit Eindhoven, Faculteit Technologie Management
drs. F.J.G. van de Linde	RAND Europe, Leiden
Y. Lu, MSc	Technische Universiteit Eindhoven, Faculteit Technologie Management
ir. S. Minderhoud	Philips CFT, Manager PCP Improvement, Eindhoven
ir. J.M. Nederend	Aveco de Bondt bv, Driebergen
ir. den Ouden	Philips CFT, Sector Innovation and Industrial Support, Eindhoven
drs. M.J.C.M. Vromans	Erasmus Universiteit Rotterdam, Faculteit Bedrijfskunde
ing. J.A.M. Wiegerinck	Shell Global Solutions International BV, Den Haag

Projectleiding

Het project stond onder leiding van Mark de Graef, projectleider bij STT. Bij de organisatie van de studie werd hij bijgestaan door Rosemarijke Otten, en door Annette Potting die meehielp met de organisatie van een aantal vergaderingen. De discussies met en de adviezen van de oud-directeur van STT, Erik van de Linde, hebben het project mede vormgegeven. Aan de redactie van de publicatie is meegewerkt door Rosemarijke Otten die de taalkundige redactie voor haar rekening nam.

STT-publicaties

Alle publicaties waarbij het ISBN is vermeld, zijn verkrijgbaar via STT of via de boekhandel.

De overige publicaties zijn alleen te verkrijgen bij
STT
Postbus 30424
2500 GK Den Haag
Telefoon + 31 70 3029830
Fax + 31 70 3616185
E-mail info@stt.nl

De meest recente publicatielijst voor derden is op de homepage te vinden:
http://www.stt.nl

64 Betrouwbaarheid van technische systemen, anticiperen op trends
Redactie: dr. M.R. de Graef, 2001 (ISBN 9084496 5 2)

63 Toekomst@werk.nl. Reflecties op Economie, Technologie en Arbeid
Redactie: drs. Rifka M. Weehuizen, 2000 (ISBN 80 4496 4 4)

62 Vernieuwing in productontwikkeling, strategie voor de toekomst
Redactie: ir. Arie Korbijn, 1999

61 Stroomversnelling, de volgende elektrische innovatiegolf
Redactie: ir. J. M. Meij, 1999 (ISBN 90 804496 2 8)

60 Nanotechnology, towards a molecular construction kit
Edited by Arthur ten Wolde, 1998 (ISBN 90 804496 1 X)

59 Bouwwijs, materialen en methoden voor toekomstige gebouwen
Redactie: ir. Annemieke Venemans, 1997 (ISBN 90 6155 816 6)

58 Gezonde productiviteit, innoveren voor betere arbeidsomstandigheden
Redactie: ir. Arie Korbijn, 1996 (ISBN 90 6155 744 5)

57 Digitale leermiddelen in beroepsopleidingen (incl cd-i en samenvatting)
Redactie: dr. A. ten Wolde, 1996 (ISBN 90 6155 730 5)

56 Microsystem technology: exploring opportunities
Edited by Gerben Klein Lebbink, 1994 (ISBN 90 14 05088 7)

55 Schone kansen, denkbeelden over ondernemerschap en milieu-management
Redactie: ir. E.W.L. van Engelen, J. van Goor, 1994 (ISBN 90 14 04929 3)

54 Goederenvervoer over korte afstand
Redactie: ir. M.J. Venemans, 1994 (ISBN 90 14 04928 5)

53 Elektriciteit in perspectief, 'energie en milieu'
Redactie: ir. E.W.L. van Engelen, 1992 (ISBN 90 14 04715 0)

52 Inspelen op complexiteit
Redactie: drs. M.J.A. Alkemade, 1992 (ISBN 90 14 03883 6)

51 Plantaardige grondstoffen voor de industrie
Redactie: drs. W.G.J. Brouwer, 1991 (ISBN 9014 03882 8)

50 Opleiden voor de toekomst: instrument voor beleid
ir. H.B. van Terwisga en drs. E. van Sluijs, 1990 (ISBN 90 14 04506 9)

49 Grenzen aan techniek
Redactie: ir. A.J. van Griethuysen, 1989 (ISBN 90 14 03880 1)

48 Kennissystemen in de industrie
Redactie: ir. J.J.S.C. de Witte en drs. A.Y.L. Kwee, 1988

47 Kennissystemen in de dienstensector
Redactie: drs. A.Y.L. Kwee en ir. J.J.S.C. de Witte, 1987

46 Kennissystemen en medische besluitvorming
Redactie: ir. J.J.S.C. de Witte en drs. A.Y.L. Kwee, 1987

45 Kennissystemen in het onderwijs
Redactie: ir. J.J.S.C. de Witte en drs. A.Y.L. Kwee, 1987

44 Onderhoudsbewust ontwerpen nu en in de toekomst
Redactie: ir. G. Laurentius, 1987

43 Nieuwe toepassingen van materialen
Redactie: ir. A.J. van Griethuysen, 1986

42 Techniek voor ouderen
Redactie: ir. M.H. Blom Fuhri Snethlage, 1986 (ISBN 90 14 03822 4)

41 De toekomst van onze voedingsmiddelenindustrie
Redactie: drs. J.C.M. Schogt en prof.dr.ir. W.J. Beek, 1985

40 Bedrijf, kennis en innovatie
Redactie: ir. H. Timmerman, 1985

39 De kwetsbaarheid van de stad; verstoringen in water, gas, elektriciteit en telefonie
Samensteller: ir. G. Laurentius, 1984

38 Man and information technology: towards friendlier systems
Edited by J.H.F. van Apeldoorn, 1983

37 Nederland en de rijkdommen van de zee: industrieel perspectief en het nieuwe zeerecht
Redactie: ir. J.F.P. Schönfeld en mr.drs. Ph.J. de Koning Gans, 1983

36 Informatietechniek in het kantoor; ervaringen in zeven organisaties
Samensteller: drs. F.J.G. Fransen, 1983

35 Automatisering in de fabriek; vertrekpunten voor beleid
Redactie: ir. H. Timmerman, 1983

34 Flexibele automatisering in Nederland; ervaringen en opinies
Redactie: ir. G. Laurentius, ir. H. Timmerman en ir. A.A.M. Vermeulen, 1982

33 Toekomstige verwarming van woningen en gebouwen
Eindredactie: ir. A.C. Sjoerdsma, 1982

32 Micro-elektronica voor onze toekomst; een kritische beschouwing
Samenstellers: burggraaf E. Davignon e.a., 1982

31-9 Micro-elektronica: de belastingdienst
Samensteller: ir. H.K. Boswijk, 1981

31-8 Micro-elektronica: het reiswezen
Samensteller: ir. H.K. Boswijk, 1981

31-7 Micro-elektronica: het kantoor
Samensteller: ir. H.K. Boswijk, 1981

31-6 Micro-elektronica: het bankwezen
Samensteller: ir. H.K. Boswijk, 1981

31-5 Micro-elektronica: het ontwerpproces
Samensteller: ir. H.K. Boswijk, 1981

31-4 Micro-elektronica: productinnovatie van consumentenprodukten en diensten voor gebruik in huis
Samensteller: ir. H.K. Boswijk, 1981

31-3 Micro-elektronica: procesinnovatie in de sector elektro-metaal
Samensteller: ir. H.K. Boswijk, 1981

31-2 Micro-elektronica: de grafische industrie en uitgeverijen
Samensteller: ir. H.K. Boswijk, 1981

31-1 Micro-elektronica: de rundveehouderij
Samensteller: ir. H.K. Boswijk, 1981

31 Micro-elektronica in beroep en bedrijf; balans en verwachting
Samensteller: ir. H.K. Boswijk, 1981

30 Biotechnology; a Dutch perspective
Edited by J.H.F. van Apeldoorn, 1981

29 Wonen en techniek; ervaringen van gisteren, ideeën voor morgen
Redactie: ir. J. Overeem en dr. G.H. Jansen, 1981

28 Distributie van consumentengoederen; informatie en communicatie in perspectief
Redactie: ir. R.G.F. de Groot, 1980

27 Steenkool voor onze toekomst
Eindredactie: ir. A.C. Sjoerdsma, 1980

26 Bos en hout voor onze toekomst
Redactie: ir. T.K. de Haas, ir. J.H.F. van Apeldoorn, ir. A.C. Sjoerdsma, 1979

25 Arts en gegevensverwerking
Redactie: ir. R.G.F. de Groot, 1979

24 Toekomstbeeld der industrie
prof.dr. P. de Wolff e.a., 1978

23 De industrie in Nederland: verkenning van knelpunten en mogelijkheden
Redactie: ir. H.K. Boswijk en ir. R.G.F. de Groot, 1978

22 Materialen voor onze samenleving
Redactie: ir. J.A. Over, 1976

21 Stedelijk verkeer en vervoer langs nieuwe banen?
Redactie: ir. J. Overeem, 1976

20 Voedsel voor allen, plaats en rol van de EEG
prof.dr. J. Tinbergen e.a., 1976

19 Energy conservation: ways and means
edited by J.A. Over and A.C. Sjoerdsma, 1974

18 Mens en milieu: kringlopen van materie
Stuurgroep en Werkgroepen voor Milieuzorg, 1973

17 Mens en milieu: zorg voor zuivere lucht
Stuurgroep en Werkgroepen voor Milieuzorg, 1973

16 Mens en milieu: beheerste groei
Stuurgroep en Werkgroepen voor Milieuzorg, 1973

15 Technologisch verkennen: methoden en mogelijkheden
ir. A. van der Lee e.a., 1973

14 Techniek en preventief gezondheidsonderzoek
dr. M.J. Hartgerink e.a., 1973

13 Communicatiestad 1985: elektronische communicatie met huis en bedrijf
prof.dr.ir. J.L. Bordewijk e.a., 1973

12 Elektriciteit in onze toekomstige energievoorziening: mogelijkheden en consequenties
dr.ir. H. Hoog e.a., 1972

11 Transmissiesystemen voor elektrische energie in Nederland
prof.dr. J.J. Went e.a., 1972

10 Barge carriers: some technical, economic and legal aspects
drs. W. Cordia e.a., 1972

9 Het voeden van Nederland nu en in de toekomst
prof.dr.ir. M.J.L. Dols e.a., 1971

8 Mens en milieu: prioriteiten en keuze
ir. L. Schepers e.a., 1971

7 Electrical energy needs and environmental problems, now and in the future
ir. J.H. Bakker e.a., 1971

6 De invloed van goedkope elektrische energie op de technische ontwikkeling in Nederland
dr. P.J. van Duin, 1971

5 De overgangsprocedures in het verkeer
prof.ir. J.L.A. Cuperus e.a., 1969

4 Hoe komt een beleidsvisie tot stand?
Ir. P.H. Bosboom, 1969

3 Verkeersmiddelen
prof.ir. J.L.A. Cuperus e.a., 1968

2 Techniek en toekomstbeeld; telecommunicatie in telescopisch beeld
prof.dr.ir. R.M.M. Oberman, 1968

1 Toekomstbeeld der techniek
ir. J. Smit, 1968

Overige uitgaven:

- Techniek verlegt grenzen, als u begrijpt wat ik bedoel
  STT/Toonder, 1997
- New applications of materials
  edited by A.J. van Griethuysen, 1988 (ISBN 0 95 13623 0 5)
- Mariene ontwikkelingen in de Verenigde Staten, Japan, Frankrijk, West-Duitsland, het Verenigd Koninkrijk en Nederland: organisatie, aandachtsgebieden en budgets
  Redactie: ir. J.F.P. Schönfeld en mr.drs. Ph.J. de Koning Gans, 1984
- Het belang van STT (toespraak bij het 15-jarig bestaan van STT)
  door prof.ir. Th. Quené, 1983
- De innovatienota; een aanvulling
  H.K. Boswijk, J.G. Wissema, en W.C.L. Zegveld, 1980

Deze studie kwam tot stand dankzij de financiële steun van bedrijfsleven, overheid en het Koninklijk Instituut van Ingenieurs.

Subsidieverleners STT

Akzo Nobel
Arcadis
Bank Nederlandse Gemeenten
CMG Nederland
Commissie van Overleg Sectorraden
Corus Group
Cosun
CSM
Delft Instruments
DHV Beheer
Dow Benelux
DSM
Eldim
EnergieNed
Energieproduktiebedrijf UNA
Gamma Holding
Heineken Nederland
Holland Railconsult
Hollandsche Beton Groep
ING Bank
IQUIP Informatica
KEMA

Koninklijk Ingenieurs en Architectenbureau HASKONING
Koninklijk Instituut van Ingenieurs
Koninklijke PTT Nederland
Koninklijke Schelde Groep
Koninklijke Ten Cate
Lucent Technologies
Micro*Montage
Ministerie van Economische Zaken
Ministerie van Landbouw, Natuurbeheer en Visserij
Ministerie van Onderwijs, Cultuur en Wetenschappen
Nederlandsche Apparatenfabriek Nedap
Nederlandse Gasunie
Nederlandse Unilever Bedrijven
NIB Capital
Océ-Technologies
Philips Electronics
Rabobank Nederland
PinkRoccade
Schneider MGTE
Sdu
Shell Nederland
Siemens Nederland
Simac Techniek
Solvay Nederland
Stichting Energieonderzoek Centrum Nederland
Stork
TBI Holdings
TNO
TNT Post Groep
Urenco
VNU
Vredestein

Index

Stichting
Toekomstbeeld
der Techniek

Toenemende complexiteit, kortere ontwikkelcycli, globalisering, grotere mondigheid van de klant zijn begrippen die we vrijwel dagelijks lezen. Deze trends hebben echter naast de vaak besproken economische voordelen ook invloed op de betrouwbaarheid van technische systemen. In dit boek worden deze ontwikkelingen op het gebied van betrouwbaarheid geschetst.

Betrouwbaarheid van technische systemen wordt in het boek vanuit drie perspectieven behandeld: vanuit de techniek, de bedrijfsprocessen en de organisatie. In het eerste deel van het boek wordt de geschiedenis van betrouwbaarheid beschreven vanuit deze drie perspectieven en worden de trends toegelicht. In het tweede deel worden de gevolgen van de trends duidelijk gemaakt in een aantal cases die door een groot aantal deskundigen zijn geschreven vanuit de verschillende perspectieven. Deze cases zijn afkomstig uit verschillende sectoren en laten zien dat betrouwbaarheid veel facetten kent. In het derde deel wordt een integraal overzicht gegeven van de gevolgen van de trends en worden toekomstperspectieven aangegeven.

Dit boek is het tastbare resultaat van een gezamenlijke inspanning van veel deskundigen van bedrijfsleven, universiteiten en kennisinstituten. Het is bedoeld voor beleidsmakers en managers in de industrie, onderwijs- en kennisinstellingen, de overheid en brancheorganisaties.

ISBN 90-804496-5-2

Laser Proof

9 789080 449657