# De (on)betrouwbare organisatie

*Over de ruimteveer Challenger, de gezonken Herald of Free Enterprise en' zero-fault organizations'*

A.F.A.Korsten

**1 Inleiding**

Wat is een betrouwbare organisatie? We kiezen het vertrekpunt voor beantwoording in de literatuur over crises. En dan komen we uit bij

- de theorie van de menselijke fouten,
- de theorie van organisatorische gebreken en
- de theorie van systeemgebreken bij riskante technologie.

Vervolgens gaan we in op

- de theorie van hoogst betrouwbare organisaties, die nul fouten mogen maken.

**2 De studie van crises: crisis duidt op onbetrouwbaarheid**

Een betrouwbare organisatie kan men in eerste instantie beschouwen als een organisatie waarin geen sprake is van afwijkingen. Wie wil kijken naar (beleids)afwijkingen kan een crisis als een beleidsafwijking beschouwen: een treinbotsing, een overstroming (1993, 1995, Limburg), een gijzeling (provinciehuis Assen), een neerstortend vliegtuig (Bijlmerramp; Herculesramp), een ontploffend ruimteveer (Challenger-ramp), een gezonken veerboot (Herald of Free Enterprise), brand op een boorplatform (Piper Alpha).

Studies naar crises zijn onder meer gericht op het opsporen van de oorzaken van crisis, preventie en crisisbeheersing. Deze studies zijn te verdelen:

- de theorie van de menselijke fouten (Wagenaar);
- theorievorming over organisatorische gebreken, waaronder theorie over condities die menselijke fouten in de hand werken, zoals bijvoorbeeld de theorie van 'groupthink' (Janis) of bureaupolitiek (Allison);
- de theorie van de riskante technologie, in casu de theorie over complexiteit en onderling versterkende samenhang tussen bestanddelen van een systeem (Perrow);
- de theorie van de betrouwbare organisatie, zoals over de vraag waarom elektriciteitscentrale juist betrouwbaar zijn (Schulman).

*Menselijke fouten*

De theorieën van de menselijke fout is geworteld in de psychologie. De centrale stelling in deze theorievorming uit met name de cognitieve psychologie is dat een crisis, zoals

een ramp, te herleiden is tot een of meer menselijke fouten. De theorie geeft aan dat fouten en miscalculaties doorwerken en zo een ramp laten ontstaan.

*Organisatorische gebreken*

De theorieën over organisatorische gebreken stellen centraal dat een crisis is terug te voeren op gebreken in de organisatie en slordigheden, die tot gevolg hebben dat een ramp kan optreden en een moeilijke situatie niet tijdig kan worden gezien, voorkomen of gekeerd. Organisatorische condities van antecedente aard kunnen menselijke fouten in de hand werken. Er is iets mis met de signalering van zwakheden, met het bespreekbaar maken daarvan, met voorbereidingsomstandigheden en handelingen. Zo gezien, is de theorievorming over organisatorische gebreken aanvullend op de theorievorming over menselijke fouten.

*Riskante technologie als interpretatiekader*

De theorie van de riskante technologie is een derde theorie, die een crisis, bijvoorbeeld een ramp, verklaard uit risicodragende kenmerken van technologische systemen, waarmee organisaties werken. De systeemtheorie vraagt aandacht voor sterk risicodragende technologie. Elke fout of miscalculatie kan een kettingreactie van verstoringen tot gevolg hebben en zo een ramp veroorzaken. Deze theorie onderstreept dat zelfs als mensen perfect handelen en ook de organisatie goed functioneert, een ramp niet uitgesloten is. Deze theorie is onder meer van toepassing op nucleaire en chemische industrie, maar ook te gebruiken bij de interpretatie van het Heizeldrama in Brussel, zoals 't Hart en Pijnenburg lieten zien.

De verschillende theorieën geven in samenhang een goede doorkijk naar crises en verhelderen het inzicht in crisis. Er zijn gedragsaanbevelingen aan te ontlenen. De drie theoriecomplexen leveren inzichten op over menselijke fouten, organisatorische gebreken en technologische kwetsbaarheden. Rijpma en Otten (1998) spreken over *ramppathogenen*. Het beeld van een ziektekiem van de mens wordt zo metaforisch getransplanteerd naar crises in de vorm van een ramp.

*Theorie van de betrouwbare organisatie*

De vierde theorie van de betrouwbare organisaties kiest niet de analyse van de crisis tot uitgangspunt *maar een (meer) positieve invalshoek*. Het gaat niet erom te verklaren wat er fout ging, maar de verklaring van wat goed gaat. Hoe slagen organisaties er toch in om ..... veilig te functioneren, ondanks dat menselijke fouten natuurlijk ook in dergelijke organisaties plaatsvinden, ondanks organisatorische zwakheden, ondanks zwakten in technische systemen.

Schema: Ordening van enige theoriecomplexen over crises in de vorm van een ramp

| theoriecomplex | typen fouten | theoreticus: casus |
|---|---|---|
| crisis: ramp door menselijke fout | a skill-based errors: fouten in de automatische, routinematige acti | Wagenaar: Prinsendam; Weick: botsing vliegtuigen op Tenerife |
| | b rule-based errors: fouten door het volgen van verkeerde routine en procedures | Herald of Free Enterprise |
| | c knowledge-based errors: fouten door gebrek aan kennis | explosie in Cindufabriek |
| crisis: ramp door organisatorische gebreken | a general failure type (GFT): het ontbreken van rampbestrijdingsmiddelen | Wagenaar |
| | b GFT: hiaten en onduidelijkhede in procedures | verouderde en incomplete handleiding: ontploffing op boorplatform Piper Alpha |
| | c GFT: gebrekkige training van personeel | geen aanvullende training op verouderde handleiding: Piper Alpha |
| | d GFT: gebrekkige signalering va fouten of het niet verhelpen hiervan | Vaughan: Challenger |
| | e GFT: het ontbreken van een compleet beeld van de relevante informatie | Turner; veiligheidsvoorschriften die strijdig zijn - Herald of Free Enterprise |
| | f GFT: conflicterende belangen | Allison: bureaupolitieke strijd |
| crisis: ramp door riskante technologie waardoor condities ontstaan waaronder menselijke fouten optreden | a complexiteit | Perrow |
| | b strakke/losse koppeling | Perrow |
| tegendeel van crisis: theorie van de betrouwbare organisatie | kenmerken: missie, socialisatie, gedeelde organisatie-cultuur | Schulman; La Porte; Mannarelli e.a.; Rochlin |
| | kenmerk betrouwbare organisat redundantie, reserves | |
| | kenmerk: gecontoleerde decentralisatie | |
| | kenmerk betrouwbare organisat ontkoppeling | |

## 3 Theorietraditie 1: De theorie van de menselijke fouten

Als de kapitein van de *Exxon Valdez* niet dronken was geweest, was de milieuramp in 1992 in Alaska wellicht voorkomen. Als de assistent-bootsman op de veerboot, de

*Herald of Free Enterprise*, niet slaperig was geweest, was de boot mogelijk niet ten onder gegaan. Mensen maken fouten zoals de Leidse hoogleraar psychologie Wagenaar al vaststelde in zijn studie naar de ondergang van het cruiseschip *de Prinsendam*. Vele bemanningsleden maakten fouten. De reeks van menselijke fouten voorafgaand aan de ramp duurde een week. De reconstructie van andere rampen laat zien dat gemiddeld enkele tientallen menselijke fouten voorgaan aan een ramp (Wagenaar, 1987). Een menselijke fout staat meestal niet op zich. Een menselijke fout komt niet alleen maar dient zich nogal eens aan in een reeks (Rijpma en Otten, 1998: 25).

*Menselijke fouten komen niet alleen*
De menselijke fout is een erkende oorzaak van een crisis, in de vorm van een ramp. Maar let wel, niet alle rampen zijn hierop terug te voeren. En de verklaring van 'de menselijke fout' is nogal eens niet voldoende om een ramp helemaal te begrijpen. Er gaat veel of op zijn minst het een en ander aan vooraf. Men moet goed proberen te zien wat de samenhang is in de oorzaken. De ene fout of omstandigheid lokt niet zelden de andere uit.

*Drie typen menselijke fouten*
Rampstudies gericht op de menselijke fout hebben drie typen menselijke fouten opgeleverd:
a 'skill-based errors',
b 'rule-based errors', en
c 'knowledge-based errors'.

- *a 'Skill-based errors'.*

Hierbij gaat het om menselijke fouten in het routinematig patroon van (operationele) handelingen. Kleine fouten kunnen grote gevolgen hebben, en zo uitlopen op een ramp.

> ***Casus: Tenerife***
> Karl Weick (1993) analyseerde de frontale botsing van een KLM-vliegtuig met een Amerikaans toestel op Tenerife, in 1977. De piloot van de KLM-Boeing 747 volgde de startprocedure in 1977, het fatale jaar toen de botsing optrad, maar gedeeltelijk. De piloot kreeg wel waarschuwingen van zijn copiloot om te controleren of de baan vrij was, maar sloeg de waarschuwingen in de wind. De piloot zag daarom niet dat er zich nog een toestel op dezelfde baan bevond. Het gevolg was een frontale botsing.

- *b 'Rule-based errors'.*

Bij dergelijke regelgebaseerde fouten van menselijke aard gaat het om het volgen van verkeerde procedures en routines bij het diagnosticeren of oplossen van een

probleem. In veel organisaties zijn hiervoor operationele werkwijzen geformuleerd. Denk aan laswerkzaamheden op het dak van een oud kasteel. Of aan reparatie bij stroomstoringen. Er worden fouten gemaakt bij onderhoudswerkzaamheden doordat ervan wordt uitgegaan dat een storing volgens 'de boekjes', een storing die gelijk is aan eerdere bekende storingen.

• *c 'Knowlegde-based errors'.*
Kennisgebaseerde fouten zijn fouten van menselijke aard waarbij essentiële kennis ontbreekt om gerezen problemen het hoofd te bieden. Denk aan iemand die aanwijzingen volgt van een handleiding waardoor een explosief mengsel ontstaat. De aanwijzingen op het document waren fout maar de betrokkene kon ze niet ontdekken (Rijpma en Otten, 1998).

**4 Theorietraditie 2: de theorievorming over organisatorische gebreken**
Als menselijke fouten samenhang vertonen, is de vraag welke factoren daartoe bijdroegen of ze opriepen. Waren er omstandigheden die een voedingsbodem, een kiem opleverden, waarin een crisis niet kon uitblijven?

Er bestaan verschillende typen omstandigheden. Ze worden GFT's genoemd: *general failure types*. GFT's zijn:
het ontbreken van rampbestrijdingsmiddelen; hiaten en onduidelijkheden in procedures; gebrekkige training van personeel; gebrekkige signalering van fouten of het niet verhelpen hiervan; het ontbreken van een compleet beeld van de relevante informatie. We lopen ze na.

*a Het ontbreken van rampbestrijdingsmiddelen.*
Denk hierbij aan niet werkende blusapparatuur, onvoldoende reddingsboten.

***Casus***
Het Heizeldrama laat voorbeelden zien van het ontbreken van voldoende geschikte rampbestrijdingsmiddelen. Gebrekkige communicatiemiddelen waren debet aan de chaos bij de rampbestrijding op het Eindhovense vliegveld ten tijde van de Hercules-ramp (COT, 1996).

Het komt ook voor dat een indicator die aangeeft of iets in orde is of niet ontbreekt. Met andere woorden, we zitten hier op het vlak van gebrekkige kwaliteitszorg als GFT.

*b Hiaten, onduidelijkheden of inconsistenties in procedures.*
Veel veiligheidsprocedures hebben een complement in menselijk gedrag. Veiligheidsprocedures impliceren vaak dat er waarschuwingssignalen worden

gegeven. Die signalen moeten dan ook worden waargenomen, wat niet altijd gebeurt.
Er kan ook wat misgaan als veiligheidsprocedures in strijd zijn met elkaar, waardoor personeel een keuze maakt.
Als de procedures niet deugen, bijvoorbeeld op een olieplatform, kan de veiligheid in gevaar komen. Dan kan grote kwaliteit van het personeel geen fouten voorkomen.
Of twee procedures moeten worden uitgevoerd door een en dezelfde persoon, maar dat kan niet gelijktijdig. Dat was een probleem op de veerboot, de Herald of Free Enterprise.

*c Gebrekkige training van personeel.*
Deze GFT-factor 'gebrekkige training' ligt erg voor de hand.

> ***Casus Piper Alpha***
> De heranalyse van de ontploffing van het boorplatform Piper Alpha bracht aan het licht dat personeel, dat op het platform kwam werken verouderde handleidingen kregen uitgereikt. Het personeel kreeg geen training in het hanteren van crisisomstandigheden (Rijpma en Otten, 1998: 25).

*d Gebrekkige signalering van fouten of het niet verhelpen hiervan.*
Deze factor is heel belangrijk, omdat deze zichtbaar maakt of willens en wetens grotere risico's genomen worden.

> ***Casus El Al-vliegtuigen***
> De El Al-vliegtuigen, waarvan er een in 1992 op de Bijlmermeer neergestorte, waren niet alle steeds goed onderhouden, zo leerde de parlementaire enquête.

Meestal is er wel tijd voorafgaande aan de ramp geweest om een fout of zwakke antecendente situatie te voorkomen. Turner (1978) spreekt in dit verband van de *incubatietijd*. In die incubatietijd worden fouten geaccepteerd en risico's genomen (El Al-vliegtuigen stegen toch, ondanks mankementen vanuit Schiphol op) of worden degenen die ze signaleren in concrete gevallen door hogergeplaatsten 'overruled'. Voorafgaand aan een ramp blijkt er vaak wel informatie voorhanden over mogelijke gevaren, maar waren betrokken autoriteiten 'los' in de acceptatie hiervan.

> ***Casus Hercules-ramp***
> Het Herculus-vrachtvliegtuig met een fanfare aan boord, verongelukte bij de landing in Eindhoven, vermoedelijk mede door de aanwezigheid van zwermen vogels. De Hercules-ramp leerde dat de vogelverjager op het

ramptijdstip niet zijn werk deed, waarvoor hij was aangesteld. Er waren ook bezuinigingen op het vliegveld geweest, die nadelig waren voor de veiligheid (COT, 1996).

Zijn er dan geen waarschuwingssignalen? Gaan er tevoren geen rode lichtjes branden? Meestal wel, maar ze worden genegeerd of veronachtzaamd, en dan slaat de menselijke fout toe.

De Challenger-casus laat hiervan voorbeelden zien (erosie van de zgn. O-ringen; Vaughan, 1996).

Soms is ook sprake van een foutieve interpretatie.

Soms is het erger en komen waarschuwingssignalen helemaal niet aan. Intrigerend is waarom signalen niet opgevangen worden. Soms zit de wijze van kijken mensen in de weg. Psychologen en anderen wijzen op stress. Besluitvorming vindt onder druk plaats, er is een overheersend beeld binnen een groep door overoptimisme en personen met een afwijkende mening, die zich baseren op andere inschattingen of andere informatie, worden genegeerd (Janis, 1989; 't Hart, 1994).

*e Het ontbreken van een compleet beeld van de relevante informatie.*
Deze GFT-factor houdt in dat relevante informatie over een aantal personen verspreid is en er zo een gebrek aan centraal overzicht is.

***Casus: Bijlmer-ramp, 1992***
Rijpma en Otten (1998) geven een voorbeeld hiervan. Er blijken wel waarschuwingssignalen te werken maar de signalen worden niet gekoppeld, laat staan dat er een oplossing uit voortvloeit. Of signalen komen ergens aan en worden vervolgens niet doorgegeven. De parlementaire commissie die de Bijlmerramp onderzocht, constateerde in 1999 dat ruim anderhalf uur nadat het El Al-vrachtvliegtuig in de Bijlmermeer was neergestort op het hoofdkantoor van politie in Amsterdam een telefoontje binnenkwam van de dienst luchtvaart van de rijkspolitie op Schiphol. De boodschap luidde: er bevinden zich geen explosieven ('high explosives') in het toestel, maar de lading bevat wel gevaarlijke stoffen. De medewerker van de luchtvaartpolitie verzocht de telefonist op het hoofdbureau deze mededeling direct door te geven aan een collega van hem op de rampplek, omdat hij er zelf op de gebruikelijke frequentie niet doorheen kwam. Dat ... gebeurde echter niet. Bernard Welten, de commissaris die de bergings- en reddingswerkzaamheden coördineerde, werd hiervan niet in kennis gesteld. Hij hoorde pas in 1999 van het telefoontje. De politiecommandant wist

destijds ook niet dat er uranium in het vliegtuig had gezeten. Had hij het wel geweten dan had hij op de avond van de ramp zelf de hulpverlening op een volstrekt andere wijze vormgegeven, zo meldde hij de parlementaire enquêtecommissie begin februari 1999.

*f Conflicterende belangen*

Informatie over gevaren en risico's kan worden genegerd door conflicterende belangen binnen een organisatie. De theorie over bureaupolitiek (Allison) vraagt hier aandacht voor. Het ene organisatiedeel pleit bijvoorbeeld voor het vasthouden aan veiligheidseisen terwijl een ander deel meer oog heeft voor het commerciële aspect, waardoor met veiligheid een loopje genomen wordt.

***Casus: Piper Alpha***

Bij de eerste ontploffingen op het boorplatform Piper Alpha werd de productie niet stilgelegd omdat het weer opstarten van de productie veel tijd en geld zou vergen. Een fatale beslissing (Rijpma en Otten, 1998: 280).

**5 Theorietraditie 3: systeemgebreken bij riskante technologie**

De theorie van de riskante technologie is een ander theoriecomplex, die een crisis, bijvoorbeeld een ramp, verklaart uit risicodragende kenmerken van technologische systemen, waarmee organisaties werken. Het gaat hier om een systeemtheorie die aandacht vraagt voor sterk risicodragende technologie. Een fout in een riskante technologie is *'normaal'* (Perrow, 1984). Dat is niet zozeer een probleem. Erger is, elke fout of miscalculatie kan ..... een *kettingreactie* van verstoringen tot gevolg hebben en zo een ramp veroorzaken (Perrow, 1984). Sectoren als de chemische industrie of nucleaire industrie zijn gevoelig vanwege het gebruik van *'risky technologies'*.

***Casus Piper Alpha***

Neem het voorbeeld van het olieplatform Piper Alpha. Het platform was een verzamel- en verdeelstation in een netwerk van boorplatforms. Gas- en olieleidingen verbonden de omringende olieplatforms met het centrale platform. Op 6 juli 1998 vond op Piper Alpha een groot ongeluk plaats. Een defecte pomp veroorzaakte een explosie. Daardoor werd een groot deel van de controlekamer vernietigd. Communicatie met de omringende platforms was vanaf dat moment niet meer mogelijk. Ongeveer twintig minuten later volgden nieuwe explosies. De tot dan beperkte brand groeide uit tot een vuurzee die 165 mensen het leven kostte. Deze ramp kon niet alleen worden teruggebracht tot menselijke fouten of tot genoemde *'general failure types'* (GFT's), dus tot bepaalde typen van organisatorisch falen. Er waren andere soorten variabelen in het spel. Essentieel was dat Piper Alpha gekoppeld was aan de andere platforms.

Wie de catastrofe 'Piper Alpha' wil begrijpen, moet kijken naar de koppelingen, naar het technisch netwerk, dus de verbindingen. De theorie van *'normal accidents'* van Perrow (1984) is hiervoor relevant. De kans op een catastrofe bij riskante technologie is groter naarmate de complexiteit van de toegepaste technologie groter is.

Complexiteit verwijst naar het volgende.
1 Naar de onderling versterkende connectie tussen onderdelen van een systeem. Verbindingen zijn er natuurlijk vaak in een technologie. Onvoorzienbare gevolgen kunnen optreden als er ergens in of bij het systeem iets gebeurt dat doorwerkt, en zo andere onderdelen/ subsystemen beïnvloedt.
2 Complexiteit van een systeem kan gepaard gaan met risicovolle compactheid. Op het olieplatform Piper Alpha was dat het geval.
3 De complexiteit van een 'risky technology' is groot in geval van common-mode. Een onderdeel vervult dan meerdere functies voor of binnen het geheel. Dubbelfuncties zijn efficiënt in een compact geheel maar ook gevaarlijk.

Complexiteit is een, en waarneming is twee. In de chemische en nucleaire industrie komt het voor dat verstoring in een technologisch systeem niet rechtstreeks worden waargenomen, maar via computeruitdraaien en waarschuwingslampjes. Geven de indicatoren goede signalen? Duidelijke signalen?

Naast complexiteit is *strakke koppeling* een tweede systeemkenmerk. Strakke koppeling betekent dat een verstoring in een systeem onderdeel een kettingreactie oplevert. Losse koppeling kan de voorkeur verdienen. Een militaire operatie is een voorbeeld van een complex systeem dat los gekoppeld is omdat de militaire eenheden betrekkelijk los van elkaar opereren. Een auto is ook een los gekoppeld systeem. Het systeem van *automatische treinbeïnvloeding* (ATB) is een voorbeeld van geautomatiseerde ontkoppeling. Als treinen in elkaars baanvak dreigen te belanden of daadwerkelijk beland zijn, treedt automatisch een remmend effect in werking. Dat vermindert de kans op een botsing aanzienlijk. Een vliegtuig is een voorbeeld van strakke koppeling. Een breuk in de staart heeft desastreuze gevolgen omdat die de rest van het systeem ontregelt.

De kunst is om niet strak te koppelen, om de strakke koppeling te manipuleren. Dat kan volgens Perrow door 'back-up'- of reservesystemen te hebben, die een hapering of uitval moeten opvangen. Als in een kerncentrale maar een koelsysteem voorkomt, is bij uitval oververhitting het onvermijdelijke gevolg. Het koelsysteem is in dat geval strak gekoppeld aan de reactortemperatuur.

## 6 Theorietraditie 4: de betrouwbare organisatie (HRO)

De verschillende genoemde theoriecomplexen, genoemd onder 1 tot en met 3, geven in samenhang een goede kijk op crises en verhelderen het inzicht. Ze leveren inzichten op over menselijke fouten, organisatorische gebreken en technologische kwetsbaarheden. Er zijn gedragsaanbevelingen aan te ontlenen. Rijpma en Otten (1998) spreken over *ramppathogenen*. Het beeld van een ziektekiem van de mens wordt zo metaforisch getransplanteerd naar crises in de vorm van een ramp.

Daarmee is het theoretiserend vermogen niet op. De theorie van de betrouwbare organisaties (*'high reliability organisation'*; HRO) kiest een positieve invalshoek. Het gaat niet erom te verklaren wat er fout ging, maar wat goed gaat. Hoe slagen organisaties er toch in om veilig te functioneren, ondanks dat menselijke fouten natuurlijk ook in dergelijke organisaties plaatsvinden, ondanks organisatorische zwakheden, ondanks zwakten in technische systemen?

*Voorbeelden van betrouwbare organisaties*
Een voorbeeld van een betrouwbare organisatie is een nutsbedrijf, zoals een waterleidingmaatschappij, kerncentrale, elektriciteitsmaatschappij, radarsysteem. Rijpma en Otten (1998) vatten de literatuur over dit onderwerp samen.

*Waarop onderzoek naar betrouwbare organisaties zich richt*
Onderzoek naar de werkwijzen van dergelijke organisaties heeft inzichten opgeleverd in de praktijken van HRO's.

*Profiel van HRO's als betrouwbare organisaties*
Er is een profiel op te stellen van de betrouwbare organisatie. Het profiel van de betrouwbare organisatie kent vier kenmerken:
a homogeniteit;
b redundantie en reservecapaciteit;
c gecontroleerde decentralisatie;
d ontkoppeling (Rijpma en Otten, 1998).

**7 Kenmerken van HRO's**
We lopen vier kenmerken van betrouwbare organisaties na:
a homogeniteit; b redundantie en reservecapaciteit; c gecontroleerde decentralisatie; d ontkoppeling (Rijpma en Otten, 1998; LaPorte en Consolini, 1991; La Porte, 1996; Mannarelli, Roberts & Bea, 1996; Rochlin, 1996a).

> *a De betrouwbare organisatie is een homogene organisatie door missie, socialisatie en cultuur.*
> Hoe slaagt een *'high reliable organisation'* erin zo betrouwbaar, zo veilig, te zijn? De betrouwbare organisatie - de HRO - is homogeen door een gemeenschappelijk

gedragen missie, waarover in alle onderdelen van de organisatie en in alle geledingen - van hoog tot laag - overeenstemming bestaat. Er is geen interne strijd over de doelen. De productie moet hoogwaardig zijn en de kwaliteitszorg is daarop afgestemd. Veiligheid heeft de eerste prioriteit. De eventuele reservecapaciteit wordt niet gecommercialiseerd en zo opgeofferd aan de veiligheid.

Veiligheid gaat voor alles.
1 Omdat veiligheid zo belangrijk is, wordt daarin ook veel geïnvesteerd. De professionals in de organisatie weten dat.
2 Veiligheid doordesemt de organisatiecultuur. De personeelsleden kennen veel toewijding.
3 Bij de recrutering van personeel wordt veel aandacht besteed aan professioneel werken, kennis, ervaring en precisie. Competentie telt en werkt daarom stevig door in andere onderdelen van personeelsbeleid en -management.
4 Personen die zeer goede prestaties geleverd hebben op het gebied van veiligheid worden hogelijk gewaardeerd (Schulman, 1996).
In HRO's bestaat betrekkelijke openheid over het maken van fouten (La Porte, 1996: 64).

*b De betrouwbare organisatie beschikt over redundantie en reserves.*
Betrouwbare organisaties beschikken over reserves, dus over middelen om moeilijke situaties het hoofd te bieden. Ze hebben wat over. Operators kunnen werk van anderen begrijpen en overnemen. Technische systemen overlappen elkaar zodat het ene systeem het falen van het ander kan signaleren (Rijpstra en Otten, 1998; Sagan, 1993).

*c De betrouwbare organisatie kent gecontroleerde decentralisatie.*
Professionaliteit wordt erkend. De werkvloer heeft dus veel te zeggen. In HRO's is sprake van instructies, overlappende bevoegdheden en discussie in teams. Hierdoor wordt de kans op fouten verkleind.

In sommige HR's en bij bepaalde handelingen hebben professionals een vetorecht.

> De spotter aan boord van vliegdekschepen is hiervan een voorbeeld. Deze is laag in de hiërarchie maar kan wel de landing van een vliegtuig verbieden. Hij krijgt instructies over de omstandigheden onder welke hij een landing kan verbieden, maar de instructies blijven instructies en ze zijn niet meer. De spotter heeft discretionaire ruimte. Deze functionaris kan uiteindelijk bij een landingsverzoek naar eigen inzicht handelen. Dat wordt erkend door hogeren in de hiërarchie (Schulman, 1993a; Roberts, Stout & Halpern, 1994; Rijpstra en Otten, 1998: 33).

Betrouwbare organisaties werken evenwel niet volledig decentraal. Hoewel erkenning van professionaliteit van deskundige medewerkers met zich brengt dat personeel op de werkvloer over autonomie beschikt, bestaan er 'checks and balances'.

*d In de betrouwbare organisatie is sprake van ontkoppeling.*
Rijpma en Otten (1998) maken duidelijk dat bepaalde betrouwbare organisaties technische subsystemen kunnen ontkoppelen, waardoor het risico op een negatief sneeuwbaleffect bij een fout wordt verlaagd.

De volledig betrouwbare - veilige of rampvrije - organisatie bestaat niet. Uitgaande van de theorie van Perrow ('normal accidents') kunnen HRO's fouten nooit volledig uitsluiten. Een crisis ontstaat vaak ook als één procent van alle handelingen fout gaat. Het is niet voldoende om de veiligheid van 90 naar 99 procent, bij wijze van spreken, op te schroeven. Hoewel het woord 'betrouwbare organisatie' de indruk gewekt dat de HRO foutenvrij opereert, is de werkelijkheid anders. Dat neemt niet weg dat de opdracht van een HRO om op 'zero faults' te koersen krachtig is. De stroom moet niet uitvallen, de kwaliteit van het drinkwater moet niet zo zijn dat burgers ziek worden of geen water beschikbaar is.

**8 Effecten van de betrouwbare organisatie**
Het concept 'betrouwbare organisatie' is vooral geschikt voor detectie, voor diagnose. Welke betekenis hebben HRO-strategieën en kenmerken voor de rampgevoeligheid van een systeem? Dat is een vraag die Rijpma en Otten (1998) zich stellen.

*a De betrouwbare organisatie is een homogene organisatie door missie, socialisatie en cultuur.*
HRO koersen op een degelijke 'aanpak' van de veiligheid. Homogeniteit in de beleving van het belang van de missie van een HRO, en dus het organisatiedoel, heeft in beginsel een positieve inwerking op een organisatiecultuur, waarin veiligheid centraal staat. Wie weet dat het doel is om burgers en organisatie continu van stroom te voorzien, weet ook dat alles in het werk gesteld moet worden om geen stroomstoring te laten optreden. De betekenis van de organisatiecultuur in HRO's is dat de kans op menselijke fouten verkleind wordt. En inderdaad, de kans op twee van de drie typen menselijke fouten is klein. Welke, denkt u? Er waren drie typen menselijke fouten: 'skill-bases faults', 'knowledge-based faults', en 'rule-based faults'.

Personeelsleden van een elektriciteitsbedrijf zullen weinig fouten maken tegen geprogrammeerde, routinematige handelingen. Operationele acties worden binnen teams aan controle onderworpen. Zoals we zagen, competentie staat

centraal. Deskundigheid en ervaring telt. De hele cultuur is gericht op precisie. Dus zal de kans gering zijn dat in een HRO 'skill-based faults' voorkomen. Hetzelfde kan gezegd worden van de 'knowledge-based rules'. De kans hierop is eveneens gering. De professionals zijn getraind in het onderkennen van waarschuwingssignalen en dus in het signaleren van afwijkingen. Veiligheid telt, en als er al medewerkers zijn die iets dreigen te missen dan volgt een extra training. Er is weinig ruimte voor het ontstaan van 'general failure types', die menselijke fouten bevorderen. Dat houdt in dat weinig achterstallig onderhoud zal bestaan, en verouderde apparatuur snel vervangen zal worden. De teams doen aan kwaliteitszorg. Ze bespreken zwakke punten, rapporteren en zoeken naar verbeteringen.

Tot zover het optimisme. Is er geen kans op een zwakte? Een HRO acht competentie. Dat kan tot arrogantie leiden. Een betrouwbare organisatie kan een gevangene van het eigen denken worden, van het aangeleerde en gekoesterde denken. Ze kan een blinde vlek krijgen voor bepaalde fouten, die nooit in beeld kunnen komen. Wie veel op veiligheid let, let automatisch minder op andere zaken. Er zal juist veel personeel aangenomen worden dat past in het veiligheidsdenken. Met afwijkingen in een technisch systeem zal men minder makkelijk kunnen omgaan.

De kans op 'rule-based faults' is bij betrouwbare organisaties *groter* dan die op 'skill-based faults' of 'knowledge-based faults' (Rijpma en Otten, 1998: 36).

*b De betrouwbare organisatie beschikt over redundantie en reserves.*
Redundantie komt in betrouwbare organisatie voor. Het is een positief kenmerk. HRO verwerven zich zo zekerheid en stabiliteit. Er kan eigenlijk 'niets fout gaan' of het wordt tijdig gesignaleerd en verholpen. Maar .... als er twee systemen bestaan die elkaar overlappen in scanning van fouten, kan een aantal soorten gevolgen optreden.

1 Het gevaar is niet uitgesloten dat beide systemen *uitvallen*.

2 De 'overlappende' systemen zitten elkaar in de weg.
'Door redundantie kan (..) de veiligheid in technologische systemen afnemen' stellen Perrow (1984; Sagan, 1993, 1994; Rijpma en Otten, 1998: 37). Daarmee bedoelen deze auteurs niet zozeer de overlap maar dat twee of meer gekoppelde systemen *elkaar kunnen verstoren*. Ze vergroten de complexiteit en bemoeilijken de doorzichtigheid. Er bestaat een kans als er ergens een fout geregistreerd wordt dat het goede systeem (ten onrechte) gerepareerd wordt en de fout in het andere systeem blijft bestaan.

***Casus Three Mile Island***
Kijk maar naar de kerncentrale van Three Mile Island. Het koelsysteem van de centrale faalde, waarna twee noodpompen in werking traden. Een klep ging open omdat de druk in de reactor te groot werd. Het water werd in de kern gebracht om de kern af te koelen. Toch nam de temperatuur in de kern toe. Hoe kon dat? Doordat het water in een afgesloten buis werd gespoten en zo de kern niet bereikte. Het koelwater stroomde uit de reactor. De temperatuur in de reactor steeg. De kernreactor had zoveel noodsystemen dat uiteindelijk niemand meer wist welk systeem wel of niet werkte. Wat men wel wist en toepaste, vergrootte het probleem.

3 Derde mogelijk gevolg van redundantie: *het valse veiligheidsgevoel*. Werknemers nemen meer risico's omdat er eigenlijk niks kan gebeuren!

***Casus ruimteveer Challenger***
De illustratieve casus is hier de space shuttle Challenger. Eerdere problemen met de O-ringen waren niet serieus genomen. De kans dat beide geijktijdig stuk gingen, werd gering geacht.

4 De vierde mogelijkheid bij redundantie is *doorschuiven*. Bij redundantie kan de veronderstelling bij een medewerker opkomen dat een andere ploeg of andere verantwoordelijke het dreigende probleem wel zal oppakken (Rijpma & Otten, 1998: 38).

*c De betrouwbare organisatie kent gecontroleerde decentralisatie.*
Betrouwbare organisaties hadden ook gecontroleerde decentralisatie als kenmerk. De hoog gewaardeerde professionaliteit, die gepaard gaat met zekere autonomie, leidt tot snelle signalering van zaken die mis gaan of dreigen mis te gaan. Het gebruiken van concurrerende analytische perspectieven kan ook positief inwerken op veiligheid. Maar is er dan helemaal geen gevaar? Dat gevaar is er wel. Verstoringen in een strak gekoppeld systeem vereist centralisatie van beslissingen (Rijpma en Otten, 1998: 39). Omdat er kettingreacties optreden, komt men er niet uit met decentrale reflectie. Er is juist overzicht over het geheel nodig. Een combinatie van strakke koppeling en decentrale verantwoordelijkheid is in betrouwbare organisaties, zoals elektriciteitscentrales, gevaarlijk. Decentralisatie brengt de kans op conflicten binnen de organisatie over het verantwoordelijkheidsprimaat dichterbij, iets dat nog versterkt wordt door een cultuur van competentie waardoor competente professionals niet van wijken willen weten (Perrow, 1986; Rijpma & Otten, 1998: 40).

*d In de betrouwbare organisatie is sprake van ontkoppeling.*
Ja, kan men tegenwerpen, HRO's kennen toch vaak geen strakke koppeling, dus is de kans op conflicten ook minder groot. De tegenwerping heeft wel iets. Maar, in bepaalde bedrijven is een zekere mate van koppeling onvermijdelijk, en dus een kans op kettingreacties. Wat te doen? Toch buffers of andere voorzieningen in het leven roepen, die leiden tot (meer)ontkoppeling.

De theorie van de betrouwbare organisatie is een interessant uitgangspunt voor de bestudering van organisatie en management van nutsbedrijven, en bijvoorbeeld 'human resources management' in een waterleidingbedrijf, of de rol van teams.

**Vraag:** Wat is het verband tussen high reliability organizations en de risicosamenleving? Lees de volgende tekst uit Binnenlands Bestuur van A. Korsten van 13 december 2002.

***De risicosamenleving***
Op de verjaardag van Sinterklaas in 2002 viel bij bij 300.000 inwoners van Rotterdam en verre omgeving in de vroege ochtend de elektriciteit uit terwijl zich elders stroomdips voordeden. De aanleiding was een botsing van een heftruck met een bovengrondse transportleiding voor elektriciteit. Daardoor werd het openbare leven in een deel van het Rijnmondgebied stilgelegd. Het treinverkeer in geheel Zuid-Holland stond stil, trams reden niet meer en stoplichten werkten niet langer. In het centrum van Rotterdam viel de stadsverwarming uit en het mobiele telefoonnetwerk lag gedeeltelijk plat. Het Dijkzigt ziekenhuis moest overschakelen op een noodaggregaat en kranten werden elders gedrukt. Het gemeentehuis was wel open maar van reguliere dienstverlening was geen sprake. De bussen waren overbelast en op bepaalde scholen werd de lesorde verstoord. Na enkele uren keerde de stroom in delen van de stad weer terug, minderde de verkeerschaos, konden winkels weer open en scholen weer het normale lesprogramma vervolgen. Een incidentele stroomstoring heeft dus grote gevolgen. De olievlekwerking is enorm. Keteneffecten treden ook op bij gastransportbreuken of haperingen in de waterdistributie.Vroeger waren de haperingen in de energiedienstverlening wat minder maar was het niveau ook lager. Nederland was ruim veertig jaar terug minder druk en minder kwetsbaar. Destijds konden de meeste burgers de woning nog met de kolenkachel verwarmen. Toen werkte het fornuis, de typemachine en de telefoon nog zonder stroom. Tegenwoordig kunnen de centrale verwarming, de keramische kookplaat, de isdn-telefoonlijn, de computer, het onderwijslokaal, de winkelbeveiliging en het railvervoer niet zonder elektriciteit.

Nu zult u misschien zeggen dat de stroom toch maar zelden uitvalt? Het is maar wat je zelden noemt. In 2002 deden zich al meer dan dertig *grotere* stroomstoringen voor.

Maar dan kan toeval zijn? Neen. De *'high reliability organizations'*, want dat zijn energiebedrijven, faalden niet allemaal door leidingbreuken. Het typerende van deze organisaties is dat ze juist geen fouten *mogen* maken. Daarom heten ze ook *'zero fault organizations'*, dus nulfouten-organisaties. Daar komt nog iets bij: de doorwerking is groot en de betrokken bevolking weet zich geen raad. Het belang van de zaak is dus enorm.
In geval van een calamiteit treedt direct een ontregeling op. Noodscenario's moeten uit de kast en de communicatie moet slim op gang komen. Burgemeester Job Cohen meldde onlangs tweemaal rechtstreeks in het tv-programma Barend & Van Dorp de stroomuitval in een deel van Amsterdam. Dat was een illustratieve noviteit. Het vervelende van een stroomstoring is namelijk dat een advies uit de crisistheorie – informeer direct de bevolking om onrust te voorkomen – niet kan worden toegepast. De betrokken slachtoffers zijn immers onbereikbaar. Blijkbaar gokte Cohen op informatieverstrekking langs een omweg zoals via een op gang komend sms-berichtenverkeer want sms'jes kunnen stroomgestoorden, als ze geen digibeet zijn, wel ontvangen.

Denk niet dat stroomuitval het enige actuele veiligheidsrisico is. Onlangs kon Vaals bijna een dag niet over water beschikken.

Wie stroomuitval, computerstoringen op het spoor en de 'drooglegging' van Vaals wil duiden, komt uit bij *de theorie van de risicosamenleving*. Nederland heeft met *toenemende* veiligheidsrisico's in de publieke dienstverlening te maken. Zijn onze politici hiermee bezig? Tot nu toe ging de aandacht van politici vooral uit naar een *beperkt* veiligheidsconcept van fysieke veiligheid in de vorm van terrorisme, geweld en andere misdrijven. Er is evenwel sprake van toenemende andere risico's op het gebied van veiligheid in *brede* zin: de continuïteit van levering van elektriciteit, gas en water, en railvervoer via het spoor. Bij al deze distributieve diensten is sprake van een kans op haperende capaciteiten en verbindingen. Dat kunnen we niet hebben. Privatisering kan de problemen verergeren want de uitkomst daarvan is vaak een verminderde aandacht voor onderhoud en noodvoorzieningen.

Ik kan er daarom niet omheen, er is dringend behoefte aan een doordenking van de *ketenrisico's van de risicosamenleving vanuit een breed veiligheidsconcept*. Dat plan ontbreekt tot nu toe, laat staan de link tussen een eng en een breed veiligheidsconcept. Wie die relatie wel legt, komt uit bij de mogelijkheid om publieke voorzieningen met één ingreep lam te leggen.
Ik zie daarom graag in de volgende kabinetsformatie en het komende regeerakkoord een bezinning op de kwaliteit van *'nul fouten'*-organisaties. Het aantal stroomstoringen moet immers dalen en niet verder toenemen. De Nederlandse electriciteits-, gas- en waterleidingsector moet nadrukkelijk op veiligheidsrisico's en

aanwezigheid van noodscenario's doorgelicht worden. Tot nu toe hebben Nederlandse kabinetten hiervoor onvoldoende zichtbaar aandacht gehad.
Het ligt voor de hand dat kandidaten voor het minister-presidentschap al in de campagne een *toekomstschets van de risicosamenleving* gaven. Ik heb al een titel: *'Niet bij een kabel alleen'*.

Naschrift: Tussen het schrijven van deze bijdrage op 7 en de verschijning op 13 december deden zich nog nieuwe stroomstoringen voor.

***Literatuur: Over de betrouwbare organisatie***


- Korsten, A.F.A., De risicosamenleving, in: Binnenlands Bestuur, 13 december 2002, p. 25.
- Weick, K.E. & K. Sutcliffe, Managing the Unexpected – Assuring High Performance in the Age of Complexity, University of Michigan Business School, Jossey-Bass, San Francisco, 2001.
- Kramer, R.M. & T. Tyler (eds.), Trust in organizations, Sage, Londen, 1996.
- La Porte, T.R. & Consolini, P.M., Working in practice but not in theory: theoretical challenges of 'high reliability organizations', in: Journal of Public Administration Research and Theory, jrg. 1, 1991, nr. 1, pp. 19-47.
- La Porte, T.R., High reliability organizations: unlikely, demanding and at risk, in: Journal of Contingencies and Crisis Management, jrg. 4, 1996, nr. 2, pp. 60-71.
- Mannarelli, T., K.H. Roberts & R.G. Bea, Learning how organizations mitigate risk, in: Journal of Contingencies and Crisis Management, jrg. 4, 1996, nr. 2, pp. 83-92.
- Nye, J.S., P.D. Zelikow & D.C. King (eds.), Why people don't trust government, Cambridge, 1997.
- Rijpma, J. en M. Otten, Betrouwbaar management: een recept voor veiligheid?, in: Rosenthal, U, e.a., Crisis, Samsom, Alphen, 1998, pp. 21-42.
- Roberts, K.H. (ed.), New challenges to understanding organizations, Maxwell MacMillan, New York, 1993.
- Roberts, K.H., S.K. Stout & J.J. Halpern, Decision dynamics in two high reliability military organizations, in: Management and Science, jrg. 40, 1994, nr. 5, pp. 614-624.
- Rochlin, G.I., Reliable organizations: present reseach and future decisions, in: Journal of Contingencies and Crisis Management, jrg. 4, 1996a, nr. 2, pp. 67-80.
- Rochlin, G.I., The computer trap, Princeton UP, Princeton, 1996b.
- Sagan, S.D., The limits of safety: organizations, accidents and nuclear weapons, Princeton UP, Princeton, 1993.
- Sagan, S.D., Toward a political theory of organizational reliability, in: Journal of Contingencies and Crisis Management, 1994, nr. 4, pp. 228-240.
- Schulman, P.R., Heroes, organizations and high reliability, in: journal of Contingencies and Crisis Management, jrg. 4, 1996, nr. 2, pp. 72-82.

- Schulman, P.R., The analysis of high reliability organizations: a comparative framework, in: Roberts, R.K. (ed.), New challenges to understanding organisations, Maxwell MacMillan, New York, 1993b, pp. 33-53.
- Schulman, P.R., The negotiated order of organizational reliability, in: Administration and Society, jrg. 25, 1993a, nr. 3, pp. 353-372.