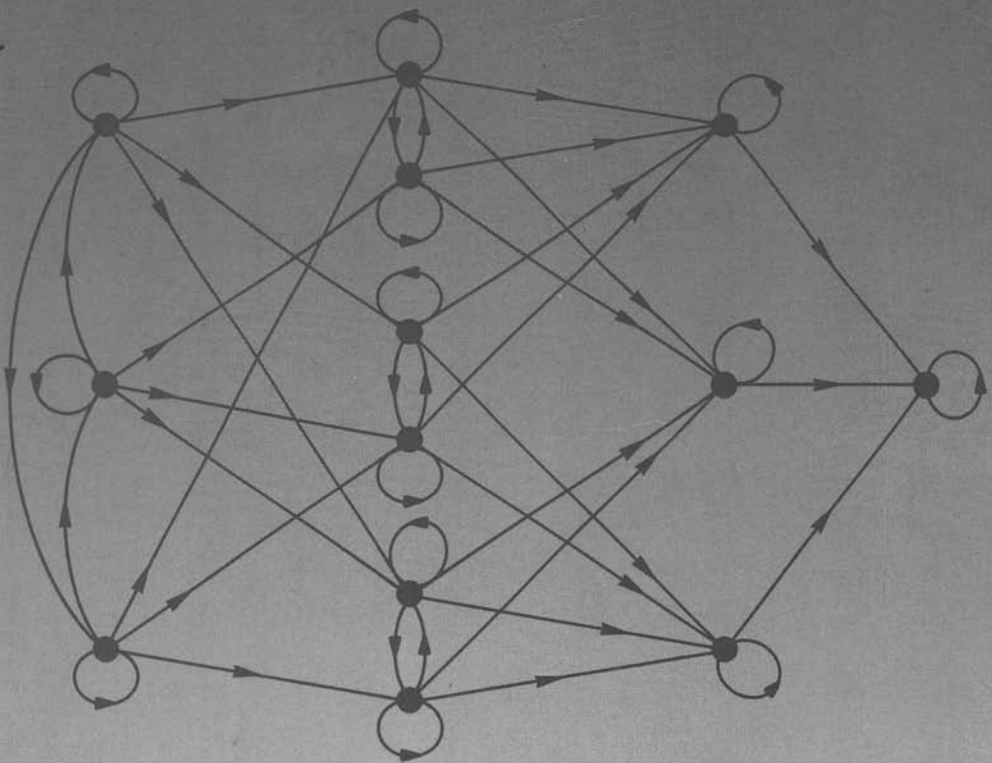
bedrijfszekerheid theorie en techniek



B. Klaassen, J.C.L. van Peppen, A. Bossche

bedrijfszekerheid

theorie en techniek

bedrijfszekerheid

theorie en techniek

dr.ir. K.B. Klaassen
ir. J.C.L. van Peppen
dr.ir. A. Bossche

Delftse Uitgevers Maatschappij - 1988

CIP-gegevens Koninklijke Bibliotheek, Den Haag

Klaassen, K.B.

Bedrijfszekerheid : theorie en techniek / K.B. Klaassen, J.C.L. van Peppen, A. Bossche.
– Delft : Delftsche U.M. – Ill.
Met index, lit. opg.
ISBN 90-6562-073-7
SISO 642 UDC 658.511.5 : 658.274
Trefw.: bedrijfszekerheid.

Eerste druk 1988

Delftse Uitgevers Maatschappij b.v.

P.O. Box 2851, 2601 CW Delft, The Netherlands

Tel. 015–123725

ISBN 90 6562 073 7

Ten Geleide

De enorme industriële expansie van de laatste decennia heeft tot gevolg gehad dat we in ons dagelijks leven gebruik maken en afhankelijk geworden zijn van een groot aantal technische systemen. Het betreft hier een breed spectrum reikend van eenvoudige technische systemen zoals een elektronisch horloge tot zeer complexe systemen, bijvoorbeeld een vliegtuig. Vaak zijn we ons het gebruik van een bepaald technisch systeem niet eens meer bewust (een gedeelte van onze elektrische energie komt van nucleaire reactoren) tot we er op onprettige wijze aan worden herinnerd (Chernobyl).
Dat deze technische systemen realiseerbaar zijn, met andere woorden dat ze zonder mankeren kunnen werken ten tijde van de ingebruikneming, is inmiddels wel bewezen. Een hogere orde eis is evenwel dat ze ook naar behoren *blijven werken*: dat ze *bedrijfszeker* zijn. Dit aspect van onze industriële activiteit heeft pas de laatste tijd meer nadruk gekregen. Produceerbaarheid, opbrengst en kwaliteit zijn eerste vereisten voor een industrieel produkt, maar een goede bedrijfszekerheid over de gehele geplande gebruiksduur van het produkt is een minstens even belangrijke parameter.
De aarzeling die zich bij de producenten met betrekking tot de aanvaarding van bedrijfszekerheid als een van de ontwerpdoelstellingen voor een produkt voordoet, moet voornamelijk verklaard worden uit de extra kosten die ermee gepaard gaan, en uit het voor de klant 'ongrijpbare' karakter ervan. Of het produkt al dan niet werkt kan hij onmiddellijk vaststellen, of het blijft werken is voor hem een open vraag. De afnemer weet bij aanschaf niet dat het ene systeem meer bedrijfszeker is dan het andere en dat het initiële prijsverschil bij aanschaf meer dan gewettigd is door de latere besparingen op 'narigheden' zoals reparatiekosten, ergernis, produktieverlies, ongelukken en milieuverwoesting. Te oordelen naar het grote aantal bedrijfsonzekere systemen wordt het motto achter de techniek van de bedrijfszekerheid 'invest now, save later' nog steeds niet door iedereen onderkend.

Een secundaire oorzaak voor de aarzeling bedrijfszekerheid te beschouwen als een der produktspecificaties is dat men vaak niet weet hoe men een produkt bedrijfszekerder moet maken. Om in deze lancune bij afstuderende ingenieurs te voorzien werd door K.B. Klaassen in 1982 een college Bedrijfszekerheidstechniek (*Reliability Engineering*) opgezet aan de afdeling der Elektrotechniek van de Technische Hogeschool te Delft. Door de grote belangstelling voor dit college, mede van de zijde van de studenten in de Avionica opleiding, werd een goed collegedictaat een eerste vereiste. Dit

dictaat bleek zo'n grote belangstelling buiten de TH op te wekken dat het wenselijk bleek over te gaan tot de publicatie van een boek. Het betreffende college wordt thans verzorgd door ir. A. Bossche. De beide andere auteurs zijn thans werkzaam bij het IBM Research Laboratorium in San Jose, Californië, USA.

Bij het tot stand komen van dit boek is met dank gebruik gemaakt van de vele opmerkingen van studenten aan de TU-Delft. In het bijzonder willen wij noemen J.C. van Dijk voor zijn vele coördinerende werkzaamheden tussen San Jose en Delft, de heer G. van Berkel voor het maken van de vele illustraties en J.D. Schipper die assisteerde bij de eerste versie van het collegedictaat.

Voorjaar 1988
San Jose, Californië — Delft

K.B. Klaassen
J.C.L. van Peppen — A. Bossche

Inhoud

1. Inleiding

Het vak bedrijfszekerheidstechniek bestrijkt een groot en zeer gevarieerd terrein; het is daarom niet doenlijk de vele facetten van dit vak alle in één boek tot hun recht te laten komen. Het totale terrein van de bedrijfszekerheidstechniek is globaal als volgt in te delen:

- *Bedrijfszekerheidstheorie:* de mathematische benadering van de bedrijfszekerheidsproblematiek met statistische en stochastische middelen, bijvoorbeeld: levensduurschattingstheorieën, vernieuwingstheorie, wachttijdtheorie, voorraadtheorie.
- *Meten, testen en toetsen:* het meten van de behaalde bedrijfszekerheid van een produkt op basis van experimenten (*tests*)*, uitgevoerd op slechts een deel van de produkten (*sample*), gedurende een relatief korte spanne tijds (*accelerated test*) die niet voortgezet worden tot de hele sample gefaald heeft (*truncated tests*) en het bepalen van de statistische betrouwbaarheid van de metingen.
- *Bedrijfszekerheidsanalyse:* het verzamelen van foutgegevens, het reduceren van deze gegevens en op andere wijze bewerken daarvan voor gebruik bij toekomstige ontwerpen. De optredende fouten kunnen fysisch worden geanalyseerd (*physics of failure*), maar ook statistisch. De informatie over faaloorzaken, faalmechanismen en faalwijzen van komponenten wordt teruggekoppeld naar de ontwerpfase om in toekomstige produkten de gevolgen van zulke fouten te beperken.
- *Ontwerptechnieken:* het verhogen van de inherente bedrijfszekerheid van een produkt door: speciale bedrijfszekere componenten (*hi-rel components*), verlagen van het belastingsniveau van de componenten (*derating*), op gezette tijden bijstellen van het ontwerp (*design reviews*), aanpassen van het produkt aan gebruiker en gebruiksomgeving (*human engineering, protection*), goed onderhoudbaar maken (modulaire opbouw, standaardisatie) en het toepassen van extra onderdelen (*hardware redundancy*) of extra berekeningen of operaties (*software redundancy*).
- *Management:* het opbouwen en in stand houden van een (bedrijfs-) organisatie geschikt voor het ontwerpen, ontwikkelen, produceren en onderhouden van bedrijfszekere produkten. Het ontwikkelen van de benodigde administratieve en logistieke ondersteuning daarvan. Verder vallen ook opleidingsprogramma's en inspectie-, test- en onderhoudsprocedures hier-

*) *In het boek zullen vele begrippen uit de bedrijfszekerheidstechniek tussen haakjes in het Engels worden opgenomen.*

onder, alsmede de kosten-baten analyses van de toegepaste bedrijfszekerheidstechnieken.

Van de bovenstaande onderwerpen zal in dit boek over bedrijfszekerheidstechniek het management-aspect niet worden besproken. De bedrijfszekerheidstheorie zal worden behandeld aan de hand van een aantal voorbeelden uit gebieden zoals de energietechniek, de avionica, de elektronica, de regel- en procestechniek, de computertechniek en het alledaagse leven. Verder zal een aantal aspecten van de bedrijfszekerheidsanalyse worden behandeld. Daarnaast zal een aantal ontwerptechnieken worden geëvalueerd, evenals een aantal onderhoudstechnieken.

N.B.: 1. Het begrip "bedrijfszekerheid" moet niet verward worden met het begrip "betrouwbaarheid". Beide begrippen komen in de bedrijfszekerheidstechniek voor. De term betrouwbaarheid is daarbij gereserveerd voor de kans dat de werkelijke waarde van een stochastische parameter van de totale populatie valt binnen een zeker interval rondom de geschatte waarde die is bepaald op basis van een eindige steekproef uit die populatie (Engels: confidence, confidence level).
2. Het begrip "bedrijfszekerheid" wordt ook vaak verward met "kwaliteit" of andersom kwaliteit met bedrijfszekerheid. De kwaliteit wordt bepaald door de mate waarin de eigenschappen van een produkt (of een dienst) vallen binnen van tevoren vastgestelde specificatietoleranties. Als in de produktspecificatie geen eisen ten aanzien van de levensduur voorkomen, dus als de kwaliteit alleen slaat op het tijdstip van de oplevering door de producent aan de gebruiker, drukt men de fractie van het totale aantal produkten dat aan de specificaties voldoet uit in de conformiteit (*conformity*).
Als in de specificaties ook eisen ten aanzien van de levensduur van het produkt vermeld staan, dus als de eigenschappen van het geleverde produkt ook na het tijdstip van oplevering van (in de specificaties) onderkend belang zijn, drukt men de fractie van het totale aantal geleverde produkten dat op een tijdstip na het tijdstip van oplevering t_0 nog steeds volgens de specificaties functioneert uit in de bedrijfszekerheid (*reliability*).

In de volgende paragraaf zal worden uiteengezet wat we precies verstaan onder bedrijfszekerheid.

1.1. Definities

In dit boek zal met *bedrijfszekerheid* worden aangeduid de *kans* dat een bepaald *systeem* nauwkeurig *gespecificeerde functies* uitvoert gedurende een bepaald interval van een *levensduurvariabele*, onder de conditie dat het systeem bedreven wordt binnen een bepaald *omgevingsgebied*. Deze algemene definitie omvat zes elementen die we hieronder kort zullen toelichten:

- *Bedrijfszekerheid*: dit is een kans die helaas vaak onjuist aangeduid wordt met betrouwbaarheid en ook vaak verward wordt met het begrip kwaliteit. Beide begrippen komen uit de kwaliteitsbeheersing (Engels: quality control), een vakgebied waaruit zich later de bedrijfszekerheidstechniek heeft afgesplitst.
- *Kans*: men dient onderscheid te maken tussen de voorspelde of a priori bedrijfszekerheid die gedefinieerd is als een zuivere kans, en de bewezen of a posteriori bedrijfszekerheid die een zekerheid achteraf is, en gedefinieerd is als de fractie overlevende produkten. Voor een toekomstig ontwerp kan men slechts voorspellen; achteraf bijvoorbeeld in een "case history" heeft men zekerheid.
- *Systeem*: onder een systeem wordt hier verstaan een verzameling elementen (componenten, units, modules) die in onderlinge wisselwerking met elkaar staan (samenhangen) en afgescheiden kunnen worden van de omgeving van het systeem (systeemgrens). De onderlinge wisselwerking tussen de elementen van het systeem realiseert de systeemfunctie, die in het algemeen uitgesplitst kan worden in een aantal gespecificeerde eigenschappen.
  De aanduiding "systeem" omvat niet alleen technische systemen zoals componenten, apparaten, installaties en machines, maar ook niet-technische systemen zoals biologische organismen, organisaties en diensten. Wij zullen onze voorbeelden gemakshalve voornamelijk beperken tot technische systemen.
- *Gespecificeerde functie*: het doel dat met een bepaald systeem wordt beoogd komt tot uiting in de systeemfuncties, die bestaan uit één of meerdere gespecificeerde eigenschappen. Bij systemen met tussen bepaalde grenzen continu variërende signalen (analoge systemen) is een systeemfunctie (bijvoorbeeld versterking) uit te splitsen in een aantal eigenschappen (spanningsversterking 100, bandbreedte 2 MHz) die onderworpen zijn aan toleranties (spanningsversterking $100 \pm 5\%$, bandbreedte > 2 MHz). Een voorbeeld hiervan is gegeven in tabel 1.1. Zijn een of meer van de tolerantie-intervallen overschreden dan is het systeem niet langer bedrijfszeker: het heeft gefaald. In het geval van analoge systemen (in casu de versterker) kan het systeem dan nog wel functioneren, maar buiten de toleranties. Bij systemen die werken met binaire signalen (digitale systemen) treft men meestal aan dat een bepaalde functie (bijvoorbeeld toegang tot een achtergrondgeheugen) of een eigenschap daarvan (het kunnen wegschrijven van informatie) volledig wegvalt, d.w.z. niet meer te gebruiken is, nadat er een fout is opgetreden. De verleiding om met een defect systeem te blijven doorwerken is daar niet aanwezig.
- *Levensduurvariabele*: in verreweg de meeste gevallen zal men de tijd als

Name	Instrumentation Amplifier	
Manufacturer	XXX Corporation	
Model Number	3456-B	
All specifications traceable to US Bureau of Standards		
Function	Voltage Amplification	
Specifications	Gain	100 ± 5%
	Frequency Range (–3 dB)	DC –2 MHz
	Noise (referred to input)	$< 1.5\ nV/\sqrt{Hz}$
	Input Impedance	> 1 Mohm
	Output Impedance	< 0.1 ohm
	Nonlinearity (input < 1 V)	$< 10^{-3}$
	Max. Output Current	> 100 mA (short circuit protected)
	Required Line Power	< 42 VA
Environment	Temperature Range	
	Operational	0 °C to 50 °C
	Storage	–40 °C to 75 °C
	Humidity Range	< 95%,no condensation
	Altitude	
	Operational	< 4.5 km
	Mechanical Shocks	$< 50\ m/s^2$
	Line Voltage Range	120 V +5%,–10%
	Line Frequency Range	48 Hz to 440 Hz
Reliability	Mean time to failure (no maintenance)	5 years

Tabel 1.1. Een voorbeeld van een systeem (meetversterker) met een bepaalde functie (spanningsversterking) die gespecificeerd is, evenals het omgevingsgebied. De bedrijfszekerheid is gegeven in de verwachte gemiddelde levensduur.

levensduurvariabele aantreffen. Dit kan de kalendertijd zijn, maar ook de geaccumuleerde gebruikstijd (bedrijfsuren). Ook kan de tijd dat het systeem niet in gebruik is toch worden meegewogen, als deze tijd wel bijdraagt tot een levensduurverkorting. De gewogen tijd is dan $t = t_b + at_{bb}$, waarin t_b de bedrijfstijd is en t_{bb} de tijd dat het systeem buiten bedrijf is. De coëfficiënt a is in zulke gevallen altijd kleiner dan 1. Er zijn echter gevallen waarin systemen buiten bedrijf, per eenheid van tijd, een grotere uitval vertonen dan in bedrijf. Denk aan elektrolytische condensatoren,

effecten van condensatie in systemen buiten bedrijf en ook aan mensen met een te lichte of geen taak die door verveling fouten maken. De levensduurvariabele kan, naast de tijd, ook zijn het aantal in- en uitschakelingen (relais), het aantal belastingswisselingen (vermoeiingsbreuken in vliegtuigvleugels, landingsgestellen, straalturbineschoepen) en de afgelegde afstand (auto's).

- *Omgevingsgebied*: elk systeem bevindt zich in een bepaalde omgeving. Alle elementen die geen deel uitmaken van het systeem behoren tot deze omgeving, dus ook de gebruiker en de rest van de installatie waar het beschouwde systeem op zijn beurt deel van uitmaakt. Als men een systeem al dan niet opzettelijk in een verkeerde omgeving plaatst (dus buiten het gespecificeerde omgevingsgebied), kan het systeem uitvallen of versneld verouderen. Te denken valt aan een te hete, te natte omgeving, een te hoge voedingsspanning, te grote ingangssignalen, een te grote of te kleine belasting (onbelast vol gas geven bij een automotor). Dit zogenaamde verkeerde gebruik (Engels: misuse) van een systeem buiten het gespecificeerde omgevingsgebied is niet van te voren in te calculeren en is daarom in de bedrijfszekerheidsdefinitie uitgesloten.
  N.B.: De meeste systemen sneuvelen in de praktijk door 'misuse' òf van de zijde van de gebruiker òf van de zijde van de ontwerper die componenten van het systeem verkeerd toepast: door menselijke fouten dus.

In het bovenstaande is de definitie van bedrijfszekerheid nader toegelicht. Hierbij blijkt dat zonder een expliciete, duidelijk geformuleerde omschrijving van het beschouwde *systeem*, de *systeemfuncties* en het *toegestane omgevingsgebied*, er geen uitspraak over de bedrijfszekerheid van zo'n systeem mogelijk is. Wat is bijvoorbeeld de bedrijfszekerheid van een mens. Valt een mens als hij hoofdpijn heeft buiten de specificaties?
Bij technische systemen, maar ook bij diensten en dergelijke, is het derhalve van groot belang deze zaken zo precies mogelijk te omschrijven, zulks onder meer in verband met de latere juridische en financiële consequenties (wettelijke aansprakelijkheid voor en garantie van produkten en dergelijke).

We zullen later zien dat het van belang is onderscheid te maken tussen systemen die worden onderhouden en systemen waarbij dit niet het geval is. We verstaan hierbij onder *onderhoud* (Engels: maintenance) elke vorm van menselijk ingrijpen die het systeem in een bruikbare toestand houdt of weer in een bruikbare toestand terugbrengt.
Als een systeem wel onderhoudbaar is maar door de gebruiker niet onderhouden wordt behoort zo'n systeem defacto tot de tweede bovengenoemde groep van systemen zonder onderhoud. Liever dan de term 'onderhoud-

baar' die een intentie aangeeft, gebruiken we daarom de term 'onderhouden'. De bovenstaande twee categorieën zullen we derhalve aanduiden met 'onderhouden' en 'niet-onderhouden' systemen.

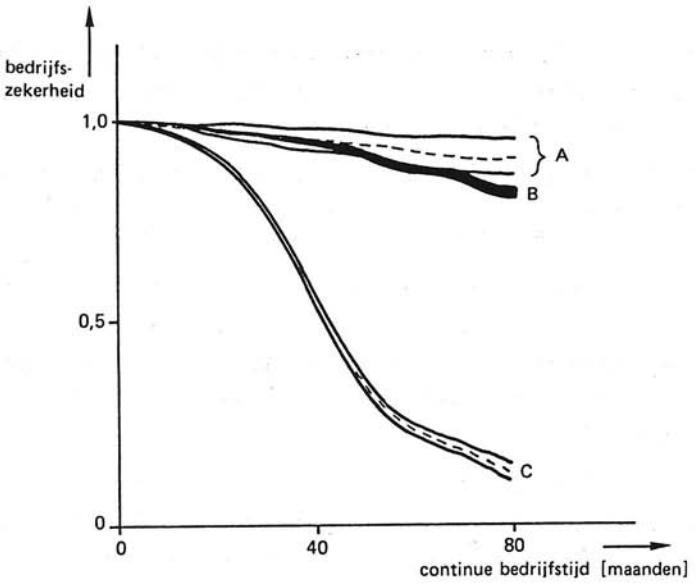
Het begrip bedrijfszekerheid slaat alleen op niet-onderhouden systemen, daar het systeem in het beschouwde interval van de levensduurvariabele moet blijven werken. Er mogen dus geen fouten optreden. Reparatie is niet toegestaan.

Men heeft daarom voor onderhouden systemen een algemener begrip ingevoerd: de *beschikbaarheid* (Engels: availability). Voor niet-onderhouden systemen is de beschikbaarheid gelijk aan de bedrijfszekerheid. We zullen op de beschikbaarheid uitvoerig terugkomen in hoofdstuk 7, bij het bespreken van repareerbare systemen.

De *bedrijfszekerheidstechniek* kan men nu definiëren als het geheel van wiskundige, organisatorische en andere toegepast wetenschappelijke technieken, methoden en strategieën om te geraken tot een bedrijfszeker produkt. Het omvat ook de bepaling van de mate van bedrijfszekerheid van dit produkt.

1.2. Noodzaak van bedrijfszekerheidstechniek

De noodzaak van het beoefenen van de bedrijfszekerheidstechniek kan eenvoudig afgeleid worden uit de relatie tussen de elementen van de bedrijfszekerheidsdefinitie die in de vorige paragraaf is gegeven. De systeemomvang, de gespecificeerde functies, het interval van de levensduurvariabele, de omvang van het omgevingsgebied beïnvloeden alle de bedrijfszekerheid.
Het zal duidelijk zijn dat de actuele trend naar systemen van grotere omvang, dat wil zeggen systemen met grotere aantallen componenten, de bedrijfszekerheid verlaagt als niet gelijktijdig de ontwikkeling van meer bedrijfszekere systeemcomponenten en -structuren daarmee gelijke tred houdt. Zulke systemen met een grote *kwantitatieve complexiteit* zijn er te over, zoals energiedistributienetten, telecommunicatienetten, digitale telefooncentrales en ruimtesondes.
Daarnaast is er een trend naar complexere systeemfuncties, dat wil zeggen er worden meer functies van een systeem geëist, de functies zijn ingewikkelder (wat tot uiting komt in meer gespecificeerde eigenschappen) en de toegestane toleranties worden kleiner. Deze toename van *kwalitatieve complexiteit* doet ook de bedrijfszekerheid dalen als er geen adequate tegenmaatregelen genomen worden. Hierbij valt te denken aan : multi-functie meetapparatuur met een hogere, vereiste nauwkeurigheid, automatische landingssystemen voor vliegtuigen, procesregelapparatuur en dergelijke.
Verder wordt het correct functioneren van een systeem over een langer interval van de levensduurvariabele hoe langer hoe belangrijker naarmate we meer van zulke systemen afhankelijk zijn (energieopwekkingssyste-



Figuur 1.1. De bedrijfszekerheid van verschillende energiebronnen voor pacemakers.
a) nucleaire batterijen (140 stuks);
b) lithium batterijen (5600 stuks);
c) kwik-zink batterijen (2000 stuks).

men, pacemakers en dergelijke). Deze zogenaamde kritische systemen vereisen een hoge bedrijfszekerheid over vaak lange tijden (bijvoorbeeld 25 jaar voor telecommunicatiesystemen). Zo is in pacemakers bijvoorbeeld het zorgenkind de energiebron, want circuitfouten in een pacemaker komen voor met een kans van minder dan 140×10^{-9} per uur. In figuur 1.1 is de bedrijfszekerheid van een aantal verschillende energiebronnen voor pacemakers geschetst.

Bovendien worden onze technische systemen meer en meer blootgesteld aan onvriendelijke omgevingen; zij moeten geschikt zijn voor een groter omgevingsgebied. Denk maar aan toepassingen in de procesindustrie (hitte, vocht, chemische stoffen), mobiele toepassingen in vlieg-, vaar- en voertuigen (mechanische trillingen, schokken, slecht gedefinieerde voedingsspanningen, hoog storingsniveau).

Al met al voldoende redenen waarom de bedrijfszekerheidstechniek tegenwoordig volop in de belangstelling staat. Voeg daar nog aan toe de nadruk die op bedrijfszekerheid valt als er geen onderhoud mogelijk is door een geïsoleerde locatie (afgelegen: onbemande arctische weerstations, onbereikbaar: ruimtesondes, onder water: versterkerstations bij transatlantische kabels, enzovoort). Zelfs al zou er wel onderhoud mogelijk zijn, dan is het vaak verantwoord de initiële bedrijfszekerheid van een systeem te vergroten vanwege de hoge kosten die gepaard gaan met buiten bedrijf zijn, reparatie enzovoort. Ondanks de hogere initiële kos-

ten kunnen dan toch de kosten over de gehele nuttige levensduur van het systeem (Engels: life cycle cost) lager uitvallen. Men duidt dit aan als het 'invest now, save later' principe.
Ook de sociaal-ethische aspecten van produkten met een te lage bedrijfszekerheid mag men niet uit het oog verliezen. Deze wegwerpprodukten leiden tot een verspilling van arbeidsinspanning, energie en steeds schaarser wordende grondstoffen.

1.3. Statistische versus deterministische benadering

Zoals we in paragraaf 1.1 reeds gezien hebben moet men onderscheid maken tussen *a priori* of voorspelde bedrijfszekerheid en *a posteriori* of bewezen bedrijfszekerheid.
Bij de statistisch voorspellende benadering van het bedrijfszekerheidsvraagstuk zal men op basis van gegevens omtrent het praktijkgedrag van vroeger geproduceerde componenten en op basis van de uitkomsten van (kunstmatig versnelde) bedrijfszekerheidsmetingen aan huidige componenten een uitspraak proberen te doen over de te verwachten bedrijfszekerheid van toekomstige systemen. Bij deze benaderingswijze doet zich een aantal problemen voor.
Met de snelle ontwikkeling van de techniek zullen toekomstige produkten zelden nog componenten bevatten waarvan we de bedrijfszekerheidshistorie kennen; in het algemeen beschikken we dus niet over statistische gegevens voor de berekening van de systeembedrijfszekerheid. Zelfs al zouden we wel vroeger ontwikkelde componenten met een bekende historie gebruiken, de toe te passen componenten zijn vrijwel zeker op een ander tijdstip vervaardigd. Het produktieproces is tussen deze tijdstippen in meestal bijgesteld. Uit onderzoek blijkt dat deze op het eerste gezicht kleine bijstellingen grote gevolgen voor de bedrijfszekerheid kunnen hebben. De later geproduceerde componenten voldoen dan niet meer aan de eerder bewezen bedrijfszekerheid (produktie-inhomogeniteit in de tijd).

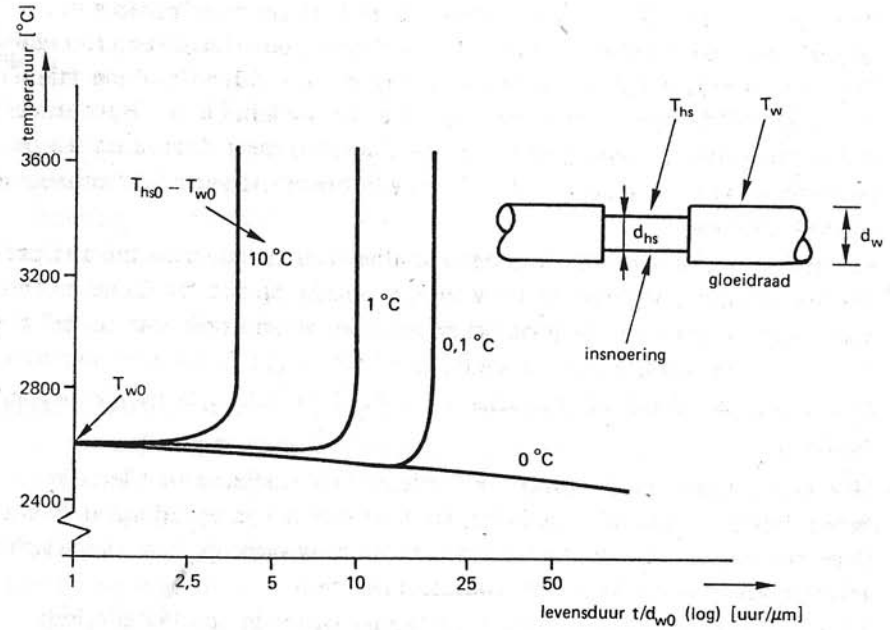
Een alternatief zou zijn het meten van de bedrijfszekerheid van componenten door ze versneld te verouderen. Ook hierbij doet zich een aantal problemen voor.
Hoe groot is de versnellingsfactor precies? Zijn de parameters waarop de komponenten versneld verouderd worden ook werkelijk representatief voor de veroudering in de praktijk, of worden ook andere faalmechanismen op gang gebracht (te lage uitkomst), of worden bepaalde faalmechanismen uit de praktijk niet of met een afwijkende versnellingsfactor gerealiseerd (te hoge uitkomst)?
Een ander probleem is dat we doorgaans niet 100% van de componenten kunnen meten (bijvoorbeeld omdat ze een lagere resterende levensduur

hebben) en we dus moeten volstaan met een monster (Engels: sample) uit de totale verzameling van componenten (populatie). Als de produktie niet voldoende homogeen is leidt vooral een klein monster tot onbetrouwbare uitspraken over de gehele verzameling (produktie-inhomogeniteit binnen één partij).
Al met al is de conclusie dat de statistici ons zeer fraaie bemonsterings-, test- en berekeningswijzen aanreiken die we in de bedrijfszekerheidstechniek goed kunnen gebruiken maar dat we vaak moeten erkennen dat we een ontstellend tekort aan gegevens hebben. We moeten vaak volstaan met veel geschatte gegevens. De eindresultaten zijn dan zo weinig betrouwbaar dat we weinig meer kunnen doen dan een tamelijk vage uitspraak omtrent de te verwachten bedrijfszekerheid van een toekomstig systeem. In dit verband dient te worden opgemerkt dat de statistische aanpak (met veel geschatte componentgegevens) vaak een goede benadering geeft in de *verhouding* van de bedrijfszekerheden die men krijgt wanneer men verschillende ontwerpalternatieven met elkaar vergelijkt.

Om de bovenstaande redenen is naast de statistische benadering van het bedrijfszekerheidsvraagstuk de deterministische benadering van groot belang. De deterministische aanpak bestaat daaruit dat men bestudeert welke fysische aftakelingsprocessen (faalmechanismen) in de praktijk in een component op gang kunnen komen, hoe zij leiden tot uitval van het produkt en hoe deze processen tot staan gebracht of vertraagd kunnen worden. Op basis van de kennis van het (dominante) aftakelingsproces (bijvoorbeeld verdamping van een gloeidraad) en de snelheid van het proces (afhankelijk van de temperatuur en dus van de stroom en de weerstand) kan men een voorspelling doen van de levensduur (in branduren tot het moment van doorbranden).

Als voorbeeld van de deterministische aanpak van een bedrijfszekerheidsprobleem volgt hier een studie van faalmechanismen in gloeilampen. Gloeilampen worden gemaakt voor een bepaalde netspanning U (bijvoorbeeld 220 volt effectief), zodanig dat het gedissipeerde vermogen P ($P = U^2 / R_{heet}$) een bepaalde waarde heeft (bijvoorbeeld P = 100 watt). Dit bepaalt onder andere de lengte en dikte van de wolfraam gloeidraad. De gloeidraad is meestal gespiraliseerd (en soms zelfs dubbel gespiraliseerd) om de hitteopbrengst (temperatuur/vermogen) en daarmee de lichtopbrengst (lumen/watt) groot te maken. Na het inschakelen bereikt de gloeidraad in 10 tot 20 ms een eindtemperatuur van 2500 tot 2600 °C. Het daarmee gepaard gaande snelle uitzetten (en krimpen bij het afschakelen) kan aanleiding geven tot vermoeidheidsbreuken in de gloeidraad (thermal fatigue). Dit faalmechanisme heeft als levensduurvariabele het aantal aan/uit cycli van de lamp.

Als de gloeidraad continu blijft branden is het dominante faalmechanisme de verdamping van de gloeidraad. De levensduurvariabele is hier het totaal aantal branduren. Men stuit hier evenwel op een paradox: *een uniform verdampende gloeidraad, gevoed uit een constante spanning, kan niet falen door verdamping*. De werkelijke oorzaak van overlijden van de lamp is daarom een lokaal sterk toegenomen verdamping, bijvoorbeeld op de plaats van een scheurtje of een vernauwing door de oppervlakteruwheid van de getrokken gloeidraad. Ter plaatse van deze vernauwing is de dissipatie en dus ook de temperatuur hoger, waardoor de verdamping daar veel sneller gaat. In figuur 1.2 is aangegeven hoe de levensduur t afneemt naarmate de temperatuur T_{hs} van een 'hot spot' verder ligt boven de temperatuur T_w van de rest van de gloeidraad.
N.B.: Kleine verschillen in diameter en dus in temperatuur hebben grote gevolgen. De conclusie is dan ook dat kwaliteitsbeheersing van de gloeidraad bij de produktie van doorslaggevend belang is voor de latere levensduur van de lamp.



Figuur 1.2. Genormaliseerde levensduur t/d_{w0} van een gloeidraad ten gevolge van een initieel, locaal verhoogde temperatuur T_{hs0} die veroorzaakt wordt door een insnoering. De initiële draaddiameter is d_{w0}, de initiële 'hot spot' temperatuur is T_{hs0}, de initiële draadtemperatuur is T_{w0}. Een klein temperatuurverschil heeft grote gevolgen!

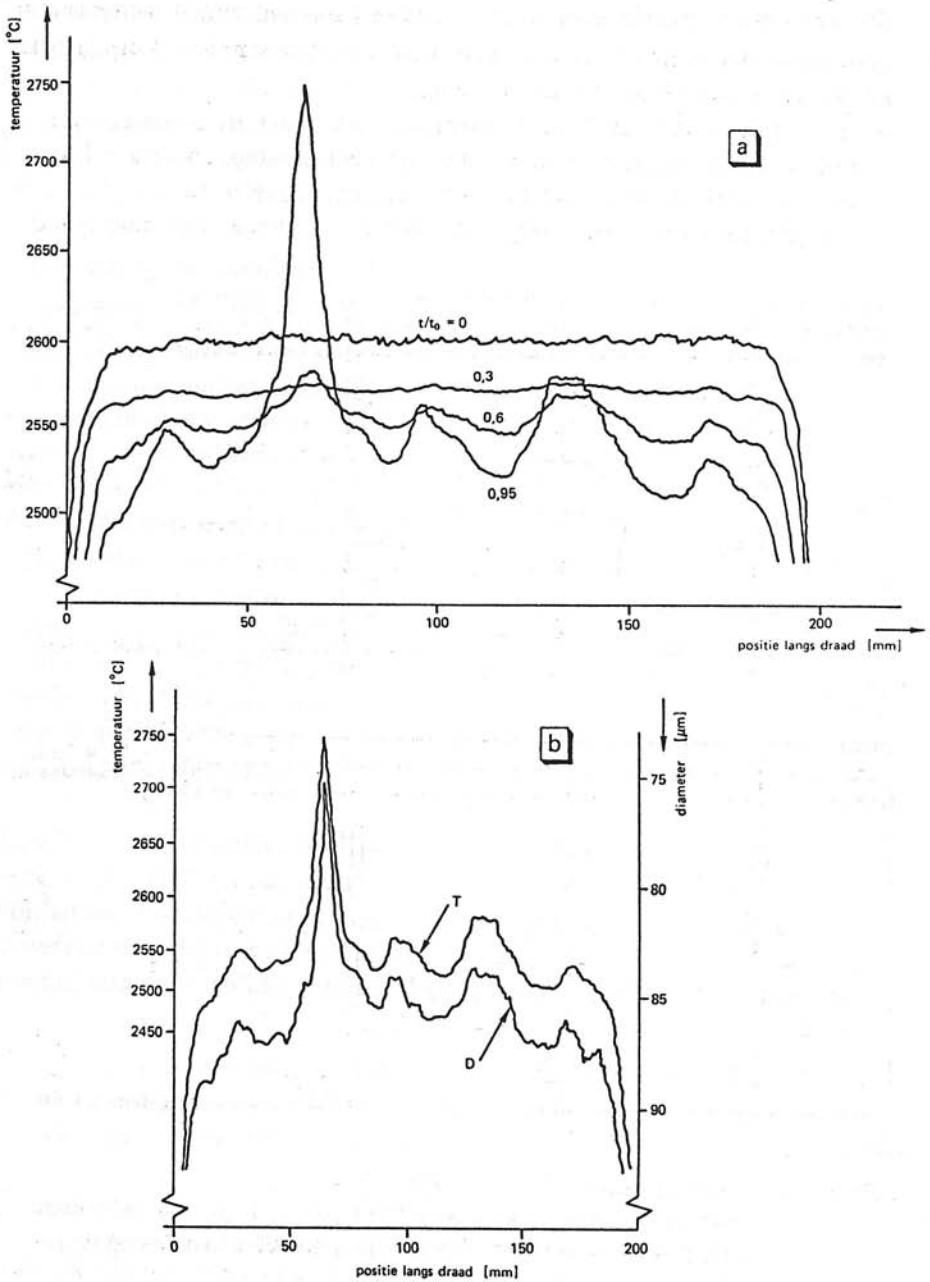
In figuur 1.3a is het temperatuurprofiel langs een continu brandende gloeidraad uitgezet. Dit is gedaan op vier tijdstippen namelijk op 0, 30, 60 en 95 % van de levensduur t_0 van de gloeidraad. We zien duidelijk de ontwikkeling van een 'hot spot'. In figuur 1.3b tenslotte is aangegeven hoe het temperatuurprofiel (aangeduid met T) correleert met het gemeten diameterprofiel van de gloeidraad (aangeduid met D).
Tenslotte nog een laatste opmerking. Veel gloeilampen overlijden voortijdig door netspanningspieken. Een te hoge netspanning werkt namelijk als versnellende factor op de beide bovengenoemde faalmechanismen.

De informatie die men bij een versnelde meting voor statistische doeleinden vaak negeert is de informatie over de opgetreden faalmechanismen in de defecte componenten. Deze faalmechanismen zullen waarschijnlijk ook in de overige componenten aanwezig zijn, maar hebben onder de testomstandigheden binnen de testduur bij die componenten niet tot falen geleid. In de praktijk (zonder versnelling) zou dit anders kunnen uitpakken indien de versnellingsfactoren voor de diverse faalmechanismen verschillend zijn.
De vragen die opwellen bij uitsluitend onderzoek naar de 'physics of failure' zijn onder andere: kunnen bijvoorbeeld door statistische fluctuaties in het produktieproces sommige componenten falen door een faalmechanisme dat bij de meeste componenten niet waarschijnlijk is? Bijvoorbeeld kleine scheurtjes die ontstaan in een gloeidraad tijdens fluctuaties in het trekproces, waar de normale gloeidraad een oppervlakteruwheid begrensde levensduur heeft.
Een andere vraag is of veel van deze studies naar faalmechanismen (Engels: physics of failure studies) niet teveel zijn gericht op het 'typische' exemplaar, waardoor de gehele produktiepopulatie, waarin ook 'a-typische' exemplaren kunnen voorkomen, te weinig aandacht krijgt. Juist deze a-typische exemplaren zouden later wel eens het faalgedrag van de populatie kunnen bepalen.

Men kan derhalve niet volstaan met alleen de statistische of alleen de deterministische aanpak. Beide benaderingswijzen zijn eenzijdig: de statisticus interesseert zich niet voor wat er fout is gegaan, de fysicus is slechts geïnteresseerd in de 'typische' foutmechanismen.
Al met al redenen om de beide benaderingswijzen in goede onderlinge harmonie samen toe te passen om te geraken tot een bedrijfszeker produkt.

1.4. Methoden ter verhoging van de bedrijfszekerheid

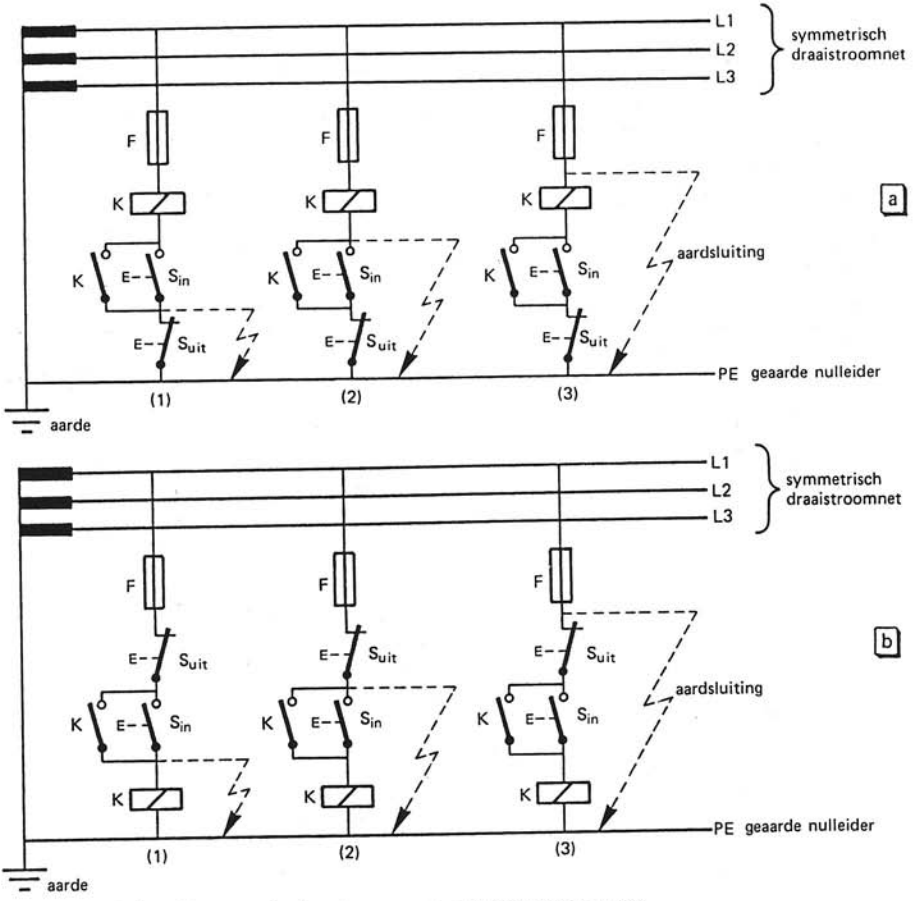
Er zijn verschillende wijzen waarop de inherente bedrijfszekerheid van een systeem veilig gesteld kan worden. Dit is de bedrijfszekerheid die het systeem inherent meekrijgt en die ook gerealiseerd zal worden in de prak-



Figuur 1.3. Temperatuurverloop langs een gloeidraad van een gloeilamp.
a) Temperatuurprofiel op vier verschillende tijdstippen t/t_0 gedurende het leven $(0, t_0)$ van een gloeidraad.
b) Correlatie tussen het temperatuurprofiel (aangeduid met T) en het profiel van de gloeidraaddiameter (aangeduid met D) voor het tijdstip $t/t_0 = 0{,}95$.

tijk als er geen 'misuse' plaatsvindt. In deze paragraaf zullen we de meest belangrijke maatregelen die men kan nemen kort bespreken. Vele hiervan komen later nog uitgebreid aan de orde.

- Het introduceren van bedrijfszekerheid als een van de doelstellingen in een zo vroeg mogelijke fase van het systeemontwerp. In figuur 1.4 is een voorbeeld gegeven van hoe belangrijk in dit verband een goed doordacht ontwerp is. Deze vroege introductie is noodzakelijk daar, als de



Figuur 1.4. Ontwerpfouten in een geaard draaistroomnet.
Het relais K dient, ondanks aardsluitingsfouten, afschakelbaar te zijn of (doordat de zekering F smelt) afgeschakeld te worden. Aardsluitingen mogen K niet inschakelen. S_{in} is een normaal open drukcontact voor het inschakelen, S_{uit} een normaal gesloten afschakeldrukcontact.
a) Fout ontwerp. Vóór het inschakelen kan aardsluiting 2 K inschakelen zonder commando. Ná het inschakelen maken aardsluiting 1 en 2 dat K niet meer afgeschakeld kan worden.
b) Goed ontwerp. Zowel vóór als ná inschakelen kunnen aardsluitingen niet leiden tot ongewenst inschakelen of weigering af te schakelen.

bedrijfszekerheidsspecificatie pas op tafel komt in een latere fase waarin het ontwerp definitief of bijna definitief is, het enige wat de ontwerper nog kan doen is zijn toevlucht nemen tot het gebruik van erg bedrijfszekere (en dus erg dure) componenten, of het toepassen van redundantie op systeemniveau (wat erg in-effectief is), of het verbeteren van de zwakste schakel in de keten. Dit zijn alle methoden die niet erg 'cost effective' zijn. We komen hierop later nog terug.

- De keuze van die technische middelen en technologieën die zich bij uitstek lenen tot het realiseren van de vereiste systeemfuncties zonder dat daarvoor 'hoogstandjes' nodig zijn. Na de keuze van een bepaalde techniek of combinatie van technieken moet de configuratie van het systeem ontworpen worden op minimale kwantitatieve en kwalitatieve complexiteit. Het ontwerp moet erop gericht zijn dat de systeemfuncties bepaald worden door slechts enkele, bedrijfszekere componenten en het ontwerp moet de ruimte bieden voor variaties in de tijd van de eigenschappen van de overige componenten.
- Het toepassen van onderbelasting (Engels: derating). Hierbij worden de operationele en de omgevingsbelasting (Engels: stress) die de componenten van een systeem in de praktijk moeten ondergaan gereduceerd waardoor, zolang de belastingskansdichtheidsfunctie en de sterktekansdichtheidsfunctie van een component elkaar nog overlappen, een reductie in de uitvalkans wordt bewerkstelligd. We komen hierop terug in paragraaf 5.2.
- Het grondig testen van de prototypen van het systeem op bedrijfszekerheid en het tussentijds inspecteren van de systemen gedurende de produktie.
- Het introduceren van een 'inbrandperiode' (Engels: burn in) ten einde kinderziekten (Engels: early failures) op te sporen door het systeem enige tijd eventueel onder verzwaarde belasting te laten inlopen. In paragraaf 2.3 wordt dit verder behandeld.
- Het uitvoeren van levensduurexperimenten, die resulteren in 'failure-rate data' die weer gebruikt worden om het initiële ontwerp bij te stellen. Meer failure-rate data worden verkregen van de gebruiker onder actuele gebruiksomstandigheden. Deze zijn van belang voor validitatie van de levensduurexperimenten en latere ontwerpen.
- Het gebruik van redundantie, dat wil zeggen alternatieve middelen voor het realiseren van de vereiste systeemfunctie wanneer de primaire middelen gefaald hebben. Om afhankelijke fouten te vermijden moeten de redundante (sub-)systemen de vereiste functie bij voorkeur op een andere wijze realiseren dan het primaire (sub-)systeem en uit andere componenten bestaan en door andere fabrikanten gemaakt zijn. Naarmate

de bedrijfszekerheid van het primaire (sub-)systeem hoger is, is het parallel geschakelde (sub-)systeem meer effectief, dat wil zeggen wordt de bedrijfszekerheid van de combinatie sterker verhoogd. Dit maakt dat men redundantie op een zo laag mogelijk hiërarchiek niveau in een systeem moet toepassen, dus op componentniveau (zie paragraaf 6.4).

- De introductie van onderhoud waar zulks mogelijk is. Preventief onderhoud verdient daarbij de voorkeur. Doordat deze vorm van onderhoud volgens een van te voren opgesteld schema plaats vindt zijn de kosten lager dan die van correctief onderhoud (reparatie). Ook worden de kosten tengevolge van ongewild uitvallen van het systeem vermeden. Niet bij alle systemen is preventief onderhoud echter zinvol. Bovendien is altijd nog wel enig correctief onderhoud nodig (zie paragraaf 7.3).
- Het opbouwen van een bedrijfsorganisatie die gericht is op het ontwerpen, ontwikkelen, produceren en onderhouden van een bedrijfszeker produkt. De belangrijkste management aspecten zijn daarbij de organisatie, opleiding en coördinatie van mankracht en middelen.

Opgaven

1.1. Wat zijn de essentiële bestanddelen van de definitie van bedrijfszekerheid?

1.2. Is bedrijfszekerheid hetzelfde als betrouwbaarheid? Zo niet, wat is dan betrouwbaarheid?

1.3. Waarom zal een uniforme gloeidraad gevoed uit een constante spanningsbron nooit falen?

1.4. Waarom is in tabel 1.1 het toegestane temperatuurbereik onder operationele condities lager dan onder 'storage' condities?

1.5. Wat wordt verstaan onder 'deterministische bedrijfszekerheidstechniek'?

1.6. Leg uit waarom een goede organisatie onontbeerlijk is om een bedrijfszeker product te realiseren.

1.7. Wat voor omgevingselementen zouden van invloed kunnen zijn op het verouderingsproces van een elektronisch geïntegreerd circuit?

2. Deterministische bedrijfszekerheidstechniek

Zoals we reeds gezien hebben is men bij de deterministische benadering van de bedrijfszekerheid vooral geïnteresseerd in het fysische proces dat tot falen leidt. Dit proces duidt men ook wel aan als het *faalmechanisme* (Engels: failure mechanism). Het leidt tenslotte tot het niet meer functioneren of tot het buiten de toleranties functioneren van een component. De gevolgen van zo'n te ver voortgeschreden inwendig faalmechanisme kan men extern waarnemen. De waargenomen fout duidt men aan als de *faalwijze* (Engels: failure mode) van de component. Een faalmechanisme wordt doorgaans geactiveerd en versneld door een bepaalde omgevingsgrootheid of combinatie van omgevingsgrootheden. Zulke grootheden noemt men *stressgrootheden*. Als we het voorbeeld van de gloeilamp uit paragraaf 1.3 even hanteren: één van de *faalmechanismen* is steeds sterker wordende lokale verdamping door de vorming van 'hot spots'. De extern te constateren *faalwijze* is een open gloeidraad. De gloeilamp faalt dus in de open mode. Een *stressgrootheid* bij deze wijze van falen is de voedingsspanning (netspanning). De stress tengevolge van een verhoogde voedingsspanning is groot: de netspanning hoeft slechts zeer weinig verhoogd te worden voor een zeer veel kortere levensduur.

2.1. Model van Arrhenius

Een van de belangrijkste stressgrootheden is de verhoging van de *temperatuur* van een component. De temperatuur van een component wordt bepaald door de omgevingstemperatuur (uitwendige stress) en de vermogensdissipatie in de component in combinatie met de warmteweerstand naar de omgeving (inwendige stress). Een verhoging van de temperatuur doet allerlei fysisch-chemische processen sneller verlopen.
Vaak wordt aangenomen dat het faalproces zich gedraagt als een chemisch proces met een bepaalde reactiesnelheid Q waarvoor geldt:

$$Q(T) = Q_0 \, e^{-E_A/kT}$$

Hierin is Q_0 een constante, E_A de activeringsenergie in elektron-volt, k de constante van Boltzmann ($k = 8{,}6 \times 10^{-5}$ eV/K) en T de absolute temperatuur. Deze uitdrukking werd in 1880 door Arrhenius experimenteel bepaald.

Als we nu aannemen dat de drift in de eigenschappen (parameters) van een component als functie van de tijd t evenredig is met:

$$t^n Q(T)$$

waarbij lineaire drift in de tijd een speciaal geval is: n = 1, dan kunnen we faaltijden bij twee verschillende temperaturen T_1 en T_2 als volgt vergelijken. Stel dat bij temperatuur T_1 de tijd benodigd om een parameter van de component van de oorspronkelijke nominale waarde te laten wegdriften tot de tolerantiegrens (foutwaarde) t_1 is. De parameterdrift wordt dan gekarakteriseerd door $Q(T_1)t_1^n$, zodat de tijd t_2 benodigd voor dezelfde parameterdrift bij temperatuur T_2 wordt gevonden uit:

$$Q(T_2)t_2^n = Q(T_1)t_1^n$$

of algemener:

$$Q(T)t^n = K'.$$

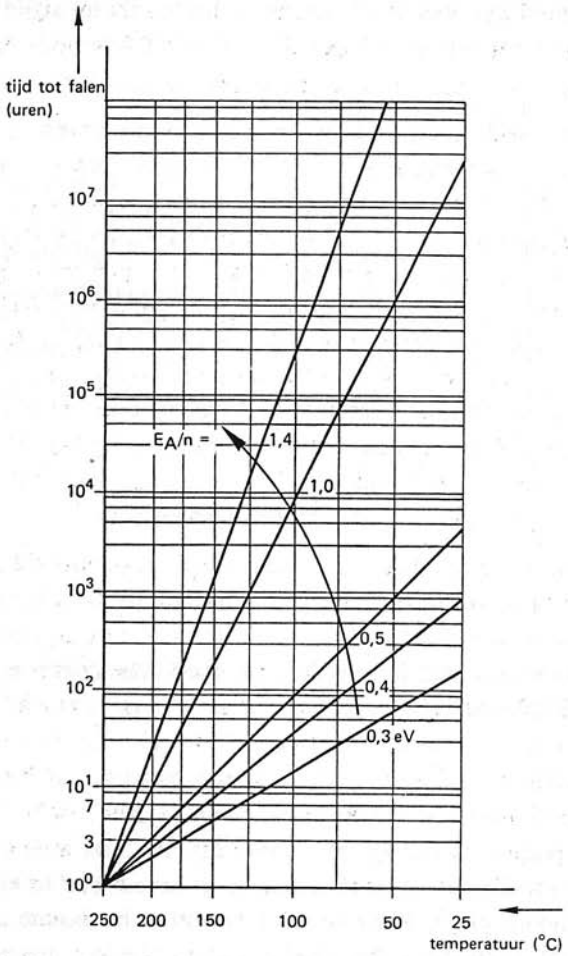
Hierin is t de levensduur bij de temperatuur T en K' een arbitraire constante. Dus geldt ook:

$$\ln t = K + \frac{E_A}{nkT}.$$

Hierin is de nieuwe constante $K = \ln(K'/Q_0)^{1/n}$. Het belang van deze relatie ligt daarin dat veel faalmechanismen op deze wijze te karakteriseren zijn. Door de resultaten van twee experimenten bij verschillende temperaturen T_1 en T_2 op logaritmisch papier te plotten kan men op eenvoudige wijze de effectieve activeringsenergie E_A/n behorende bij een bepaald faalmechanisme bepalen, want:

$$\ln t_2 - \ln t_1 = \ln\frac{t_2}{t_1} = \frac{E_A}{nk}\left(\frac{1}{T_2} - \frac{1}{T_1}\right).$$

Als een keer E_A/n bekend is kan men de *versnellingsfactor* t_2/t_1 met bovenstaande uitdrukking ook voor andere temperaturen berekenen. We zien uit de bovenstaande uitdrukking dat de exponent n van de drift in de tijd t hetzelfde effect geeft als een wijziging in de activeringsenergie E_A. Daarom wordt E_A/n de *effectieve activeringsenergie* genoemd. In figuur 2.1 is een voorbeeld van een en ander gegeven. We hebben hierin vijf faalprocessen met verschillende effectieve activeringsenergieën E_A/n vergeleken. De *stressgrootheid* is hier de omgevingstemperatuur waaraan de geteste



Figuur 2.1. Grafiek van de relatie van Arrhenius voor een bepaald faalproces bij vijf verschillende 'faalresistenties'. De faalresistentie wordt tot uitdrukking gebracht in de effectieve actieveringsenergie E_A/n.

onderdelen worden blootgesteld. Langs de (logaritmische) verticale as is uitgezet hoelang een onderdeel het gemiddeld bij die omgevingstemperatuur uithoudt. Als bekend is (of als wordt aangenomen) dat componenten aan de relatie van Arrhenius voldoen, zijn levensduurmetingen bij twee verschillende stresswaarden (in casu temperaturen) voldoende om de rest van het verloop van de levensduur-stress-curve te bepalen.
Een ander model dat wel gebruikt wordt voor het bepalen van de versnelling ten gevolge van een verhoogde temperatuur is de relatie van Eyring:

$$Q(T) = \alpha T\, e^{-E_A/kT}$$

Deze is ontleend aan kwantum-mechanische beschouwingen. Als de (absolute) temperatuurvariatie klein is kan men αT beschouwen als een constante Q_0. Dit resulteert weer in de relatie van Arrhenius.

Een stressgrootheid, die van belang is voor komponenten samengesteld uit verschillende materialen, is het *sprongsgewijze variëren van de temperatuur* tussen twee waarden. Er zijn uitdrukkingen die de daardoor ontstane vermoeiingsbreuken, die bijvoorbeeld aanleiding geven tot open contactbanen, relateren aan het aantal temperatuurcycli en de grootte van de temperatuursprong. Als zo'n uitdrukking de opgemeten faalgegevens past, kan men dezelfde weg bewandelen als hierboven voor de temperatuur gedaan is. Doorgaans zijn de resultaten sterk afhankelijk van de aard van de mechanische structuur, de gebruikte materialen en de reeds aanwezige materiaalspanningen. Met name het vroeger gebruikte 'epoxy A' voor kunststof-transistorbehuizingen was berucht om de vele fouten door draadbreuk in de behuizing bij thermische vermoeiingsproeven.

Het effect van de *omgevingsvochtigheid* als stressgrootheid is sterk afhankelijk van twee factoren: de permeabiliteit van de behuizing of de coating van de component en het effect van vocht op de component zelf. Soms kan men waarnemen dat het vocht elektrolytische corrosie veroorzaakt tussen metallische geleiders die een zeker potentiaalverschil hebben en ingebed zijn in een kunststofbehuizing. Vrijwel alle literatuur toont dat als het componentoppervlak (bijvoorbeeld een chip) wordt blootgesteld aan relatieve vochtigheden van meer dan 1% en de elektrische dissipatie in de komponent gering is (dus de lokale reductie in de relatieve vochtigheid is klein), er al spoedig grote problemen ontstaan. In systemen met grotere dissipatie kunnen uitgerekend problemen ontstaan tijdens de tijdintervallen waarin de component niet gebruikt wordt (bijvoorbeeld tijdens transport) en dus de relatieve vochtigheid hoog is.

Bij componenten waarin hoge spanningsgradiënten over een isolator worden opgebouwd (zoals bijvoorbeeld MOS-structuren) heeft de *aangelegde spanning* meestal een verkortende werking op de levensduur. Het is veelal niet mogelijk een systematische beschrijving hiervan te geven.

Het *in- en uitschakelen van de voedingsenergie* van een component of de spanning erover of de stroom erdoor geeft temperatuursprongen vanwege de inwendige dissipatie in de component. De thermische weerstand tussen het inwendige van de component en de omgeving bepaalt de grootte van de temperatuursprong. Deze stress lijkt tamelijk veel op die, veroorzaakt door temperatuurcycli, met dien verstande dat de temperatuurvariaties meestal veel sneller zijn, lokaal in de component voorkomen en van binnenuit komen.

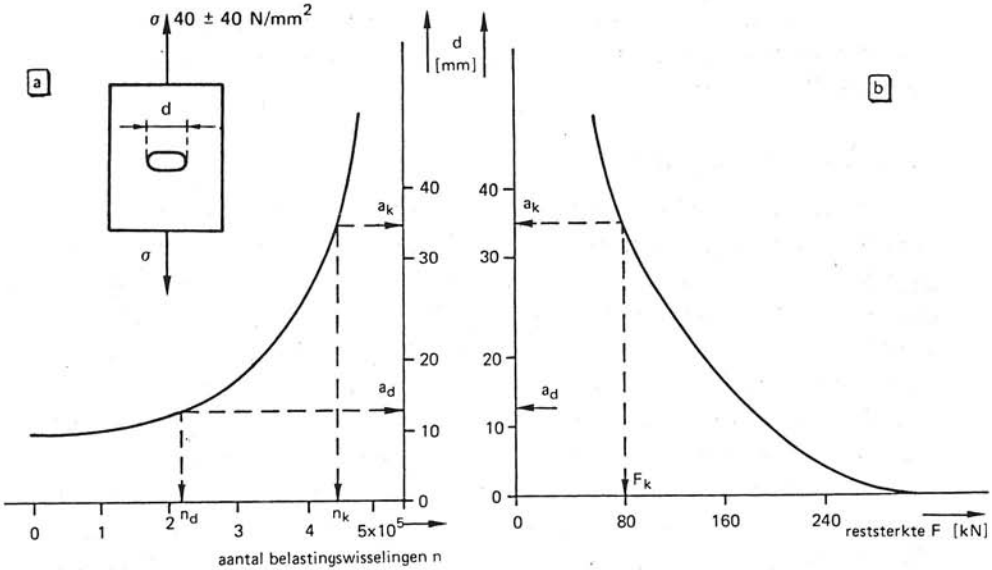
Het is al geruime tijd bekend dat bipolaire transistoren bij bestraling met *ioniserende straling* stuk gaan door ladingen die gegenereerd worden in de gasvulling van de behuizing of in de oxidelaag van de halfgeleider. Door een thermische behandeling kunnen deze componenten weer in hun oorspronkelijke staat teruggebracht worden. Als remedie stelt men daarom de componenten bloot aan de te verwachten dosis, de bruikbare komponenten worden uitgezocht en deze worden vervolgens door een thermische behandeling weer in hun oorspronkelijke staat teruggebracht (Engels: radiation hardening).
Meer recentelijk is gepubliceerd over het effect van alfadeeltjes op de lading in de geheugencellen van 'charge coupled devices' en dynamische halfgeleidergeheugens. Daar de 'soft-error rate' die door deze ladingen wordt gecreeerd lineair van de fluxdichtheid afhangt, uitgezet op dubbel logaritmisch papier, is dit type fouten tamelijk eenvoudig te voorspellen. Door het groter maken van de lading in de geheugencellen is de error rate sterk terug te dringen, evenals door het groter maken van de celafmetingen. Daar de trend juist omgekeerd is, namelijk naar kleinere celafmetingen en lagere cellading, is een andere oplossing gevonden door Hitachi en Motorola in de vorm van een afschermende polyamide-laag van circa 10 μm dik die als stralingsfilter tegen α-deeltjes uit de omhulling van de komponent dienst doet.

2.2. Faalmechanismen

In de deterministische bedrijfszekerheidstechniek is men bovenal geïnteresseerd in de faalmechanismen die in de operationele praktijk tot falen leiden, hoe deze mechanismen verlopen en op welke wijze dit faalproces kan worden voorkomen. In principe kan dit laatste door de component een gewijzigde fysische opbouw en/of chemische samenstelling te geven zodat dit faalproces niet optreedt of slechts sterk vertraagd optreedt. Een andere mogelijkheid die bij niet-dominante faalmechanismen kan worden gebruikt, is het zodanig verhogen van de voor dit faalmechanisme specifieke stress dat de overlevende componenten vrij zijn van falen door dit mechanisme (inbranden van zwakke componenten). Aan deze laatste methode van screening zijn nadelen verbonden. De toegepaste stressgrootheid kan ook de levensduur van de overblijvende componenten aantasten, de produktie-opbrengst wordt kleiner en het produkt wordt onder meer door de screening duurder. Daarom ligt de nadruk op het zodanig wijzigen van het produkt dat de levensduur aan de verwachtingen voldoet. Pas als dat niet mogelijk is (of niet meer mogelijk), kan men overgaan op het opbouwen van screens voor componenten die behept zijn met kinderziekten (Engels: early failures), dat wil zeggen die

fouten die voornamelijk in het begin van het leven van een component optreden.

Als illustratie is in figuur 2.2 een voorbeeld van scheurgroei door vermoeiing in een mechanische constructie gegeven. Bij het ontwerp dienen mechanische spanningsconcentraties zoveel mogelijk te worden vermeden. Door het testen van vervaardigde constructies kan men de eventuele scheurgroei in de tijd meten. In figuur 2.2a is de relatie tussen het aantal belastingswisselingen en de resulterende scheurlengte aangegeven voor een proefstuk met een 10 mm proefsleuf, in figuur 2.2b de relatie tussen de scheurlengte en de reststerkte van dezelfde constructie. Een scheurlengte groter dan a_d is detecteerbaar. De minimaal vereiste sterkte is F_k. Als de scheur propageert tot een lengte groter dan a_k treedt breuk op. Op grond van de breukmechanica kan men tot de navolgende periodieke inspectie besluiten. De eerste inspectie is na $n_d + (n_k - n_d)/2$ belastingcycli. Vindt men dan geen scheurtjes ($d < a_d$) dan is de minimumlevensduur $n_k - n_d$ en zal de volgende inspectie na bijvoorbeeld $(n_k - n_d)/2$ plaats moeten vinden.



Figuur 2.2. Scheurgroei door vermoeiing tengevolge van belastingswisselingen (in 2024-T3 aluminiumlegering). Hier is n het aantal belastingswisselingen, d de totale (scheur) lengte, en F de reststerkte. De constructie wordt belast met 80 kN. $4{,}5 \times 10^5$ belastingswisselingen is juist kritiek (n_k). a_k is de bijbehorende kritieke scheurlengte, a_d is de juist detecteerbare scheurlengte. De eerste inspectie voor scheurtjes kan worden uitgevoerd voor $n = n_d + (n_k - n_d)/2$. Als dan geen scheuren worden gevonden, wordt besloten tot een minimum levensduur van $n_k - n_d$.

De studie van de faalprocessen die zich in componenten van technische systemen afspelen is vooral sterk ontwikkeld in de micro-elektronica. In het navolgende zullen we daarom kort de natuurkundige processen bespreken achter een aantal veel voorkomende foutmechanismen in halfgeleidercomponenten.

- *Corrosie*: bij IC's kan de aluminiummetallisatie door corrosie worden aangetast. Deze corrosie vindt plaats door de inwerking van vocht, verontreinigingen en een elektrische spanning. Het vocht dringt binnen door de plastic omhulling of langs de materiaalovergang plastic-connectiepen. Verontreinigingen worden gevormd door ionen die vanuit het epoxymateriaal tot de metallisatie doordringen. De aangelegde elektrische spanning veroorzaakt een elektrisch driftveld voor deze ionen dat groter is naarmate de voedingsspanning hoger is en de afstand tot de metallisatiesporen kleiner is. Dit brengt twee corrosieprocessen op gang, namelijk de anodische corrosie die niet temperatuur- maar slechts stroomdichtheidsafhankelijk is:

$$Al \rightarrow Al^{3+} + 3e^-$$

$$2\,Al^{3+} + 3\,H_2O \rightarrow Al_2O_3 + 6H^+$$

De Al_2O_3 vormt een beschermende, niet-geleidende laag en gaat verdere corrosie tegen. Het tweede corrosieproces is de kathodische corrosie:

$$2\,H_2O + 2\,e^- \rightarrow 2\,OH^- + H_2\uparrow,$$

$$2\,H_2O + 2\,Al + 2\,OH^- \rightarrow 2\,AlO_2^- + 3\,H_2\uparrow.$$

De tweede chemische reactie maakt deze corrosie temperatuurafhankelijk met een activeringsenergie van 0,5 eV. AlO_2^- is oplosbaar in water en vormt $Al(OH)_3$ wat aanleiding geeft tot het scheuren van de SiO_2-passiveringslaag over de metallisatie. Passivering met siliciumnitridelagen geeft een betere bescherming tegen deze corrosie.

- *Elektromigratie*: Als in de metallisatie de stroomdichtheid groot is en de temperatuur hoog is, treedt elektromigratie op. Als door te smalle sporen of te hoge stromen de stroomdichtheid groter wordt dan ca. 1 mA/μm^2 (voor aluminium) treedt dit effect merkbaar aan de dag en leidt na enige tijd tot onderbrekingen. Te kleine spoordoorsneden ontstaan ter plaatse van krassen, insnoeringen bij stapbedekkingen en dergelijke.
  De verklaring is als volgt: het positieve metaalion dat door thermische agita-

tie bevrijd is uit zijn potentiaalput in het metaalrooster ondervindt twee krachten, namelijk een kracht tengevolge van het aanwezige elektrische veld die tegengesteld is aan de elektronenstroom, en een kracht met de elektronenstroom mee die wordt veroorzaakt door de impuls van elektronen die 'botsen' met het geactiveerde metaalion (dat nog deel uitmaakt van de geleider). Door het afschermende effect van de vele elektronen in de geleider is de eerste kracht klein, ten opzichte van de tweede kracht tengevolge van de 'elektronenwind'. Deze vrije metaalionen hebben een grotere kans een vrije plaats te bezetten dan de gebonden metaalionen rondom deze plaats. Zo vindt er materiaaltransport plaats van ionen in de richting van het positieve uiteinde van de geleider, waardoor uitstulpingen en insnoeringen ontstaan. Dit vergroot de stroomdichtheid waardoor het proces hoe langer hoe sneller verloopt. Dit kan tot uitdrukking gebracht worden met de uitdrukking van Arrhenius in de onderstaande vorm:

$$\ln t = K + \frac{E_A}{nkT}$$

waarbij uit experimenten blijkt dat $K = -m \cdot \ln(AJ)$ waarin m en A constanten zijn en J de stroomdichtheid. Dit levert voor de faaltijd t:

$$t = (AJ)^{-m} . e^{\frac{E_A}{nkT}}$$

Voor de effectieve activeringsenergie E_A/n voor elektromigratie geldt: $0{,}5 \text{ eV} < E_A/n < 0{,}8 \text{ eV}$. De constanten m en A zijn afhankelijk van de korrelgrootte en de verontreinigingen in het materiaal.

- *Purple plague*: dit faalmechanisme ontstaat doordat bij thermocompressie-bonding van gouddraden op de aluminium bond flaps van een IC na verloop van tijd goud en aluminium in elkaar diffunderen. Hierdoor ontstaan tussenlagen van diffusieprodukten namelijk het purperkleurige $AuAl_2$ en het witte AuAl. Deze lagen zijn echter sterker dan de gouddraad zelf en veroorzaken dus niet de losse verbindingen die men na enige tijd kan waarnemen. Dit loslaten wordt veroorzaakt door de ongelijke diffusiesnelheid van Al en Au en de invloed van lokale verontreinigingen daarop. Deze verontreinigingen precipiteren op het diffusiefront en beïnvloeden de lokale diffusiesnelheid en vormen aanleiding tot zwakke plekken in de lasverbinding. Dit proces is uiteraard temperatuurgevoelig en heeft een activeringsenergie $E_A/n \approx 1$ eV.

2.3. Screening

We zullen de term 'screening' hier gebruiken voor proeven gedaan op alle af te leveren produkten met het doel kapotte of potentieel zwakke produkten te verwijderen. Het gebruiken van screening-methoden houdt in dat men de bedrijfszekerheid van de produktielijn als gegeven aanneemt en (ad hoc) nog probeert deze te verhogen.
Een vrij voor de hand liggend screen is het automatisch doormeten van alle componenten op hun specificaties. Daarbij kunnen soms extra parameters gemeten worden die bewezen hebben een goede correlatie met de levensduur te hebben. Zo hebben bijvoorbeeld weerstanden met een hoge excess-ruis en een 'grote' niet-lineariteit een lage levensduurverwachting.

Daarnaast kunnen 'burn-in screens' worden gehanteerd om de zwakke componenten reeds tijdens de test te laten falen. Alleen als de screening ideaal zou zijn, zouden alle componenten met kinderziekten (Engels: early failures) uit de produktie kunnen worden verwijderd. Een burn-in screen wordt ontworpen door de faalmechanismen gepaard met de 'early failures' te versnellen; dit zoveel mogelijk zonder de levensduur van de overlevende componenten aan te tasten.
Bij halfgeleidercomponenten worden early failures meestal veroorzaakt door produktiefouten zoals slechte draad-metallisatie lassen, krassen in de metallisatie, slechte soldering van het IC op de basis. Screens tegen deze kinderziekten vormen respectievelijk mechanische schokproeven, het bedrijven van het IC bij volle voedingsspanning, volle belasting en eventueel verhoogde omgevingstemperatuur. Een voorbeeld van een strenge screening test van een halfgeleiderfabrikant is aangegeven in figuur 2.3.

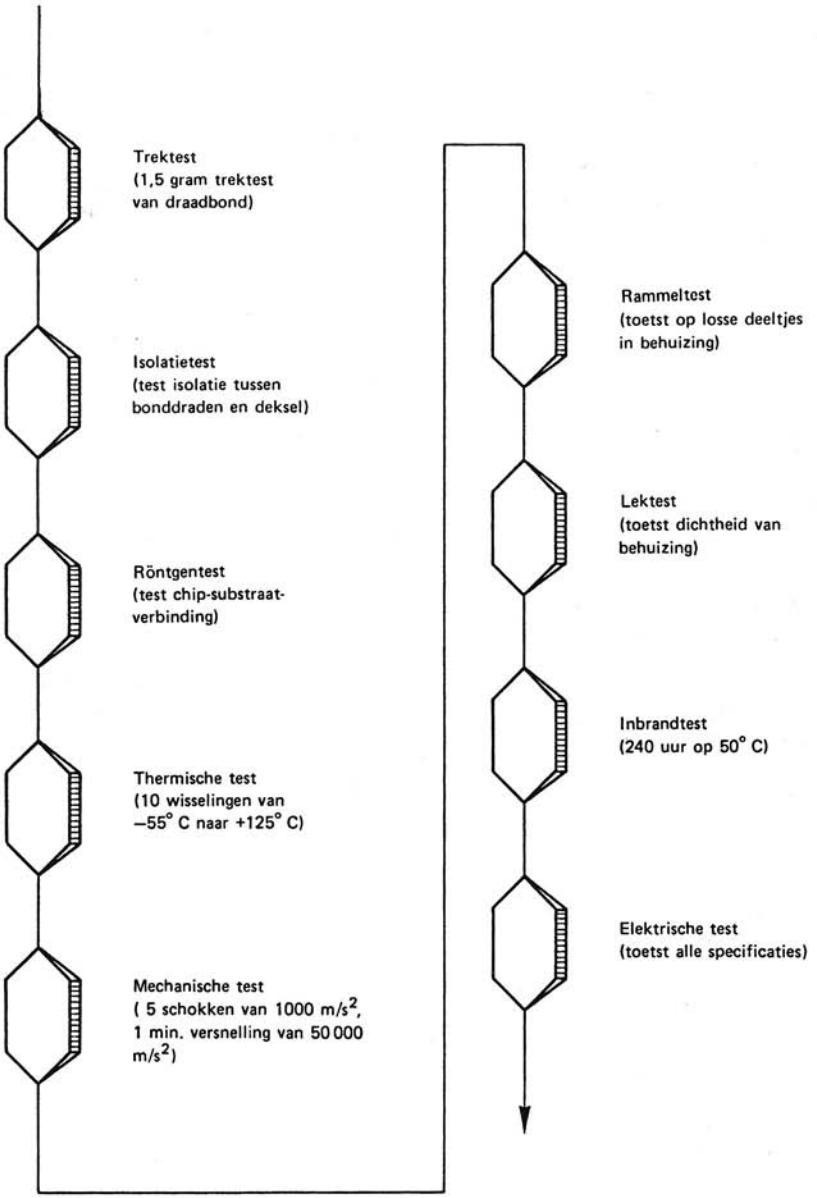
Opgaven

2.1. Van een nieuwe monolithische digitaal-analoogomzetter wil men de MTTF bepalen bij 25°C (298 K). Daartoe heeft men 60 omzetters gedurende 1000 uur laten werken bij 100°C (373 K) en 60 omzetters gedurende 1000 uur bij 85°C (358 K).
Bij 100°C bleek de MTTF $6{,}5\times10^3$ uur te zijn. Bij 85°C was dit $2{,}4\times10^4$ uur. Als we mogen aannemen dat het faalproces zich gedraagt als een chemisch proces met een reactiesnelheid

$$Q = Q_0 \cdot e^{(-E_A/kT)} \text{ (relatie van Arrhenius),}$$

wat is dan de MTTF van deze omzetter bij 25°C?
T is de absolute temperatuur in Kelvin.
k is de constante van Boltzman.

2.2. Zou elektromigratie ook in sterkstroomapparaten als generatoren



Figuur 2.3. Voorbeeld van een strenge screeningtest bedoeld om potentiële faalmechanismen in multi-chip, hybride geïntegreerde schakelingen voor de ruimtevaart te activeren. De gefaalde componenten worden verwijderd. N.B.: de volgorde mag niet worden verstoord daar anders een volgende test een faalmechanisme kan opwekken waartegen niet meer wordt gescreend.

en transformatoren voorkomen?

2.3. Weet U hoe galvanische corrosie van een scheepsschroef wordt voorkomen (c.q. verminderd)?

2.4. Wat zou het dominante faalmechanisme van een auto zijn als we de olie nimmer zouden verversen?
Wat zou de faalwijze zijn?

2.5. Wat is 'screening' en wat probeert men ermee te bereiken?

2.6. 'Early failures' (kinderziekten) treden vrij snel op na het in bedrijf nemen van componenten. Geef hier een verklaring voor.

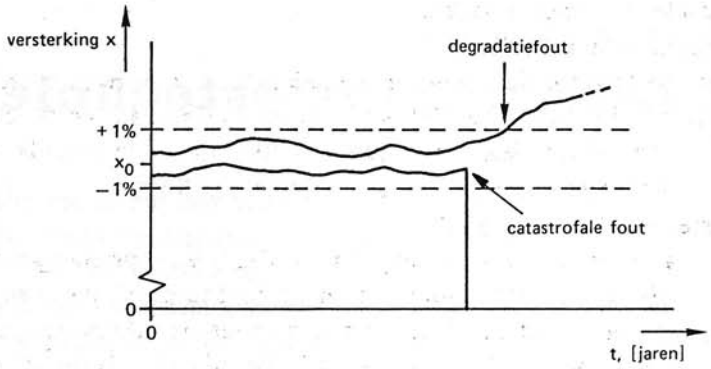
3. Statistische bedrijfszekerheidstechniek

De statistische bedrijfszekerheidstechniek omvat te veel om in één boek te kunnen behandelen. Bij het maken van een keuze is bijvoorbeeld afgezien van het meten van de gerealiseerde bedrijfszekerheid met aanverwante onderwerpen zoals: statistische bemonsteringsmethoden en -strategieën, schattingstheorie, beslissingstheorie en statistische data-analyse. In dit boek is slechts die stof opgenomen die direct leidt tot inzicht in stochastische faalprocessen, bedrijfszekere systeemconfiguraties, berekeningsmethoden, bedrijfszekerheidsmodellen en onderhoudsstrategieën.

3.1. Nomenclatuur

De nuttige levensduur van een systeem eindigt met het optreden van een fout. We zullen een *fout* dan ook definiëren als de beëindiging van het vermogen van een systeem de van dat systeem vereiste functies te realiseren.

- *Restricties.* Hierbij nemen we aan, in overeenstemming met het bedrijfszekerheidsbegrip gegeven in paragraaf 1.1, dat de fout niet (mede) veroorzaakt is door *misuse*. Het systeem wordt dus altijd bedreven binnen het gespecificeerde omgevingsgebied. Verder nemen we aan dat de fout niet *intermitterend* is, dat wil zeggen vanzelf, zonder menselijk ingrijpen zich weer herstelt. Eens gefaald blijft het systeem defect tot er onderhoud wordt gepleegd. Bovendien stellen we dat een systeem *òf correct functioneert òf defect is*; tussentoestanden zijn niet mogelijk. Ten leste nemen we aan dat de *levensduurvariabele* de tijd t is na de oplevering van het systeem door de producent aan de gebruiker.
  In figuur 3.1 is aangegeven dat een systeem met continue parameters (bijvoorbeeld een analoog elektronisch systeem) op twee manieren in de fout kan gaan. De betreffende parameter x (de versterking) heeft een nominale waarde x_0 en een toegestane tolerantie van ±1%. Door een *degradatiefout* wordt deze tolerantiegrens geleidelijk overschreden, door een *catastrofale fout* valt de functie (versterking) plotseling totaal weg. We zullen in dit boek geen rekenmethoden behandelen die speciaal voor degeneratiefouten ontwikkeld zijn. Vaak is namelijk de parameterdrift in de tijd als statistisch proces niet analytisch te beschrijven en moet men zijn toevlucht nemen tot "Monte Carlo"-simulaties; dit

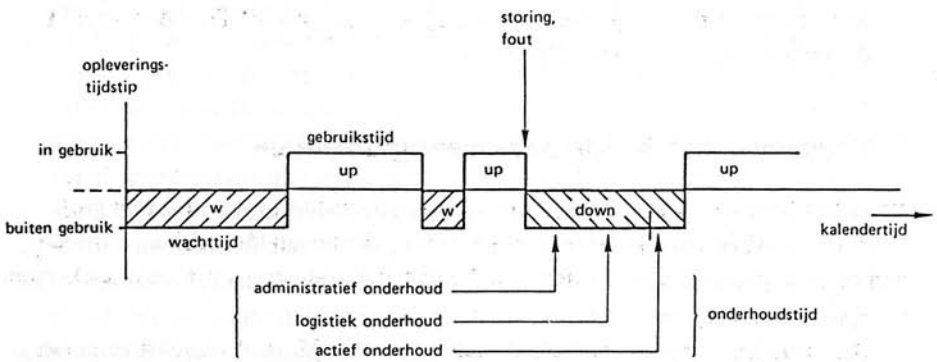


Figuur 3.1. Twee verschillende fouten; een totale of catastrofale fout, bijvoorbeeld door een kortsluiting en een geleidelijke en gedeeltelijke fout, bijvoorbeeld door drift van de versterker.

zijn statistische modelexperimenten uitgevoerd op de computer. We zullen ons hier niet bezig houden met zo'n aparte benadering van degeneratiefouten. We huldigen dus het standpunt: buiten de toleranties is defect, binnen de toleranties is correct. Verder gaat een systeem met degeneratiefouten defect op het eerste tijdstip waarop de toleranties worden overschreden en blijft daarna defect, al drift de parameterwaarde terug binnen de toleranties.

- *Tijdsindeling*

  Men kan in de tijd na het opleveringstijdstip waarin het systeem bestaat, een aantal onderverdelingen aanbrengen die zinvol zijn met betrekking tot de in de volgende paragraaf te definiëren operationele systeemgrootheden. Voor het meest algemene systeem, dat is een systeem waaraan onderhoud wordt gepleegd, zijn de belangrijkste tijdintervallen aangegeven in figuur 3.2.



Figuur 3.2. Hoofdindeling van de kalendertijd van een systeem met onderhoud.

We onderscheiden twee gevallen.

• Het systeem is in gebruik.

Gedurende de zogenaamde *'up-time'* functioneert het systeem correct. De gebruiker zal tijdens deze tijd het systeem volop benutten (voorbeeld: daadwerkelijk rijden in een auto) ofwel voor direct gebruik gereedhouden (auto stationair laten draaien voor stoplicht).

• Het systeem is buiten gebruik.

Deze tijd kan men in tweeën delen, al naar gelang een systeem gewild buiten gebruik is (auto staat voor het huis geparkeerd) of ongewild buiten gebruik is (auto niet beschikbaar wegens onderhoud). De eerste tijd duidt men aan als *wachttijd*, de tweede tijd als *onderhoudstijd* of *'down-time'*. De onderhoudstijd kan gebruikt worden voor preventief onderhoud (olie verversen, doorsmeren, banden op spanning brengen), maar ook voor correctief onderhoud (reparatie van een gefaalde ontsteking). De onderhoudstijd valt in het algemeen uiteen in drie delen.

De *actieve* onderhoudstijd is de tijd waarin een monteur de fout daadwerkelijk herstelt. De *logistieke* tijd, dat is de tijd die het kost om de voor het onderhoud benodigde onderdelen ter plaatse te krijgen. De *administratieve* tijd is de tijd die verloopt met het foutzoeken, de bestelling plaatsen, het voorrijden van een monteur en dergelijke.

Vooral bij grote onderhoudbare systemen zoals transportsystemen (vliegtuigen, schepen) is een goede definitie van de verschillende tijdintervallen van groot belang voor de hierna te behandelen operationele grootheden. Vergelijk: de tijd die nodig is om een afgemeerd vaartuig te bemannen, van brandstof en voedsel te voorzien, de machines op te starten en dergelijke voordat het kan wegvaren (de voorbereidingstijd) wordt doorgaans tot de actieve gebruikstijd gerekend. De tijdsintervallen genoemd in figuur 3.2 sluiten elkaar wederzijds uit; een reparatie die uitgevoerd wordt tijdens een wachttijd onderbreekt de wachttijd; het systeem is 'down'.

3.2. Operationele bedrijfszekerheidsgrootheden

Voor het in de praktijk bedrijven van een technisch systeem, maar ook voor de bedrijfsvoering van een organisatie, dienst en dergelijke, zijn een aantal operationele grootheden van belang met het oog op bedrijfszekerheid:

- *Effectiviteit (system effectiveness)*
  Dit is de kans dat men, binnen een gegeven tijd, met een systeem een bepaalde gegeven taak met succes kan volbrengen, indien dat systeem binnen een bepaald omgevingsgebied wordt bedreven.

De effectiviteit is dus een ruimer begrip dan de bedrijfszekerheid. Het is geöriënteerd op de *taak*, het doel waarvoor het systeem aangeschaft is. Indien deze taak binnen een gespecificeerde tijd kan worden volbracht is het systeem effectief voor het beoogde doel. Deze gespecificeerde tijd omvat tevens opwarmtijd, voorbereidingstijd, tijd voor korte reparaties, naast de tijd die gepaard gaat met het uitvoeren van de eigenlijke taak.

- *Bedrijfszekerheid (reliability)*
  De definitie hiervan is reeds gegeven in paragraaf 1.1. Kort gesteld is het de kans dat een systeem tot de tijd t nog goed functioneert als het niet verkeerd is gebruikt.
  Deze definitie spreekt niet van een taak of doel, maar van goed, dat wil zeggen volgens de specificaties, functioneren. Bedrijfszeker is een systeem pas als het over het gehele tijdinterval [0,t] goed functioneert.
- *Taakgebonden bedrijfszekerheid (mission reliability)*
  Dit is een nog beperkter begrip, waarvan de definitie luidt: de kans dat een systeem gedurende een bepaalde taak bedrijfszeker functioneert, als gegeven is dat het bij het begin van de taak bedrijfszeker functioneerde.
  Voorbeeld: bij een transatlantische vlucht (taak) is een hoge taakgebonden bedrijfszekerheid van het grootste belang. De goede werking van het vliegtuig kan (voor een groot deel) vóór de start worden beproefd. Eenmaal in de lucht, vooral boven de oceaan, is een tussentijdse reparatie onmogelijk.

N.B.: De bovenstaande operationele grootheden zijn nuanceringen van het bedrijfszekerheidsbegrip. In het navolgende zullen wij gemakshalve afzien van deze nuanceringen en uitsluitend het begrip bedrijfszekerheid gebruiken.

Naast niet-onderhouden systemen zoals componenten, IC's, en ook pocket-calculators en dergelijke, onderscheidt men onderhouden systemen. Dit zijn systemen waarvan door menselijke tussenkomst de correcte werking weer kan worden hersteld. De menselijke tussenkomst is essentieel; als een systeem "zichzelf repareert" door ingebouwde redundantie is dit geen onderhoud. Het (menselijk) onderhoud kan preventief zijn, maar ook correctief. Preventief onderhoud geschiedt volgens een van te voren vastgesteld schema, bijvoorbeeld na verloop van een bepaald interval van de levensduurvariabele (elke maand, elke 7500 km, elke 1000 bedrijfsuren, enzovoort). Het kan ook geschieden op basis van de conditie van een systeem. Bijvoorbeeld de lagers verwisselen of de machine uitbalanceren als een bepaald trillingsniveau wordt bereikt.
Correctief onderhoud, ook wel curatief onderhoud of kortweg *reparatie* genoemd, vindt pas plaats nadat een systeem gefaald heeft.

Voor onderhouden systemen is er een tweetal operationele grootheden dat de vlotheid aangeeft waarmee het onderhoud verloopt:

- *Onderhoudbaarheid (maintainability)*
  De onderhoudbaarheid van een systeem is gedefinieerd als een kans dat het systeem teruggebracht is in correct functionerende toestand in een gespecificeerde down-time.
  De onderhoudbaarheid heeft betrekking op de totale down-time, dus de tijd nodig voor administratieve en logistieke handelingen zowel als de tijd die nodig is voor de feitelijke correctieve ingreep.
- *Repareerbaarheid (repairability)*
  Dit begrip is gelijk aan het bovenstaande met dien verstande dat het betrekking heeft uitsluitend op de tijd nodig voor de correctieve ingreep (de zogenaamde actieve reparatietijd).

N.B.: In het navolgende zullen wij afzien van deze nuancering en uitsluitend het begrip onderhoudbaarheid M(t) gebruiken.

Een drietal andere grootheden heeft betrekking op de continuïteit in de tijd waarmee men bij onderhoudbare systemen over het systeem kan beschikken:

- *Operationele gereedheid (operational readiness)*
  Dit is de kans dat een systeem, op welk tijdstip ook, òf correct functioneert, òf geschikt is om correct te functioneren wanneer het niet verkeerd wordt gebruikt. Bij het "geschikt om correct te functioneren" mag men een bepaalde voorbereidings- of opwarmtijd incalculeren.
- *Beschikbaarheid (availability)*
  Dit is de kans dat het systeem correct functioneert of kan functioneren op het tijdstip t, mits het niet verkeerd gebruikt wordt. De beschouwde tijd omvat hier alleen de gebruikstijd en de totale onderhoudstijd (administratieve, logistieke en actieve onderhoudstijd).
- *Intrinsieke beschikbaarheid (intrinsic availability)*
  Deze is net zo gedefinieerd als de beschikbaarheid, behalve dat de beschouwde tijd nu slechts bestaat uit de gebruikstijd en actieve reparatietijd. De overige tijdelementen worden bij de bepaling van deze grootheid weggelaten.

N.B.: In het navolgende zullen wij deze details weer verwaarlozen en uitsluitend het begrip beschikbaarheid A(t) hanteren.

Een laatste belangrijke operationele systeemgrootheid is die welke te maken heeft met de gevolgen van een in een systeem optredende fout voor de mens, het milieu of overige (met name kostbare) systemen. Men onderscheidt daartoe fouten waarvan de gevolgen gevaarlijk of schadelijk zijn (*onveilige fouten*) en fouten waarbij dit niet het geval is (*veilige fouten*).

- *Risico en veiligheid (risk and safety)*
  Risico is de kans dat een systeem faalt op een wijze waarbij mens, milieu en/of andere systemen daar gevaarlijke of schadelijke gevolgen van ondervinden.
  N.B.: uit deze definitie volgt niet dat een klein risico betekent dat er weinig fouten optreden.
  Een systeem is *veilig* als het risico gepaard gaande met het bedrijven van dat systeem aanvaardbaar wordt geacht. Het subjectieve begrip 'aanvaardbaar' en het derhalve ook subjectieve begrip 'veiligheid' komen in paragraaf 8.4 uitvoerig aan de orde.

3.2.1. Afgeleide grootheden

Het faaltijdstip t is in de statistische bedrijfszekerheidstechniek een stochastische variabele $\underline{t}$ waarvan de distributie, de zogenaamde *faaldistributie* of *levensduurverdeling*, gegeven is door:

$$F(t) = P(\underline{t} \leqslant t).$$

F(t) is dus de kans dat het systeem voor of op het tijdstip t sneuvelt. Men noemt deze sneuvelkans ook wel de *bedrijfsonzekerheid* (*unreliability*).
Daar elk fysisch realiseerbaar systeem tenslotte defect raakt, is $F(\infty) = 1$.
Meestal veronderstelt men $F(0) = 0$, dat wil zeggen dat bij ingebruikneming alle systemen correct functioneren. Voor de meeste berekeningen is deze aanname evenwel niet nodig. Als $F(0) = \gamma$, $0 \leqslant \gamma \leqslant 1$, noemt men $1 - \gamma$ de *opbrengst* (*yield*) van het produktieproces.
De overlevingskans voor het tijdinterval [0,t] is:

$$R(t) = P(\underline{t} > t) = 1 - F(t).$$

Deze relatie is duidelijk; een systeem heeft of gefaald of het leeft nog: de som der kansen is één. De overlevingskans is dus identiek met de *bedrijfszekerheid.*
De *faalkansdichtheidsfunctie* f(t) die bij de faaldistributie F(t) hoort is:

$$f(t) = \frac{dF(t)}{dt} = -\frac{dR(t)}{dt},$$

als F(t) differentieerbaar is. Omgekeerd geldt dus ook:

$$F(t) = \int_0^t f(t)\,dt$$

en:

$$R(t) = \int_t^\infty f(t)\,dt,$$

daar:

$$\int_0^\infty f(t)\,dt = 1.$$

De conditionele kans dat het systeem faalt in het tijdinterval $(t, t + \Delta t]$ onder de conditie dat het ten tijde t nog goed functioneerde is de *conditionele faaldichtheid* z(t) die wij met de Engelse benaming *hazard rate* zullen aanduiden. Heuristisch kan deze conditionele faaldichtheid als volgt worden bepaald:

$$z(t)\cdot\Delta t = P(t < \underline{t} \leqslant t+\Delta t \mid \underline{t} > t) = \frac{P(t < \underline{t} \leqslant t+\Delta t)}{P(\underline{t} > t)} =$$

$$= \frac{f(t)}{R(t)}\Delta t.$$

De hazard rate is daarom gedefinieerd als

$$z(t) = \lim_{\Delta t\to 0} \frac{F(t+\Delta t) - F(t)}{\Delta t}\cdot\frac{1}{R(t)}$$

$$= \frac{dF(t)}{dt}\cdot\frac{1}{R(t)} = \frac{f(t)}{R(t)}.$$

Een relatie tussen R(t) en z(t) krijgen we door de bovenstaande uitdrukking te integreren naar de tijd:

$$\int_0^t z(t)\,dt = \int_0^t \frac{f(t)}{R(t)}dt = -\int_{R(0)}^{R(t)} \frac{1}{R(t)}dR(t) = -\ln\frac{R(t)}{R(0)},$$

dus:

$$R(t) = R(0)\exp\left[-\int_0^t z(t)\,dt\right].$$

De hierboven genoemde grootheden R(t), F(t), f(t) en z(t) kunnen in elkaar herleid worden en bevatten dus alle informatie omtrent het faalproces van de systemen die we beschouwen.

N.B.: Als z(t) onafhankelijk van t is, geven we deze constante aan met $z(t) = \lambda$. Deze constante duidt men aan als *faaltempo* of *failure rate*. terwijl de tijdafhankelijke z(t) wordt aangeduid als hazard rate.

De gemiddelde levensduur θ van een systeem is gelijk aan de mathematische verwachting van de stochastische variabele $\underline{t}$, dus:

$$\theta = \int_0^\infty t f(t)\,dt.$$

De gemiddelde levensduur is een globale grootheid die niet meer de tijdnuancering bevat die R(t), F(t), f(t) en z(t) bevatten.
In de bedrijfszekerheidstechniek geeft men het tijdgemiddelde van het fa-

len aan met een drietal begrippen. Bij niet-onderhouden systemen spreekt men van MTTF (Mean Time To Failure). Dit is dezelfde grootheid als hierboven is afgeleid, dus MTTF $\equiv \theta$. Bij repareerbare systemen kan men twee tijdgemiddelden onderscheiden; de gemiddelde tijd tussen opeenvolgende fouten: MTBF (Mean Time Between Failures), en de gemiddelde tijd die verloopt tot de eerste fout optreedt: MTTFF (Mean Time To First Failure). Deze laatste twee begrippen komen in hoofdstuk 7 aan de orde.

De gemiddelde levensduur van een niet-onderhouden systeem, de MTTF dus, kan men als volgt in de bedrijfszekerhied R(t) uitdrukken:

$$\text{MTTF} \equiv \theta = \int_0^\infty t f(t)\,dt = -\int_0^\infty t \frac{dR(t)}{dt} dt = -\int_{R(0)}^{R(\infty)} t\,dR(t).$$

Partiële integratie levert:

$$\text{MTTF} = \lim_{T\to\infty} \left(-t R(t)\Big|_0^T + \int_0^T R(t)\,dt\right).$$

Als we aannemen dat

$$\lim_{T\to\infty} T R(T) = 0,$$

wat voor vrijwel alle praktische R(t)-functies geldt, dan verdwijnt de eerste term in de bovenstaande uitdrukking en deze wordt dan:

$$\text{MTTF} = \int_0^\infty R(t)\,dt.$$

We zien dus dat de gemiddelde levensduur gelijk is aan het oppervlak onder de bedrijfszekerheidsfunctie R(t).

Samenvattend kunnen we het volgende over de bovengenoemde afgeleide grootheden zeggen:

- F(t) is een faaldistributie (een cumulatieve distributie);
- R(t) daarentegen is geen distributie maar een (mathematische) functie: de bedrijfszekerheidsfunctie;
- f(t) is de faalkansdichtheid die bij de distributie F(t) behoort.

Het feit dat f(t) naar nul gaat wanneer t naar oneindig gaat zou kunnen suggereren dat een systeem, als het erg oud is, geen fouten meer vertoont. Een betere maat bereikt men daarom door de conditie te stellen dat het systeem op t nog moet functioneren en dan te vragen naar de sterftekans in het eerstvolgende tijdintervalletje Δt. Zo komt men dan tot de *hazard rate* z(t).

z(t) is veel gevoeliger voor fouten dan R(t). Als R(t) nog vrijwel gelijk is aan één, toont het verloop van z(t) heel duidelijk wat met R(t) gebeurt

als t toeneemt. Daar:

$$z(t) = -\frac{dR(t)}{dt} \cdot \frac{1}{R(t)} = -\frac{dR(t)}{R(t)} \frac{1}{dt}$$

zien we dat z(t) ook gezien kan worden als de relatieve afname in R(t) per eenheid van tijd. De bovenstaande uitdrukking kunnen we ook schrijven als:

$$z(t) = -\frac{d\{\ln R(t)\}}{dt} .$$

De hazard rate is dus de afname in de logaritme van R(t) per eenheid van tijd.

Opgaven

3.1. Hoe luidt de definitie van de *hazard rate*?

3.2. Hoe luidt de definitie van *onderhoudbaarheid*?

3.3. Hoe luidt de definitie van *beschikbaarheid*?

3.4. Toon aan dat:

$$\lim_{t \to \infty} \int_0^t z(t)\,dt \to \infty.$$

3.5. De gemiddelde levensduur van een niet-repareerbaar systeem is gelijk aan het oppervlak onder de R(t)-functie mits . . . . Aan welke conditie moet R(t) hiertoe voldoen?

3.6. Bewijs dat de hazard rate z(t) van een systeem gelijk is aan de relatieve afname van de bedrijfszekerheid R(t) per eenheid van tijd.

3.7. Stel een uitdrukking op voor de faalkansdichtheidsfunctie f(t) als functie van de hazard rate z(t).

3.8. a. Schets een willekeurige R(t)-functie en noem de voorwaarden waaraan een geldige bedrijfszekerheidsfunctie moet voldoen.

b. Als verder gegeven is dat:

$$R(t) = e^{\int_0^t z(t)\,dt} ,$$

aan welke voorwaarden moet een geldige hazard-rate functie dan voldoen?

3.9. De hazard rate van een systeem wordt gegeven door $z(t) = A + Bt$ voor $t \geqslant 0$. Aan welke voorwaarden (dimensie, waardebereik) moeten de constanten A en B voldoen opdat deze functie z(t) inderdaad een correcte hazard rate beschrijft en bepaal de faalkansdichtheidsfunctie f(t) van dit systeem.

3.10. De gevoeligheidscoëfficiënt S van de bedrijfszekerheid R(t) voor de tijd noteren we als S_t^R. Zij is gedefinieerd als:

$$S_t^R = \lim_{\Delta t \to 0} \frac{\Delta R(t)}{R(t)} \cdot \frac{1}{\Delta t}$$

Aan welke afgeleide grootheid is $-S_t^R$ gelijk (let op het minteken): F(t), f(t), z(t), MTTF?

3.11. Een apparaat heeft een constante hazard rate $\lambda = 10^{-6}$/uur.

a. Wat is de bedrijfszekerheid voor t = 1000 uur?

b. Als er 10.000 van zulke apparaten zijn, wat is dan het te verwachten aantal dat zal falen gedurende deze 1000 uur?

c. Wat is de bedrijfszekerheid na een tijd t die gelijk is aan de gemiddelde levensduur (MTTF)?

d. Wat is de overlevingskans voor nog eens 1000 uur, als gegeven is dat het apparaat de eerste 1000 uur heeft overleefd?

3.12. Wanneer de hazard rate z(t) constant en gelijk aan λ is in het interval $[t_1, t)$, waarbij $t \geqslant t_1$, bewijs dan dat: $R(t) = R(t_1)\exp\{-\lambda(t-t_1)\}$ voor $t \geqslant t_1$. *Het verloop van z(t) voor $t < t_1$ is niet gegeven.*

3.13. Iemand wil met zijn auto een reis maken van 1000 km. De auto heeft een constant uitvalstempo van $\lambda = 10^{-4}$ per afgelegde kilometer. (De levensduurvariabele is hier dus de afgelegde afstand).
Wat is de kans dat de bestemming zonder problemen bereikt wordt?

3.14. Gegeven is van een systeem een faalkansdichtheidsfunctie van de vorm:

$$f(t) = at \exp(-\frac{a}{2}t^2).$$

a. Bepaal R(t) en z(t) van dit systeem.

Op tijdstip t = 0 heeft men 5 000 goed functionerende systemen, ieder met de bovenstaande faalkansdichtheidsfunctie. Van deze 5 000 blijken er na 10 uur nog 4 700 correct te functioneren.

b. Wat is ongeveer het aantal te verwachten fouten in het tijdsinterval van 10 tot 20 uur?

4. Faalgedrag van systeemcomponenten

Een systeem bestaat uit componenten of subsystemen die in onderlinge wisselwerking met elkaar de vereiste systeemfuncties realiseren. Zo'n systeemcomponent hoeft niet noodzakelijkerwijze een elektronische component te zijn zoals een IC, transistor, diode of weerstand, het kan bijvoorbeeld ook een mechanische component zijn zoals een connector, een bout, een draagarm, een kogellager, enzovoort. Ook behoeft een component zich niet te bevinden op het laagste complexiteitsniveau in een systeem. Een component kan zelf weer uit subcomponenten bestaan. Vergelijk systeemcomponenten zoals printed-circuit boards met daarop elektronische componenten, plug-in units voor grotere apparatuur, opwekkingseenheden in een elektrische centrale, treinen in een vervoerssysteem, pompen in een chemische installatie, enzovoort.

De wijze waarop men het gegeven, te beschouwen systeem onderverdeelt (Engels: *system partitioning*), hangt onder andere af van de bedrijfszekerheidsgegevens die men heeft; heeft men wel gegevens over een unit of module uit het systeem maar niet over de onderdelen waar deze uit bestaat, dan is het in de meeste gevallen niet zinvol verder te detailleren dan het unit-niveau. Als men op elk complexiteitsniveau over bedrijfszekerheidsgegevens kan beschikken, of als men bereid is deze zelf te verzamelen, dan is de detaillering begrensd door de zinvolheid. Het is in het algemeen niet zinvol het systeem op te splitsen in delen die geen functionele fysische entiteit vormen, men heeft dan onnodig ver gedetailleerd. Bij onderhouden systemen is het slechts zinvol te gaan tot het niveau van in hun geheel vervangbare componenten (gloeilampen, IC's in sockets, printkaarten in connectors, enzovoort). Dus in het algemeen tot het niveau van samenhangende onderdelen die een volledige (deel)taak uitvoeren.

In het navolgende zullen we het levensduurgedrag van zulke onderscheidbare entiteiten uit een systeem nader bezien. Het faalgedrag van zo'n systeemcomponent heeft men vaak aan de hand van 'case histories' of uit levensduurproeven bepaald.

4.1. Faaldistributies

Afhankelijk van het soort faalmechanisme dat een systeemcomponent kan doen falen, zijn er vele verschillende faaldistributies mogelijk. Men noemt deze faaldistributies ook wel levensduurverdelingen. Men denkt zich een

faaldistributie als volgt ontstaan. We stellen ons voor dat we over een (theoretisch) onbeperkt grote verzameling componenten beschikken (de totale populatie) waarvan het faalpatroon in de tijd is geregistreerd. Uit dit tijdafhankelijke faalpatroon volgt de faaldistributie. In werkelijkheid kan men slechts over een eindig aantal componenten (een monster dus) beschikken dat men slechts gedurende een beperkte tijd kan observeren. Dit leidt tot een geschatte distributie. Op deze statistische aspecten zullen wij niet nader ingaan. Wij zullen aannemen dat we de faaldistributie van de volledige populatie kennen.

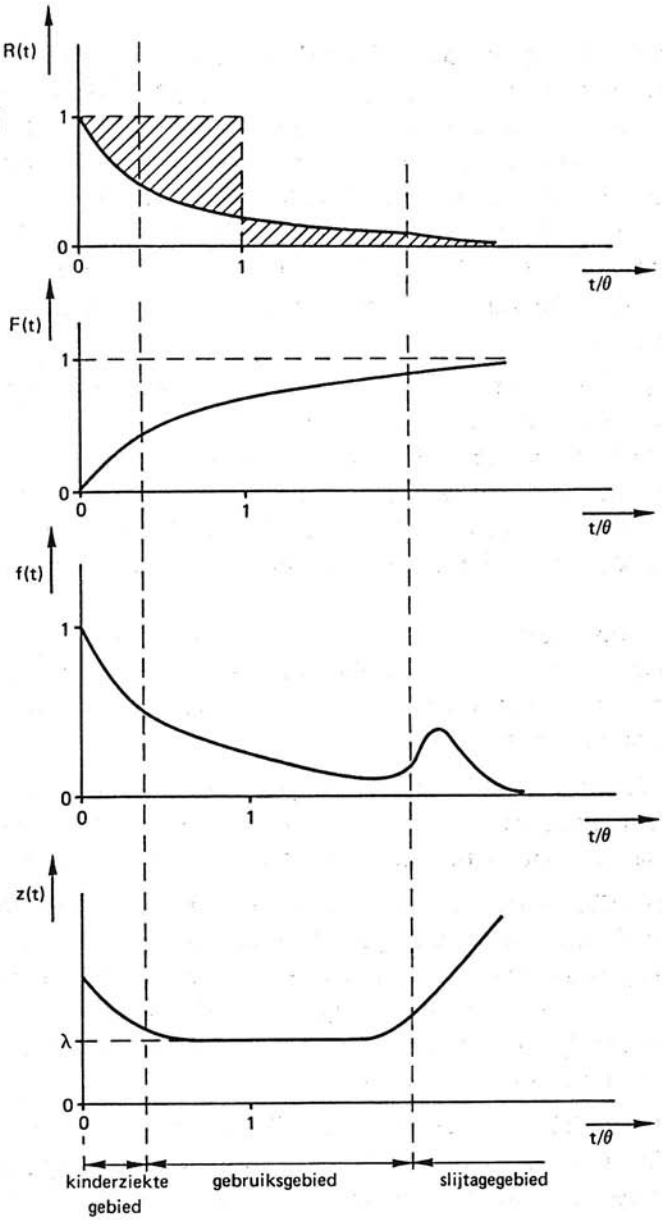
In de bedrijfszekerheidstechniek kiest men een bepaalde faaldistributie voor een component op de volgende gronden.

- Het dominante faalmechanisme sluit aan bij de meeste of alle veronderstellingen die ten grondslag liggen aan een bepaalde distributie.
- Er zijn bedrijfszekerheidsgegevens beschikbaar. De keuze is dan beperkt tot de faaldistributie die het beste bij deze gegevens aansluit (*curve fitting*).
- Er wordt een eenvoudige distributie gekozen die zich goed voor berekeningen leent. Hierop kan een globale afschatting van de bedrijfszekerheid berusten die des te nauwkeuriger is naarmate sterker aan de twee bovenstaande punten wordt voldaan.

Behalve als faaldistributie kunnen sommige van de onderstaande distributies ook dienst doen als *reparatietijddistributie*. Zij beschrijven dan niet de tijd tot falen, maar de tijd die verloopt tot de reparatie geslaagd is.

Als de faaldistributie een keer vastligt, kan men speciaal voorgedrukt grafiekenpapier (Engels: probability paper) gebruiken waarvan de schaalverdeling zodanig is ingericht dat de desbetreffende distributie een rechte lijn geeft te zien. Op deze wijze is het mogelijk relatief geringe afwijkingen van het verwachte faalpatroon reeds tijdens het plotten van uit de praktijk vergaarde meetresultaten te ontdekken.

Een faalpatroon dat men vaak in de praktijk aantreft is dat waarbij in het begin relatief veel componenten uitvallen, daarna relatief weinig en tenslotte, na lange tijd, weer relatief veel. Zo'n faalpatroon geeft dus een hazard rate die als functie van de tijd de vorm van een badkuip heeft (zie figuur 4.1); de hazard rate is immers een weerspiegeling van het percentage van de overlevende componenten dat in de eerstvolgende tijdseenheid sneuvelt. Het vroegtijdig falen wordt door zwakke componenten veroorzaakt. Deze periode duidt men wel aan als de '*early failure*'-periode of *kinderziekte*-periode. Dit is de periode waarover de hazard rate dalende is. De zwakke componenten zijn veelal het gevolg van onvolkomenheden in het produktieproces. Zij kunnen na afloop van de produktie in het alge-



Figuur 4.1. Voorbeeld van de zogenaamde 'badkuipdistributie'. Voor de duidelijkheid zijn de drie verschillende gebieden van deze distributie overdreven weergegeven. De parameter θ is de gemiddelde levensduur. De tijdasschaal is genormeerd voor de (gemiddelde) levensduur.

meen slechts (ten dele) verwijderd worden door het toepassen van screening (zie paragraaf 2.3).

Het tussenliggende tijdinterval (waar de hazard rate constant is) met relatief weinig fouten noemt men wel het *gebruiksgebied* of de *'normal life'*-

periode. De hierin optredende fouten zijn willekeurig van aard (*random failures*). Het einde van de 'normal life' periode, dus het weer toenemen van de hazard rate, wordt bepaald door het begin van de *slijtage (wear out).* Deze oude dag van een component gaat gepaard met verouderingsverschijnselen die tenslotte tot falen aanleiding zullen geven.
Voor de 'badkuipdistributie' bestaan geen analytische uitdrukkingen; wel kan met behulp van de hierna volgende distributies de vorm ervan gedeeltelijk worden benaderd.
N.B.: Vele componenten (met name elektronische) hebben zo'n lange levensduur dat (nog) niet is aangetoond dat ze een verouderingsgebied hebben. Met name mechanische componenten hebben soms een faaldistributie waarbij de kinderziekte-periode zonder een tussenliggende periode direct overgaat in de verouderingsperiode. Men mag dus beslist niet veronderstellen dat de 'badkuipdistributie' een soort hoger gegeven is achter het falen van technische systemen; er zijn vele componenten die niet volgens deze distributie falen, zij dient dan ook alleen om een drietal perioden van elkaar te onderscheiden: de garantieperiode (early failures), de gebruiksperiode en de vervangingsperiode (wear-out failures). In deze perioden is de hazard rate dalend, constant, respectievelijk stijgend in de tijd.

We zullen nu een voorbeeld geven van de badkuipdistributie uit het alledaagse leven: de bedrijfszekerheid van de mens. We nemen daarbij gemakshalve aan dat de mens bedrijfszeker functioneert zolang hij in leven is.
In tabel 4.1 is het aantal mensen N(t) vermeld dat in een bepaald land op de leeftijd t in leven is. Als we aannemen dat deze getallen niet veranderen als we ze in plaats van over een ensemble zouden nemen over de levensduur van de mensen (in de tijd), met andere woorden als het sterfteproces als stochastisch proces ergodisch is, kunnen we uit deze tabel de bedrijfszekerheid R(t), de faaldistributie F(t), de faalkansdichtheid f(t) en de hazard rate z(t) afleiden.

t	N(t)	t	N(t)	t	N(t)	t	N(t)
0	1 023 102	15	962 270	50	810 900	85	78 221
1	1 000 000	20	951 483	55	754 191	90	21 577
2	994 230	25	939 197	60	677 771	95	3 011
3	990 114	30	924 609	65	577 822	99	125
4	986 767	35	906 554	70	454 548		
5	983 817	40	883 342	75	315 982		
10	971 804	45	852 554	80	181 765		

Tabel 4.1. Bevolkingsopbouw van een klein, fictief land.

Voor R(t) geldt:

$$R(t) = N(t)/N(0).$$

Voor F(t) geldt:

$$F(t) = 1-R(t) = \{N(0) - N(t)\}/N(0);$$

f(t) wordt bepaald uit:

$$f(t) = \frac{F(t+\Delta t)-F(t)}{\Delta t},$$ | faalkansdichtheid.

waarin voor Δt 5 jaar wordt genomen. Tenslotte volgt z(t) uit:

$$z(t) = \frac{f(t)}{1-F(t)}.$$ | hazard rate.

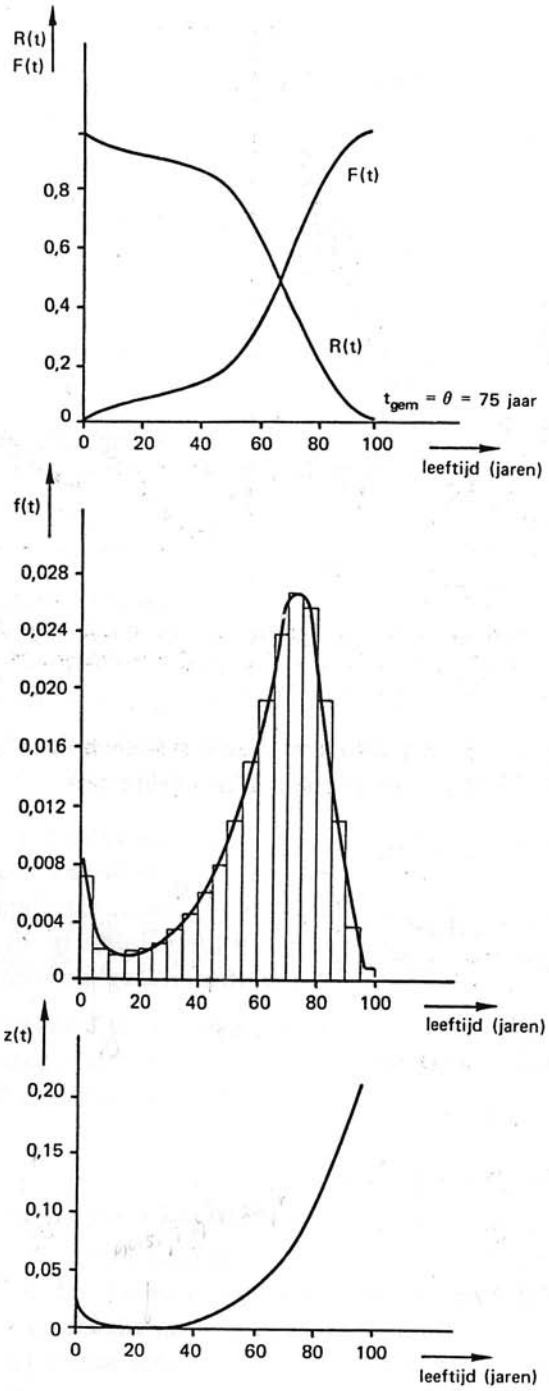
De resultaten zijn in figuur 4.2 uitgezet. Deze resultaten correleren zeer goed met het 'onderhoud' dat aan de mens moet worden gepleegd om hem in leven te houden (en het leven aangenaam te houden).
Ter illustratie hiervan toont figuur 4.3 een deel van de kosten die voor dit 'onderhoud' worden gemaakt: de verpleegkosten. Deze kosten zijn nauw gecorreleerd aan de hazard rate uit figuur 4.2.

In figuur 4.2 ziet men een periode van afnemende hazard rate, een periode van (vrijwel) constante hazard rate en een periode van toenemende hazard rate, die respectievelijk afbakenen de periode van kinderziekten (*infant mortality*) en de oude dag (*end of life period*). In dit verband wordt de hazard rate ook wel de 'force of mortality' genoemd.

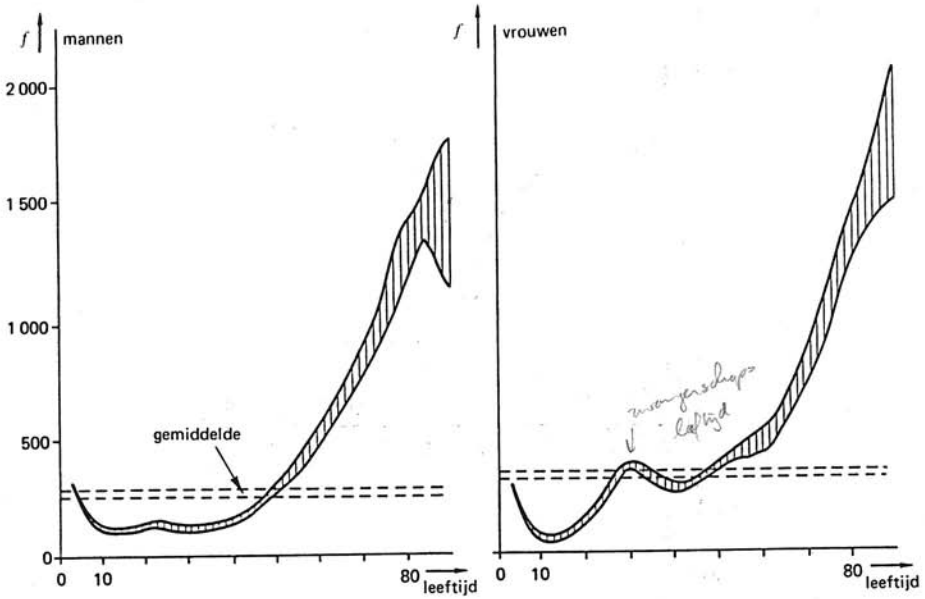
Wij zullen nu een aantal van de meest voorkomende faaldistributies bespreken. Deze distributies worden vaak ook voor andere parameters gebruikt, dus als reparatiedistributie, voorbereidingstijddistributie, enzovoort.

4.1.1. Negatief-exponentiële distributie

De negatief-exponentiële distributie is verreweg de meest gebruikte faal- en reparatiedistributie uit de bedrijfszekerheidstechniek. Men kan zich deze distributie als volgt afgeleid denken. Als we uit het faalpatroon waarnemen dat componenten onafhankelijk van elkaar, op willekeurige tijdstippen falen en bovendien dat het gemiddelde aantal dat in een tijdinterval $(t, t+\Delta t)$ faalt niet van de tijd t afhangt maar evenredig met Δt toeneemt, dan is dat faalproces een zogenaamd *poissonproces*. De kans



Figuur 4.2. Levensduurverdeling van de mensen uit het land van tabel 4.1.



Figuur 4.3. Verpleegkosten per jaar afhankelijk van de leeftijd voor de Nederlandse bevolking in het jaar 1981. Het gearceerde gebied geeft het 75% betrouwbaarheidsinterval aan.

$P_n(\Delta t)$ dat er in een tijdinterval Δt precies n systemen falen, als er in dat interval gemiddeld $\lambda\Delta t$ systemen falen, is dus gelijk aan:

$$P_n(\Delta t) = \frac{(\lambda\Delta t)^n}{n!} e^{-\lambda\Delta t}.$$

De bedrijfszekerheidsdefinitie vereist dat er in het tijdinterval [0,t] géén fouten voorkomen. Dit geeft met $\Delta t = t$ en $n = 0$ voor de bedrijfszekerheid:

$$R(t) = P_0(t) = e^{-\lambda t}.$$

De faaldistributie is dus:

$$F(t) = 1 - e^{-\lambda t},$$

de faalkansdichtheid:

$$f(t) = \lambda e^{-\lambda t},$$

de hazard rate:

$$z(t) = \lambda,$$

de gemiddelde levensduur:

$$\theta = 1/\lambda,$$

de spreiding in de gemiddelde levensduur:

$$\sigma = 1/\lambda,$$

en, tenslotte, de mediane levensduur:

$$\theta_m = \frac{\ln 2}{\lambda}.$$

Algemeen geldt dat voor een naar rechts scheve distributie zoals die van F(t) in figuur 4.4 de *meest voorkomende waarde* (de top van de kansdichtheidsfunctie f(t)) het meest naar links ligt. Dan volgt de *mediane waarde* met 50% van het oppervlak van de kansdichtheidsfunctie f(t) aan weerszijden van de mediaan. Het meest naar rechts ligt de *gemiddelde waarde.* Het omgekeerde geldt voor een naar links scheve distributie.

We willen benadrukken dat een Poissonproces *geheugenloos* is voor de tijd die verstreken is sedert het ontstaan van de component. Anders gezegd: als een systeem met zo'n faalproces op een willekeurig gekozen tijdstip τ nog goed werkt, dan zal het zich in de tijd na τ statistisch gezien gedragen als een nieuw systeem. Men kan dit als volgt inzien: de resterende levensduur Δt na het tijdstip $t = \tau$ wordt bepaald door:

$$R(\tau + \Delta t \mid \underline{t} > \tau) = R(\tau + \Delta t)/R(\tau).$$

Voor een negatief-exponentiële verdeling geldt

$$R(\tau + \Delta t) = R(\tau)R(\Delta t).$$

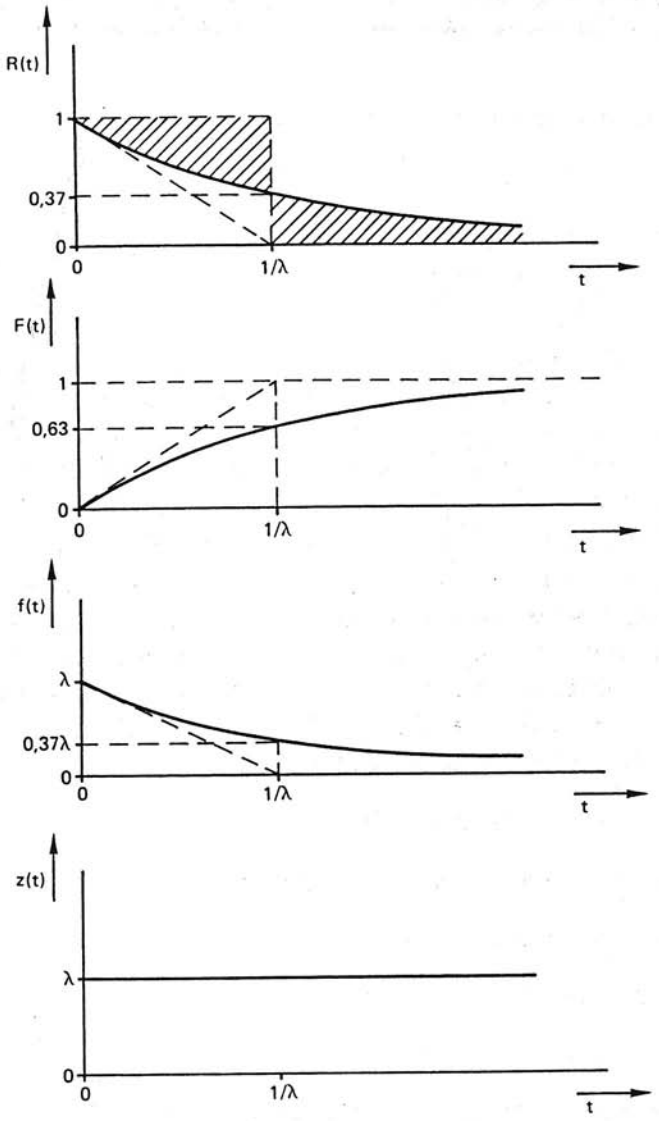
De resterende levensduur wordt dus

$$R(\tau + \Delta t \mid \underline{t} > \tau) = R(\Delta t).$$

De resterende levensduur is dus onafhankelijk van τ.

N.B.: Men neemt in de bedrijfszekerheidstechniek zeer vaak aan dat componenten een constant faaltempo hebben. Men moet deze aanname meer zien als een eerste orde benadering van een tijdafhankelijk faaltempo (voortspruitend uit een gebrek aan gegevens) dan als een bewezen feit.

In figuur 4.4 zijn de verschillende grootheden van de negatief-exponentiële distributie weergegeven. Voorbeelden van negatief-exponentieel verdeelde faalmechanismen zijn: lekke banden veroorzaakt door spijkers of andere scherpe, losse voorwerpen versus het aantal afgelegde kilometers en



Figuur 4.4. De negatief-exponentiële distributie. De gemiddelde levensduur θ is gelijk aan 1/λ. De beide gearceerde oppervlakken zijn even groot.

de verdeling van de inslagen van radioactieve deeltjes in halfgeleidergeheugens, waarin zij zogenaamde herstelbare fouten (*soft errors*) veroorzaken door de vrijgekomen ladingen.

Samenvattend kunnen we stellen dat de negatief-exponentiële distributie de tijd beschrijft tussen onafhankelijke fouten die optreden in een constant tempo. De levensduurverdeling van complexe systemen met een gro-

te variëteit aan componenten met verschillende levensduren is daarom negatief-exponentieel verdeeld (als het systeem tenminste niet redundant is).

4.1.2. Normale distributie

De normale distributie is een van de bekendste distributies uit de waarschijnlijkheidsrekening. Zij wordt ook wel aangeduid als de distributie van Gauss. Dit is eigenlijk ten onrechte: De Moivre gebruikte als eerste in 1733 deze distributie. Ook Laplace gebruikte haar al in 1774. Toch, door een historische fout, is de distributie vernoemd naar Gauss die haar pas in 1809 ten tonele voerde.

Een normale distributie beschrijft componenten die uitsluitend stuk gaan ten gevolge van een slijtageproces. De hazard rate neemt daarom aanvankelijk monotoon toe. De uitval is normaal verdeeld $N(\theta,\sigma)$ met een bepaalde gemiddelde levensduur θ en een spreiding σ (zie figuur 4.5).

De faaldistributie is:

$$F(t) = \frac{1}{\sigma\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{(t-\theta)^2}{2\sigma^2}} dt,$$

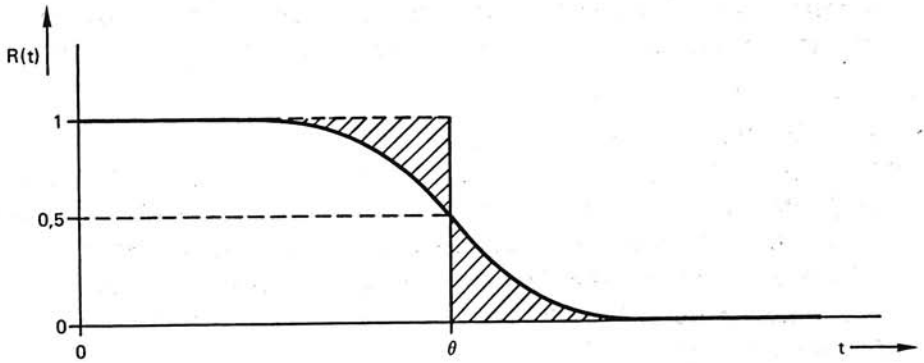
dus:

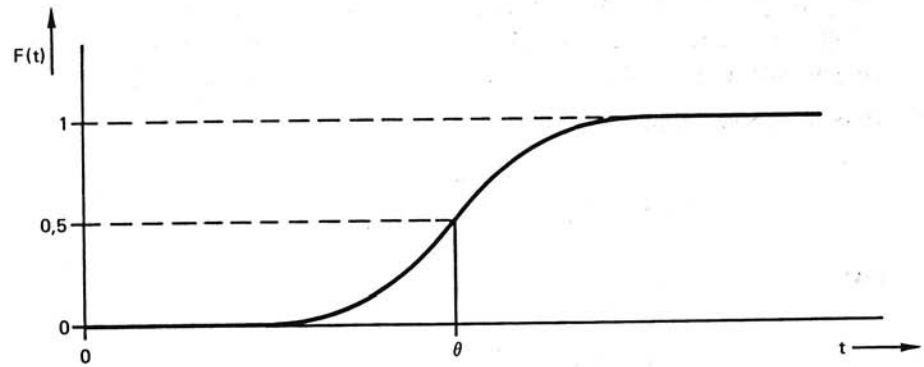
$$f(t) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(t-\theta)^2}{2\sigma^2}},$$

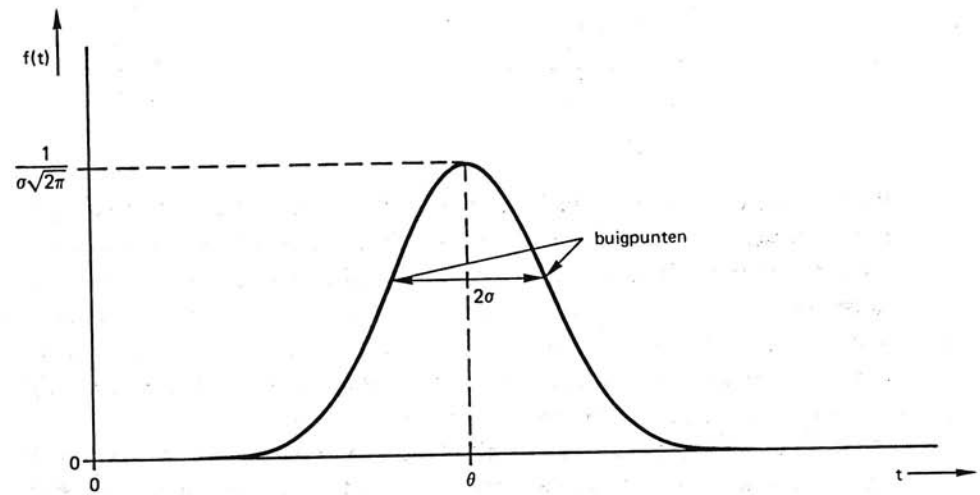
en:

$$z(t) = \frac{e^{-\frac{(t-\theta)^2}{2\sigma^2}}}{\int_{t}^{\infty} e^{-\frac{(t-\theta)^2}{2\sigma^2}} dt}.$$

We kunnen deze faaldistributie zien als ontstaan uit de som van een groot aantal verschillende, onderling stochastisch onafhankelijke foutoorzaken waarvan de individuele faaldistributie een willekeurige, dus ook een niet normale, vorm mag hebben (*centrale limiet stelling*). Een nadeel is dat ook voor negatieve tijd de distributie van nul verschillende waarden heeft. Bij grote waarden van de variatiecoëfficiënt θ/σ is dit meestal niet hinderlijk in de praktijk, daar de distributie dan zeer smal is.
Voorbeelden van de normale distributie in de bedrijfszekerheidstechniek zijn de faaldistributie van gloeilampen, de distributie van parameterwaarden van ongeselecteerde analoge elektronische componenten, de distributie van afmetingen van mechanische componenten, enzovoort.

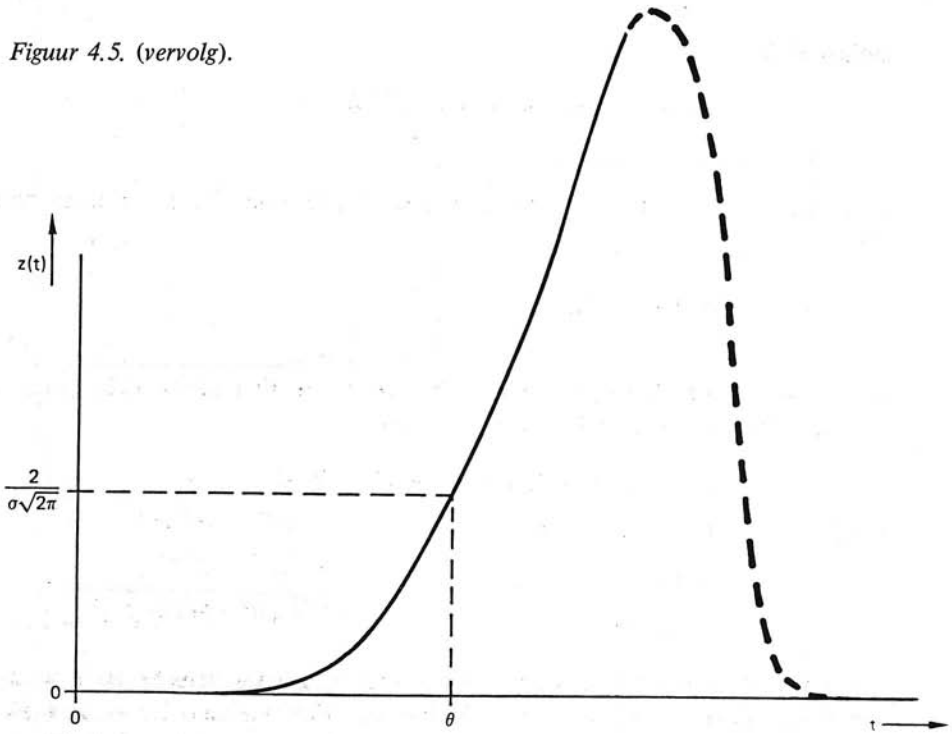






Figuur 4.5 (*zie verder op de volgende bladzijde*).

Figuur 4.5. (vervolg).



Figuur 4.5. De normale distributie weergegeven voor een spreiding $\sigma = 0{,}2\,\theta$ en een gemiddelde levensduur θ.

4.1.3. Lognormale distributie

Uit de normale distributie kan men een aantal andere, voor de bedrijfszekerheidstechniek van meer belang zijnde distributiefamilies afleiden. Daartoe stelt men dat niet de random variabele t normaal verdeeld is, maar de random variabele g(t), waarin g(t) een eenwaardige expliciete functie van t is. Eén van deze getransformeerde distributies is de logaritmisch normale distributie die alleen voor $t > 0$ geldig is. Deze lognormale faaldistributie kan eenvoudig berekend worden met behulp van de transformatie:

$$g(t) = \ln kt \qquad (t > 0),$$

waarmee men de navolgende twee-parameter lognormale faaldistributie verkrijgt:

$$F(t) = \frac{1}{\sigma'\sqrt{2\pi}} \int_0^t \frac{1}{t} \exp\{-\frac{(\ln kt - \theta')^2}{2(\sigma')^2}\}\,dt.$$

Hierin zijn θ' en σ' dimensieloos en heeft de constante k de dimensie s^{-1}. Verder is $e^{\theta'}$ de locatieparameter en σ' de vormparameter. De faalkans-

dichtheid is:

$$f(t) = \frac{1}{\sigma' t\sqrt{2\pi}} \exp\{-\frac{(\ln kt - \theta')^2}{2(\sigma')^2}\}.$$

De hazard rate kan met de uitdrukkingen uit paragraaf 3.2.1 berekend worden:

$$z(t) = \frac{f(t)}{1 - F(t)}.$$

De diverse grootheden zijn geschetst in figuur 4.6. Een aantal belangrijke waarden van de lognormale distributie zijn:

mediane waarde (50 % uitval)	$k^{-1}e^{\theta'}$
gemiddelde waarde	$k^{-1}e^{(\theta' + (\sigma')^2/2)}$
top van f(t)	$k^{-1}e^{(\theta' - (\sigma')^2)}$
variantie	$k^{-2}e^{(2\theta' + (\sigma')^2)}(e^{(\sigma')^2} - 1)$

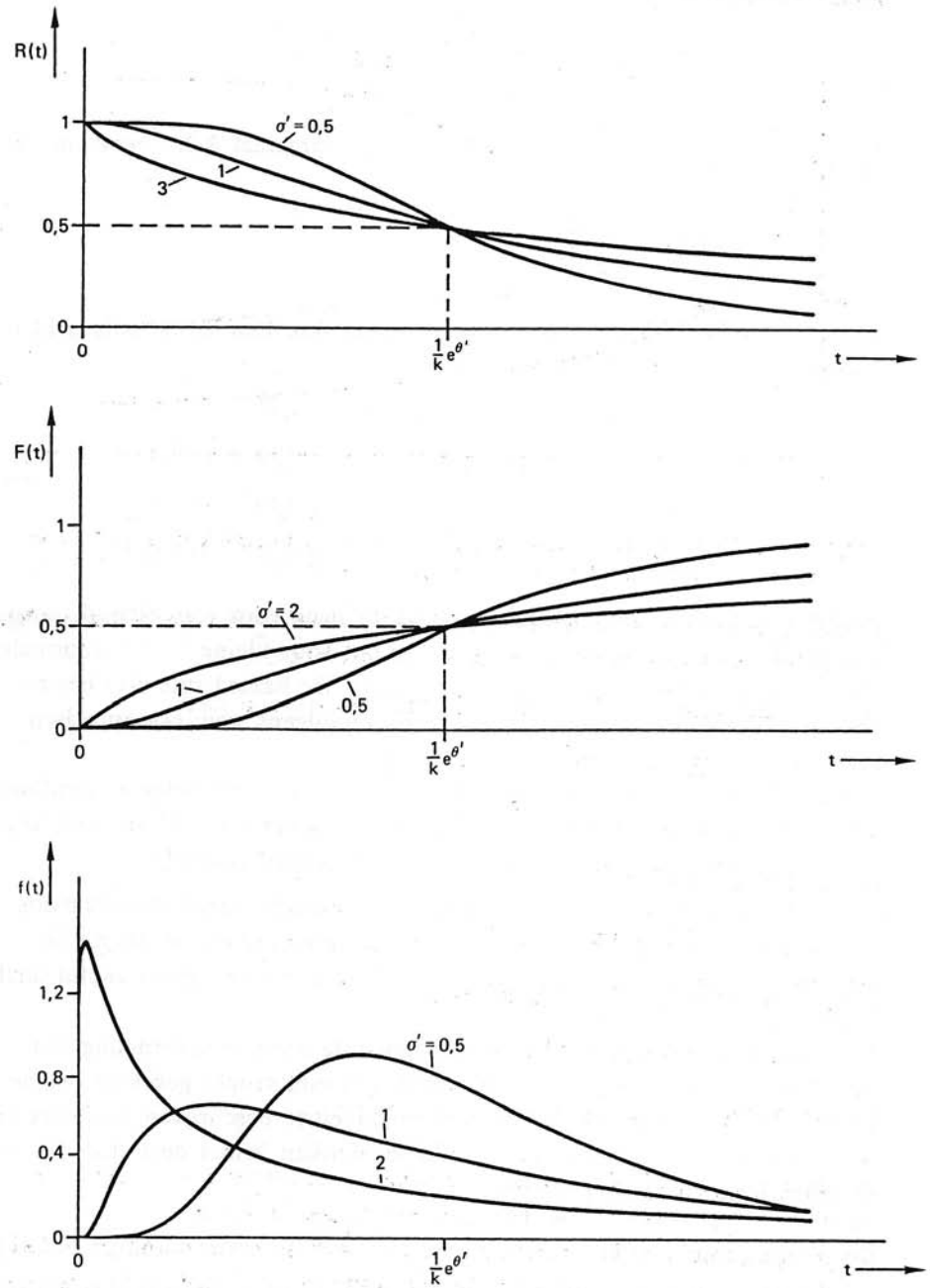
In figuur 4.6 is een aantal lognormale verdelingen voor verschillende waarden van σ' uitgezet. Uit de figuur zien we dat voor kleine σ' de lognormale distributie overgaat in de normale distributie. De hazard rate z(t) begint bij nul, stijgt dan naar een piek en neemt vervolgens weer asymptotisch af tot nul (voor alle waarden van σ'!).
Evenals de *som* van een aantal onafhankelijke, normaal verdeelde randomvariabelen weer een normale distributie heeft, is het *produkt* van een aantal lognormaal verdeelde variabelen weer lognormaal verdeeld.

De lognormale distributie representeert stochastische variabelen waarvan de logaritme normaal verdeeld is. Zij treedt onder andere op als de beschouwde stochastische variabele het produkt is van een groot aantal onafhankelijke stochastische variabelen.
De lognormale distributie weerspiegelt goed de levensduurverdeling van veel halfgeleidercomponenten. Zij wordt ook met vrucht gebruikt om de reparatieduurverdeling van technische systemen te beschrijven. Ook het falen tengevolge van materiaalvermoeidheidsbreuken is met deze distributie te beschrijven (haarscheurtjes).

4.1.4. Weibulldistributie

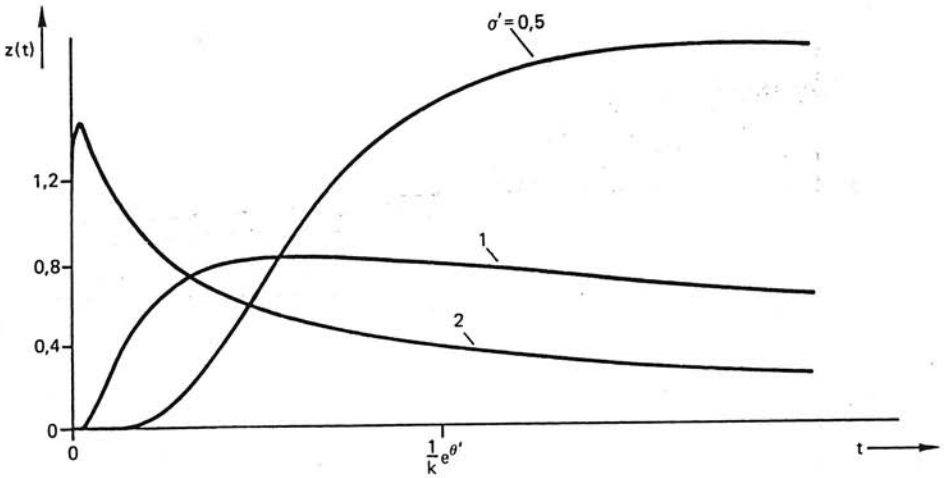
De Weibulldistributie kan men ontstaan denken uit de exponentiële distributie, beschreven in paragraaf 4.1.1, door de transformatie:

$$g(t) = t^c, \qquad (t > 0,\ c > 0).$$



Figuur 4.6. (*zie verder op de volgende bladzijde*).

Figuur 4.6. (vervolg).



Figuur 4.6. De lognormale distributie. De mediane levensduur is $k^{-1}e^{\theta'}$. $e^{\theta'}$ is de locatieparameter. De vormparameter is σ'.

Dus als g(t) negatief-exponentieel verdeeld is, heeft t een Weibullverdeling. c geeft een verandering in de vorm van de distributie.

De bedrijfszekerheid R(t) en de faaldistributie worden dan:

$$R(t) = e^{-\alpha t^c}, \qquad (\alpha \geqslant 0),$$

$$F(t) = 1 - e^{-\alpha t^c},$$

de faaldichtheid wordt:

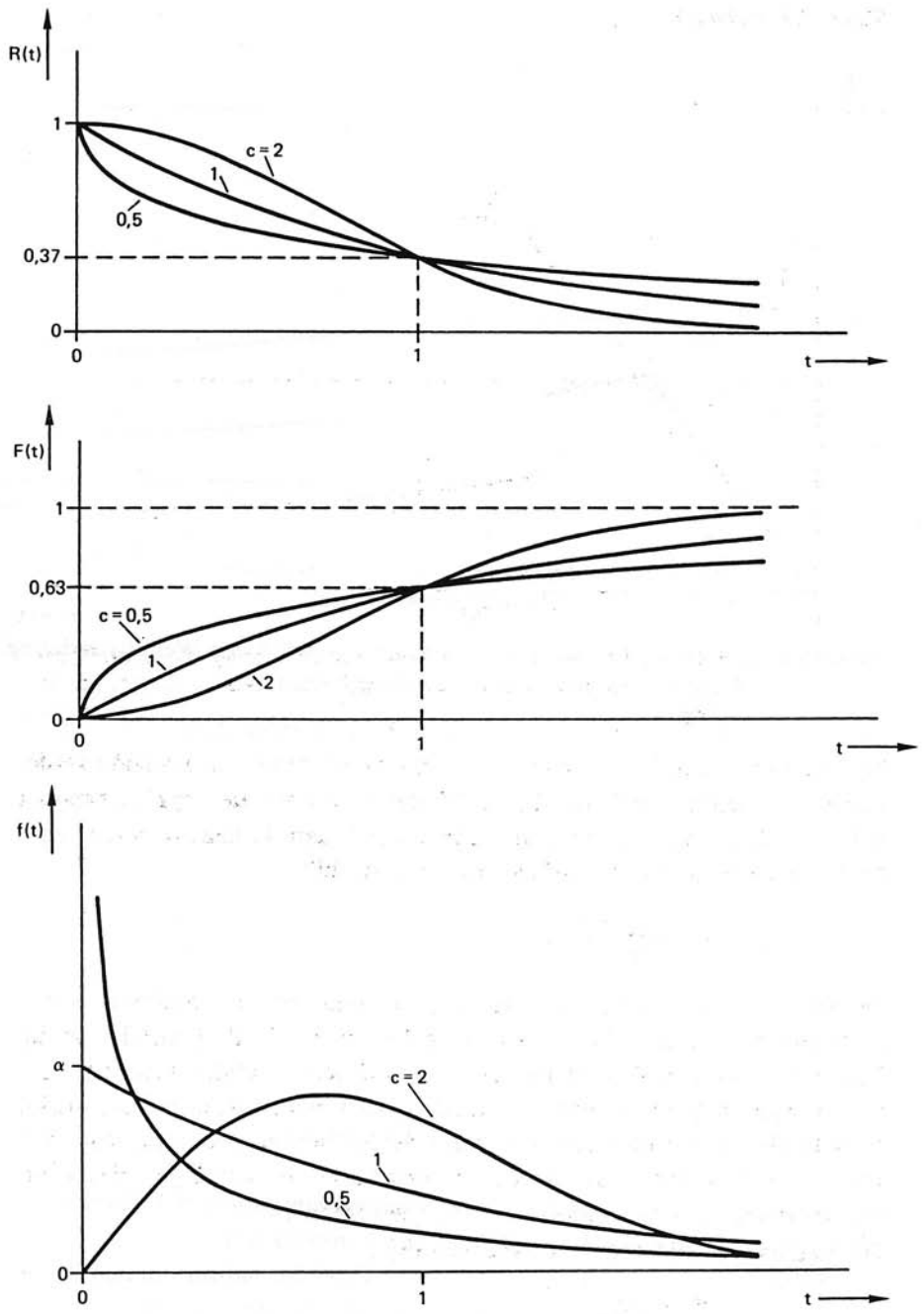
$$f(t) = \alpha c t^{c-1} e^{-\alpha t^c},$$

en de conditionele faaldichtheid wordt:

$$z(t) = \alpha c t^{c-1}.$$

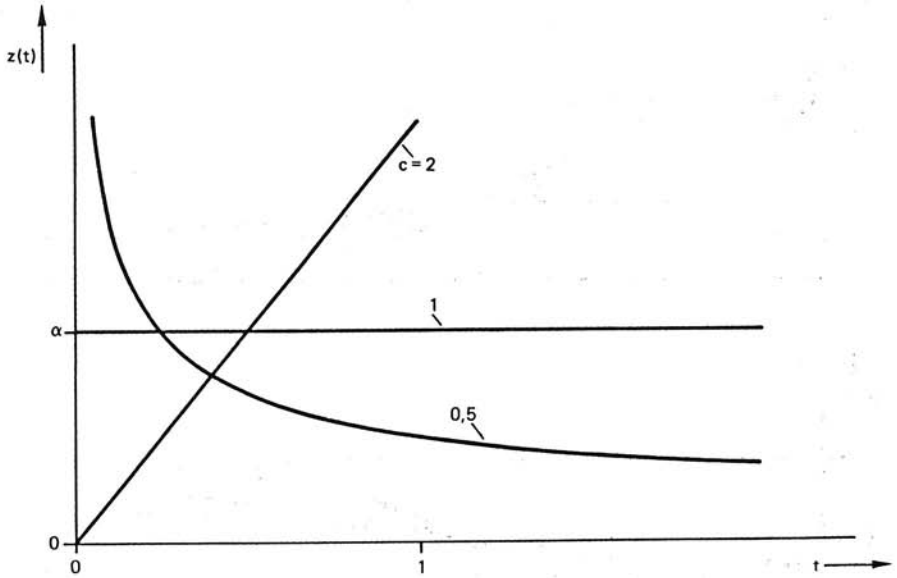
c is de vormparameter en α is de locatieparameter.

In figuur 4.7 is de Weibulldistributie weergegeven voor $\alpha = 1$. Merk op dat voor $t = 1$, $R(t) = e^{-1} \approx 0{,}37$ dus onafhankelijk van c.
De Weibulldistributie is vernoemd naar de Zweedse natuurkundige Waloddi Weibull die deze distributie in 1939 gebruikte om de breeksterkte van diverse materialen te beschrijven.
De kracht van de Weibulldistributie ligt niet zozeer in een bepaald theoretisch faalmodel dat aanleiding tot deze distributie zou geven, maar in



Figuur 4.7. (*zie verder op de volgende bladzijde*).

Figuur 4.7. (vervolg).



Figuur 4.7. De Weibulldistributie. Als c = 1 ontstaat de negatief-exponentiële verdeling waarbij α gelijk is aan de hazard-rate λ. Als c = 2 ontstaat de Raleighdistributie.

haar flexibiliteit als praktische benadering voor empirisch bepaalde verdelingen. We zien namelijk uit figuur 4.7 dat voor $c = 1$ de negatief-exponentiële verdeling ontstaat (waarbij α dan gelijk is aan de hazard rate λ) en voor $c > 1$ een faalkansdichtheid met een top bij:

$$t = \left(\frac{c-1}{\alpha c}\right)^{1/c}.$$

De hazard rate is voor $c > 1$ monotoon stijgend, wat overeenkomt met systemen met slijtage (het rechtse gedeelte van de 'badkuipdistributie' uit figuur 4.1). Voor $0 < c < 1$ nadert de conditionele faaldichtheid $z(t)$ voor $t \to \infty$ asymptotisch tot nul, een karakteristiek voor systemen met uitsluitend kinderziekten (het meest linkse gedeelte van de 'badkuipdistributie' van figuur 4.1). Dit maakt de Weibulldistributie bij uitstek geschikt voor 'curve fitting' met experimenteel verkregen waarden.
De mediane levensduur wordt gegeven door

$$\theta_m = \left(\frac{1}{\alpha}\ln 2\right)^{c^{-1}};$$

de gemiddelde levensduur door

$$\theta = \left(\frac{1}{\alpha}\right)^{c^{-1}} \Gamma\left(\frac{1}{c}+1\right);$$

waarin de functie $\Gamma(x)$ de zogenaamde gammafunctie is (zie paragraaf 4.1.5).
De spreiding σ in de levensduur is:

$$\sigma = \frac{1}{\alpha}\sqrt{\Gamma(\tfrac{2}{c}+1) - \Gamma^2(\tfrac{1}{c}+1)}.$$

4.1.5. Gammadistributie

De *gammadistributie* is bepaald door:

$$F(t) = \int_0^t \frac{\lambda}{\Gamma(c)} (\lambda t)^{c-1} e^{-\lambda t} dt, \qquad (c > 0,\ \lambda > 0,\ t \geqslant 0).$$

Hierin is c de vormparameter en is λ een tijdschaalparameter met de dimensie s^{-1}. Verder is de *gammafunctie* $\Gamma(c)$ gegeven door:

$$\Gamma(c) = \int_0^\infty \lambda(\lambda t)^{c-1} e^{-\lambda t} dt.$$

Deze gammafunctie heeft de volgende eigenschappen:

- $\Gamma(c) = (c-1)\Gamma(c-1)$;
- $\Gamma(c) = (c-1)!$ voor positieve gehele getallen;
- $\Gamma(\frac{1}{2}) = \sqrt{\pi}$.

De faalkansdichtheid is met $f(t) = \dfrac{dF(t)}{dt}$ dus:

$$f(t) = \frac{\lambda}{\Gamma(c)} (\lambda t)^{c-1} e^{-\lambda t}.$$

De gemiddelde levensduur is $\theta = c/\lambda$ en de spreiding in de levensduur is $\sigma = \sqrt{c/\lambda}$.

Opmerkingen

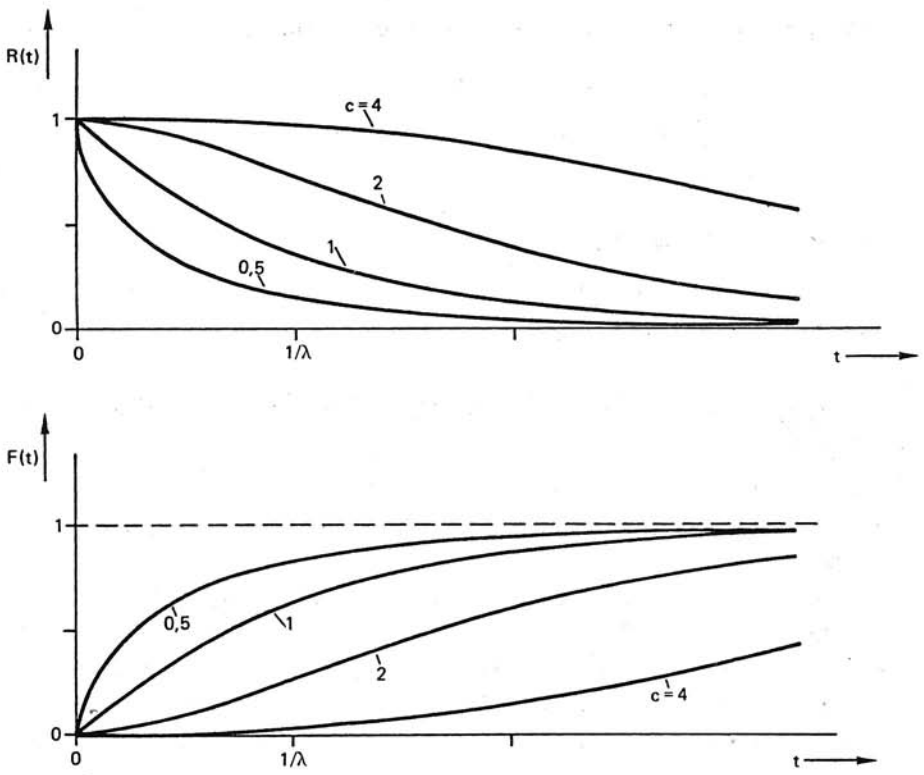
- Als $c = 1$ ontaardt de gammafunctie in de negatief-exponentiële distributie.
- Als c een positief geheel getal is ontstaat een distributie die we aanduiden als de Erlangdistributie.
- Als c een geheel getal is kan de integraaluitdrukking voor F(t) door middel van herhaalde partiële integratie opgelost worden.
  Dit geeft dan

$$F(t) = \sum_{i=c}^{\infty} \frac{(\lambda t)^i e^{-\lambda t}}{i!},$$

en dus

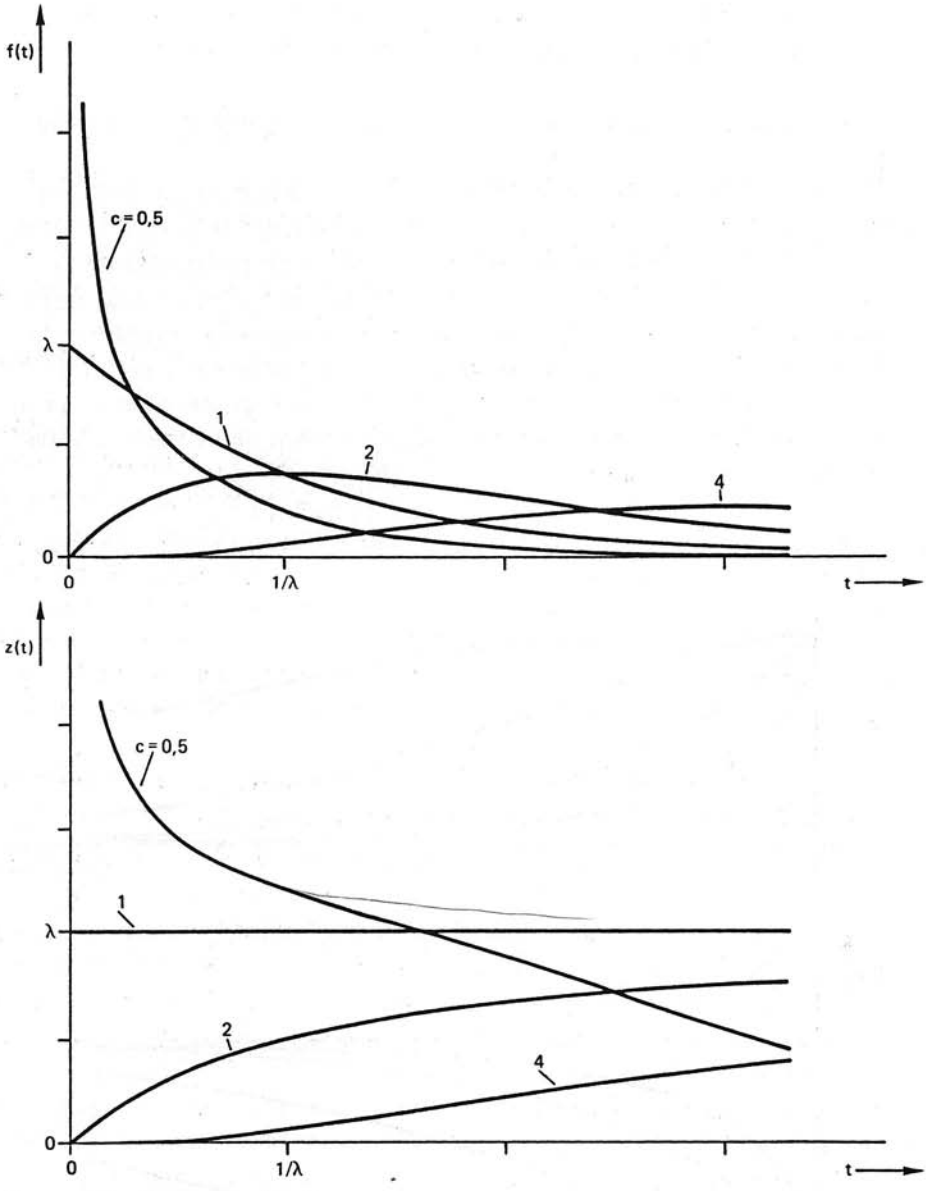
$$R(t) = 1 - F(t) = \sum_{i=0}^{c-1} \frac{(\lambda t)^i e^{-\lambda t}}{i!}.$$

In figuur 4.8 is de gammadistributie geschetst voor een aantal verschillende waarden van de vormparameter c.
De gammadistributie neemt vormen aan die veel lijken op die welke de Weibulldistributie kan aannemen. Voor "curve fitting" is de Weibulldistributie echter beter geschikt. Bepaalde vormen van de gammadistributie, met name de Erlangdistributie, lenen zich echter beter voor berekening in analytische vorm. De Erlangdistributie is bekend uit de wachttijdtheorie: Als de tijd tot falen $\underline{t}_1$ een stochastische variabele is met een negatief-exponentiële verdeling met een failure rate λ, dan is de distributie van de tijd $\underline{t}_m$ die verloopt tot m eenheden gefaald hebben de Erlangdistributie met parameters λ en $c = m$.



Figuur 4.8. (*zie verder op de volgende bladzijde*).

Figuur 4.8. (vervolg).



Figuur 4.8. De gammadistributie.

We zien dus dat een bepaalde vorm van gammadistributie (de Erlangdistributie) optreedt in systemen met passieve redundantie waarbij m identieke units functioneel parallel staan en daardoor van elkaar de taak kunnen overnemen. Anders dan de Weibulldistributie heeft de gammadistributie dus een theoretische achtergrond.

Een voorbeeld van een toepassing uit de onderhoudstechniek is de distributie van de tijd die verloopt tussen twee herkalibraties van een instrument dat na m keer gebruiken weer gekalibreerd moet worden.

4.2. Levensduurmetingen

Het meten van een faaldistributie is in principe een eenvoudig proces. Zoals we in het navolgende zullen zien zijn er evenwel een aantal praktische factoren die roet in het eten gooien. De meting gaat in principe als volgt: men verricht een levensduurproef en registreert de uitval (of men registreert de uitval die optreedt bij het praktische gebruik van de produkten). Uit deze gegevens kan men de faaldistributie construeren en de karakteristieke parameters van deze distributie bepalen.
Een kleine praktische opmerking is hier op zijn plaats. Vaak weet men van te voren welke distributie men kan verwachten. Het is dan zinvol de resultaten van de levensduurproef te tekenen op speciaal grafiekenpapier (*probability paper*), waarop de assen zodanig zijn voorgedrukt dat de desbetreffende distributie een rechte lijn geeft. Als men op zulk papier de cumulatieve faalfrequentie tekent, heeft men het voordeel dat in de zo verkregen faaldistributie erg grote willekeurige variaties worden vermeden (alle overige bedrijfszekerheidsgrootheden bevatten immers de afgeleide van de faaldistributie) en dat bovendien afwijkingen van de verwachte distributie reeds tijdens de proef aan het licht treden.
In paragraaf 4.2.1 zullen we nader ingaan op de a priori kennis omtrent de faaldistributie die men bij de levensduurproef mag verwachten.

Een fundamenteel probleem dat zich bij een levensduurproef voordoet is dat men niet alle beschikbare componenten in zo'n proef wil opofferen. Aan de ene kant is het uit economische overwegingen voordelig zo weinig mogelijk componenten in een levensduurtest op te nemen, aan de andere kant vereist de nauwkeurigheid (betrouwbaarheid) van de meting een zo groot mogelijke monstergrootte. Op dit onderwerp zullen we in paragraaf 4.2.2 nader ingaan.
De bedrijfszekerheid van halfgeleidercomponenten is relatief hoog. Dit brengt met zich mee dat men zeer lange levensduurproeven zou moeten doen. Derhalve voert men meestal kunstmatig versnelde levensduurproeven uit. De vraag is dan: hoe groot is de versnellingsfactor. Op dit onderwerp zullen we in paragraaf 4.2.3 ingaan.

4.2.1. Faaldistributie bij levensduurmetingen

Het verdient aanbeveling de nodige terughoudendheid te betrachten in het bepalen van de aard van een faaldistributie uitsluitend en alleen op grond van het feit dat deze distributie de gegenereerde meetgegevens goed past.

Daar men in de praktijk de metingen verricht aan eindige (en om economische redenen zo klein mogelijke) monsters uit de totale produktiepopulatie en verder de meting zo kort mogelijk laat duren (afgebroken levensduurexperiment) heeft men te maken met van nul verschillende betrouwbaarheidsintervallen rondom de gemeten waarden. Hoe kleiner het monster en hoe korter de testduur, hoe groter het betrouwbaarheidsinterval, dus hoe groter de kans die men loopt onjuiste conclusies te trekken uit een bepaalde (toevallige) combinatie van meetresultaten.
Men gaat minder arbitrair te werk als men kan aantonen dat er een rationeel verband bestaat tussen de faaldistributie enerzijds en de fysisch-chemische processen die het falen veroorzaken anderzijds.
Zo heeft men bijvoorbeeld kunnen vaststellen dan de meeste levensduurmetingen van halfgeleidercomponenten het beste worden weergegeven door de lognormale distributie. De verklaring hiervoor is dat de meeste faalprocessen in halfgeleiders chemisch of chemisch-fysisch zijn, en vaak veroorzaakt worden door een aantal willekeurige variabelen die een multiplicatief effect hebben op de bekorting van de levensduur.
Zoals we gezien hebben is de distributie van het produkt van een (groot) aantal (statistisch onafhankelijke) variabelen lognormaal, ongeacht de distributie van de individuele variabelen (zie paragraaf 4.1.3).

4.2.2. Betrouwbaarheid van levensduurmetingen

Bij het bespreken van de faaldistributies in paragraaf 4.1 hebben we aangenomen dat we over een monster van oneindige grootte beschikken. We kunnen de faaldistributie dan exact bepalen; we behoeven geen schatting te maken. Bij een monster van eindige grootte kunnen we alleen maar een schatting maken van de distributie (of bepaalde stochastische parameters) van de eigenlijke populatie. Hoe kleiner het monster hoe groter de onnauwkeurigheid is van deze schatting.
Als maat voor de nauwkeurigheid heeft men het begrip betrouwbaarheidsgrens (*confidence level*) geïntroduceerd. De betrouwbaarheidsgrenzen (ondergrens en bovengrens) bakenen een interval af rondom de geschatte waarde.
Als de kans op overschrijding van dit interval α is, mag men dus verwachten dat bij $100 \times \alpha\,\%$ van de componenten, getrokken uit dezelfde populatie als waar de levensduurtest op is verricht, de werkelijke levensduur buiten het betrouwbaarheidsinterval rondom de geschatte (gemeten) waarde valt.
Voor de geschatte waarde $\hat{F}(t_1)$ van de (cumulatieve) faaldistributie $F(t_1)$ op een arbitrair tijdstip t_1, bepaald op grond van een monster ter grootte n nemen we:

$$\hat{F}(t_1) = m(t_1)/n,$$

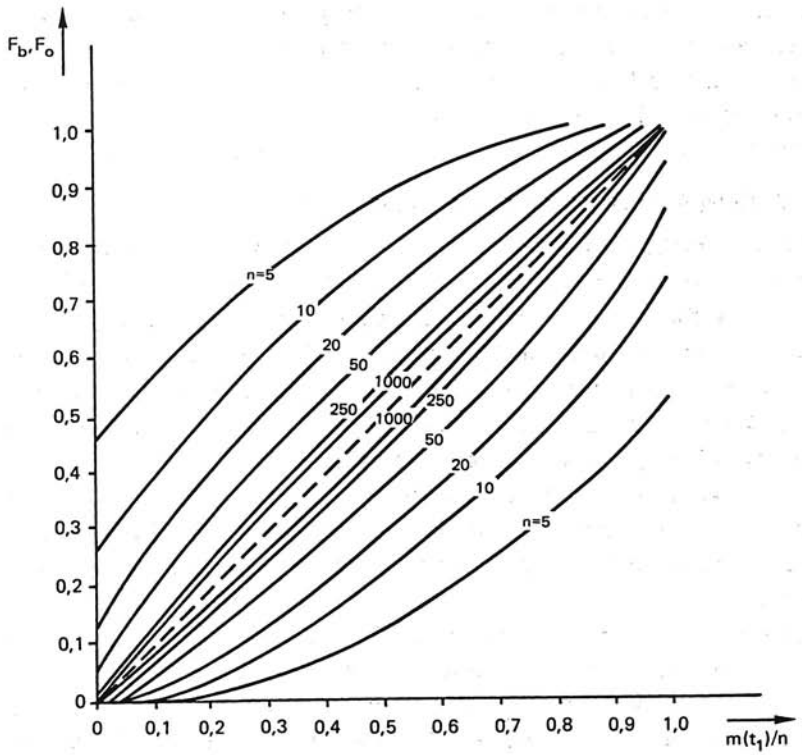
waarin $m(t_1)$ het aantal gefaalde exemplaren in het monster is tot en met de tijd t_1. De werkelijke waarde is $F(t_1)$.
Eenvoudig is in te zien dat $\hat{F}(t_1)$ een binomiale distributie heeft (de kans op $m(t_1)$ fouten uit n met een gemiddelde foutkans $F(t_1)$). De ondergrens F_o en bovengrens F_b voor $F(t_1)$ bij een betrouwbaarheid $1 - \alpha$ is dus te berekenen uit:

$$\sum_{i=m(t_1)}^{n} \binom{n}{i} F_o^i (1 - F_o)^{n-i} = \tfrac{1}{2}\alpha,$$

respectievelijk:

$$\sum_{i=0}^{m(t_1)} \binom{n}{i} F_b^i (1 - F_b)^{n-i} = \tfrac{1}{2}\alpha.$$

In figuur 4.9 zijn de betrouwbaarheidsgrenzen aangegeven voor $\alpha = 0{,}1$ en verschillende waarden van de monstergrootte n.



Figuur 4.9. Bovengrens F_b en ondergrens F_o van het 90% betrouwbaarheidsinterval ($\alpha = 0{,}1$) rondom de geschatte (gemeten) waarde $m(t_1)/n$ bij een monstergrootte n en een gemeten uitval $m(t_1)$.

Op deze wijze kan men rondom de opgemeten faaldistributie $\hat{F}(t)$ (en ook om de opgemeten bedrijfszekerheid $\hat{R}(t)$) een betrouwbaarheidsband aangeven. De gezochte distributie zal dan met een kans $1 - \alpha$ in deze band liggen. Duidelijk zal zijn dat er door deze betrouwbaarheidsband oneindig vele distributies lopen. Men dient dus over extra informatie te beschikken om tot een bepaalde distributie te besluiten (zie in dit verband het geponeerde in paragraaf 4.2.1).

Als men van tevoren weet welke distributie men kan verwachten, kan men schatters berekenen voor de parameters van zo'n distributie. Daar nu meer informatie voorhanden is dan in het bovenstaande geval (waar we de distributie onbekend veronderstelden), mag men verwachten dat de $1 - \alpha$ betrouwbaarheidsintervallen rond deze geschatte (of gemeten) waarden nauwer is dan zonder distributie-informatie. In het navolgende zullen we voor referentiedoeleinden een aantal van deze schatters en hun betrouwbaarheidsinterval geven.

Verreweg de belangrijkste parameter van een faaldistributie is de gemiddelde waarde (of mathematische verwachting) van de levensduur τ_g. We zullen dan ook voor verschillende bekende distributies een schatter voor τ_g geven met het bijbehorende betrouwbaarheidsinterval.
We gaan er van uit dat we beschikken over een monster n dat we volledig uittesten totdat alle n componenten gefaald hebben. De faaltijdstippen zijn t_i ($i = 1,2, \ldots ,n$).
Voor de normale distributie nemen we als schatter:

$$\hat{\tau}_g = \frac{1}{n} \sum_{i=1}^{n} t_i.$$

(Dit is een zogenaamde *unbiased maximum likelihood estimator*). Als van de normale distributie de spreiding σ bekend is, is het $1 - \alpha$ betrouwbaarheidsinterval rond deze schatter:

$$\hat{\tau}_g \pm N_{1-\alpha/2}\, \sigma/\sqrt{n}.$$

Hierin is $N_{1-\alpha/2}$ de bovenste $\frac{1}{2}\alpha$ percentiel van de standaard normale distributie N.
Als ook de spreiding σ geschat moet worden gebruiken we als schatter:

$$\hat{\sigma} = \sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (t_i - \hat{\tau}_g)^2}.$$

We krijgen dan als betrouwbaarheidsinterval:

$$\hat{\tau}_g \pm T_{1-\alpha/2,\, n-1}\, \hat{\sigma}/\sqrt{n}.$$

Hierin is $T_{1-\alpha/2,\, n-1}$ de bovenste $\frac{1}{2}\alpha$ percentiel van de T distributie van Student met $n - 1$ vrijheidsgraden. Deze distributie vindt men getabelleerd in de meeste statistische handboeken. Zij is genoemd naar de Engelse statisticus W.S. Gosset die publiceerde onder het pseudoniem Student.

Men kan de bovenstaande schatters en betrouwbaarheidsintervallen ook voor de lognormale distributie gebruiken als men zich realiseert dat met $g(t) = \ln t$ de lognormaal verdeelde variabele t overgaat in de normaal verdeelde variabele g(t). De schatter:

$$\hat{g} = \frac{1}{n} \sum_{i=1}^{n} \ln t_i$$

voor de gemiddelde waarde van de natuurlijke logaritme uit de faaltijd t_i heeft dan een $1 - \alpha$ betrouwbaarheidsinterval zoals in het bovenstaande is aangegeven voor $\hat{\tau}_g$. De schatter voor de spreiding van de resulterende normale verdeling is:

$$\sqrt{\frac{1}{n-1} \sum_{i=1}^{n} (\ln t_i - \hat{g})^2}.$$

De schatting voor de gemiddelde levensduur van een negatief exponentiële distributie is:

$$\hat{\tau}_g = \frac{1}{n} \sum_{i=1}^{n} t_i.$$

We kunnen het levensduurexperiment algemener maken door niet meer te veronderstellen dat alle n componenten falen maar slechts m ($m \leqslant n$, afgebroken test) en dat na het falen van een component deze door een nieuwe mag worden vervangen. We krijgen dan als schatter:

$$\hat{\tau}_g = \frac{T}{m}.$$

Hierin is T de totaal geaccumuleerde testtijd van alle componenten, dus de som van alle levensduren plus de som van de tijden die de nog niet gefaalde componenten onder de testomstandigheden hebben doorgebracht. De distributie van $\hat{\tau}_g$ is $\tau_g/2m$ keer de chi-kwadraat distributie met 2m vrijheidsgraden. Dus de grenzen:

$$2m\hat{\tau}_g/\chi^2_{\alpha/2,2m},\ 2m\hat{\tau}_g/\chi^2_{1-\alpha/2,2m}$$

bepalen dan het $1 - \alpha$ betrouwbaarheidsinterval voor $\hat{\tau}_g$.

Voor complexere distributies en voor afgebroken levensduurexperimenten kan men vaak geen analytische uitdrukking meer geven voor de betrouw-

baarheidsintervallen. Deze moeten dan door middel van Monte Carlo simulaties experimenteel bepaald worden.

4.2.3. Versnelde levensduurmetingen

De levensduur van de meeste elektronische componenten is zo hoog dat men geen levensduurexperimenten kan opzetten zonder gebruik te maken van een *verhoogde stress*. Daarmee haalt men meteen een arbitraire factor in huis, namelijk welke stress en hoe groot mag de versnelling zijn.
In het algemeen kan men stellen dat de aan te wenden stressgrootheden (zoals temperatuur, vochtigheid en trillingsniveau) de praktische operationele omgeving waaraan de component later wordt blootgesteld zo goed mogelijk moeten nabootsen. Dit houdt in dat zich tijdens het verhoogde stressexperiment geen faalmechanismen mogen voordoen die later in de praktijk niet voorkomen en omgekeerd dat er ook geen faalmechanismen door het experiment worden gemaskeerd die in de praktijk wel voorkomen. Verder moet het experiment zo gedaan worden dat men de versnellingsfactor behorende bij de verhoogde stress kent. Daar de versnellingsfactor voor verschillende stressgrootheden verschillend is en ook afhangt van het (dominante) faalmechanisme dat er door versneld wordt, ontwerpt men de versnelde levensduurexperimenten meestal met één stressgrootheid.
Voor wat de grootte van de versnellingsfactor betreft, hoe kleiner de versnellingsfactor (dus hoe dichter de stress tijdens het experiment ligt bij de stress onder operationele omstandigheden) hoe betrouwbaarder de uitkomsten van het experiment. De stressverhoging mag in geen geval zo groot zijn dat een ander dominant faalmechanisme op gang gebracht wordt.
Doorgaans bepaalt men het interval waarin de stress tijdens een versnelde levensduurmeting mag liggen uit een zogenaamde *step-stress test*. Dit is een experiment waarbij de stressgrootheid niet zoals bij het versnelde levensduurexperiment op een constante, verhoogde waarde wordt gehouden, maar waarbij het stressniveau in stappen wordt verhoogd. Deze verhoging gaat door tot een nieuw faalmechanisme actief wordt dat onder praktische omstandigheden niet interessant is (bijvoorbeeld het smelten of vervormen van een kunststof IC-behuizing door de hoge temperatuur).
Als men een keer het 'veilige gebied' van een stressgrootheid weet kan men op grond van fysische beschouwingen omtrent het faalmechanisme of uit een aantal versnelde levensduurproeven met verschillende stressniveaus de grootte van de versnellingsfactor als functie van de intensiteit van de stressgrootheid bepalen. De betrouwbaarste methode (maar ook de duurste en tijdrovendste) is beide te doen.
Bij een versnelde levensduurmeting (met een constant, verhoogd stress-

niveau) moet men er niet alleen op bedacht zijn dat de stress niet zo hoog wordt gekozen dat er een ander (dominant) faalmechanisme optreedt, maar bovendien moet men er (althans theoretisch) op bedacht zijn dat de vorm van de faaldistributie zich niet wijzigt bij hogere stressniveaus. Dan zou men immers de gemiddelde levensduur niet meer kunnen gebruiken als statistische parameter voor het karakteriseren van de faaldistributie. In het algemeen is aan deze eis voldaan als men het stressniveau tijdens de meting veel lager houdt dan dat waarbij andere faalmechanismen dominant worden.

In paragraaf 2.1 hebben we reeds een aantal levensduurbekortende stressors besproken die aan het model van Arrhenius voldeden. In principe komt voor versnellende stressfactor elke stress in aanmerking die het produkt ook in de latere operationele omgeving zal ondervinden: belasting, snelheid, grotere perioden tussen twee onderhoudsbeurten (doorsmeren), schokken, trillingen, elektrische ontlading (blikseminslag in voer-, vaar- en vliegtuigen) enzovoort.

Opgaven

4.1. Een faaldistributie van een passief redundant systeem bestaande uit twee eenheden met een constante failure rate λ wordt beschreven door een gammadistributie met een vormfactor c gelijk aan 2.
   a. Bepaal van dit systeem de failure rate z(t).
   b. Wat is de maximale failure rate van dit systeem en verklaar de gevonden waarde.

4.2. Bij een afgebroken levensduurexperiment test men gedurende 100 uur 100 vermogenstransistoren, die ingesteld zijn op twee maal de nominale vermogensdissipatie. Na deze 100 uur blijkt dat nog géén van de 100 transistoren gefaald is. Als we mogen aannemen dat de componenten een constante failure rate hebben, hoe groot is dan met een betrouwbaarheidsinterval van 90% deze failure rate?

4.3. Wat kunt u concluderen uit een afnemende hazard rate?

4.4. Bewijs dat voor de hazard rate van een component met een normaal verdeelde levensduur geldt:

$$\lim_{t \to \infty} z(t) = \infty.$$

4.5. Wat zijn versnelde levensduurexperimenten en onder welke condities leveren deze bruikbare resultaten op?

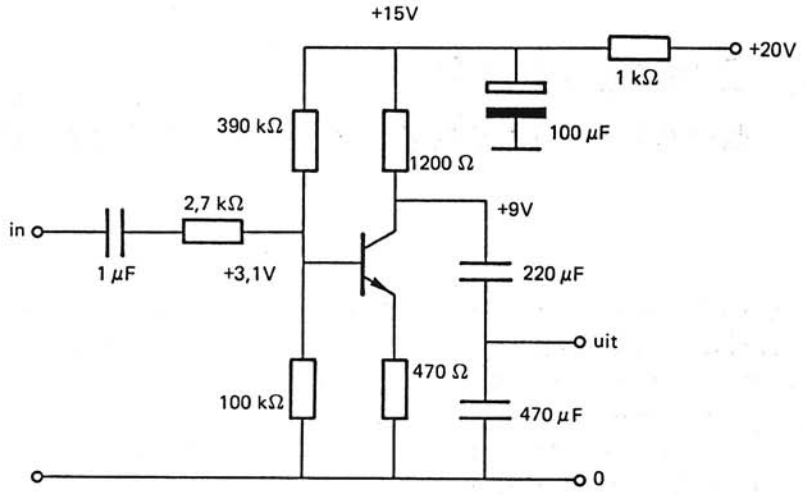
5. Statistische bedrijfszekerheidsmodellen

In dit hoofdstuk zullen we een aantal veel voorkomende bedrijfszekerheidsmodellen bespreken. Een bedrijfszekerheidsmodel wordt bepaald door het totaal van premissen (omtrent het falen van een systeemcomponent) waarvan wordt uitgegaan bij de berekening van de systeembedrijfszekerheid. Deze premissen vormen samen het model op grond waarvan men de bedrijfszekerheid bepaalt.
We hebben in paragraaf 3.1 reeds een aantal premissen genoemd. Dit was nodig, daar anders begrippen zoals R(t), F(t), f(t) en z(t) niet eenduidig vast lagen. De premissen zijn:

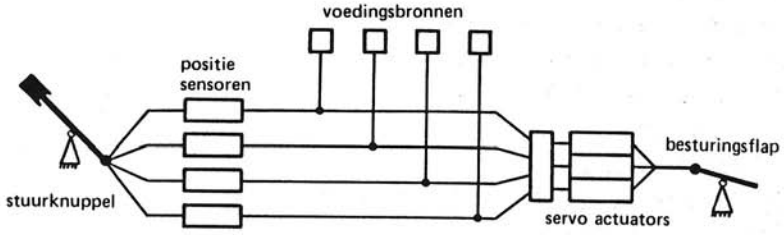
1. Een component is goed of defect; voor degeneratiefouten is de component defect vanaf de eerste keer dat hij de toleranties overschrijdt.
2. Eens defect blijft defect totdat er eventueel onderhoud wordt gepleegd; geen intermitterende fouten.
3. De levensduurvariabele is de tijd (zie paragraaf 1.1).

De bedrijfszekerheidsmodellen die wij in dit hoofdstuk zullen bespreken omvatten dan ook deze premissen naast andere, nog te noemen premissen.
N.B.: Men kan het ook zonder de bovenstaande aannamen stellen. De theorie wordt dan echter complex. Denk maar aan het weglaten van (2) wat tot gevolg heeft dat de R(t)-functie geen eenwaardige functie meer zal zijn. De bedrijfszekerheid zal immers weer stijgen als de kans dat de componenten weer gaan functioneren zal toenemen, dus als er gemiddeld over vele componenten weer meer gaan functioneren.

Naast deze bedrijfszekerheidsmodellen hebben we in de bedrijfszekerheidstechniek ook met andere modellen te maken. Voorbeelden daarvan zijn *schematische modellen* (bedradingsschema's en component lay-out tekeningen van elektronische systemen, werktekeningen van machines en dergelijke) en *functionele modellen*. Een schematisch model (of schema) bevat de hoogst zinvolle graad van detail met de individuele onderdelen, parameterwaarden en andere nuttige gegevens daarvan (zie figuur 5.1). Een functioneel model is in feite een tekening van de opbouw van een systeem uit subsystemen waarin duidelijk de informatie- en energiestromen binnen dat systeem tot uitdrukking komen (zie figuur 5.2).



Figuur 5.1. Voorbeeld van een schematisch model van een deel van een elektronisch circuit, doorgaans kortheidshalve aangeduid als 'schema'.

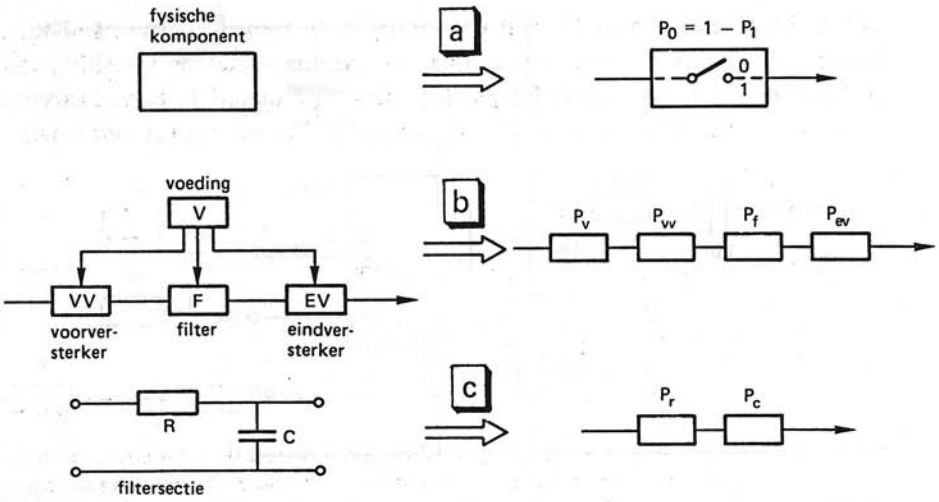


Figuur 5.2. Functioneel model van een 'fly-by-wire' systeem zoals in gebruik bij moderne vliegtuigen (viervoudig redundante voedingen, sensoren en bekabeling).

5.1. Catastrofaal faalmodel

Dit is het eenvoudigste faalmodel, waarbij men naast de eerder genoemde premissen nog aanneemt dat als een component faalt het er niet toe doet hoe de component faalt. Men neemt dus in feite aan dat de component slechts één faalwijze vertoont (*single-mode failure*). In dat geval wordt het representeren van fouten door middel van een model zeer eenvoudig. Zoals in figuur 5.3 is aangegeven, kan in dat geval de component (of het beschouwde deel van het systeem) worden vervangen door een 'black box' waarin men zich een schakelaar kan denken.

Als de component goed is, staat de schakelaar gesloten en definieert men de *toestand* van de component als "1". De toestand is "0" als de component defect is; de schakelaar staat dan open. Bij een combinatie van componenten moet er in het bijbehorende bedrijfszekerheidsmodel dus altijd nog minstens één pad door het model zijn waarlangs alle schakelaars ge-

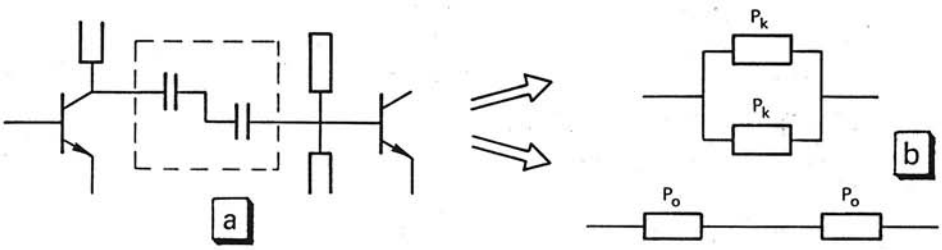


Figuur 5.3. Catastrofaal faalmodel. (a) De toestand van de component is 1 als deze goed is en 0 als deze defect is. (b) Het getoonde functionele model van een elektronisch systeem heeft een serieschakeling als bedrijfszekerheidsmodel. (c) Het getoonde RC-lid functioneert niet meer als de weerstand open of kortgesloten is (kans P_r) of als de condensator open of kortgesloten is (kans P_c).

sloten zijn, wil er nog sprake zijn van een correct functioneren. Vergelijk de figuren 5.3b en 5.3c. De toestand van een systeem wordt dus bepaald door de toestand van de samenstellende componenten. Men kan dan ook een *waarheidstabel* opstellen met een toestand van de componenten als (binaire) ingangsvariabelen en de toestand van het systeem als binaire uitgangsvariabele. De structuur van het bedrijfszekerheidsmodel bepaalt de relatie tussen deze variabelen, die met de Booleaanse algebra kan worden beschreven. Hierop berust een bepaalde berekeningsmethode voor de bedrijfszekerheid van systemen, waarop we in hoofdstuk 6 terug zullen komen.

Om de beperkingen van het catastrofale faalmodel aan te geven nemen we figuur 5.3 c als uitgangspunt. Voor het daarin geschetste RC-lid zal, wil het als filter goed functioneren, een bepaalde nominale waarde voor R en C gespecificeerd zijn met een toelaatbare tolerantie daarop. We nemen aan dat de weerstand de fout 'open' vertoont als hij de tolerantie aan de bovengrens overschrijdt, en de fout 'kortsluiting' vertoont als hij de tolerantie naar beneden toe overschrijdt. Vervolgens nemen we aan dat beide faalwijzen voor wat de bedrijfszekerhied betreft niet onderscheiden behoeven te worden en voegen we ze samen in de term 'foute component' met foutkans P_R. Voor de condensator handelen we evenzo.

Dit is niet altijd geoorloofd, wat eenvoudig in te zien is aan de hand van figuur 5.4. De twee versterkertrappen dienen voor (met de instelling van de transistoren gepaard gaande) gelijkspanning geïsoleerd te zijn. Daarvoor wordt een scheidingscondensator toegepast die dubbel is uitgevoerd. Dit



Figuur 5.4. (a) Redundante scheidingscondensatoren tussen twee punten met een verschillend DC-niveau. (b) Faalmodel voor alleen kortsluitingen resp. alleen open fouten. P_k is de kans op kortsluiting in een condensator, P_o de kans op een open condensator.

maakt dat één van de condensatoren een doorslag van het diëlektricum mag vertonen zonder dat de werking van de schakeling wordt beïnvloed. Beschouwt men alleen deze faalwijze dan bestaat het bedrijfszekerheidsmodel uit twee parallelle takken elk met een foutkans P_k. Beschouwt men alleen de faalwijze 'open condensator' dan bestaat het bedrijfszekerheidsmodel uit twee serietakken, beide met foutkans P_o.

N.B.: Een serie- c.q. parallelschakeling van componenten in een schematisch of functioneel model behoeft dus niet ook tot een serie- c.q. parallelschakeling in het bedrijfszekerheidsmodel te leiden.

In werkelijkheid komen beide faalwijzen voor. Zulke componenten met meerdere onderscheidbare faalwijzen (*multi-mode failures*) kan men niet met het catastrofale faalmodel beschrijven. Het lijkt voor de hand te liggen dit toch te doen door de beide bedrijfszekerheidsmodellen uit figuur 5.4 b in serie te plaatsen. Dit is evenwel geen goede representatie van de werkelijkheid omdat de fouten die de verschillende blokken nu weergeven stochastisch afhankelijk zijn (een kortsluiting in een condensator sluit een open fout uit). De eenvoud van de hier gegeven modellering voor componenten met één faalwijze gaat dan verloren. In dat geval moet men, door een inventarisatie van alle combinaties van toelaatbare fouten en de kans daarop, komen tot de bedrijfszekerheid van het totaal. Hiervan zullen we nu een voorbeeld behandelen.

Voorbeeld 5.1

Een diode heeft naast het goed functioneren (toestand x) twee faalwijzen. namelijk open (toestand x_o) en kortgesloten (toestand x_k). We nemen aan

dat deze toestanden elkaar wederzijds uitsluiten (disjunct zijn), in formule:

$$P(x \cup x_o \cup x_k) = P(x) + P(x_o) + P(x_k) = 1.$$

De bedrijfszekerheid van een diode is dan

$$R = P(x) = 1 - P(x_o \cup x_k) = 1 - P(x_o) - P(x_k).$$

Schakelen we twee dioden in serie, dan zal de combinatie falen als één of beide dioden open is of beide kortgesloten zijn. Dit treedt op voor

$$x_1x_{2o} + x_{1o}x_2 + x_{1o}x_{2k} + x_{1o}x_{2o} + x_{1k}x_{2o} + x_{1k}x_{2k}$$

(Gemakshalve is hier het symbool $\cup$ vervangen door een rekenkundig somteken en het symbool $\cap$ weggelaten, zodat een produkt ontstaat). Elk van deze combinaties leidt tot een scheiden van de ingang en uitgang in het bijbehorende (multi-mode) bedrijfszekerheidsmodel. Elke combinatie is een *snede*. De volledige verzameling van alle sneden vormt de *snedenverzameling* (*cut set*). In termen van deze snedenverzameling is de bedrijfszekerheid van de twee dioden in serie:

$$R = 1 - P(x_1x_{2o} + x_{1o}x_2 + x_{1o}x_{2k} + x_{1o}x_{2o} + x_{1k}x_{2o} + x_{1k}x_{2k}).$$

De verzameling (*set*) van alle goede toestandscombinaties, de zogenaamde *padenverzameling* (*tie set*), is:

$$x_1x_2 + x_1x_{2k} + x_2x_{1k}.$$

In termen van deze padenverzameling is de bedrijfszekerheid van de twee dioden in serie dus

$$R = P(x_1x_2 + x_1x_{2k} + x_2x_{1k}).$$

Als de fouten in beide dioden stochastisch onafhankelijk zijn en we aannemen dat $P(x) = p$ en $P(x_o) = q_o$ dan is $P(x_k) = 1 - p - q_o = q_k$ en geldt verder:

$$R = p^2 + 2pq_k.$$

Voor het geval men de twee dioden parallel schakelt is de kortste uitdrukking te verkrijgen door de padenverzameling op te stellen:

$$x_1x_2 + x_1x_{2o} + x_{1o}x_2.$$

De bedrijfszekerheid is dan met bovenstaande veronderstellingen:

$$R = P(x_1x_2 + x_1x_{2o} + x_{1o}x_2) = p^2 + 2pq_o.$$

N.B.: De termen snede, pad en verzameling zijn ontleend aan de grafentheorie. Men kan de bedrijfszekerheidsmodellen van de figuren 5.3 en 5.4 namelijk ook weergeven als graaf. Hierop komen we in paragraaf 6.9.2 terug.

N.B.: De termen "disjuncte" en "stochastisch onafhankelijke" gebeurtenissen moet men goed uit elkaar houden. Twee gebeurtenissen zijn disjunct als ze elkaar uitsluiten en dus niet gelijktijdig kunnen optreden. Een voorbeeld vormen elektrische componenten met twee aansluitdraden die intern niet gelijktijdig open en kortgesloten kunnen zijn. (Dit is niet het geval voor componenten met drie of meer aansluitdraden zoals transistors, IC's en dergelijke!) Voor zulke disjuncte gebeurtenissen geldt dat de kans op het voorkomen van de vereniging gelijk is aan de som van de kansen op elk der gebeurtenissen afzonderlijk:

$$P(x_o \cup x_k) = P(x_o) + P(x_k).$$

Dit kan men eenvoudig inzien daar algemeen geldt (zonder aannamen over disjunctie)

$$P(x_o \cup x_k) = P(x_o) + P(x_k) - P(x_o \cap x_k)$$

Voor disjuncte gebeurtenissen is de doorsnede $x_o \cap x_k$ leeg en dus $P(x_o \cap x_k) = 0$.

Twee gebeurtenissen zijn in stochastische zin onafhankelijk als het optreden (of het niet optreden) van de ene gebeurtenis de kans op het optreden (of niet optreden) van de andere gebeurtenis niet beïnvloedt. Zo'n beïnvloeding bestaat wel als bijvoorbeeld de fouten in componenten een gemeenschappelijke oorzaak hebben. Vergelijk het ontstaan van condensatievocht in de ontvanger van een vliegtuig dat opstijgt in de tropen (van warm en vochtig naar de koude van grotere hoogten). Als bovendien nog chemische verontreiniging aanwezig is zal dit (elektro-)chemische corrosie van componenten veroorzaken. Een andere vorm van afhankelijke fouten ontstaat doordat de ene fout de andere tot gevolg heeft of het ontstaan daarvan versnelt. Vergelijk het te warm worden van een defecte component (kogellager) wat tot gevolg heeft dat een elektrische isolatie smelt waardoor kortsluiting ontstaat.

Voor onafhankelijke gebeurtenissen geldt dat de kans op de doorsnede van de beide gebeurtenissen gelijk is aan het produkt van de kansen op de individuele gebeurtenissen:

$$P(x_1 \cap x_2) = P(x_1)P(x_2).$$

Daar algemeen geldt:

$$P(x_1 \cap x_2) = P(x_1 \mid x_2)\,P(x_2)$$

en

$$P(x_1 \cap x_2) = P(x_2 \cap x_1),$$

is het eenvoudig in te zien dat ook de volgende vergelijking geldt:

$$P(x_1 \cap x_2) = P(x_2 \mid x_1)\,P(x_1).$$

Indien de gebeurtenissen x_1 en x_2 onafhankelijk zijn is de conditionele kans $P(x_2 \mid x_1)$ gelijk aan de kans $P(x_2)$. Evenzo geldt $P(x_1 \mid x_2) = P(x_1)$. Derhalve geldt voor onafhankelijke kansen:

$$P(x_1 \cap x_2) = P(x_1)\,P(x_2).$$

5.2. Belasting-sterkte model

Bij het belasting-sterkte model (Engels: stress-strength model) nemen we aan dat een component slechts faalt als de grootte van de *belasting* x groter wordt dan de *sterkte* y. De belasting of stress x kan een mechanische, elektrische, maar bijvoorbeeld ook een thermische belasting zijn. Zoals we in hoofdstuk 2 gezien hebben bestaat de belasting uit de som van de *inwendige belasting* van de component die ontstaat door het gebruik en de *uitwendige belasting* die opgelegd wordt door de omgeving waarin de component wordt gebruikt.
We nemen aan dat de belasting een stochastische variabele is. De bedrijfszekerheid van een component is dan:

$$R = P(\underline{x} \leqslant y) = 1 - P(\underline{x} > y).$$

Als de kansdichtheidsfunctie van de belasting $\underline{x}$ bekend is en gegeven wordt door g(x), dan wordt de bedrijfszekerheid:

$$R = \int_{-\infty}^{y} g(x)\,dx = 1 - \int_{y}^{\infty} g(x)\,dx.$$

Het gearceerde deel van g(x) in figuur 5.5a geeft dus het faalgebied aan. Het zal duidelijk zijn dat de sterkte y, dus de "weerstand" van een component tegen stukgaan, van component tot component varieert; ook $\underline{y}$ heeft een kansdichtheidsfunctie f(y). Daar

$$f(y) = \lim_{\Delta y \to 0} \frac{F(y + \Delta y) - F(y)}{\Delta y},$$

? $P(y < \underline{y} < y+dy) \cap P(\underline{x} \leq y)$

waarin

$$F(y) = P(\underline{y} \leqslant y),$$

kunnen we dus schrijven voor de kans dat $\underline{y}$ in het interval $(y, y + dy]$ ligt:

$$P(y < \underline{y} \leqslant y + dy) = f(y)\,dy.$$

We nemen verder aan dat de belasting $\underline{x}$ en de sterkte $\underline{y}$ stochastisch onafhankelijk zijn. De kans dat de sterkte $\underline{y}$ in het interval $(y, y + dy]$ ligt en tegelijkertijd de belasting $\underline{x}$ de sterkte niet overschrijdt is dan

$$f(y)\,dy \int_{-\infty}^{y} g(x)\,d(x).$$

De bedrijfszekerheid van de beschouwde component is de kans dat de belasting $\underline{x}$ de sterkte $\underline{y}$ niet overschrijdt voor alle mogelijke waarden die $\underline{y}$ kan aannemen, dus

$$R = \int_{-\infty}^{\infty} f(y)\,[\int_{-\infty}^{y} g(x)\,dx]\,dy.$$

Als men het probleem anders stelt, namelijk de bedrijfszekerheid als de kans dat de sterkte $\underline{y}$ niet kleiner is dan de belasting $\underline{x}$ voor alle waarden die $\underline{x}$ kan aannemen, dan vindt men:

$$R = \int_{-\infty}^{\infty} g(x)\,[\int_{x}^{\infty} f(y)\,dy]\,dx.$$

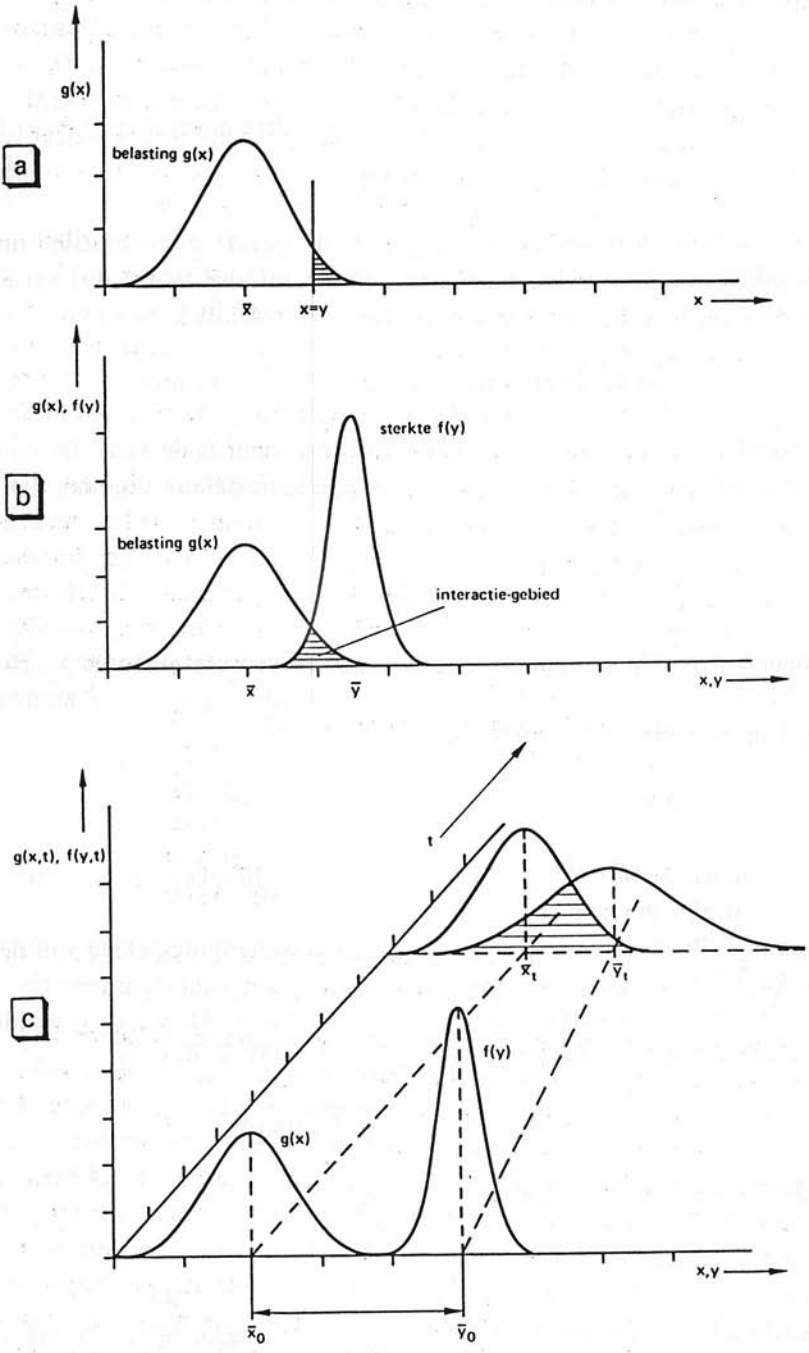
Ga dit zelf na. Beide uitdrukkingen voor de bedrijfszekerheid van een component zijn dus identiek.
In figuur 5.5b is deze situatie geschetst; het overlappingsgebied van de beide kansdichtsheidsfuncties geeft het interval aan waar de interactie tussen sterkte en belasting aanleiding geeft tot falen. Als we de gemiddelde waarde van $\underline{x}$ en $\underline{y}$ aangeven als $\overline{x}$ respectievelijk $\overline{y}$, dus als

$$\overline{x} = \int_{-\infty}^{\infty} x\,g(x)\,dx \quad \text{en} \quad \overline{y} = \int_{-\infty}^{\infty} y\,f(y)\,dy,$$

dan definieert men als *veiligheidsfactor*:

$$\eta = \frac{\overline{y}}{\overline{x}}.$$

Deze factor geeft dus aan in hoeverre de sterkte uitgaat boven de belasting. Daar deze factor betrekking heeft op gemiddelden bevat zij niet de informatie omtrent de verdeling van $\underline{x}$ en $\underline{y}$ die nodig is voor de bepaling van de bedrijfszekerheid R. Zo zal bij een bepaalde veiligheidsfactor η de



Figuur 5.5. Belastingskansdichtheid g(x) en sterktekansdichtheid f(y) als functie van de belasting x, de sterkte y en de tijd t.

bedrijfszekerheid R afnemen naarmate de spreidingen σ_x en σ_y van $\underline{x}$ respectievelijk $\underline{y}$ groter zijn. Men moet voor een hoge bedrijfszekerheid dus streven naar een grote veiligheidsfactor en gelijktijdig een lage spreiding.
Een lage spreiding van de sterktedistributie van een component krijgt men door een goede *kwaliteitsbewaking* tijdens het produktieproces. Daardoor kunnen de stochastische fluctuaties in het produktieproces die de oorzaak zijn van sterktevariaties zo klein mogelijk worden gehouden.
Een lage spreiding van de belasting moet verkregen worden door het goed vastleggen van de omgeving waarin een component moet werken. Vergelijk het trillingsniveau, het temperatuurgebied en het vochtigheidsgebied van componenten die in een vliegtuig gebruikt worden maar eens met de omgeving waaraan componenten in bijvoorbeeld een telefooncentrale worden blootgesteld. Door isolatie en andere conditionering kan men veelal deze belasting reduceren en/of de spreiding daarin kleiner maken.
Uit het bovenstaande blijkt wel dat dezelfde componenten in een andere omgeving meer of eerder kunnen falen. De mate waarin dit het geval is wordt wel tot uitdrukking gebracht in een *omgevingsfactor* (*environmental factor*). Dit is een globale maat voor de factor waarmee de failure rate in die omgeving hoger is dan in een standaardomgeving. Enige waarden voor deze omgevingsafhankelijke failure rate multiplicatie-factoren zijn:

standaardomgeving (laboratorium)	1
vaste opstelling	5-10
schepen	10-25
treinen	25-50
vliegtuigen	100-200
raketten	500-1500

Zulke omgevingsfactoren kunnen uiteraard niet meer zijn dan een globale indicatie voor de "vijandigheid" van het desbetreffende milieu.

Een andere manier om een hogere bedrijfszekerheid te realiseren is de veiligheidsfactor η groter te maken. Daartoe moet men de gemiddelde sterkte $\overline{y}$ van een component veel groter maken dan de gemiddelde belasting $\overline{x}$. Om dit te bereiken *overdimensioneert* men de componenten ($\overline{y}$ verhogen) door andere, sterkere subcomponenten te kiezen, of men verlaagt de belasting $\overline{x}$ van de componenten. Dit laatste duidt men aan als (stress-) *derating*. Dit kan men bijvoorbeeld doen door de belasting over meerdere componenten te verdelen. Vergelijk het verdelen van het gedissipeerde vermogen in een uitgangstrap over meerdere parallelle transistoren, waardoor de junctietemperatuur lager blijft en daarmee ook de failure rate. Andere voorbeelden zijn: de doorslagspanning van diodes en condensatoren, de

maximale wielbelasting van voertuigen en het landingsgewicht van vliegtuigen. Derating en overdimensionering geven aanleiding tot een factor (*derating factor*) waardoor de failure rate moet worden gedeeld. Deze factor werkt dus omgekeerd aan de omgevingsfactor.

Voorbeeld 5.2

Als men aanneemt dat de fluctuaties in belasting en sterkte ontstaan door een groot aantal, stochastisch onafhankelijke oorzaken, zullen $\underline{x}$ en $\underline{y}$ normaal verdeeld en onafhankelijk zijn. We kunnen dan met voordeel het verschil $\underline{z} = \underline{y} - \underline{x}$ als nieuwe stochastische variabele invoeren. Ook deze is dan normaal verdeeld, immers de som en het verschil van onafhankelijke, normaal verdeelde stochastische variabelen is weer normaal verdeeld. De gemiddelde waarde van $\underline{z}$ is $\overline{y} - \overline{x}$ en de spreiding van $\underline{z}$ is $\sigma_z = \sqrt{\sigma_x^2 + \sigma_y^2}$, zodat de kansdichtheidsfunctie h(z) van $\underline{z}$ is:

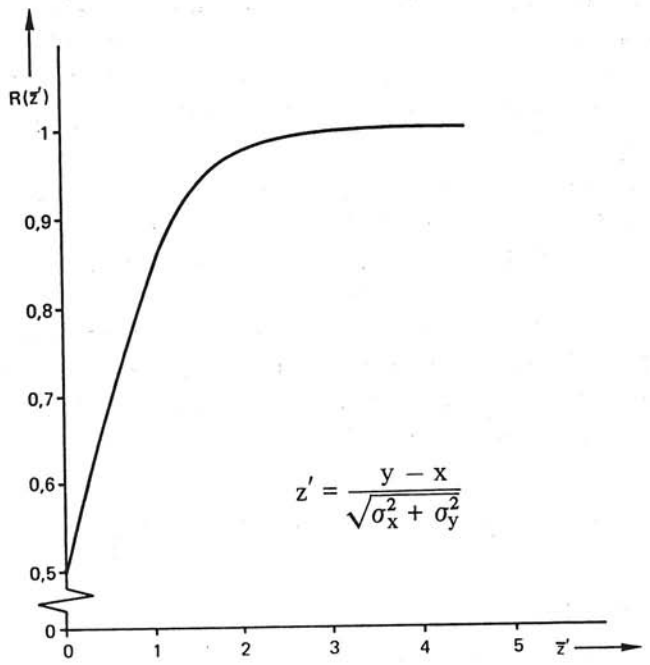
$$h(z) = \frac{1}{\sqrt{2\pi(\sigma_x^2 + \sigma_y^2)}} \exp\left(-\frac{(z + \overline{x} - \overline{y})^2}{2(\sigma_x^2 + \sigma_y^2)}\right).$$

De bedrijfszekerheid wordt dan:

$$R = P(\underline{z} \geqslant 0) = 1 - P(\underline{z} < 0) = \int_0^\infty h(z)\,dz.$$

In figuur 5.6 is deze bedrijfszekerheid voor een genormeerde waarde $\underline{z}'$ van z uiteengezet.

Zoals in figuur 5.5c is geschetst, zal de verdeling van de belasting $\underline{x}$ en de sterkte $\underline{y}$ afhangen van de tijd. Dit maakt dat de berekende bedrijfszekerheid ook een functie van de tijd wordt. Dit zal met name geschieden doordat de sterktedichtheidsfunctie f(y) met het verlopen van de tijd niet alleen een lagere gemiddelde sterkte $\overline{y}$ vertoont maar ook een grotere spreiding σ_y. Dit wordt teweeg gebracht door allerlei verouderingsprocessen die in de component plaats vinden (zoals vermoeidheidsverschijnselen).
We zien ook uit figuur 5.5c dat voor t = 0 de veiligheidsfactor η en de spreidingen σ_x en σ_y zodanig zijn dat er ook dan reeds een overlappend interactiegebied is, dat tot de zogenaamde "early failures" aanleiding geeft. In deze kinderziekte-periode sneuvelen dus de zwakste componenten door (relatief weinig voorkomende) pieken in de belasting. De elkaar overlappende staartjes van de beide verdelingen geven in het begin, direct na t = 0, dus de "Frühausfall".
De tijdafhankelijkheid van de sterkte en de belasting zullen we hier niet bespreken. Volstaan zij met de opmerking dat men deze tijdafhankelijkheid meestal sterk vereenvoudigd modelleert. In de praktijk doet men dat vaak door deze tijdafhankelijkheid op te meten bij een vaste waarde van



Figuur 5.6. De bedrijfszekerheid van een komponent met normaal verdeelde sterkte y en belasting x, als functie van het genormeerde verschil $\bar{z}'$ tussen sterkte en belasting.

de belasting meestal in de vorm van de hazard rate. Vervolgens brengt men dan een correctiefactor aan voor de invloed van de belasting. Dit laat zich eenvoudig als volgt toelichten.
Stel dat de belasting gevormd wordt door de temperatuur. Stel verder dat de hazard rate bij een bepaalde temperatuur T_0 is opgemeten: $z(t, T_0)$ is dus bekend. Verder nemen we nog aan dat de foutversnellende werking van de temperatuur is aan te geven in een *versnellingsfactor* $\beta(T)$ die aan de relatie van Arrhenius in paragraaf 2.1 wordt ontleend:

$$\frac{z(t,T)}{z(t,T_0)} = \exp\left(-\frac{E_A}{nk}\left(\frac{1}{T} - \frac{1}{T_0}\right)\right) = \beta(T).$$

N.B.: Daar het hier hazard rates in plaats van faaltijden betreft is het rechterlid de inverse van dat uit de overeenkomstige uitdrukking in paragraaf 2.1.

De hazard rate bij temperatuur T wordt dan voor $t \leqslant t_0$ (kinderziektegebied):

$$z(t,T) = \beta(T)\, z(t,T_0),$$

en voor $t > t_0$ (gebruiksgebied):

$$z(t,T) = \beta(T)\, z(t_0, T_0).$$

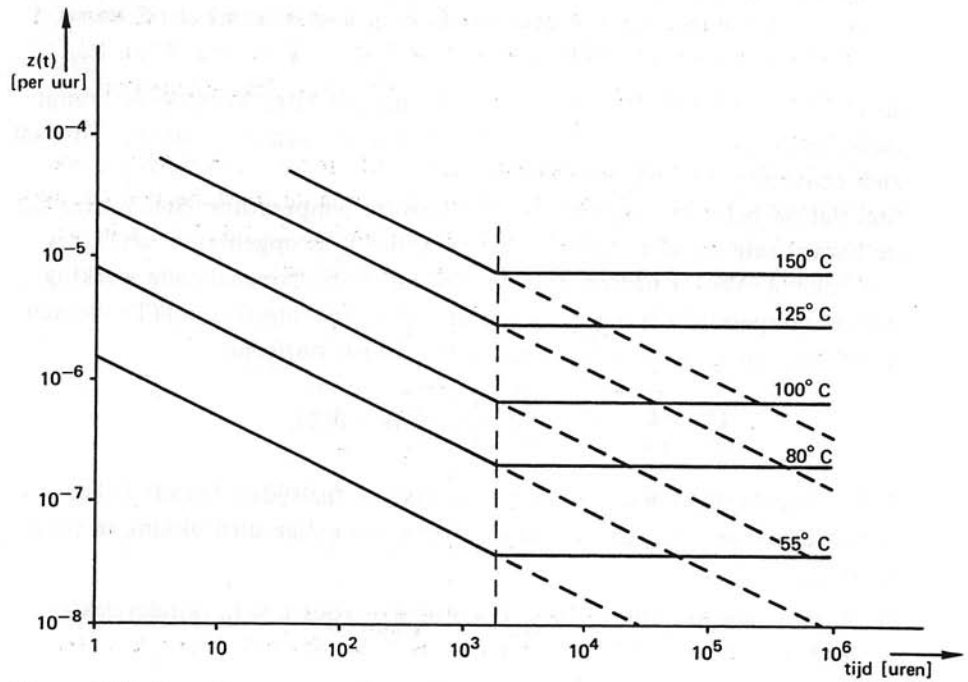
Het een en ander wordt toegelicht voor analoge IC's in voorbeeld 5.3.

Voorbeeld 5.3

De hazard rate als functie van de tijd voor analoge IC's blijkt goed te benaderen met de Weibulldistributie. Bij T_0 en $t \leqslant t_0$ geldt:

$$z(t,T_0) = \lambda c t^{c-1}.$$

Bij $T_0 = 373$ K blijkt uit metingen dat $c = 0{,}5$ en $\lambda^2 = 4{,}5 \cdot 10^{-9}$ per uur. De versnellingsfactor $\beta(T)$ tengevolge van een verhoogde temperatuur is gelijk aan de boven gegeven uitdrukking. Met de navolgende gegevens, effectieve activeringsenergie $E_A/n = 0{,}7$ eV (1 eV = $1{,}6 \cdot 10^{-19}$ J), $t_0 = 2000$ uur, constante van Boltzmann $k = 1{,}38 \cdot 10^{-23}$ J/K, geeft dit het beeld zoals in figuur 5.7 is geschetst. Uit dit voorbeeld is duidelijk het effect te zien dat "derating" geeft. Als men zo'n analoog IC gebruikt bij een lagere omgevingstemperatuur en/of minder vermogen dissipeert in het IC, daalt de hazard rate aanzienlijk en zal de bedrijfszekerheid dus hoger komen te liggen.



Figuur 5.7. Hazard rate van analoge IC's versus tijd en temperatuur (omgevingstemperatuur plus inwendige temperatuurverhoging door dissipatie).

5.3. Markovmodel

In Markovmodellen spelen fundamenteel twee stochastisch variabelen een rol, de toestand $\underline{S}$ van het beschouwde systeem en de tijd $\underline{t}$. Al naar gelang $\underline{S}$ en $\underline{t}$ discreet dan wel continu verdeeld zijn, kan men vier verschillende Markovmodellen onderscheiden. Het eenvoudigste is het zogenaamde *Markovketen-model.* Dit is een model dat discreet in de tijd zowel als in de toestand is (Engels: discrete-time, discrete-state model). Deze discretisatie kan in de aard van het beschouwde stochastische gebeuren liggen (men denke bijvoorbeeld aan catastrofale fouten), maar ook ontstaan door het gekwantiseerd bemonsteren van een continu verdeeld stochastisch proces (bijvoorbeeld degeneratiefouten).
Voor de bedrijfszekerheidstechniek is van de hierboven bedoelde vier combinaties van het meeste belang de combinatie van continue tijd $\underline{t}$ en discrete toestand $\underline{S}$. Dit continue tijd, discrete toestand model wordt aangeduid als een *Markovproces.*

Bij elk Markovmodel zijn een aantal veronderstellingen gemaakt:

- *Toestand.* De toestand $\underline{S}$ van het systeem is een element uit de volledige verzameling van alle discrete, elkaar wederzijds uitsluitende toestanden waarin het systeem door alle fysisch mogelijke faalwijzen terecht kan komen. Als het bedrijfszekerheidsmodel van het systeem uit meerdere elementen (componenten) bestaat, is de toestand van het systeem een gerangschikte rij van toestanden van deze elementen.

  Voorbeeld 5.4

  Als we aannemen dat de vier elementen uit figuur 5.3b slechts twee toestanden kennen (goed = 1, fout = 0), dan is de toestand van het systeem een rij van vier binaire elementtoestanden. In tabel 5.1 zijn de toestanden S_i gegeven in een willekeurige volgorde.

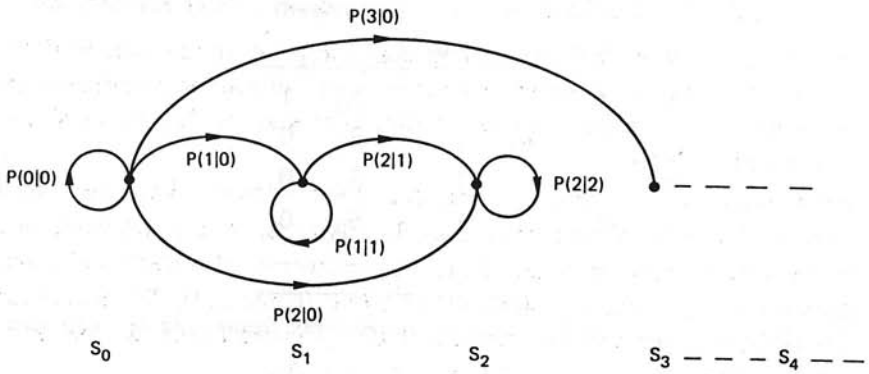
elementen				systeem	
V	VV	F	EV		
1	1	1	1	S_0	1
0	1	1	1	S_1	0
0	0	1	1	S_2	0
1	0	1	1	S_3	0
–	–	–	–	–	–

Tabel 5.1. Toestanden S_i waarin het systeem van figuur 5.3b kan verkeren.

Daar het hier een seriesysteem betreft functioneert het systeem alleen

in de toestand S_0 en zijn alle overige toestanden systeemfouten. Let wel: de elementen behoeven hier niet noodzakelijkerwijze slechts twee toestanden te hebben; meer toestanden zijn ook geoorloofd, ze maken alleen de inventarisatie van alle mogelijke systeemtoestanden S_i complexer.

- *Overgangskansen*. Een Markovmodel wordt mede bepaald door de overgangskansen (*transition probabilities*) tussen de toestanden (*states*) van het model. Het is overigens niet noodzakelijk dat alle overgangen een van nul verschillende overgangskans hebben. In het bovenstaande voorbeeld zijn voor een niet-onderhouden systeem de overgangskansen van S_i ($i \neq 0$) naar S_0 alle identiek nul. Een belangrijke eigenschap van een Markovmodel is dat de overgangskans p_{ij} van de toestand S_i naar de toestand S_j alleen van S_i en S_j afhangt en niet van eerder door het systeem doorlopen toestanden. Indien deze overgangskans wel zou afhangen van een (eindig) aantal toestanden dat in het verleden is doorlopen, kan men nieuwe toestanden S_i' en S_j' invoeren waarvoor de bovenstaande eigenschap weer geldt. Deze eigenschap maakt dat p_{ij} te schrijven is als een conditionele kans P(j|i), de kans dat het systeem naar S_j overgaat als het daarvoor in S_i was. Zo hangt in het gegeven voorbeeld de kans p_{01} alleen af van S_0 en S_1 en is gelijk aan de kans op het stuk gaan van het voedingsapparaat V onder de conditie dat de overige elementen heel blijven. De overgang van S_1 naar S_2 hangt alleen van deze twee toestanden af; p_{12} is de kans dat de voorversterker VV stuk gaat onder de conditie dat de voeding al stuk is en de overige elementen blijven werken. De overgang van S_0 naar S_2 is de kans dat V en VV beide stuk gaan onder de conditie dat F en EV blijven werken, enzovoort. Ga zelf na wat de overgang van S_2 naar S_3 inhoudt.
In figuur 5.8 is voor de eerste vier toestanden het één en ander weergegeven.



Figuur 5.8. Toestandsmodel (gedeeltelijk) voor het systeem van figuur 5.3b.

- *Tijdcontinuïteit.* In het bovenstaande speelde het element tijd nog geen rol. We beschouwden het systeem statisch; dat wil zeggen het moment van een toestandswijziging (in casu stukgaan) was niet in de beschouwingen betrokken. We kunnen dit voor de bedrijfszekerheidstechniek zo belangrijke tijdelement invoeren door de (in werkelijkheid tijdcontinue) toestand van het systeem te bemonsteren in de tijd met intervallen Δt. We maken na iedere Δt als het ware een momentopname van het systeem en registreren in welke toestand het zich op dat tijdstip bevindt; dus welke elementen nog functioneren en welke gefaald hebben.
  De conditionele overgangskansen $p_{ij} = P(j|i)$ uit het bovenstaande gaan dan over in conditionele overgangskansdichtheden. Dit is als volgt in te zien. De overgangskans van toestand S_i naar toestand S_j in het tijdelementje $(t, t+\Delta t]$ is met het overgangstijdstip (faaltijdstip) $\underline{t}$ als continue stochastische variabele:

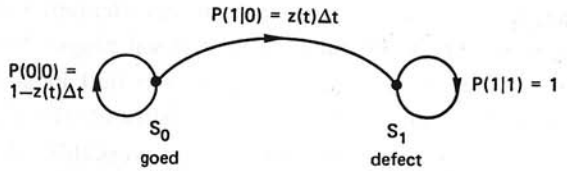
$$p_{ij}(t, t+\Delta t) = P(t < \underline{t} \leqslant t+\Delta t \,|\, \underline{t} > t) = \frac{P(t < \underline{t} \leqslant t+\Delta t)}{P(\underline{t} > t)}.$$

  In de termen van falen, faaldistributie en bedrijfszekerheid wordt dit:

$$p_{ij}(t, t+\Delta t) = \frac{f(t)}{R(t)}\Delta t = z(t)\Delta t.$$

  In het tijdcontinue geval is de hazard rate $z(t)$ klaarblijkelijk gelijk aan het tempo waarmee de overgangen in de tijd gezien plaatsvinden: $z(t)$ kan men dan ook aanduiden als een conditionele faalkans*dichtheid* (zie paragraaf 3.2.1).
  Indien in een Markovmodel deze overgangstempi (*transition rates*) niet afhankelijk zijn van de tijd (dus als men te doen heeft met failure rates), dan spreekt men van een (tijd-) *homogeen* Markovmodel. Als er tijdafhankelijkheid in het spel is, dan is het model *inhomogeen*.

We zullen nu laten zien hoe men op eenvoudige wijze met een Markovmodel kan rekenen. Daarvoor nemen we een wel zeer eenvoudig systeem, namelijk een component die niet gerepareerd kan worden en die slechts één faalwijze heeft.
Eerst stellen we alle mogelijke disjuncte toestanden op. Voor deze component zijn dat er slechts twee, namelijk S_0 en S_1, waarin de component respectievelijk goed en defect is. In feite bezien we dus slechts één overgang uit een (complexer) Markovmodel (zie figuur 5.9). We nemen aan dat de hazard rate van de component $z(t)$ is en we bezien de toestand van de component op de tijdstippen t en $t + \Delta t$.



Figuur 5.9. Toestandsmodel van een enkele component die slechts catastrofaal kan falen.

De kans dat de component op het tijdstip $t + \Delta t$ in de toestand S_0 is zullen we aangeven als $P_{S_0}(t + \Delta t)$. Deze kans is gelijk aan de kans dat de component op t in S_0 is $(P_{S_0}(t))$ maal de kans dat er in het interval Δt geen fouten optreden $(1 - z(t)\Delta t)$ vermeerderd met de kans dat de component op t in S_1 is maal de kans dat deze in Δt gerepareerd wordt. We hebben een niet-repareerbare component dus we vergeten het laatste en vinden:

$$P_{S_0}(t+\Delta t) = [1 - z(t)\Delta t]P_{S_0}(t) + 0 \cdot P_{S_1}(t).$$

Evenzo kunnen we afleiden voor de kans dat de component in S_1 is op $t+\Delta t$:

$$P_{S_1}(t+\Delta t) = [z(t)\Delta t]P_{S_0}(t) + 1 \cdot P_{S_1}(t).$$

We hebben bij deze dus gebruik gemaakt van de wetenschap dat S_0 en S_1 *alle* toestanden waren waarin de component kon verkeren en dat deze toestanden *disjunct* zijn.

Hierbij is aangenomen dat er geen meervoudige gebeurtenissen in Δt *plaatsvinden (bijvoorbeeld door een intermitterende fout); de kans op meer dan één overgang in* Δt *is een infinitesimaal van hogere graad en zal dus na de limietovergang voor* $\Delta t \to 0$ *(die nodig is om naar het tijdcontinue geval te gaan) nul worden.*

De beide bovenstaande vergelijkingen kunnen we als volgt herschrijven:

$$\frac{P_{S_0}(t+\Delta t) - P_{S_0}(t)}{\Delta t} + z(t)P_{S_0}(t) = 0,$$

en

$$\frac{P_{S_1}(t+\Delta t) - P_{S_1}(t)}{\Delta t} - z(t)P_{S_0}(t) = 0.$$

Deze differentievergelijkingen moeten we, om te geraken tot het tijdcontinue geval, doen overgaan in differentiaalvergelijkingen door de limiet te nemen voor $\Delta t \to 0$. We krijgen dan:

$$\frac{dP_{S_0}(t)}{dt} + z(t)P_{S_0}(t) = 0$$

en

$$\frac{dP_{S_1}(t)}{dt} - z(t)P_{S_0}(t) = 0.$$

De oplossing van dit stelsel differentiaalvergelijkingen kan geschieden door scheiding van variabelen:

$$\frac{dP_{S_0}(t)}{P_{S_0}(t)} = -z(t)\,dt, \quad \text{dus} \quad \ln P_{S_0}(t) = -\int_0^t z(t)\,dt + C.$$

Met de beginvoorwaarde $P_{S_0}(0) = \alpha$ $(0 \leqslant \alpha \leqslant 1)$ levert dit de welbekende uitdrukking (zie paragraaf 3.2.1):

$$R(t) = P_{S_0}(t) = \alpha \exp\left[-\int_0^t z(t)\,dt\right].$$

Op soortgelijke wijze vindt men voor $P_{S_1}(t)$:

$$P_{S_1}(t) = 1 - \alpha \exp\left[-\int_0^t z(t)\,dt\right].$$

Daartoe behoeft men niet de differentiaalvergelijkingen te hanteren, daar

$$P_{S_0}(t) + P_{S_1}(t) = 1.$$

Zoals we al wisten wordt de oplossing zeer eenvoudig voor $z(t) = \lambda$.

N.B.: De bovenstaande uitdrukkingen zijn algemener dan die uit paragraaf 3.2.1, daar zij niet aannemen dat $R(0) = 1$ maar $R(0) = \alpha$. Kennelijk laat het Markovmodel een van 1 afwijkende $R(0)$ toe. Ook laat het voor de componenten van een systeem meerdere, onderscheidbare faalwijzen toe (Engels: multi-mode failures). De introductie van reparatie levert ook geen problemen bij dit model. Men kan er ook afhankelijke fouten mee modelleren en berekenen. Tenslotte geeft de methode voor een constante $z(t)$, dus voor constante overgangstempi, zeer eenvoudig rekenwerk.

Voor ingewikkelder Markovmodellen met drie of meer toestanden bestaat veelal slechts een analytische oplossing indien het bijbehorende stelsel differentiaalvergelijkingen alleen constante coëfficiënten bevat. Dit is het geval als alle overgangstempi tijdonafhankelijk zijn (dus voor constante failure en repair rates). In dat geval is de eenvoudigste oplossing de Laplacetransformatie te hulp te roepen om de differentiaalvergelijkingen (voor een Markovmodel met n toestanden zijn dat er n) met constante coëfficiënten om te zitten in n lineaire vergelijkingen met n onbekenden.

We kunnen de differentievergelijkingen ook rechtstreeks uit het toestandsmodel opstellen. Als we het toestandsmodel van figuur 5.9 nog eens nader bezien, zien we dat een overgang door een tak wordt aangegeven met een bijbehorende overgangskans. Deze kans zullen we beschouwen als de "overdracht" van de desbetreffende tak. De toestanden S_i worden gerepresenteerd door knooppunten. In elk knooppunt denken we ons een signaalbron met een sterkte $P_{S_i}(t)$. We kunnen dan het volgende stellen:

- De som van de overgangskansen van alle takken die een knooppunt verlaten is één; het systeem moet immers altijd overgaan in één der toestanden S_i $(i = 0, 1, \ldots, n)$.
- De kans dat het systeem op het tijdstip $t+\Delta t$ in de toestand S_i is, kan rechtstreeks uit het toestandsmodel worden opgemaakt. Zij is namelijk gelijk aan de som van alle inkomende 'signalen' op het knooppunt behorende bij S_i. Alle knooppunten zien we daarbij als 'signaalbronnen' die een sterkte hebben gelijk aan de kans dat het systeem op het tijdstip t in de bij dat knooppunt behorende toestand verkeert. Een inkomend signaal is dan gelijk aan de sterkte van zo'n knooppuntsbron maal de overdracht van de tak tussen dit knooppunt en dat behorende bij S_i.

Ook de differentiaalvergelijkingen kunnen we rechtstreeks uit het toestandsmodel opstellen. Er geldt namelijk dat de afgeleide naar de tijd van de kans dat het systeem in een bepaalde toestand S_i verkeert, gelijk is aan de som van de signalen van de op het knooppunt behorende bij S_i binnenkomende takken verminderd met de som van de signalen van de het knooppunt verlatende takken.
In formulevorm wordt dit:

$$\frac{dP_{S_i}(t)}{dt} = \sum_{k=0}^{n} P_{S_k}(t)\, z_{ki}(t) - \sum_{k=0}^{n} P_{S_i}(t)\, z_{ik}(t) =$$

$$= \sum_{k=0}^{n} P_{S_k}(t)\, z_{ki}(t) - P_{S_i}(t) \sum_{k=0}^{n} z_{ik}(t) \qquad (i = 0,1,\ldots,n)$$

Het signaal van die takken die terugkeren in hetzelfde knooppunt, dat dus weergeeft de mogelijkheid dat het systeem gedurende het infinitesimale kleine tijdinterval dt in dezelfde toestand blijft, is:

$$P_{S_i}(t)\, z_{ii}(t).$$

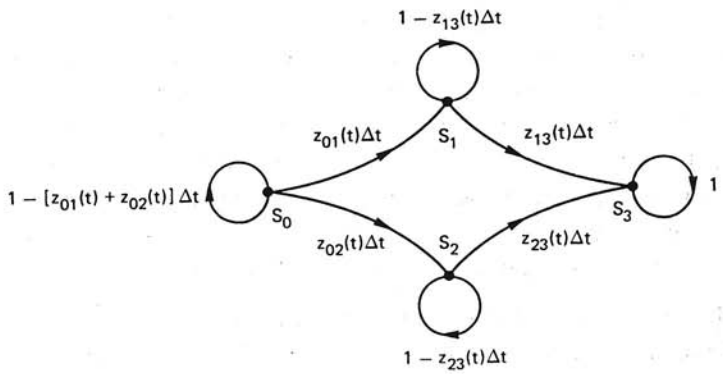
Deze bijdragen worden zowel bij de binnenkomende takken als bij de uitgaande takken meegeteld en leveren derhalve geen bijdrage in de differentiaalvergelijkingen. We moeten dus bij het opstellen van de differentiaalvergelijkingen deze bijdragen of consequent in rekening brengen of consequent

weglaten. Dit laatste is gebeurd in de onderstaande vergelijking:

$$\frac{dP_{S_i}(t)}{dt} = \sum_{\substack{k=0 \\ k\neq i}}^{n} P_{S_k}(t)\, z_{ki}(t) - P_{S_i}(t) \sum_{\substack{k=0 \\ k\neq i}}^{n} z_{ik}(t) \qquad (i = 0,1,\ldots,n)$$

Voorbeeld 5.5

We willen tenslotte eindigen met een voorbeeld dat veel meer omvattend is als dat van figuur 5.9. We hebben in figuur 5.10 het Markovmodel gegeven. Het systeem bestaat uit twee componenten A en B. Het doet er bij



Figuur 5.10. Toestandsmodel voor een systeem bestaande uit twee elementen. Zie tabel 5.2 voor de toestandsidentificatie.

de berekening (althans voorlopig) niet toe of deze componenten in serie of parallel staan of dat de tweede component wordt gebruikt om de eerste te repareren. We nemen aan dat A en B slechts goed of fout kunnen zijn. Zoals aangegeven is in tabel 5.2 kan het systeem dan slechts in één van de vier toestanden S_i verkeren. Probeer nu zelf eens de differentiaalvergelijkingen uit het Markov toestandsmodel op te stellen. U zult dan vinden:

$$\frac{dP_{S_0}(t)}{dt} = -[z_{01}(t) + z_{02}(t)]P_{S_0}(t),$$

$$\frac{dP_{S_1}(t)}{dt} = z_{01}(t)P_{S_0}(t) - z_{13}(t)P_{S_1}(t),$$

$$\frac{dP_{S_2}(t)}{dt} = z_{02}(t)P_{S_0}(t) - z_{23}(t)P_{S_2}(t),$$

$$\frac{dP_{S_3}(t)}{dt} = z_{13}(t)P_{S_1}(t) + z_{23}(t)P_{S_2}(t).$$

A	B	S
1	1	S_0
0	1	S_1
1	0	S_2
0	0	S_3

Tabel 5.2. Toestanden S_i waarin het systeem met twee componenten A en B kan verkeren. We hebben nog niet aangegeven in welke van de vier toestanden het systeem goed of fout is.

Deze differentiaalvergelijkingen zijn niet op te lossen voor een algemene hazard rate z(t). Als we eenvoudigheidshalve stellen:

- $z_{01}(t) = \lambda_1$, $z_{02}(t) = \lambda_2$, $z_{13}(t) = \lambda_3$, $z_{23}(t) = \lambda_4$ en
- beginvoorwaarden: $P_{S_0}(0) = 1$, $P_{S_1}(0) = P_{S_2}(0) = P_{S_3}(0) = 0$,

dan is de oplossing:

$$P_{S_0}(t) = e^{-(\lambda_1 + \lambda_2)t},$$

$$P_{S_1}(t) = \frac{\lambda_1}{\lambda_1 + \lambda_2 - \lambda_3}\,[e^{-\lambda_3 t} - e^{-(\lambda_1 + \lambda_2)t}],$$

$$P_{S_2}(t) = \frac{\lambda_2}{\lambda_1 + \lambda_2 - \lambda_4}\,[e^{-\lambda_4 t} - e^{-(\lambda_1 + \lambda_2)t}],$$

$$P_{S_3}(t) = 1 - \sum_{i=0}^{2} P_{S_i}(t).$$

Nu moeten we de configuratie van de twee componenten A en B in het systeem invoeren:

a) Laten we aannemen dat we met twee componenten in serie te doen hebhebben. Geen van beide mag falen dus:

$$R(t) \equiv P_{S_0}(t) = e^{-(\lambda_1 + \lambda_2)t}.$$

b) We nemen aan dat we met twee componenten parallel hebben te doen. Het systeem functioneert zolang niet meer dan één component defect is, dus:

$$R(t) \equiv P_{S_0}(t) + P_{S_1}(t) + P_{S_2}(t) = 1 - P_{S_3}(t).$$

c) Stel dat we te doen hebben met een parallelsysteem van twee gelijke componenten die samen de belasting delen en daardoor een lage failure rate λ_0 bezitten. Als er één stuk gaat, krijgt de andere component de volle belasting en heeft daardoor een hogere failure rate λ_h. Met bovenstaande uitdrukking en de substitutie $\lambda_0 = \lambda_1 = \lambda_2$ en $\lambda_h = \lambda_3 = \lambda_4$ krijgen

we dan de volgende uitdrukking voor de bedrijfszekerheid van dat systeem:

$$R(t) = \frac{2\lambda_0 e^{-\lambda_h t} - \lambda_h e^{-2\lambda_0 t}}{2\lambda_0 - \lambda_h}.$$

Ga na waar dit systeem toe leidt voor $\lambda_0 = \lambda_h = \lambda$.

d) De eerstgegeven algemene uitdrukking voor de bedrijfszekerheid van een parallelsysteem kan ook als volgt geïnterpreteerd worden. Een komponent staat ingeschakeld met failure rate λ_1. De tweede component is niet geactiveerd en heeft in deze toestand een failure rate nul; dus $\lambda_2 = 0$ (althans $\lambda_2 \ll \lambda_1$). Wordt de tweede component geactiveerd dan heeft deze de failure rate λ_3. We vinden dan:

$$R(t) = \frac{\lambda_1}{\lambda_1 - \lambda_3} e^{-\lambda_3 t} - \frac{\lambda_3}{\lambda_1 - \lambda_3} e^{-\lambda_1 t}.$$

N.B.: $P_{S_2} = 0$ voor elke t daar $P_{S_2}(0) = 0$ en $\lambda_2 = 0$. Dus de waarde van λ_4 doet er niet toe. Daar in de praktijk bij twee identieke componenten geldt $\lambda_1 \approx \lambda_3$, vinden we door teller en noemer van bovenstaande uitdrukking naar λ_3 te differentiëren en de regel van De l'Hôpital toe te passen:

$$R(t) = e^{-\lambda t} + \lambda t e^{-\lambda t};$$

rechtstreeks substitueren leidt immers tot een onbepaalde uitdrukking.

Naarmate het aantal toestanden en de overgangen daartussen toeneemt wordt het oplossen van het bijbehorende stelsel differentiaalvergelijkingen steeds complexer. Voor systemen met vier of meer toestanden verdient het aanbeveling daarom een oplosmethode te gebruiken waarbij men het overzicht niet snel verliest en de kans op rekenfouten klein wordt gehouden. Voor een Markovmodel met n + 1 toestanden kan het volgende stelsel differentiaalvergelijkingen worden opgesteld:

$$\frac{dP_{S_0}(t)}{dt} + \lambda_{u_0} P_{S_0}(t) - \lambda_{10} P_{S_1}(t) - \lambda_{20} P_{S_2}(t) - \ldots - \lambda_{n0} P_{S_n}(t) = 0$$

$$\frac{dP_{S_1}(t)}{dt} - \lambda_{01} P_{S_0}(t) + \lambda_{u_1} P_{S_1}(t) - \lambda_{21} P_{S_2}(t) - \ldots - \lambda_{n1} P_{S_n}(t) = 0$$

$$\vdots \qquad\qquad \vdots$$

$$\frac{dP_{S_n}(t)}{dt} - \lambda_{0n} P_{S_0}(t) - \lambda_{1n} P_{S_1}(t) - \lambda_{2n} P_{S_2}(t) - \ldots + \lambda_{u_n} P_{S_n}(t) = 0$$

Hierin vormt λ_{u_i} de som van de failure rates behorende bij alle takken

die knooppunt S_i verlaten. In matrixnotatie krijgen we de volgende vergelijking:

$$\begin{bmatrix} \frac{dP_{S_0}(t)}{dt} \\ \frac{dP_{S_1}(t)}{dt} \\ \vdots \\ \frac{dP_{S_n}(t)}{dt} \end{bmatrix} + \begin{bmatrix} +\lambda_{u_0} - \lambda_{10} - \lambda_{20} \ldots - \lambda_{n0} \\ -\lambda_{01} + \lambda_{u_1} - \lambda_{21} \ldots - \lambda_{n1} \\ \vdots \\ -\lambda_{0n} - \lambda_{1n} - \lambda_{2n} \ldots + \lambda_{u_n} \end{bmatrix} \cdot \begin{bmatrix} P_{S_0}(t) \\ P_{S_1}(t) \\ \vdots \\ P_{S_n}(t) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \text{ of}$$

$$\left[\frac{dP_{S_i}(t)}{dt}\right] + U \cdot \left[P_{S_i}(t)\right] = \left[0\right],$$

waarbij U de overgangsmatrix wordt genoemd.
Na de Laplace-transformatie van alle tijdfuncties krijgen we de volgende vergelijking:

$$s \cdot \left[P_{S_i}(s)\right] - \left[P_{S_i}(0)\right] + U \cdot \left[P_{S_i}(s)\right] = \left[0\right].$$

Hierin is s de Laplace-variabele. Door het overbrengen van de vector met de beginvoorwaarden $P_{S_i}(0)$ naar de rechterkant van de vergelijking krijgen we:

$$\left[s \cdot I + U\right] \cdot \left[P_{S_i}(s)\right] = A \cdot \left[P_{S_i}(s)\right] = \left[P_{S_i}(0)\right].$$

De matrix A ziet er dan als volgt uit:

$$A = \begin{bmatrix} s + \lambda_{u_0} & -\lambda_{10} & -\lambda_{20} \ldots & -\lambda_{n0} \\ -\lambda_{01} & s + \lambda_{u_1} & -\lambda_{21} \ldots & -\lambda_{n1} \\ \vdots & & & \vdots \\ -\lambda_{0n} & -\lambda_{1n} & -\lambda_{2n} \ldots & s + \lambda_{u_n} \end{bmatrix}.$$

Daar geldt:

$$A^{-1}A\left[P_{S_i}(s)\right] = A^{-1}\left[P_{S_i}(0)\right],$$

geldt ook:

$$\left[P_{S_i}(s)\right] = A^{-1}\left[P_{S_i}(0)\right].$$

Daar we veelal voor de beginvoorwaarden mogen aannemen dat:

$$P_{S_0}(0) = 1 \text{ en } P_{S_i}(0) = 0 \qquad (i = 1, 2, \ldots, n),$$

is alleen de eerste kolom van de inverse matrix A^{-1} van belang. De elementen a_{ij} van deze matrix kunnen dan gevonden worden met:

$$a_{ij} = \frac{(\text{cofactor})_{ij}}{|A|}.$$

Voorbeeld 5.6
Eenvoudig is na te gaan voor het Markov-toestandsmodel van figuur 5.10 dat dit aanleiding geeft tot de navolgende matrix A:

$$A = \begin{bmatrix} s+\lambda_{01}+\lambda_{02} & 0 & 0 & 0 \\ -\lambda_{01} & s+\lambda_{13} & 0 & 0 \\ -\lambda_{02} & 0 & s+\lambda_{23} & 0 \\ 0 & -\lambda_{13} & -\lambda_{23} & s \end{bmatrix}.$$

Hierin zijn λ_{ij} de failure rates behorende bij overgangen i naar j.
Als A een keer bekend is kan $P_{S_i}(s)$ worden uitgeschreven en teruggetransformeerd om $P_{S_i}(t)$ te krijgen.

Samenvattend kunnen we stellen:
Het Markovmodel is goed toepasbaar voor systemen met een eindig aantal toestanden, met tijdonafhankelijke faalprocessen die een constante failure rate en repair rate vertonen. Dit leidt tot de beperking dat de faaldistributies van de elementen van het systeem negatief-exponentieel moeten zijn, of een faaldistributie moeten hebben die ontstaat bij een serie/parallel-combinatie van zulke elementen (dan kan immers gewerkt worden met dummy toestanden).

We zullen in paragraaf 6.9.4. Markovmodellen gebruiken om de bedrijfszekerheid van complexe systemen te berekenen. Ook bij de evaluatie van onderhoudbare systemen zullen we dit model veel gebruiken.

Opgaven

5.1. Om kortsluitfouten en openfouten tegen te gaan zou men voor een diodewerking vier dioden kunnen gebruiken: twee takken met elk twee dioden in serie, parallel aan elkaar geschakeld. Bij welke q_o en q_k is het

nuttig al dan niet een verbinding te maken tussen de middens van de beide paralleltakken?

5.2. Kunnen twee disjuncte gebeurtenissen die ieder een van nul verschillende kans van optreden hebben, onafhankelijk zijn?

5.3. Gegeven is de navolgende uniforme distributie:

$$f(t) = \frac{1}{L} \qquad \text{voor } 0 \leqslant t < L \text{ en } f(t) = 0 \text{ voor } t \geqslant L.$$

Bepaal R(t), F(t) en z(t).

5.4. Het weer-radarsysteem van een passagiersvliegtuig heeft een MTTF van 1140 uur. Neem aan dat de failure rate constant is en beantwoord de volgende vragen:

a. Wat is de kans op falen gedurende een vlucht van 4 uur?

b. Wat is de maximale duur van een vlucht waarbij de bedrijfszekerheid niet onder 0,99 komt? (Gedurende de vlucht is het systeem continu in werking.)

5.5. Gegeven is van een systeem een faalkansdichtheidsfunctie van de vorm:

$$f(t) = at\, e^{-\frac{1}{2}at^2}$$

a. Bepaal R(t) en z(t) van dit systeem.

Op tijdstip t = 0 heeft men 5000 goed functionerende systemen, ieder met bovenstaande faalkansdichtheidsfunctie. Van deze 5000 blijken er na 10 uur nog 4700 correct te functioneren.

b. Wat is ongeveer het aantal te verwachten fouten in het tijdsinterval van 10 tot 20 uur?

5.6. Geef aan wat verstaan wordt onder de veiligheidsfactor η aan de hand van een schets van een belastingskansdichtheid g(x) en een sterktekansdichtheid f(y). (In één figuur!)

5.7. In een ziekenhuis bevindt zich altijd een voorziening die de elektrische-energielevering overneemt zodra het openbare net uitvalt. Stel de failure rate van het net is λ_n en die van de noodstroomgenerator λ_{g_1} in de toestand buiten gebruik, terwijl de noodstroomgenerator tijdens gebruik een failure rate λ_{g_2} heeft. Stel een Markov-diagram op voor het gehele stroomvoorzieningensysteem, waarbij reparatie buiten beschouwing moet worden gelaten.

6. Niet-onderhouden systemen

Wij zullen onderscheid maken tussen *onderhoudbare systemen* en *onderhouden systemen.* Het laatste begrip is beperkter dan het eerste: een auto is een onderhoudbaar systeem, of het ook een onderhouden systeem is hangt van de eigenaar af. Uit bedrijfszekerheidsoogpunt wint men weinig als men een systeem onderhoudbaar maakt (dus toegankelijk voor onderhoud) en de gebruiker laat bijvoorbeeld uit misplaatste zuinigheid onderhoud achterwege. Zo'n systeem is qua bedrijfszekerheid dan een niet-onderhouden systeem.

6.1. Inleiding

Een *niet-onderhouden systeem* is of een niet-onderhoudbaar systeem òf een onderhoudbaar maar niet onderhouden systeem. Voorbeelden van niet-onderhoudbare systemen zijn goedkope systemen waarbij onderhoud niet economisch verantwoord is (zakrekenmachine, enzovoort), systemen waarbij onderhoud niet mogelijk is (aardsatelliet en dergelijke) of systemen die slechts eenmalig gebruikt worden (bijvoorbeeld een vaste brandstofraket). Een *onderhouden systeem* moet èn onderhoudbaar zijn èn onderhouden worden.

Een *onderhoudbaar systeem*, zo hebben we reeds in paragraaf 3.2 gezien, is een systeem dat nadat het gefaald heeft weer door *menselijk ingrijpen* kan worden teruggebracht in een *werkende toestand.* Menselijk ingrijpen is essentieel in deze definitie; een systeem dat 'zichzelf onderhoudt' door het inschakelen van een ingebouwd redundant subsysteem is daarom nog niet onderhoudbaar. Men maakt dit onderscheid omdat het menselijk ingrijpen slechts effect heeft na een zekere vertragingstijd: de onderhoudstijd. Hieronder vallen: waarschuwingstijd van de onderhoudsman, opsporingstijd van de fout, besteltijd van de nodige componenten en gereedschappen. Bovendien is deze tijd afhankelijk van de ervaring en opleiding van de onderhoudsman en van de componenten en gereedschappen die men lokaal op voorraad heeft. Al met al laat zich deze vertraging slechts beschrijven met behulp van een stochastisch proces: de onderhoudstijd-distributie. Bovendien blijkt dat menselijk ingrijpen niet altijd 100% effectief is. Na onderhoud is het systeem niet *'als nieuw'*; het is slechts teruggebracht in

een '*werkende toestand*'. Dit vindt haar oorzaak in zaken als beschadigingen elders in een systeem veroorzaakt door slordige reparatie, het gebruik van verkeerde componenten of gereedschappen die niet voor dat doel gemaakt zijn, onjuiste reparatieprocedures (bouten met verkeerd moment vastgezet, enzovoort). Ook deze effecten kunnen slechts met stochastische methoden in rekening worden gebracht.

Men kan ook beide doen: extern menselijk onderhoud van een systeem dat is uitgerust met intern, zichzelf inschakelende redundantie. Een uit bedrijfszekerheidsoogpunt zeer machtige combinatie is *preventief onderhoud* van zo'n *redundant systeem.* Het onderhoud vervangt de gefaalde redundante subsystemen door nieuwe *voordat* het systeem door uitputting van de redundantie heeft gefaald. Vaak is dit zelfs mogelijk zonder het systeem buiten bedrijf te stellen. We komen hier in paragraaf 7.3.4 nader op terug.

We nemen in dit hoofdstuk gemakshalve een tweetal dingen aan:
- de systeemcomponenten hebben een *constante failure rate*;
- de systeemcomponenten falen *stochastisch onafhankelijk.*

Wat het eerste betreft: de componenten hebben dus geen levensduurgeheugen, als ze nog werken zijn ze als nieuw. Deze aanname is niet noodzakelijk, zij vergemakkelijkt slechts het rekenwerk.
Wat het tweede betreft: de fouten in verschillende componenten mogen bijvoorbeeld geen gemeenschappelijke oorzaak hebben (Engels: *common-cause failures*) die gelijktijdig falen veroorzaakt of de kans op het ontstaan van fouten in andere componenten vergroot. Dit houdt bijvoorbeeld in dat we secundaire fouten (*secondary failures*) uitsluiten. Dit zijn fouten die ontstaan tengevolge van een eerder opgetreden fout (primary failure) of waarvan het ontstaan waarschijnlijker wordt door een primaire fout. Als deze secundaire fout niet optreedt in dezelfde komponent als de primaire fout maar bijvoorbeeld in een redundante component, dan heeft men te maken met een oneigenlijke redundantie die veel sneller uitvalt dan men in eerste instantie zou verwachten.
N.B.: In de praktijk zijn met name common-cause failures daarom zeer gevreesd. Men moet bij de modellering van het systeem deze foutmogelijkheden daarom terdege in de gaten houden en in het model betrekken. We zullen dit type fouten in paragraaf 6.4.1 nader bespreken.

Een voorbeeld van een common-cause failure is een aardbeving waardoor in een kernreactor op meerdere plaatsen fouten kunnen ontstaan en, wat erger is, als één unit door deze oorzaak faalt zullen met een hoge mate van waarschijnlijkheid ook identieke, redundante units falen. Om dit te vermijden voert men redundantie vaak niet-identiek uit en tracht men de redundantie op verschillende lokaties te plaatsen.

We zullen nu nader ingaan op de invloed van de *structuur van een systeem* op de bedrijfszekerheid.

6.2. Seriesystemen

Onder een *seriesysteem* verstaan we in de bedrijfszekerheidstechniek een systeem waarvan het bedrijfszekerheidsmodel een *serie- of kettingstructuur* heeft. Dit houdt in dat *alle* componenten van het systeem goed moeten werken om het systeem goed te kunnen laten functioneren; het defect raken van één willekeurig element beëindigt het leven van het systeem. Daar we hebben aangenomen dat defecten in componenten onafhankelijk van elkaar optreden, geldt dus voor de bedrijfszekerheid R(t) van zo'n seriesysteem met n componenten:

$$R(t) = \prod_{i=1}^{n} R_i(t),$$

als $R_i(t)$ de bedrijfszekerheid van de i-de component is.
Uit de bovenstaande produktregel, die geldt onafhankelijk van de faaldistributies van de systeemcomponenten, ziet men eenvoudig dat de bedrijfszekerheid daalt naarmate er meer componenten aan een seriesysteem worden toegevoegd; des te groter de (numerieke) complexiteit, des te lager de bedrijfszekerheid. Verder blijkt de bedrijfszekerheid van een seriesysteem lager te zijn dan die van de zwakste component:

$$R(t) < \min_i \{R_i(t)\}, \qquad (i = 1,2,\ldots,n).$$

De bovenstaande uitdrukking geeft een eenvoudige doch grove bovengrens voor de bedrijfszekerheid.

N.B.: Zoals we in figuur 5.4 hebben geïllustreerd, heeft het voorvoegsel 'serie' hier *niet* te maken met de fysische opbouw van het systeem. Zo staat bijvoorbeeld bij het autorijden 's nachts, hoe vreemd het ook moge klinken, de verlichting in serie met de besturing, de aandrijving, de remmen en andere noodzakelijke functies van de auto.

Met behulp van

$$R(t) = R(0) \exp\left[-\int_0^t z(t)\,dt\right]$$

uit paragraaf 3.2.1 is een eenvoudige somregel te geven voor de hazard rate z(t) van een seriesysteem:

$$z(t) = \sum_{i=1}^{n} z_i(t),$$

waarin $z_i(t)$ de hazard rate van de i-de component is.

Voor een negatief-exponentiële faaldistributie worden de uitdrukkingen wel zeer eenvoudig. Nemen we aan dat $z_i(t) = \lambda_i$, dan geldt voor een seriesysteem met n onafhankelijk falende componenten:

$$R_i(t) = e^{-\lambda_i t},$$

$$z(t) \equiv \lambda = \sum_{i=1}^{n} \lambda_i,$$

dus

$$R(t) = e^{-\lambda t} = \exp\left[-\left(\sum_{i=1}^{n} \lambda_i\right)t\right].$$

De faaldistributie van een seriestructuur van componenten met negatief-exponentiële faaldistributies is dus zelf ook weer negatief-exponentieel. De gemiddelde levensduur van een seriesysteem is dan ook:

$$\theta = \frac{1}{\lambda} = \frac{1}{\sum_{i=1}^{n} \lambda_i}.$$

We zien hieruit dat de zwakste component, relatief gezien, de grootste verkorting van de levensduur geeft.

Op het bovenstaande berust een eenvoudige doch primitieve methode voor het afschatten van de bedrijfszekerheid van een systeem. Men neemt eenvoudig aan dat alle componenten nodig zijn voor de goede werking van het systeem, ook al is het geen zuiver seriesysteem; men telt dan de failure rates van alle componenten op om tot de failure rate van het geheel te geraken.

Voorbeeld 6.1

Voor een milieu (trein) met een bekende versnellingsfactor (35) gelden voor een bepaalde elektronische (filter-)schakeling bestaande uit komponenten op een printed-circuit board de failure rates zoals gegeven in tabel 6.1. De gemiddelde levensduur is dus 380 jaar, dat wil zeggen na 380 jaar zou 63 % van het aantal circuits zijn uitgevallen. Als voor een bepaalde kritische toepassing, zoals de automatische treinbeveiliging, wordt geëist dat de bedrijfszekerheid hoogstens mag dalen tot 0,999, dan is de bijbehorende tijd echter slechts 139 dagen. De toepassing van redundantie is voor zulke systemen dus essentieel.

Opmerkingen

- De bovenstaande methode geeft een ondergrens van de bedrijfszekerheid van het systeem (dus een pessimistische schatting) als het geen zuiver seriesysteem betreft, en er ook sommige componenten mogen falen zonder dat deze het systeem doen uitvallen.

Aantal	Component	Failure rate		Sub-totaal
10	metaalfilmweerstand	$2 \cdot 10^{-9}$/u	=	$20 \cdot 10^{-9}$/u
4	tantaalcondensator	$10 \cdot 10^{-9}$/u	=	$40 \cdot 10^{-9}$/u
5	low-power transistor	$5 \cdot 10^{-9}$/u	=	$25 \cdot 10^{-9}$/u
1	elektrolytische condensator	$100 \cdot 10^{-9}$/u	=	$100 \cdot 10^{-9}$/u
2	analoog IC	$45 \cdot 10^{-9}$/u	=	$90 \cdot 10^{-9}$/u
2	digitaal IC	$7 \cdot 10^{-9}$/u	=	$14 \cdot 10^{-9}$/u
75	soldeerverbinding	$0{,}1 \cdot 10^{-9}$/u	=	$7{,}5 \cdot 10^{-9}$/u
20	printspoor	$0{,}01 \cdot 10^{-9}$/u	=	$0{,}2 \cdot 10^{-9}$/u
		λ_{totaal}	$\approx$	$300 \cdot 10^{-9}$/u

Tabel 6.1. *Failure rates van de componenten van een bepaalde elektronische schakeling. Als de componenten onafhankelijk falen en alle nodig zijn voor de goede werking kunnen de failure rates worden opgeteld om tot de failure rate van de schakeling te geraken.*

- Ook als er afhankelijke fouten optreden is de bovengegeven schatting aan de sombere kant.
- In het voorbeeld is de elektrolytische condensator verantwoordelijk voor $\frac{1}{3}$ van de totale failure rate. Als door een herontwerp (redesign) deze condensator vermeden kan worden, scheelt dit aanzienlijk. Zo dienen voorontwerpen (predesigns) altijd gevolgd te worden door bedrijfszekerheidsberekeningen en herontwerpen om iteratief tot een zo goed mogelijk ontwerp te komen.
- We kunnen als volgt zien dat preventief onderhoud aan seriesystemen met componenten die negatief-exponentieel falen geen zin heeft. Preventief onderhoud kan immers alleen geschieden zolang het systeem nog niet gefaald heeft. Dit is bij een seriesysteem alleen het geval als geen der komponenten gefaald heeft. Het preventief vervangen van komponenten met een negatief-exponentiële faaldistributie heeft echter geen zin, zoals we in paragraaf 4.1.1 reeds gezien hebben; nog functionerende componenten zijn "als nieuw".
- Als een component van een systeem buiten gebruik een andere failure rate (λ_o) heeft dan wanneer het systeem aanstaat (λ_a), kan men door een *duty cycle* d in te voeren komen tot een effectieve failure rate:

$$\lambda_{eff} = (1 - d)\lambda_o + d\lambda_a,$$

waarin:

$$d = \frac{\Sigma t_{ai}}{\Sigma t_{ai} + \Sigma t_{oi}},$$

waarin Σt_{ai} de geaccumuleerde gebruikstijd is en Σt_{oi} de geaccumuleerde wachttijd is.

6.3. Redundantie

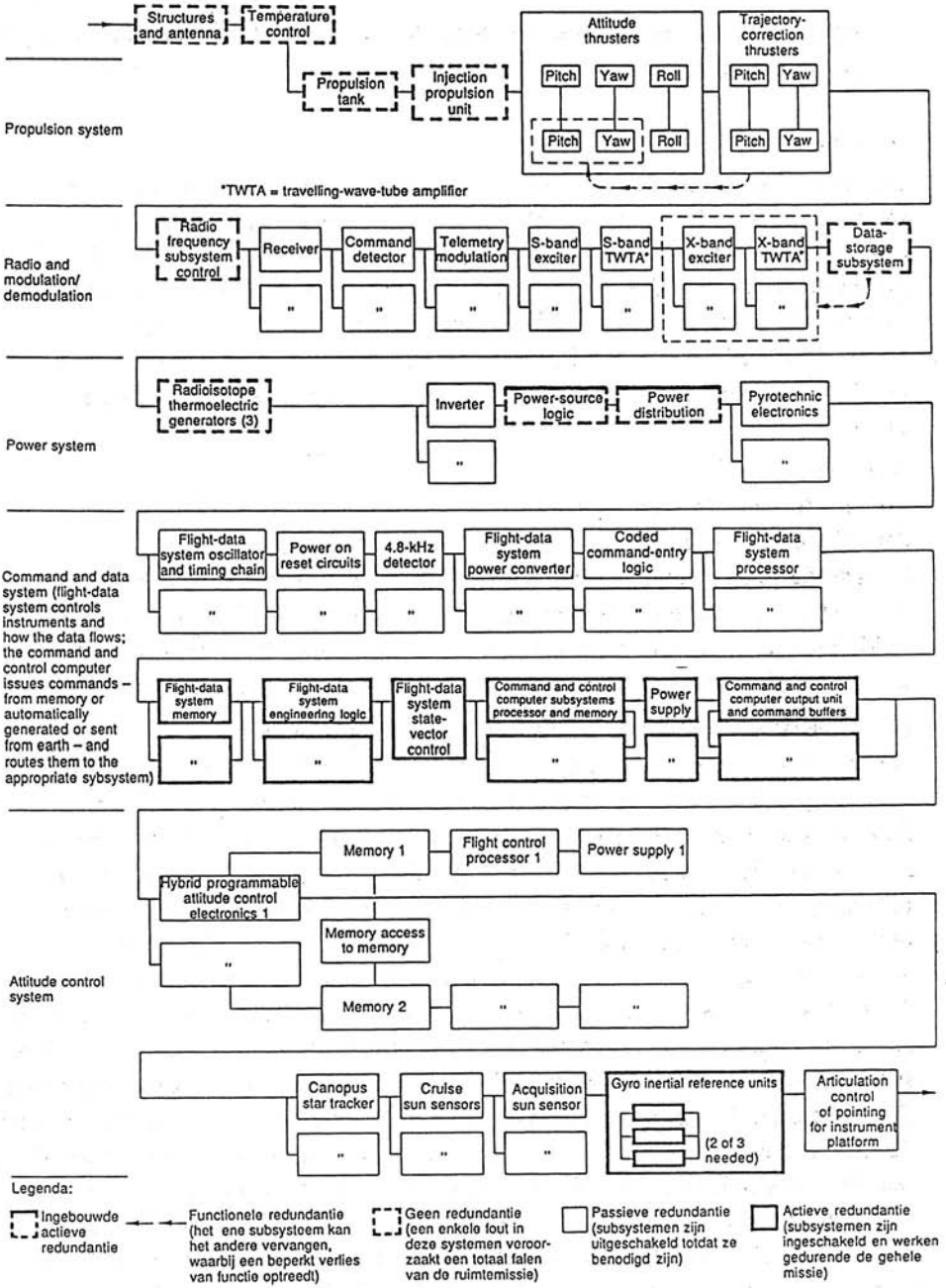
We kunnen met slechte componenten toch goede systemen maken mits we grotere aantallen componenten mogen gebruiken dan voor de vervulling van de systeemfunctie strikt vereist zijn. Er is dus een "trade in" mogelijk tussen aantallen componenten enerzijds en de bedrijfszekerheid van die componenten anderzijds. De in het systeem geïnstalleerde *overmaat* of *redundantie* wordt hierbij gebruikt om de ongestoorde werking van het systeem voort te zetten ook nadat er componenten defect geraakt zijn.

Opmerking

Intermitterende fouten in een systeem kunnen ook met andere middelen dan *"hardware"-redundantie* bestreden worden. Vaak is het voldoende de informatie in de systeemsignalen eenvoudig (een aantal malen) te herhalen of de systeemsignalen redundant te coderen. Deze vorm van redundantie duidt men aan als *informatie-* of *signaalredundantie*. Zij heeft geen effect op de bedrijfszekerheid van een systeem met niet-intermitterende fouten.

In het geval van *hardware* of *structurele redundantie* kunnen de redundante units, modules of componenten op drie verschillende activiteitsniveaus gehouden worden: volledig actief, slechts ten dele actief en volledig passief. In het geval van *actieve redundantie* zijn de reserve componenten evenals de primaire component volledig ingeschakeld. Deze "hot redundancy" kent geen verschil tussen primair ingeschakelde componenten en reservecomponenten. In het geval van *passieve redundantie* staan de reservecomponenten volledig afgeschakeld. Dit geeft in het algemeen de grootste levensduur maar het is in de operationele praktijk vaak lastig te realiseren, daar het een zekere opwarm- of aanlooptijd vergt voordat de passieve reserve de taak van de operationele systeemcomponent kan overnemen. Een oplossing die in ligt tussen deze koude redundantie en de eerder genoemde hete redundantie is de zogenaamde *'stand-by'-redundantie*. Hier staat de reserve reeds half ingeschakeld om de taak van de operationele componenten zonder dode tijd over te kunnen nemen. Een voorbeeld is de stand-by redundante eindtrap van een omroepzender. De reserve zendbuis staat hier reeds op een zekere (verlaagde) gloeidraadspanning om een snelle overname mogelijk te maken (ongeveer 1 seconde).

In figuur 6.1 is een voorbeeld gegeven van verschillende soorten redundantie die in een systeem kunnen worden geïntegreerd.



Figuur 6.1. Catastrofaal faalmodel van de ruimtesonde Voyager waarin de verschillende soorten toegepaste redundantie zijn aangegeven (zie legenda). Bron: Walter C. Williams, 'Lessons from NASA', IEEE Spectrum, okt. 1981.

N.B.: Het is niet altijd zo dat passief redundante componenten een hogere levensduur hebben in de reservetoestand dan componenten in een 'stand-by mode'. Elektrolytische condensatoren bijvoorbeeld hebben met een zekere voorspanning een grotere levensduur dan zonder spanning. In veel elektronische systemen voorkomt de natuurlijke dissipatie, die optreedt bij het in bedrijf houden, condensatie van waterdamp uit de lucht. Deze condensatie treedt wel op in passieve units. Samen met de luchtverontreinigingen geeft het gecondenseerde water zouten, basen en zuren die de metallisatiesporen van o.a. de printed-circuit boards aantasten, waardoor de levensduur bekort wordt.
Ook bij levende wezens zoals mensen en dieren is het in reserve houden voor een bepaalde taak in volledige passiviteit niet bevordelijk voor een bedrijfszeker functioneren van het systeem waar deze taak deel van uitmaakt (denk bijvoorbeeld aan brandweer-, beveiligings- en bewakingspersoneel en de EHBO-post in een ziekenhuis).

In het bedrijfszekerheidsmodel van een redundant systeem worden stand-by en passieve redundantie in beeld gebracht door een aparte faaldistributie voor de componenten in de reservetoestand die verschilt van die voor de operationele componenten (bijvoorbeeld verschillende failure rates).
Het is in een redundant systeem niet altijd zo dat voor de correcte vervulling van een bepaalde systeemtaak volstaan kan worden met één operationele component; veelal is een aantal van zulke (onderling functioneel identieke) componenten nodig om bijvoorbeeld de vermogensdissipatie aan te kunnen. Zo zullen in het algemene geval m (identieke) componenten nodig zijn voor de operationele taak, terwijl er van het totale aantal n dan nog $n - m$ componenten in reserve staan. De redundantiegraad η is dan:

$$\eta = \frac{n - m}{n - 1}.$$

Duidelijk is, dat als $m = 1$ alle units volledig opgebruikt kunnen worden ($\eta = 1$) en dat als $m = n$ er defacto geen redundantie is ($\eta = 0$). In het eerste geval ($\eta = 1$) is het systeem een *zuiver parallelsysteem*, in het tweede geval ($\eta = 0$) is het een *zuiver seriesysteem*. In het tussenliggende geval $0 < \eta < 1$ noemen we het systeem een *m-uit-n systeem*. Een speciaal geval daarvan is het zogenaamde *meerderheidskeuzesysteem*, waarvoor $\eta \approx 0{,}5$. De meeste systemen hebben een gemengde structuur, dat wil zeggen een structuur die noch zuiver parallel, noch zuiver serie van aard is. Naast parallel-, m-uit-n en meerderheidskeuze-redundantie zullen we in het navolgende daarom ook deze gemengde systemen bespreken.

6.4. Parallelsystemen

Een systeem met een zuivere parallelstructuur (redundantiegraad $\eta = 1$) bestaat uit slechts één operationele component. Als deze faalt kan elke component uit het systeem de taak overnemen. Het systeem faalt dan en slechts dan als alle n componenten uit het systeem defect zijn. In stochastische notatie luidt deze laatste zin:

$$F(t) = \prod_{i=1}^{n} F_i(t).$$

Dit is de produktregel voor de bedrijfs*onzekerheid* (unreliability) F(t) van een zuiver parallelsysteem met onafhankelijk optredende defecten. De bedrijfszekerheid en de hazard rate van zulke systemen zijn te bepalen met:

$$R(t) = 1 - F(t)$$

en:

$$z(t) = \frac{1}{R(t)} \frac{dF(t)}{dt}.$$

Nemen we voor $F_i(t)$ een negatief-exponentiële verdeling aan dan geldt:

$$F(t) = \prod_{i=1}^{n} (1 - e^{-\lambda_i t}),$$

$$R(t) = 1 - \prod_{i=1}^{n} (1 - e^{-\lambda_i t}).$$

Door integratie van R(t) naar t vinden we voor de gemiddelde levensduur:

$$\theta = \left(\frac{1}{\lambda_1} + \frac{1}{\lambda_2} + \ldots + \frac{1}{\lambda_n}\right) +$$
$$- \left(\frac{1}{\lambda_1 + \lambda_2} + \frac{1}{\lambda_1 + \lambda_3} + \ldots + \frac{1}{\lambda_{n-1} + \lambda_n}\right) +$$
$$+ \left(\frac{1}{\lambda_1 + \lambda_2 + \lambda_3} + \frac{1}{\lambda_1 + \lambda_2 + \lambda_4} + \ldots + \frac{1}{\lambda_{n-2} + \lambda_{n-1} + \lambda_n}\right) +$$
$$- \ldots\ldots + \frac{(-1)^{n+1}}{\sum_{i=1}^{n} \lambda_i}.$$

Voor een parallelsysteem bestaande uit n identieke componenten met failure rate λ wordt dit:

$$\theta = \frac{1}{\lambda} \sum_{i=1}^{n} \frac{1}{i}.$$

Ook de hazard rate z(t) is dan eenvoudig te berekenen:

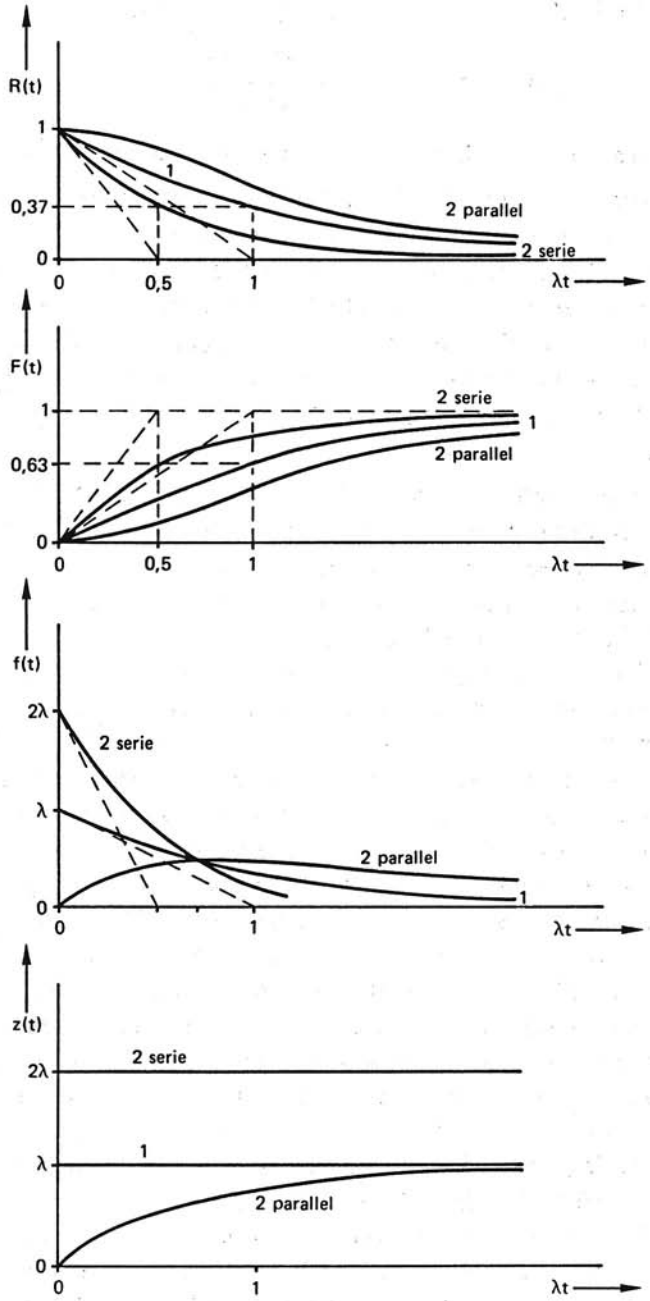
$$z(t) = n\lambda\left(1 - \frac{1-(1-e^{-\lambda t})^{n-1}}{1-(1-e^{-\lambda t})^{n}}\right).$$

De bovenstaande uitdrukkingen zijn eenvoudig af te leiden.

Ter illustratie is in figuur 6.2 de R(t), F(t), f(t) en z(t) getekend van één component en twee zulke componenten, de ene keer in serie, de andere keer parallel. De componenten zijn identiek en hebben een constante failure rate. We zien de meest drastische verschillen in de drie curven voor het tijdinterval vlak na t = 0. De nuttige gebruiksduur van zulke systemen valt hiermee samen. Deze is altijd veel kleiner dan t = $1/\lambda$, de gemiddelde levensduur van de componenten.

Conclusies

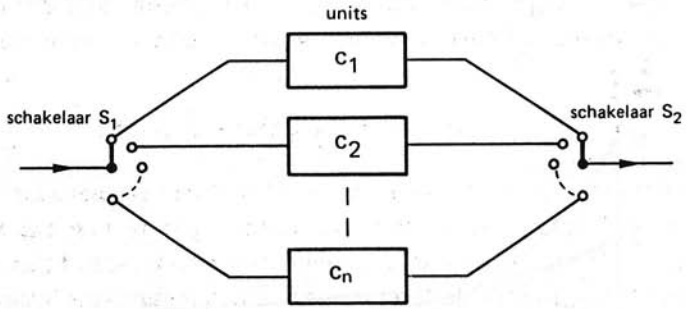
- Een parallelstructuur levert een tijdafhankelijke hazard rate op; in het begin is z(t) nul (de redundantie moet immers worden opgebruikt alvorens een systeem kan sneuvelen). z(t) nadert voor zeer grote t asymptotisch tot de constante failure rate van de ene, laatstovergebleven component, dat is die met de laagste λ_i.
- De MTTF (dus θ) hangt af van de failure rate van de componenten. Des te beter de componenten (dus des te lager λ), des te groter de absolute verlenging van de MTTF.
- Toevoeging van redundante componenten aan een bestaand systeem geeft de meeste toename in bedrijfszekerheid wanneer het systeem reeds uit goede componenten (met een lage λ) bestaat.
- De toevoeging van extra, redundante componenten heeft het meeste effect wanneer er nog weinig redundantie is (voor kleine n).
- Om de grootste bedrijfszekerheidswinst te halen moet men bij eenzelfde aantal beschikbare componenten de redundantie toepassen op een zo elementair mogelijk niveau. Men moet bijvoorbeeld bij een bepaald seriesysteem niet eenvoudigweg het gehele systeem dubbel uitvoeren, maar elke component binnen dat systeem dubbel uitvoeren. Dat kost hetzelfde aantal componenten maar is veel effectiever. Redundantie moet dus op een zo laag mogelijk hiërarchiek niveau in een systeem worden toegepast, het liefst zelfs binnenin de componenten.
- Uit de bovenstaande uitdrukking voor θ, dus voor de MTTF, ziet men dat als men een component met failure rate λ voorziet van een identieke redundante component (λ, n = 2) de MTTF van $1/\lambda$ naar $1{,}5/\lambda$ gaat; een verbetering met een factor 1,5. De kosten zullen echter (vrijwel) verdubbeld zijn omdat men in plaats van één component twee



Figuur 6.2. Bedrijfszekerheidsgrootheden van een zuivere serie- en een zuivere parallelstructuur bestaande uit twee identieke componenten vergeleken met die van één zo'n component.

nodig heeft. Als men bereid is dit dubbele bedrag voor één component uit te geven, kan men veel betere, zogenaamde 'high-rel'-componenten kopen waarvan de levensduur meestal veel méér dan een factor 1,5 groter is. Men kan derhalve (meestal) stellen dat voor een goede systeembedrijfszekerheid veel aandacht moet worden besteed aan goede componenten en men vervolgens deze moet toepassen in weinig kritische structuren zoals redundante structuren.

Tot nu toe hebben we aangenomen dat we met actieve redundantie te doen hadden. Voor *passieve redundantie* ziet het beeld er geheel anders uit. Dit is aangegeven in figuur 6.3. In het algemene geval kunnen de schakelaars S_1 en S_2 falen doordat ze ten onrechte overschakelen, blijven kleven, sluiting maken of een open circuit geven. De componenten c_1 t/m c_n kunnen falen in de actieve mode maar ook in de passieve mode. Laten we eerst aannemen dat de schakelaar ideaal is, de componenten niet falen in de passieve mode en gemakshalve dat n = 2.



Figuur 6.3. Passieve redundantie: $S_1 - S_2$ is een gekoppelde schakelaar, meerwegklep of routeringselement.

Het faaltijdstip t_1 van component c_1 is de stochastische variabele $\underline{t}_1$, en dat van de component c_2 is $\underline{t}_2$. Dan geldt voor de bedrijfszekerheid $R_n(t)$ van dit systeem:

$$R_2(t) = P((\underline{t}_1 > t) \cup (\underline{t}_1 \leqslant t \cap \underline{t}_2 > t - \underline{t}_1)).$$

De beide gebeurtenissen 'c_1 is nog goed' en 'c_1 heeft gefaald, maar c_2 is nog goed' sluiten elkaar uit, dus:

$$R_2(t) = P(\underline{t}_1 > t) + P(\underline{t}_1 \leqslant t \cap \underline{t}_2 > t - \underline{t}_1).$$

Dit geeft:

$$R_2(t) = R_{c_1}(t) + \int_0^t f_{c_1}(t_1) R_{c_2}(t - t_1) dt_1.$$

$R_{c_1}(t)$ en $R_{c_2}(t)$ zijn de bedrijfszekerheden van de eerste en de tweede component, $f_{c_1}(t)$ is de faalkansdichtheid van de eerste component.

De tweede term in deze uitdrukking is de bijdrage van de tweede component in de bedrijfszekerheid. Voor drie componenten kan worden afgeleid:

$$R_3(t) = R_2(t) + \int_0^t f_{c_1}(t_1) \int_0^{t-t_1} f_{c_2}(t_2) R_{c_3}(t - t_1 - t_2)\, dt_2\, dt_1.$$

Hierin is $R_2(t)$ de bedrijfszekerheid van het tweevoudig passief-redundante systeem.
Een iets andere aanpak is de volgende. De faalkansdichtheid van een passief-redundant systeem met n componenten kan geschreven worden als:

$$f_n(t) = \int_{t_{n-1}=0}^{t} \int_{t_{n-2}=0}^{t_{n-1}} \cdots \int_{t_1=0}^{t_2} f_{c_1}(t_1) f_{c_2}(t_2 - t_1) \ldots f_{c_n}(t - t_{n-1}) dt_1\, dt_2 \ldots dt_{n-1}.$$

We maken hierbij gebruik van het feit dat de faalkansdichtheid van de som van een aantal random variabelen gelijk is aan de convolutie der individuele faalkansdichtheden. De bovenstaande bedrijfszekerheid vinden we dan weer met:

$$R_n(t) = 1 - F_n(t) = 1 - \int_0^t f_n(t)dt = \int_t^\infty f_n(t)dt.$$

Dit is eenvoudig af te leiden als men begint met een systeem met twee componenten. Verder is natuurlijk ook eenvoudig in te zien dat voor passieve redundantie, waarbij de componenten niet kunnen falen in de 'uit-toestand', de gemiddelde levensduur van het redundante systeem gegeven wordt door:

$$MTTF = \sum_{i=1}^{n} MTTF_i\ ,$$

mits de schakelaars S_1 en S_2 in figuur 6.3 ideaal zijn.
De bovenstaande uitdrukkingen zijn onafhankelijk van de faaldistributie. Bestaat het systeem uit n identieke componenten alle met een negatief exponentiële faaldistributie dan volgt uit de bovengegeven uitdrukkingen:

$$R_n(t) = e^{-\lambda t} \sum_{i=1}^{n} \frac{(\lambda t)^{i-1}}{(i-1)!}.$$

Als de schakelaar niet ideaal is, maar bijvoorbeeld kan blijven kleven op een contact, gaat de berekening als volgt. Stel dat de schakelaar functioneert met een kans p_s op het ogenblik dat deze moet schakelen, dan wordt voor $n = 2$ de uitdrukking:

$$R_2(t) = R_1(t) + p_s \int_0^t f_{c_1}(t_1) R_{c_2}(t - t_1) dt_1.$$

Op deze wijze kan ook voor hogere waarden van n de overschakelkans p_s ingevoerd worden.
Voor twee identieke units met failure rate λ en een 'klevende' schakelaar met failure rate λ_s kan men een gemiddelde levensduur berekenen:

$$MTTF = \frac{1}{\lambda} + \frac{1}{\lambda + \lambda_s}.$$

Het is dus als het ware of de failure rate van de schakelaar opgeteld wordt bij die van één unit. Dit is ook eenvoudig direct in te zien. Als immers de schakelaar kleeft op de eerste unit is de tweede niet meer inschakelbaar; kleven op de laatste unit verkort de levensduur niet.

Het spontaan overschakelen van de schakelaar kan niet tot falen aanleiding geven. Het kan wel de volgorde van inschakelen verstoren en, in het geval de componenten niet identiek zijn, ook de bedrijfszekerheid beïnvloeden als de schakelaar ook kleeft. We zullen hier niet verder op in gaan.
Als we aannemen dat de schakelaar kan falen door een open circuit op elk tijdstip, dan staat de bedrijfszekerheid van de schakelaar $R_s(t)$ in serie met de rest van het systeem $R_n(t)$ en geldt dus de produktregel:

$$R(t) = R_s(t)R_n(t).$$

6.4.1. Afhankelijke fouten

Zoals we reeds in paragraaf 6.1 kort hebben aangestipt, kan het effect van redundantie in een systeem, dus het effect van de parallelstructuur in het bedrijfszekerheidsmodel van zo'n systeem, weer grotendeels teniet worden gedaan als de fouten in de units van zo'n systeem *stochastisch afhankelijk* zijn. De aanname dat de fouten in een systeem onderling onafhankelijk zijn is namelijk niet altijd geoorloofd.

Voorbeeld 6.2

- De redundante units van een bepaald systeem zijn tamelijk compact samengebouwd. De hitte die ontstaat door kortsluiting in een unit (de primaire fout) kan daardoor een fout in een andere unit veroorzaken of het optreden daarvan bespoedigen (de secundaire fout).
- In een gebied waarin men van luchtlijnen gebruik maakt voor het transport van energie (hoogspanningslijnen) of informatie (telefoonlijnen) heerst een kwakkelwinter. De ijzel en de daarna volgende storm doen de luchtlijnen breken. Voor een hogere bedrijfszekerheid heeft men het transportsysteem opgebouwd uit redundante (ring-)netten. De gemeenschappelijke foutoorzaak (in casu de winter) maakt hier fouten in de redundante lijnen afhankelijk en vermindert het effect van de redundantie.

- In een vliegtuig was de antenne-aarding slecht geworden door corrosie (primaire fout). Tijdens het uitzenden kwam hierdoor een deel van de uitgezonden energie terecht binnen in het vliegtuig. Het gevolg was een overvloed van waarschuwingen en foutmeldingen in de cockpit (secondaire fouten). Nadat de bemanning de correlatie met het uitzenden gemaakt had, besloot men de vlucht te vervolgen.
- In de aansluitkast voor distributie van elektrische energie van een nieuw gebouwd huis heeft een elektriciën vergeten alle klemverbindingen goed vast te zetten (primaire fout). De energiedissipatie in de overgangsweerstand van deze verbindingen geeft zoveel hitte af dat de plastic isolatie van de bedrading smelt. Eén en ander wordt tijdig ontdekt door de stank die hiermee gepaard gaat. De elektriciën vervangt de bekabeling en zet deze keer de verbindingen goed vast. Enige tijd daarna wordt de heer des huizes geëlektrocuteerd als hij met een natte dweil op de plavuizen vloer in de woonkamer een defecte metalen staande schemerlamp aanraakt (primaire isolatiefout in schemerlamp). Bij onderzoek blijkt dat de aardlekschakelaar, die in de aansluitkast recht boven het aansluitklemmenbord zit, door het corrosieve chloorgas dat is vrijgekomen bij de gesmolten isolatie, te zijn gecorrodeerd. De corrosie verhindert het afschakelen (secundaire fout). De aardlekschakelaar heeft een opschrift dat vermeldt dat elke maand de testknop moet worden ingedrukt om de goede werking te beproeven. De huiseigenaar had dit niet gedaan (misuse).

We zien uit de bovenstaande voorbeelden dat de oorzaak voor afhankelijke fouten zich vaak aan onze directe waarneming onttrekt. Dit maakt zulke fouten juist zo gevaarlijk, als men denkt dat men op de geïnstalleerde systemen kan vertrouwen door hun inherent hoge bedrijfszekerheid die bijvoorbeeld kan zijn verkregen door redundantie toe te passen.

Bij afhankelijkheid van de fouten in de verschillende units van een systeem gelden niet de in de vorige paragrafen gegeven produktregels voor serie- en parallelsystemen. Als x_i de gebeurtenis is dat de i-de unit van het systeem bestaande uit n units goed functioneert en $\bar{x}_i$ de complementaire gebeurtenis, dan geldt voor een *seriesysteem*:

$$R_s = P(x_1 \cap x_2 \cap \ldots \cap x_n).$$

Uitschrijven geeft:

$$R_s = P(x_1)P(x_2|x_1) \ldots . P(x_n|x_1 x_2 \ldots x_{n-1}).$$

Slechts voor onafhankelijkheid gaan deze conditionele kansen over in onvoorwaardelijke kansen en kan de bedrijfszekerheid geschreven worden

als

$$R_s = P(x_1)P(x_2) \ldots P(x_n).$$

Analoog hieraan geldt voor een *parallelsysteem*:

$$F_p = P(\bar{x}_1\bar{x}_2 \ldots \bar{x}_n),$$

dus ook:

$$F_p = P(\bar{x}_1)P(\bar{x}_2|\bar{x}_1) \ldots P(\bar{x}_n|\bar{x}_1\bar{x}_2 \ldots \bar{x}_{n-1}).$$

Voor de modellering van afhankelijke fouten moeten we een aantal aannamen maken. We beperken ons daarbij tot een deelverzameling van de verzameling van afhankelijke fouten, en wel tot de zogenaamde *"common-cause failures"; dit zijn fouten die gelijktijdig optreden in verschillende units en die het gevolg zijn van een gemeenschappelijke foutoorzaak.*

We nemen aan dat

- common-cause failures (CC-fouten) zich slechts manifesteren als catastrofale fouten die gelijktijdig in minstens twee verschillende units optreden. CC-fouten die beperkt blijven tot een enkele unit worden geacht te zijn inbegrepen in de hazard rate van die unit.
- CC-fouten en andere fouten onderling stochastisch onafhankelijk zijn,
- CC-fouten een constante failure rate hebben, en
- de units van de beschouwde systemen onderling identiek zijn.

We kunnen een systeem met zulke CC-fouten op eenvoudige wijze modelleren, zoals in figuur 6.4a is aangegeven.
We gaan ervan uit dat de bedrijfszekerheid van een unit opgemeten is terwijl de unit deel uitmaakt van het systeem (dus in de faalkans verhogende aanwezigheid van de overige units en de operationele omgeving) en dat deze te schrijven is als:

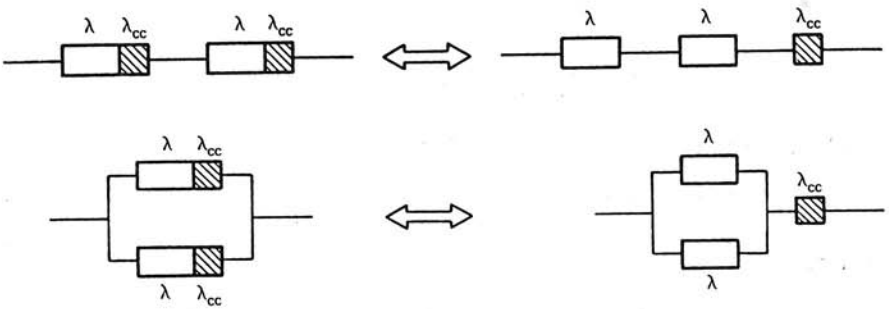
$$R = P(x_i) = e^{-\lambda_t t} \qquad (i = 1, 2, \ldots, n).$$

Voor het seriesysteem links boven in figuur 6.4a is de bedrijfszekerheid te schrijven als:

$$R_s = P(x_1x_2) = P(x_1)P(x_2|x_1),$$

waarin:

$$P(x_1) = e^{-\lambda_t t} = e^{-(\lambda + \lambda_{cc})t},$$



Figuur 6.4. (a) Modellering van common-cause failures in serie- en in parallelsystemen die veroorzaakt worden door afhankelijke faalmechanismen of faaloorzaken in de verschillende units.

en:

$$P(x_2|x_1) = e^{-\lambda t}.$$

Dus:

$$R_s = e^{-\lambda_t t} \cdot e^{-\lambda t} = e^{-(2\lambda + \lambda_{cc})t}.$$

We kunnen dit systeem kennelijk beschouwen als rechtsboven in de figuur is aangegeven. We hoeven bij een seriesysteem dus slechts één keer λ_{cc}, het common-cause aandeel in de totale failure rate λ_t van een unit, in rekening te brengen. We hebben als het ware gecorrigeerd voor het dubbel tellen van afhankelijke fouten.

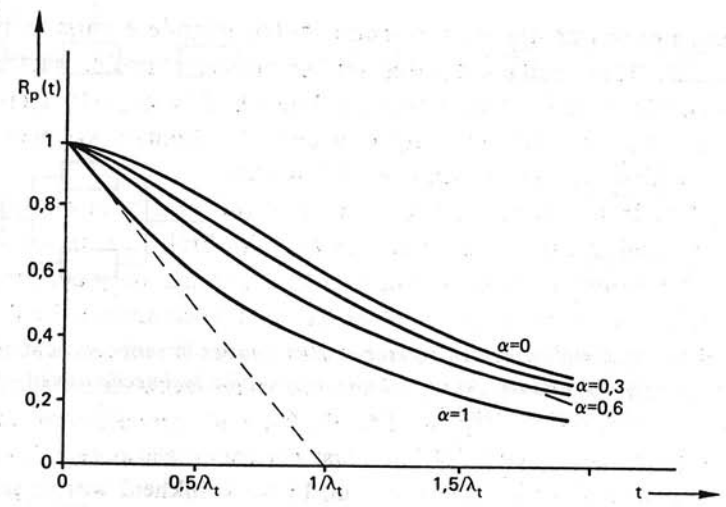
Op soortgelijke wijze vinden we voor een parallelsysteem met

$$F_p = P(\bar{x}_1 \bar{x}_2) = 1 - P(x_1 + x_2) = 1 - P(x_1) - P(x_2) + P(x_1 x_2)$$

voor de faalkans:

$$\begin{aligned} F_p &= 1 - e^{-\lambda_t t} - e^{-\lambda_t t} + e^{-(2\lambda + \lambda_{cc})t} \\ &= 1 - 2e^{-\lambda_t t} + e^{-(\lambda + \lambda_t)t}. \end{aligned}$$

Dit is juist de faalkans die ook het model rechtsonder in figuur 6.4a oplevert. We mogen kennelijk de CC-fouten uit de parallelle takken schuiven en als een enkel serie-element opnemen.
Onder de bovenomschreven voorwaarden kunnen we CC-fouten dus in rekening brengen als een enkel serie-element in het bedrijfszekerheidsmodel van het systeem, onafhankelijk of het een serie- dan wel een



Figuur 6.4. (b) Bedrijfszekerheid van twee parallelle units met common-cause failures, waarbij α de fractie van de unit failure rate is die veroorzaakt wordt door afhankelijke fouten.

parallelsysteem betreft. Dit is toegestaan mits we de failure rate λ_t van een unit corrigeren als $\lambda = \lambda_t - \lambda_{cc}$.

Als we aannemen dat het aandeel λ_{cc} in de totale failure rate λ_t van de units variabel is, dus als

$$\alpha = \frac{\lambda_{cc}}{\lambda_t}, \qquad 0 \leqslant \alpha \leqslant 1,$$

dan vinden we de grafiek van figuur 6.4b. In deze grafiek is de bedrijfszekerheid $R_p(t)$ van een systeem met twee actief-redundante parallelle units uitgezet als functie van de tijd voor verschillende waarden van α.

We zien uit deze figuur dat voor $\alpha = 0$ het CC-foutaandeel ook nul is. Dan hebben we dus een zuiver redundant systeem met uitsluitend stochastisch onafhankelijke fouten. Voor $\alpha = 1$ is de uitval van beide units volledig gecorreleerd. Dan zal het systeem nog slechts functioneren als een enkele unit en is de redundantie dus volledig om zeep geholpen.

N.B.: Beveiligingssystemen voor processen met een hoog risico voert men veelal redundant uit. (Bijvoorbeeld de beveiliging van een kernreactor.) Een significant van nul verschillende waarde van α voor zulke redundante systemen kan dan ook zeer riskant of ronduit gevaarlijk zijn; men vertrouwt op ingebouwde redundantie die slechts schijnredundantie is.

Redundantie zal in effectiviteit dus verminderen door CC-fouten. De voornaamste bronnen van CC-fouten zijn:

- Secundaire fouten die door primaire fouten in andere units worden veroorzaakt. Deze ontstaan doordat bij het ontwerp onvoldoende met deze foutmogelijkheden rekening wordt gehouden. Bijvoorbeeld oververhitting van naburige units in een compact gebouwd redundant systeem wanneer een unit door een kortsluiting te heet wordt.
  Vergelijk: In een vliegtuig trad kort na de start een waarschuwing op dat er brand in een van de motoren was uitgebroken. Kort daarop werd gemeld dat ook een tweede motor in brand stond. De vlucht werd afgebroken. Terug op de grond bleek dat de waarschuwingscircuits voor brandmelding weliswaar in aparte kasten waren ondergebracht maar dat deze kasten vlak naast elkaar in een rek waren geplaatst. Onderin het bedoelde rek was een regelweerstand oververhit geraakt door langdurig op de grond beproeven. Dit had eerst het eerste alarm getript en toen het tweede daarboven gelegen alarm. In werkelijkheid was er geen brand opgetreden (Engels: nuisance alarm).
- Elektrische, mechanische en thermische afhankelijkheid tussen de units in een systeem. Voorbeeld: het uitvallen van een ventilator in een rek met vele kaarten met digitale TTL-logica. Ook een kortgesloten ingang van een versterker uit een redundant versterkersysteem kan het hele systeem doen falen. Slordige bediening of gebrekkig onderhoud kan dit ook veroorzaken. Voorbeelden zijn: gebruik van verkeerde componenten bij reparatie, onvolkomen afregeling doordat meetapparatuur uit calibratie is (wijst bijvoorbeeld systematisch te laag aan).
- Gemeenschappelijke uitwendige oorzaken zoals: stof, vuil, condensvocht, hitte, trillingen en schokken.
- Milieu-oorzaken zoals: overstromingen, aardbevingen, brand, storm, ijzel, strenge vorst, zware sneeuwval.
- Het gebruik van redundante units van hetzelfde fabrikaat. Hierdoor kunnen dezelfde soort fouten in de units voorkomen. Hierbij kan men denken aan ontwerp-, materiaalkeuze- en produktie-fouten. Een voorbeeld hiervan: slechte soldeerverbindingen bij het automatisch solderen van printed-circuit boards.
- Gemeenschappelijke bronnen van energie, materialen en personeel. Voorbeelden: een gemeenschappelijke voeding voor redundante units, gemeenschappelijke transportleidingen, koelleidingen en dergelijke voor verschillende processen, als ook algehele stakingen onder het personeel of gijzeling van personeel en installaties.

CC-fouten zijn de meest ernstige vorm die afhankelijke fouten kunnen aannemen (en daardoor ook de meest gevreesde). Immers, door een gemeenschappelijke oorzaak falen gelijktijdig alle gelijksoortige units uit een systeem op catastrofale wijze. Veel afhankelijke fouten hebben niet een zo

drastische uitwerking. Het optreden van de gemeenschappelijke oorzaak of het falen van de ene unit verhoogt dan slechts de kans op falen van een aantal units in een systeem. Als het systeem redundant is, zal het dus mogelijk zijn de na elkaar falende units bij preventief onderhoud te vervangen en zo het systeem draaiende te houden. Dit neemt niet weg dat (alle soorten) afhankelijke fouten in een redundant systeem de effectiviteit van de redundantie aantasten en dus zoveel mogelijk vermeden dienen te worden.

6.5. M-uit-N systemen

Zoals reeds eerder gezegd: systemen met een m-uit-n redundantie zijn noch zuivere seriesystemen noch zuivere parallelsystemen. Bij zo'n systeem moeten er te allen tijde minstens m componenten goed functioneren, wil het systeem goed kunnen functioneren. Duidelijk zal zijn dat de grensgevallen voor $m = n$ en $m = 1$ een seriesysteem respectievelijk een parallelsysteem opleveren; m-uit-n redundantie is dus een algemenere vorm van redundantie dan de beide eerder behandelde vormen.
We nemen weer het geval van actieve redundantie en identieke componenten. De kans op k overlevende componenten uit n componenten volgt uit de binomiale verdeling:

$$P_k = \binom{n}{k} [R_0(t)]^k [1 - R_0(t)]^{n-k}.$$

Hierin is $R_0(t)$ de bedrijfszekerheid van een component. Het m-uit-n systeem functioneert goed zolang er minstens m componenten goed functioneren. Dus het systeem is bedrijfszeker als $m, m+1, m+2, \ldots,$ of n componenten nog goed zijn:

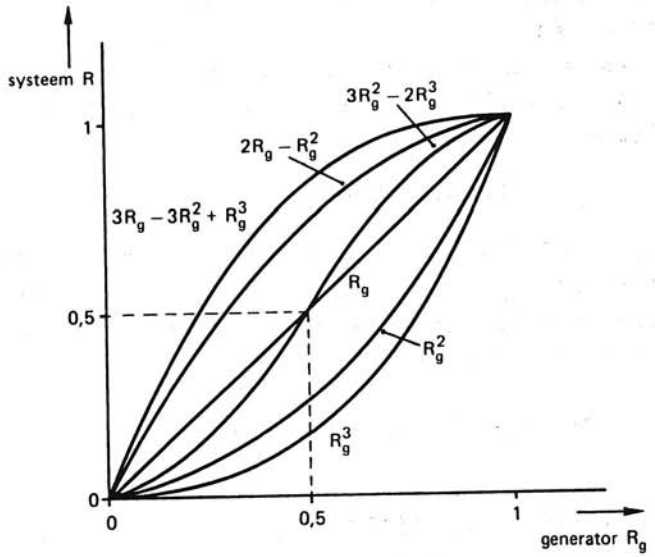
$$R(t) = \sum_{k=m}^{n} \binom{n}{k} [R_0(t)]^k [1 - R_0(t)]^{n-k}.$$

Voorbeeld 6.3
Aan boord van een transportmiddel moet men over een bepaald elektrisch vermogen kunnen beschikken voor verlichting, communicatie, navigatie en dergelijke. Voor een zeker transportmiddel (vliegtuig) heeft men maximaal 15 kW vermogen nodig; 7 kW voor gereduceerd maar aanvaardbaar gebruik, en een minimum van 5 kW vermogen onder noodomstandigheden. Men kan het transportmiddel uitrusten met één 15 kW generator, twee 8 kW generatoren parallel of drie 5 kW generatoren parallel. We nemen gemakshalve aan dat de bedrijfszekerheid R_g van alle drie typen generatoren gelijk is. We kunnen dan tabel 6.2 opstellen voor de bedrijfszekerheid onder vol gebruik, aanvaardbaar gereduceerd gebruik en noodgebruik.

	1 x 15 kW	2 x 8 kW	3 x 5 kW
Vol gebruik	R_g	R_g^2	R_g^3
Aanvaardbaar gebruik	R_g	$2R_g - R_g^2$	$3R_g^2 - 2R_g^3$
Noodgebruik	R_g	$2R_g - R_g^2$	$3R_g - 3R_g^2 + R_g^3$

Tabel 6.2. Operationele inventarisatie van een energieopwekkingssysteem.

De laatste kolom is het meest illustratief: hier gaat het systeem van een 3-uit-3 systeem via een 2-uit-3 systeem naar een 1-uit-3 systeem. In figuur 6.5 is de bedrijfszekerheid R voor deze verschillende soorten gebruik uitgezet tegen de generatorbedrijfszekerheid R_g. Wat is de beste ontwerpoplossing: het kiezen van één, twee of drie generatoren in het transportmiddel? De oorzaak van de S-vormigheid van de curve die $R = 3R_g^2 - 2R_g^3$ als functie van R_g toont zullen we in de volgende paragraaf behandelen.



Figuur 6.5. Een aantal oplossingen voor het energie-opwekkingssysteem van een transportmiddel. Zie ook tabel 6.2.

Als we aannemen dat we te doen hebben met m-uit-n redundantie waarin alle n units actief zijn en een failure rate λ hebben, dan kunnen we afleiden dat geldt:

$$R(t) = \sum_{k=m}^{n} \binom{n}{k} [e^{-\lambda k t}][1 - e^{-\lambda t}]^{n-k}$$

$$\text{MTTF} \equiv \theta = \frac{1}{\lambda} \sum_{k=m}^{n} \frac{1}{k}$$

} actieve m-uit-n redundantie

Voor passieve m-uit-n redundantie waarin steeds slechts m units actief zijn met failure rate λ en de overige passief met failure rate nul geldt:

$$R(t) = e^{-\lambda m t} \sum_{k=m}^{n} \frac{(m\lambda t)^{k-m}}{(k-m)!}$$

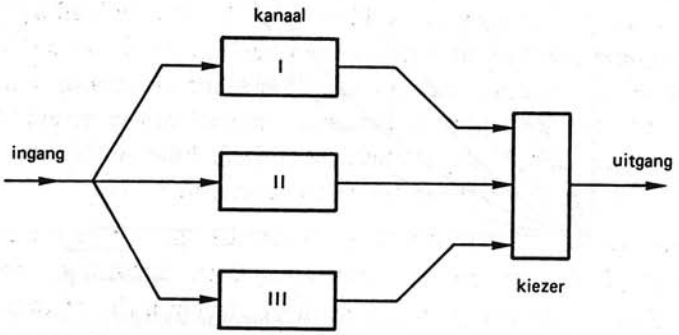
$$MTTF \equiv \theta = \frac{n-m+1}{m\lambda}$$

} passieve m-uit-n redundantie

Het belang van m-uit-n systemen ligt daarin dat het in de operationele praktijk niet altijd mogelijk is een systeem met een redundantiegraad $\eta = 1$ te ontwerpen. Zo kan men bijvoorbeeld tamelijk gemakkelijk een redundante versterkerschakeling maken die toelaat dat één uit drie parallel geschakelde operationele versterkers faalt. Dat levert dus een 2-uit-3 systeem. Denk ook aan de banden uit de 'wieltrossen' van een landingsgestel of een zware vrachtwagen. Een DC-10 kan nog vliegen en landen als er tenminste twee van de drie motoren nog werken.

6.6. Meerderheidskeuze systemen

Een meerderheidskeuze systeem is een redundant systeem dat correct functioneert zolang er nog een meerderheid van de n redundante komponenten functioneert. In figuur 6.6 is een voorbeeld van zo'n systeem gegeven. Hieruit blijkt meteen het praktische nut van deze vorm van redun-



Figuur 6.6. Voorbeeld van een meerderheidskeuzesysteem toegepast op overdrachtskanalen.

dantie. De signaalbewerkingen in het overdrachtskanaal kunnen zeer complex zijn. Dat maakt het moeilijk zo'n kanaal op correct functioneren te controleren. Met andere woorden: de foutdetectie is lastig en vergt complexe en dus weinig bedrijfszekere systemen. In figuur 6.6 worden door het keuze-circuit slechts de uitgangssignalen vergeleken. Deze kiezer selecteert vervolgens een uitgang die overeenstemt met de meerderheid van de uitgangen. In analoge systemen zullen de uitgangssignalen altijd een wei-

nig verschillen. Dan middelt de kiezer meestal over de overeenkomstige signalen. Een bepaalde, in de kiezer ingebouwde drempelwaarde bepaalt dan of een signaal als ontoelaatbaar afwijkend of toelaatbaar afwijkend van de meerderheid moet worden gezien. Daartoe wordt vaak als uitgangspunt het mediane signaal gekozen en de afwijkingen ten opzichte van dit mediane signaal bepaald. Dit soort kiezers noemt men wel '*similarity voters*', omdat zij eigenlijk de signalen op gelijkvormigheid beoordelen.
We nemen aan dat de kiezer niet faalt, dus dat deze een te verwaarlozen complexiteit heeft ten opzichte van de kanalen. Als alle drie de kanalen correct functioneren werkt het systeem dus goed. Als er nog twee correct functioneren werkt het systeem ook nog goed en kan de kiezer een waarschuwing geven dat er een kanaal defect is (*failure cautioning*). Ook kan de kiezer melden welk kanaal stuk is (*failure reporting*), wat het onderhoud bespoedigt. Als er twee kanalen stuk zijn, faalt het systeem. Als ze hetzelfde foutieve uitgangssignaal leveren wordt dit signaal op de systeemuitgang gezet en ten onrechte het goede kanaal als foutief aangewezen. Als de twee foute kanalen een verschillend foutief signaal geven 'weet' de kiezer dat het systeem defect is (drie verschillende signalen) en geeft een alarmering (*failure alarm*). Dezelfde redenering kan men volgen voor drie foute kanalen.

Voor meerderheidskeuze systemen met meer dan drie redundante eenheden kan men met voordeel de kiezer adaptief maken (*adaptive majority voting*). Dit gaat als volgt: iedere keer als de kiezer een defecte eenheid signaleert, wordt deze afgeschakeld en maakt dus geen deel meer uit van het kiesproces. Op deze wijze blijft het systeem goed functioneren zolang er nog minstens twee eenheden goed zijn. Redundantie met adaptieve meerderheidskeuze realiseert dus een 2-uit-n systeem als $n \geqslant 3$. Eenvoudig is na te gaan wat er gebeurt nadat er nog twee eenheden over zijn.

Aan adaptieve meerderheidskeuze zit een groot gevaar: als de eenheden intermitterende fouten vertonen, brengt het systeem zichzelf om zeep. Dit kan voorkomen worden door een eenheid pas definitief af te schakelen nadat deze geruime tijd 'dissident' is geweest. Over korte tijdintervallen genomen is het systeem dus niet adaptief.
We zien dat niet-adaptieve meerderheidskeuze vereist dat er $(n/2) + 1$ eenheden uit n eenheden nog goed zijn als n even is en $(n + 1)/2$ uit n als n oneven is. Dit levert met de redundantiegraad:

$$\eta = \frac{n - m}{n - 1},$$

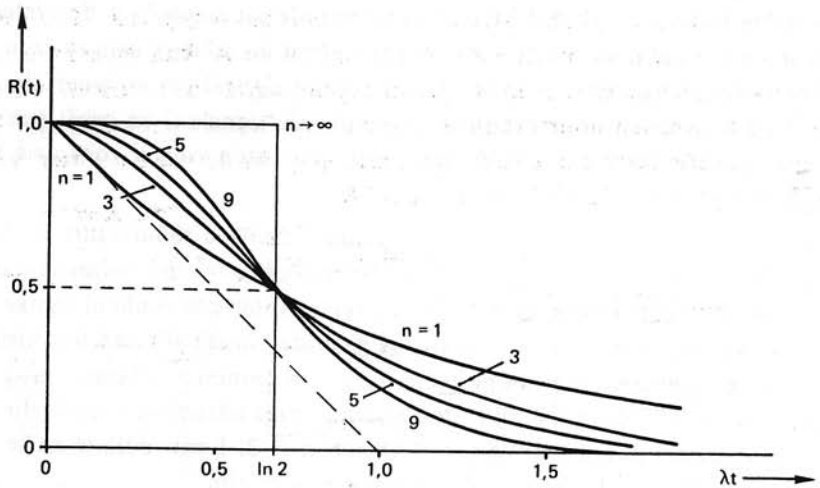
voor even n:

$$\eta_{even} = 1 - \frac{n}{2(n-1)},$$

en voor oneven n:

$$\eta_{oneven} = 1/2.$$

Daar $\eta_{even} < \eta_{oneven}$ is het dus het efficiëntst uit te gaan van een *oneven aantal* redundante *eenheden*. Het verschil wordt trouwens steeds kleiner naarmate n groter wordt. Voor adaptieve meerderheidskeuze geldt het bovenstaande niet; daar neemt de redundantiegraad monotoon toe naarmate n groter wordt: het realiseert immers een 2-uit-n systeem.
In figuur 6.7 is aangegeven hoe een niet-adaptief meerderheidskeuze systeem met een perfecte kiezer zich als functie van de tijd gedraagt voor eenheden met een negatief-exponentiële faaldistributie.



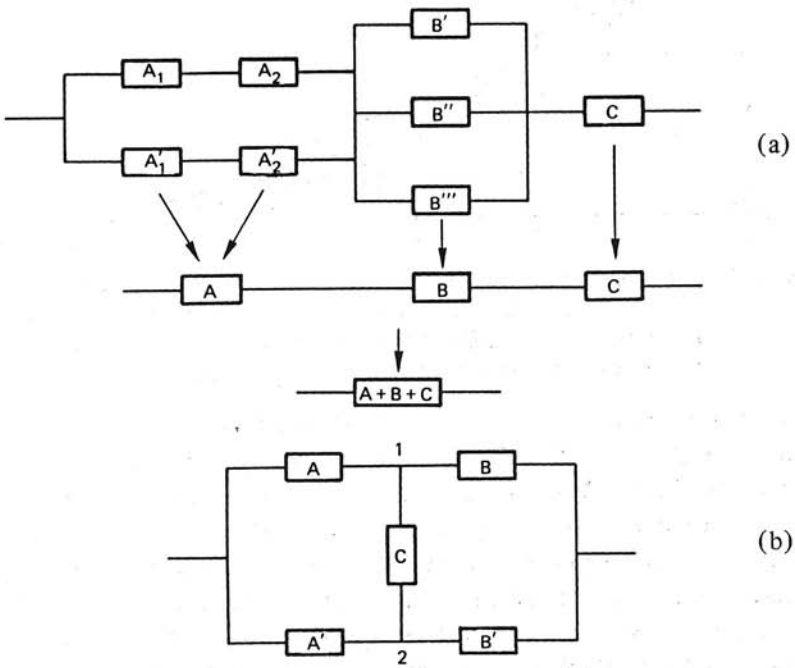
Figuur 6.7. Niet-adaptieve meerderheidskeuze uit een systeem met n identieke redundante units met een failure rate λ. Hierin is λt = ln 2 de mediane levensduur van de individuele units van het systeem, maar ook van het meerderheidskeuzesysteem: de mediane levensduur verandert niet!

We zien uit deze figuur dat zolang de bedrijfszekerheid R van de units nog groter is dan 0,5, meerderheidskeuze een verbetering van de systeembedrijfszekerheid geeft. Als R = 0,5 maakt het al dan niet toepassen van meerderheidskeuze geen verschil; immers de stemmen staken. Als R < 0,5 wordt het systeem door meerderheidskeuze zelfs slechter: er wordt immers voor de foutieve meerderheid gekozen. Naarmate het aantal units groter wordt, wordt dit gedrag steeds geprononceerder. Tenslotte, voor n → ∞ faalt het systeem exact op het tijdstip waarop de units hun *mediane levensduur* bereiken. Deze laatste uitspraak geldt onafhankelijk van de faaldistributie van

de units. Waarom niet bij het bereiken van de gemiddelde levensduur? (De curve $3R_g^2 - 2R_g^3$ in figuur 6.5 is dus niets anders dan een vorm van meerderheidskeuze redundantie.)

6.7. Gemengde systemen

In de vorige paragrafen hebben we naast m-uit-n redundantie ook speciale gevallen daarvan besproken. Er zijn echter systemen die zich niet laten herleiden tot deze vormen van redundantie. Deze zogenaamde *gemengde systemen* treden meestal op in complexe apparatuur zoals in de procesindustrie gebruikt wordt. Het eerste wat men kan doen bij de bepaling van de bedrijfszekerheid van zo'n complex systeem is alle seriecomponenten samennemen tot één component evenals alle parallelcomponenten. Dit is aangegeven in figuur 6.8a.
Er zijn systemen met structuren die niet verder samen te nemen zijn. In figuur 6.8b is als voorbeeld hiervan een brugstructuur gegeven. Men kan zich deze structuur als volgt voorstellen: unit A en A′ kunnen elkaars taak overnemen, evenals unit B en B′. De knooppunten 1 en 2 kunnen echter niet zomaar worden doorverbonden; hier is een buffercircuit C nodig. Het systeem functioneert dus zolang tenminste één van de volgende vier wegen nog functioneert: AB, A′B′, ACB′ en A′CB.



Figuur 6.8. (a) Samennemen van complexe systemen in serie- en parallelsubsystemen. (b) Voorbeeld van een niet verder samen te nemen systeem (brugstructuur).

Als we aannemen dat een unit slechts goed kan functioneren (toestand 1) of defect is (toestand 0), dus als we uitgaan van het katastrofale faalmodel, dan is een eenvoudige berekeningsmethode die welke gebruik maakt van de *volledige inventarisatie van alle toestanden* waarin het systeem kan verkeren. Voor figuur 6.8b wordt deze inventarisatie als aangegeven in tabel 6.3.

Toestand units					Toestand systeem
A	A′	B	B′	C	
1	1	1	1	1	1
1	1	1	1	0	1
1	1	1	0	1	1
1	1	1	0	0	1
1	1	0	1	1	1
1	1	0	1	0	1
1	0	0	1	1	1
1	0	0	1	0	0
—	—	—	enzovoort (totaal 32 toestanden)		

Tabel 6.3. Inventarisatie van de toestanden van het systeem uit figuur 6.7b.

Vervolgens berekent men op basis van deze inventarislijst de kans dat het systeem in toestand 1 is, uitgedrukt in de bedrijfszekerheden van de units A, A′, enzovoort. Hoewel eenvoudig, deze methode is toch bewerkelijk. Een eveneens voor de hand liggende methode is de *inspectiemethode*. Deze vraagt inzicht in het systeem. Deze methode luidt voor het voorbeeld van figuur 6.8b: het systeem is bedrijfszeker als één of meer van de wegen AB, A′B′, ACB′ en A′CB functioneren. Dit is de volledige verzameling van alle mogelijke geheel of gedeeltelijk verschillende wegen van de ingang naar de uitgang. De bedrijfszekerheid is dus:

$$R = P(AB \cup A'B' \cup ACB' \cup A'CB).$$

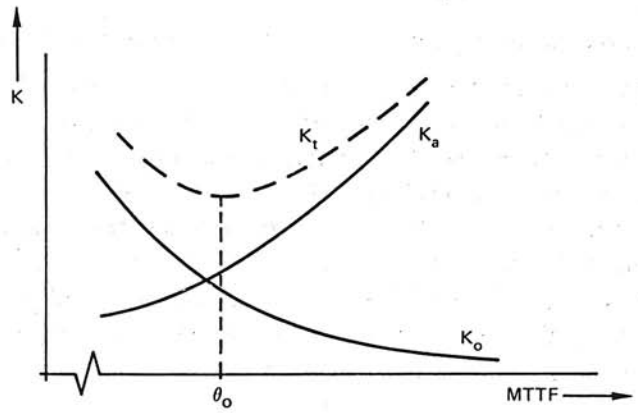
Na uitwerken en vereenvoudigen wordt dit:

$$\begin{aligned} R = {} & P(AB) + P(A'B') + P(AB'C) + P(A'BC) + \\ & - P(AA'BB') - P(ABB'C) - P(AA'BC) - P(AA'B'C) + \\ & - P(A'BB'C) + 2P(AA'BB'C). \end{aligned}$$

Hierin is P(AB) de kans dat A èn B goed functioneren.

6.8. Optimalisatie

Het streven naar systemen met een hogere bedrijfszekerheid gaat met kosten gepaard. De kostenstijging ontstaat doordat de ontwikkelingskosten hoger zijn ten gevolge van noodzakelijke levensduurbeproevingen, bedrijfszekerheidssimulaties en herziening van het ontwerp. Ook de produktiekosten zullen hoger zijn door inspectieprocedures, opleiding van produktiepersoneel en dergelijke. Verder zullen de initiële investeringskosten van het systeem ook hoger zijn, door gebruik van dure 'high reliability'-componenten, redundante structuren en dergelijke.
Het bovenstaande is echter slechts één zijde van de medaille. De gebruiker-eigenaar van het systeem is namelijk niet alleen in de aanschafkosten K_a geïnteresseerd maar ook in de onderhoudskosten K_o tijdens de nuttige gebruiksperiode van het systeem. Hij zal daarbij streven naar een zo laag mogelijke *overall cost of ownership* K_t, betrokken op de gehele levenscyclus van het systeem: ontwerp, produktie en gebruik. In figuur 6.9 is uitgezet hoe K_a en K_o voor typisch technische systemen afhangen van de gewenste MTTF van het systeem.



Figuur 6.9. Aanschafkosten K_a, onderhoudskosten K_O en totale kosten K_t van een fictief technisch systeem versus de MTTF van zo'n systeem.

Duidelijk zal zijn dat bij een bepaalde MTTF = θ_o de totale kosten betrokken op de gehele levenscyclus van het systeem het laagst zijn. Links hiervan heeft het zin hogere initiële kosten te aanvaarden omdat men later meer dan deze extra uitgave bezuinigt op het onderhoud.
Niet alle systemen bevinden zich op of in de buurt van het minimum in de K_t-curve van figuur 6.9. Rechts van het optimum voor MTTF $\approx \theta_o$ heeft men kennelijk geëist dat er zeer weinig of geen onderhoud mag worden gepleegd bijvoorbeeld omdat dit niet mogelijk is of omdat falen zeer kostbare gevolgen heeft. Wat men ook vaak tegenkomt is dat de afnemer

eenvoudigweg heeft overgespecificeerd en niet voldoende kostenbewust is geweest.
Het andere geval treft men vaak aan bij consumentenartikelen. Voor produkten in de typische 'consumentensfeer' let de afnemer vrijwel alleen op de initiële aanschafprijs K_a. De, meestal zeer grote, systemen die gemaakt worden in opdracht van de overheid (voor ruimtevaart, telecommunicatie of militaire doeleinden) bevinden zich meestal rechts van het optimum θ_o. De systemen in de industriële sfeer (de professionele markt) bevinden zich veelal zeer dicht bij θ_o door de heersende concurrentie tussen de producenten en de kostenbewustheid van de industrie.
Optimalisatie van de bedrijfszekerheid R van een systeem is een belangrijk probleem. Bij het tot stand komen van het systeem en ook bij het later in operationele toestand houden van het systeem, maakt men kosten K. Onder kosten wordt verstaan *gegeneraliseerde kosten*, dat wil zeggen niet alleen geld maar ook andere benodigde schaarse zaken zoals gewicht of volume daar waar het totaalgewicht respectievelijk de afmetingen van het systeem kritisch zijn.
Het systeem kan men in units (componenten, modules, subsystemen) verdelen. Deze '*system partitioning*' geschiedt meestal zo dat elke unit een zelfstandige functie uitvoert. De bedrijfszekerheid van de i-de unit is R_i en de prijs daarvan is K_i.
We kunnen nu twee optimaliseringsproblemen onderscheiden:
- met een minimum bedrijfszekerheidseis (*reliability constrained*);
- met een beperkt budget (*budget constrained*).

Bij de eerste aanpak wenst de ontwerper meer dan een gegeven minimum bedrijfszekerheid voor zo laag mogelijke kosten; bij de tweede aanpak wenst hij de hoogste bedrijfszekerheid voor een gegeven maximum budget. We zullen ze achtereenvolgens kort bespreken.

- *Optimalisatie met bedrijfszekerheidseis*
  We nemen aan dat voor alle n functies, dus voor elke i-de unit een aantal alternatieven m_i ter beschikking staat. Dat kunnen units van verschillende fabrikanten zijn, maar bijvoorbeeld ook parallelschakelingen, (dus redundante uitvoeringen) van units zijn. Elk alternatief voor de i-de functie heeft een bijbehorende bedrijfszekerheid R_{ij} en bijbehorende kosten K_{ij} ($j = 1,2, \ldots, m_i$). We rangschikken nu voor elk der n functies de m_i alternatieven naar toenemende bedrijfszekerheid dus:

$$R_{i1} < R_{i2} < \ldots . < R_{im_i}.$$

  De kosten moeten dan ook in toenemende volgorde staan, dus:

$$K_{i1} < K_{i2} < \ldots . < K_{im_i}.$$

Als één of meer der alternatieven hieraan niet voldoen dan zijn er te kostbare alternatieven bij die simpelweg geschrapt kunnen worden. Na deze afvalprocedure verloopt de verdere optimalisatie als volgt:
Voor de systeembedrijfszekerheid geldt:

$$R = \prod_{i=1}^{n} R_{ij}.$$

Voor de systeemkosten geldt:

$$K = \sum_{i=1}^{n} K_{ij}.$$

De waarden van j moeten nu gevonden worden zodat $R \geqslant R_{min}$ en K zo laag mogelijk is. Dit gaat als volgt:

- Neem voor elke functie het goedkoopste alternatief.
- Bereken de daarbij behorende systeembedrijfszekerheid R.
- Bepaal voor elke functie de relatieve bijdrage in systeembedrijfszekerheid per extra geïnvesteerde gulden van het eerstvolgende duurdere alternatief. Deze bijdrage is:

$$\frac{\Delta R}{\Delta K_i} = \frac{R}{R_i} \cdot \frac{\Delta R_i}{\Delta K_i}.$$

- Neem die eenheid op in het systeem waarvoor deze relatieve bedrijfszekerheidsverhoging het grootst is.
- Herhaal de voorgaande drie punten totdat geldt: $R \geqslant R_{min}$.

Nu een teleurstelling: deze methode is relatief snel, maar behoeft niet altijd het juiste antwoord te geven. Als de verschillen in $\Delta R/\Delta K_i$ groot zijn tussen de verschillende functies, en het aantal functies is groot (n is groot) dan is de enige juiste methode het afzoeken van alle mogelijke combinaties met de computer.

■ *Optimalisatie met beperkt budget*
Weer is het systeem opgedeeld in n functies die apart gerealiseerd kunnen worden en waarvoor een aantal alternatieven bestaat, ieder met hun eigen bedrijfszekerheid en kosten. Weer geldt dat alle functies nodig zijn:

$$R = \prod_{i=1}^{n} R_{ij}$$

en:

$$K = \sum_{i=1}^{n} K_{ij}.$$

Gevraagd worden nu die waarden van j waarvoor: $K \leqslant K_{max}$ en R zo

groot mogelijk.
De optimalisatie verloopt natuurlijk identiek aan de vorige optimalisatie (het probleem is symmetrisch in R en K). Nu wordt er gestopt als de laatst gekozen realisatie een budget-overschrijding geeft. Ook hier geldt weer dat dit een praktische methode is voor een snelle oplossing. De optimale oplossing wordt niet noodzakelijk gevonden, daarvoor moet een 'exhaustive search' van alle mogelijkheden worden gedaan.

Een techniek die men bij verbetering van de bedrijfszekerheid van een systeem door middel van redundantietoevoeging wel eens tegenkomt, is de evenredige toewijzing (evenredig in de failure rate). Deze door de ARINC* voorgestelde methode gaat niet uit van een kostenoverweging, maar van de overweging dat toevoeging van een (passief) redundante unit de gemiddelde levensduur met een bepaalde factor (2) vergroot. Als de n units weer een seriesysteem vormen en de i-de unit een failure rate λ_i heeft, geldt dus:

$$\lambda = \sum_{i=1}^{n} \lambda_i \geqslant \lambda_{spec}.$$

De nieuwe allocatie van failure rates λ_i' aan de n units gaat dan volgens de toekenningsprocedure:

$$\lambda_i' = \frac{\lambda_i}{\sum_{i=1}^{n} \lambda_i} \lambda_{spec} = \lambda_i \frac{\lambda_{spec}}{\lambda}.$$

De nieuwe failure rates λ_i' worden dus toegekend naar rato van de oude failure rates λ_i. Alle failure rates moeten dan dus met dezelfde factor λ_{spec}/λ verkleind worden. De toevoeging van redundantie vergroot de gemiddelde levensduur met een bepaalde factor (hoewel de faaldistributie zich ook wijzigt in een niet-exponentiële distributie). λ_{spec}/λ geeft dus een maat voor de vereiste redundantie in het systeem. Het zij nogmaals gezegd: deze methode van evenredige toewijzing is dus niet op een (kosten) optimalisering gebaseerd.

6.9. Analysemethoden

In de volgende vier paragrafen zullen we een aantal systematische berekeningsmethoden voor de bedrijfszekerheid van gemengde systemen bespreken.

6.9.1. Netwerkreductiemethode

Bij de netwerkreductiemethode neemt men de structuur van een systeem samen tot substructuren waarvan een analytische uitdrukking voor de be-

*) ARINC: Aeronautical Radio Incorporated.

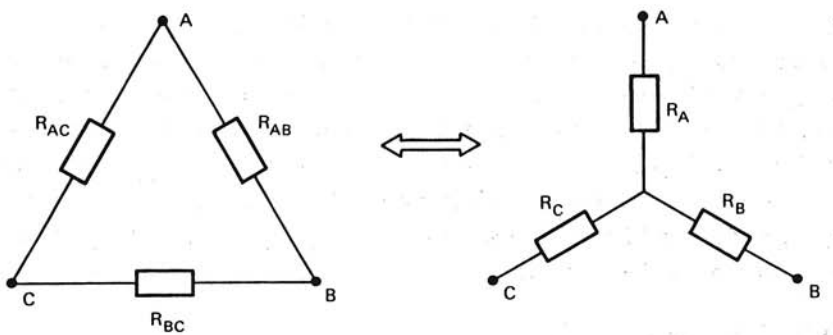
drijfszekerheid bekend is.
Voorbeelden zijn: seriestructuren, parallelstructuren, m-uit-n structuren, meerderheidskeuzestructuren, enzovoort. Na deze reductie van een systeem blijven niet-reduceerbare structuren over zoals die in figuur 6.8b. Op deze niet-reduceerbare structuren kan men dan vervolgens de *delta-ster transformatie* toepassen. (Men kan natuurlijk ook andere reeds in paragraaf 6.7 aangegeven berekeningswijzen volgen.)

In figuur 6.10 is de delta-ster transformatie voor bedrijfszekerheidsmodellen aangegeven. Als we uitgaan van een model met de links aangegeven structuur met als componentbedrijfszekerheden R_{AB}, R_{BC} en R_{AC}, dan kunnen we deze omzetten in een sterstructuur met een bedrijfszekerheid R_A, R_B en R_C waarbij

$$R_A = \sqrt{\frac{\{1-(1-R_{AC})(1-R_{BC}R_{AB})\}\{1-(1-R_{AB})(1-R_{AC}R_{BC})\}}{\{1-(1-R_{BC})(1-R_{AC}R_{AB})\}}},$$

$$R_B = \sqrt{\frac{\{1-(1-R_{AB})(1-R_{AC}R_{BC})\}\{1-(1-R_{BC})(1-R_{AC}R_{AB})\}}{\{1-(1-R_{AC})(1-R_{BC}R_{AB})\}}},$$

$$R_C = \sqrt{\frac{\{1-(1-R_{AC})(1-R_{BC}R_{AB})\}\{1-(1-R_{BC})(1-R_{AC}R_{AB})\}}{\{1-(1-R_{AB})(1-R_{AC}R_{BC})\}}}.$$



Figuur 6.10. De delta-ster equivalentie voor bedrijfszekerheidsmodellen.

Dit is eenvoudig als volgt in te zien. Het sternetwerk moet tussen A en B dezelfde bedrijfszekerheid geven als het deltanetwerk tussen A en B. Derhalve:

$$R_A R_B = 1 - (1 - R_{AB})(1 - R_{AC}R_{BC}),$$

en dus ook:

$$R_B R_C = 1 - (1 - R_{BC})(1 - R_{AC}R_{AB}),$$

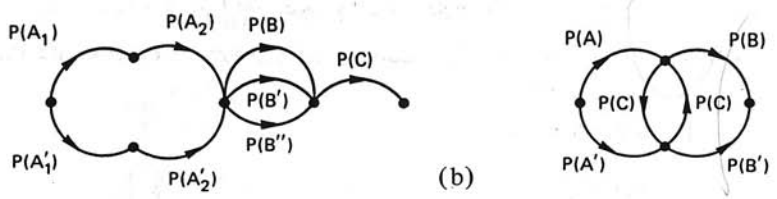
$$R_A R_C = 1 - (1 - R_{AC})(1 - R_{BC}R_{AB}).$$

Dit zijn drie vergelijkingen met drie onbekenden. Oplossing daarvan geeft de eerder gegeven uitdrukkingen. Probeer deze methode eens op het netwerk van figuur 6.8b.

6.9.2. Paden-sneden methode

Zoals we reeds in paragraaf 5.1 hebben uitgelegd, kunnen we een katastrofaal faalmodel zien als een overdrachtsmodel; zolang er nog minstens één verbindingsweg van de ingang naar de uitgang blijft bestaan functioneert het systeem goed. De paden-sneden methode gaat dan ook uit van een volledige inventarisatie van alle geheel of gedeeltelijk verschillende paden die van de ingang naar de uitgang door het bedrijfszekerheidsmodel zijn te volgen.

In paragraaf 6.7 is dat op een weinig systematische wijze gedaan. Voor het systematisch traceren van alle mogelijke paden zullen wij zoals toegezegd in paragraaf 5.1 de grafentheorie gebruiken. In figuur 6.11 is de graafpresentatie gegeven van de structuren uit de figuren 6.8a en 6.8b. De takoverdracht is de bedrijfszekerheid van de desbetreffende component.



Figuur 6.11. Bedrijfszekerheidsgrafen van de beide systemen in figuur 6.8.

Er zijn minstens evenveel takken als er componenten zijn. Er kunnen meer takken zijn (zie figuur 6.11b), namelijk als een takoverdracht in verschillende paden voorkomt en derhalve herhaald moet worden. Een pad (*tie set*) is nu een verzameling van de takken die samen een verbinding tussen de ingang en de uitgang vormen. Interessant zijn daarbij vooral de *minimale paden*, dat wil zeggen de paden bestaande uit het kleinste aantal takken. Als er geen knooppunt meer dan één keer doorlopen wordt, is het bijbehorende pad een minimumpad. Als er n van zulke minimumpaden T_i zijn ($i = 1, 2, \ldots, n$), is de systeembedrijfszekerheid:

$$R = P(T_1 \cup T_2 \cup T_3 \ldots T_n).$$

Een snede (*cut set*) is een groep takken die, als ze uit de graaf verwijderd zouden worden, de overdracht van de ingang naar de uitgang zouden

onderbreken. Een *minimumsnede* bevat een minimum aantal takken; er ontstaat reeds een systeemfout als er een minimumsnede uit de graaf wordt verwijderd. Als er m van zulke minimumsneden C_i zijn (i = 1, 2, 3, ... , m), dan is de systeemfaalkans:

$$F = P(\overline{C}_1 \cup \overline{C}_2 \ldots . \overline{C}_m),$$

als $\overline{C}_1$ aangeeft dat C_1 gefaald heeft.
De paden-sneden methode geeft een efficiënte manier van berekenen indien er geen afhankelijke fouten in een systeem voorkomen. We zullen de methode laten zien in het volgende voorbeeld.
We nemen daartoe de bedrijfszekerheidsgraaf van figuur 6.11b. We kunnen daarin verscheidene paden en sneden aanwijzen (zie tabel 6.4).

	Paden		Sneden
T_1:	AB	C_1:	AA′
T_2:	A′B′	C_2:	BB′
T_3:	ACB′	C_3:	ACA′
T_4:	A′CB	C_4:	ACB′
T_5:	ACCB	C_5:	A′CB
		C_6:	BCB′

Tabel 6.4. Inventarisatie van alle paden en sneden uit figuur 6.11b.

Duidelijk zal zijn dat het pad T_5 geen minimumpad is, evenals de sneden C_3 en C_6 geen minimumsneden zijn.
Uit het bovenstaande volgt:

$$R = P(T_1 + T_2 + T_3 + T_4) =$$
$$= P(AB + A'B' + ACB' + A'CB)$$

en:

$$F = 1 - R = P(\overline{C}_1 + \overline{C}_2 + \overline{C}_4 + \overline{C}_5) =$$
$$= P(\overline{A}\overline{A}' + \overline{B}\overline{B}' + \overline{A}\overline{C}\overline{B}' + \overline{A}'\overline{C}\overline{B}).$$

N.B.: Als er ten onrechte toch een of meer niet-minimumpaden of -sneden in deze uitdrukkingen worden opgenomen blijft het eindresultaat gelijk: niet-minimumpaden en -sneden dragen niet bij tot R respectievelijk F.

Belangrijk voor een correcte uitdrukking voor R of F is dat *alle* minimumpaden en *alle* minimumsneden in rekening zijn gebracht. We kunnen dus stellen dat R en F verkregen worden uit de *volledige verzameling van minimum-paden en -sneden* van de bedrijfszekerheidsgraaf die behoort bij het systeem.

De bovenstaande uitdrukkingen zijn algemeen te herschrijven in de vorm:

$$R = P(\sum_{i=1}^{n} T_i) = 1 - F = 1 - P(\sum_{i=1}^{m} \overline{C}_i),$$

$$P(\sum_{i=1}^{n} T_i) = P(T_1) + P(T_2) + \ldots + P(T_n) - [P(T_1 T_2) + \ldots$$
$$\ldots + P(T_{n-1} T_n)] + \ldots + (-1)^{n-1} [P(T_1 T_2 \ldots T_n)].$$

Men kan de uitdrukking voor F zelf eenvoudig opstellen.

De bovenstaande uitdrukkingen voor R en F kunnen verder worden uitgeschreven. Als we aannemen dat de elementaire gebeurtenissen A, A', B, B' en C stochastisch onafhankelijk zijn, kunnen we de kans op de doorsnede schrijven als het produkt van de kansen. Dit geeft voor dit voorbeeld dezelfde uitdrukkingen als we reeds in paragraaf 6.7 hebben gegeven.
Het uitschrijven van de bovenstaande uitdrukkingen kunnen we als volgt aangeven:

$$R = R_0 - R_1 + R_2 - R_3 + \ldots$$

Hierin is R_0 de som van de bedrijfszekerheden van alle voorwaartse minimumpaden T_i (zonder lus) dus:

$$R_0 = P(AB) + P(A'B') + P(ACB') + P(A'CB).$$

R_1 is de som van de bedrijfszekerheden van alle subgrafen met *één lus* (zie figuur 6.12):

$$R_1 = P(ABB'C) + P(ABB'A') + P(ACA'B') + P(ABA'C) + P(A'B'CB).$$

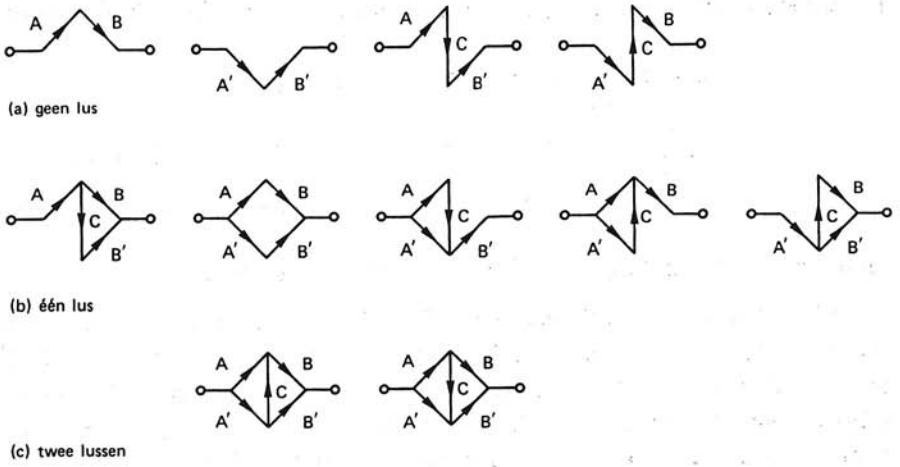
Evenzo is R_2 de som van de bedrijfszekerheden van alle subgrafen met *twee lussen*:

$$R_2 = P(ABA'B'C) + P(ABA'B'C).$$

Drie lussen komen niet voor. Dus $R_3 = 0$. Met:

$$R = \sum_{i=0}^{n} (-1)^i R_i,$$

waarin n het maximale aantal lussen en R_i de som van de bedrijfszekerheden van alle subgrafen met i lussen is, kan vervolgens de systeembedrijfszekerheid R zonder meer worden opgeschreven.



Figuur 6.12. Subgrafen in de graaf van figuur 6.11b.

6.9.3. Decompositiemethode

Het theorema van Bayes voor twee gebeurtenissen A en B luidt:

$$P(A) = \frac{P(AB)}{P(B \mid A)},$$

of:

$$P(AB) = P(A)\,P(B|A) = P(B)\,P(A|B).$$

We kunnen dit *conditionele kanstheorema* gebruiken bij het bepalen van de bedrijfszekerheid van complexe systemen. Daartoe splitsen we in het systeem een component (of groep van componenten) af die een sleutelpositie in de structuur van het bedrijfszekerheidsmodel van het systeem vervult. De gebeurtenis dat deze component goed functioneert duiden we met X aan; de complementaire gebeurtenis met $\overline{X}$. Evenzo is S de gebeurtenis dat het totale systeem goed functioneert, terwijl $\overline{S}$ de complementaire gebeurtenis daarvan is. Dan geldt:

$$R = P(S) = P(X)\,P(S|X) + P(\overline{X})\,P(S|\overline{X}).$$

Evenzo is de faalkans gegeven door:

$$F = P(\overline{S}) = P(X)\,P(\overline{S}|X) + P(\overline{X})\,P(\overline{S}|\overline{X}).$$

Het bewijs is eenvoudig. Met het theorema volgt:

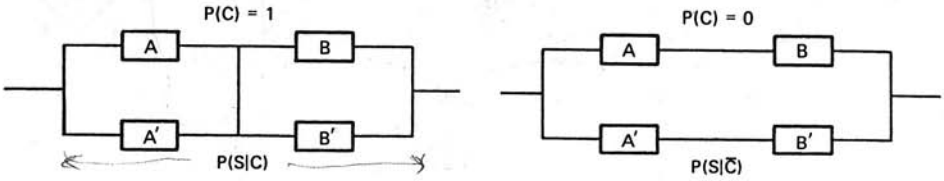
$$R = P(XS) + P(\overline{X}S) = P(S)$$

$$F = P(X\overline{S}) + P(\overline{X}\overline{S}) = P(\overline{S}) \qquad \text{Q.E.D.}$$

Voor het brugnetwerk van figuur 6.8b geldt bijvoorbeeld als we de component C afzonderen als sleutelcomponent:

$$R = P(S) = P(C)\,P(S|C) + P(\overline{C})\,P(S|\overline{C}).$$

Hierin is $P(\overline{C}) = 1 - P(C)$ en zijn de twee conditionele kansen uit figuur 6.13 te bepalen.



Figuur 6.13. Decompositiemethode toegepast op de brugstructuur van figuur 6.8b.

$$P(S|C) = \{P(A) + P(A') - P(AA')\}\{P(B) + P(B') - P(BB')\},$$

$$P(S|\overline{C}) = P(AB) + P(A'B') - P(AA'BB').$$

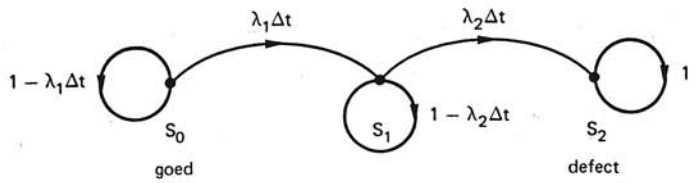
Deze decompositiemethode kan herhaalde malen achtereen worden toegepast en leidt tenslotte tot eenvoudige serie- en parallelnetwerken. De moeilijkheid bestaat daarin de juiste keuze van sleutelcomponenten te maken. Dit zijn in het algemeen die componenten die verwijderd moeten worden om eenvoudige berekenbare structuren over te houden.

6.9.4. Toestandsruimtemethode

De toestandsruimtemethode (die veronderstelt dat het faalproces kan worden opgevat als een Markovproces) is een erg algemene methode die meer gevallen aan kan dan welke andere methode ook. Deze methode kan gebruikt worden voor systemen met componenten die stochastisch onafhankelijk falen, maar ook voor afhankelijke fouten. 'Common-cause'-fouten zijn dan ook eenvoudig te representeren. Tevens kan de methode reparatie in rekening brengen. Verder ontmoet men geen moeilijkheden van theoretische aard als men componenten met meer dan één faalwijze wil beschrijven.

Zoals we reeds in paragraaf 5.3 hebben gezien bij de introductie van het Markov faalmodel, kennen we het systeem een discreet en eindig aantal toestanden toe die onderling disjunct zijn. Alle toestanden waarin het systeem in de praktijk kan geraken moeten ook in het model vertegenwoordigd zijn. Men kan door het introduceren van extra toestanden (*dummy states*) ook op eenvoudige wijze tijdafhankelijke hazard functies z(t) representeren mits die ontstaan gedacht kunnen worden als de hazard van systemen opgebouwd uit elementen met een constante failure rate λ.

We hebben van deze rekenmethode reeds bij de introductie in paragraaf 5.3 een voorbeeld gegeven. Wanneer we ons beperken tot een Markovmodel met constante failure rates λ_i kan de oplossing voor de Laplace-getransformeerde van de kans $P_{S_i}(t)$ dat het systeem ten tijde t in de toestand S_i is, als volgt gevonden worden. We gaan gemakshalve uit van het in figuur 6.14 getekende systeem met drie toestanden.



Figuur 6.14. Markovdiagram van een systeem met drie toestanden en constante failure rates.

De bijbehorende differentiaalvergelijkingen zijn:

$$\frac{dP_{S_0}(t)}{dt} + \lambda_1 P_{S_0}(t) = 0,$$

$$\frac{dP_{S_1}(t)}{dt} + \lambda_2 P_{S_1}(t) - \lambda_1 P_{S_0}(t) = 0,$$

$$\frac{dP_{S_2}(t)}{dt} - \lambda_2 P_{S_1}(t) = 0.$$

De overgangsmatrix U is dan:

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ -\lambda_1 & \lambda_2 & 0 \\ 0 & -\lambda_2 & 0 \end{bmatrix}$$

De Laplace-getransformeerden waarin de beginvoorwaarden $P_{S_0}(0)$, $P_{S_1}(0)$ en $P_{S_2}(0)$ zijn gesubstitueerd, geven:

$$(s + \lambda_1)P_{S_0}(s) + 0P_{S_1}(s) + 0P_{S_2}(s) = P_{S_0}(0),$$

$$-\lambda_1 P_{S_0}(s) + (s + \lambda_2)P_{S_1}(s) + 0P_{S_2}(s) = P_{S_1}(0),$$

$$0P_{S_0}(s) + -\lambda_2 P_{S_1}(s) + sP_{S_2}(s) = P_{S_2}(0),$$

of in matrixnotatie:

$$\begin{bmatrix} s+\lambda_1 & 0 & 0 \\ -\lambda_1 & s+\lambda_2 & 0 \\ 0 & -\lambda_2 & s \end{bmatrix} \cdot \begin{bmatrix} P_{S_0}(s) \\ P_{S_1}(s) \\ P_{S_2}(s) \end{bmatrix} = \begin{bmatrix} P_{S_0}(0) \\ P_{S_1}(0) \\ P_{S_2}(0) \end{bmatrix}.$$

De eerste matrix hier zullen we aanduiden met A.
Wanneer we aannemen dat als beginvoorwaarde geldt:

$$P_{S_0}(0) = 1 \text{ en } P_{S_1}(0) = P_{S_2}(0) = 0,$$

dan is slechts de eerste kolom van de inverse A-matrix van belang.
Dit geeft:

$$A^{-1} = \begin{bmatrix} \frac{1}{s+\lambda_1} & - & - \\ \frac{\lambda_1}{(s+\lambda_1)(s+\lambda_2)} & - & - \\ \frac{\lambda_1\lambda_2}{s(s+\lambda_1)(s+\lambda_2)} & - & - \end{bmatrix}.$$

Het resultaat is dus:

$$P_{S_0}(s) = \frac{1}{s+\lambda_1},$$

$$P_{S_1}(s) = \frac{\lambda_1}{(s+\lambda_1)(s+\lambda_2)},$$

$$P_{S_2}(s) = \frac{\lambda_1\lambda_2}{s(s+\lambda_1)(s+\lambda_2)}.$$

De terugtransformatie levert:

$$P_{S_0}(t) = e^{-\lambda_1 t},$$

$$P_{S_1}(t) = \frac{\lambda_1}{\lambda_1 - \lambda_2}(e^{-\lambda_2 t} - e^{-\lambda_1 t}),$$

$$P_{S_2}(t) = 1 - P_{S_0}(t) - P_{S_1}(t).$$

De bedrijfszekerheid R(t) van het systeem is de som van de kansen dat het systeem in een goede toestand verkeert (de toestanden zijn immers disjunct); neem aan dat dit toestanden S_0 en S_1 zijn, dan:

$$R(t) = \sum_{i=0}^{1} P_{S_i}(t) = \frac{\lambda_1}{\lambda_1 - \lambda_2} e^{-\lambda_2 t} - \frac{\lambda_2}{\lambda_1 - \lambda_2} e^{-\lambda_1 t}.$$

De gemiddelde levensduur MTTF van een systeem kan, uitgaande van het

Markovmodel, op verschillende manieren berekend worden. Wanneer zowel de gemiddelde levensduur als de bedrijfszekerheid berekend dienen te worden, dan ligt het voor de hand om eerst de R(t)-curve te berekenen en deze daarna te integreren volgens:

$$\text{MTTF} = \lim_{T\to\infty} \int_0^T R(t)\,dt.$$

Is men echter alleen geïnteresseerd in de gemiddelde levensduur dan is de procedure aanzienlijk te bekorten. Om te beginnen is het mogelijk om de inverse Laplace-transformatie te vermijden omdat volgens de begin-eindwaarde stelling geldt:

$$\text{MTTF} = \lim_{T\to\infty} \int_0^T R(t)dt \equiv \lim_{s\to 0} R(s) = \lim_{s\to 0} \sum_{i=k}^{m} P_{S_i}(s),$$

waarbij gesommeerd wordt over alle goede toestanden S_k t/m S_m van het systeem.
Verder blijkt het mogelijk om de Laplace transformatie in zijn geheel te vermijden. Om dit aan te tonen gaan we uit van het stelsel Laplace-vergelijkingen dat in matrix notatie weergegeven kan worden als:

$$[s\cdot I + U][P_{S_i}(s)] = [P_{S_i}(0)].$$

Als we nu zowel de linker- als de rechterzijde van deze vergelijking integreren (vermenigvuldigen met $\frac{1}{s}$) en daarna de begin-eindwaardestelling toepassen dan gaat de vergelijking over in:

$$\lim_{s\to 0} [s P_{S_i}(s)] + U\cdot \lim_{s\to 0} [P_{S_i}(s)] = [P_{S_i}(0)].$$

Omdat geldt:

$$\lim_{s\to 0} [s P_{S_i}(s)] = \lim_{t\to\infty} [P_{S_i}(t)] = [P_{S_i}(\infty)]$$

en

$$\lim_{s\to 0} [P_{S_i}(s)] = \lim_{T\to\infty} [\int_0^T P_{S_i}(t)\,dt] = [\theta_{S_i}],$$

waarbij θ_{S_i} de gemiddelde verblijftijd van het systeem in toestand S_i voorstelt, kunnen we het stelsel vergelijkingen herschrijven als:

$$U\cdot[\theta_{S_i}] = [P_{S_i}(0)] - [P_{S_i}(\infty)].$$

De eindwaarde vector $[P_{S_i}(\infty)]$ is echter alleen bekend als alle absorberende toestanden (faaltoestanden) samengevoegd worden tot één nieuwe

down-toestand. Dit is voor bedrijfszekerheids- en MTTF berekeningen zonder meer aan te bevelen omdat dan het aantal vergelijkingen kleiner is. Het is mogelijk om ook de eindwaarde vector te vermijden als we bedenken dat de absorberende toestanden op geen enkele wijze invloed hebben op de goede toestanden van het systeem: na falen kan het systeem nooit meer in een goede toestand terecht komen. We kunnen daarom die rijen en kolommen van de overgangsmatrix en die rijen van de vectoren schrappen waarin de absorberende toestanden voorkomen. Dit levert de volgende gereduceerde vergelijking op:

$$U'[\theta_{S_i}]' = [P_{S_i}(0)]'.$$

Deze kan ook direct uit het Markovmodel opgesteld worden. Voor het systeem uit figuur 6.14 geldt bijvoorbeeld:

$$\begin{bmatrix} \lambda_1 & 0 \\ -\lambda_1 & \lambda_2 \end{bmatrix} \cdot \begin{bmatrix} \theta_0 \\ \theta_1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

Hieruit volgt:

$$\theta_0 = \frac{1}{\lambda_1} \text{ en } \theta_1 = \frac{1}{\lambda_2},$$

zodat dit systeem een gemiddelde levensduur heeft van:

$$\text{MTTF} = \theta = \theta_0 + \theta_1 = \frac{1}{\lambda_1} + \frac{1}{\lambda_2}.$$

Opgaven

6.1. Wat verstaan we in de bedrijfszekerheidstechniek onder 'afhankelijkheid'? Noem twee soorten afhankelijke fouten en geef van beide een voorbeeld.

6.2. Bewijs dat voor een actief redundant m-uit-n systeem, bestaande uit identieke units met failure rate λ, geldt:

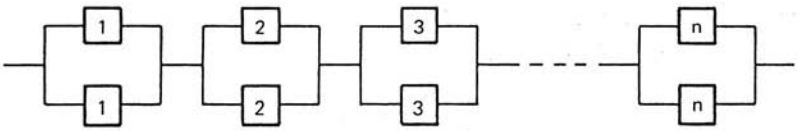
$$\text{MTTF} = \frac{1}{\lambda} \sum_{k=m}^{n} \frac{1}{k}.$$

6.3. Een bepaalde component heeft in de aan-toestand een failure rate van $4 \cdot 10^{-8}$/h en in de uit-toestand $4 \cdot 10^{-9}$/h. Gemiddeld over de levensduur van deze component wordt hij slechts 25% van de tijd gebruikt (in de aan-toestand).
Wat is de effectieve failure rate van deze component?

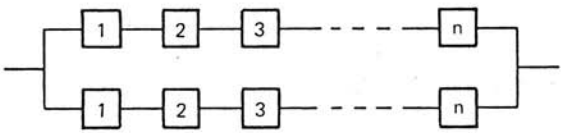
6.4. a. Leidt de bedrijfszekerheid R(t) af van een n-voudig, actief-redundant systeem met een redundantiegraad 1, als de units alle identiek zijn en een bedrijfszekerheid $e^{-\lambda t}$ hebben. Fouten treden stochastisch onafhankelijk op.

b. Bepaal uit hierboven gevonden uitdrukking voor R(t) de gemiddelde levensduur θ van dit systeem.

6.5. Een systeem bestaat uit n identieke units in serie die onafhankelijk van elkaar kunnen falen. De bedrijfszekerheid van één unit is R.
Het systeem wordt op de onderstaande twee manieren a en b redundant gemaakt. De systeembedrijfszekerheid is dan R_a, respectievelijk R_b.



(a)



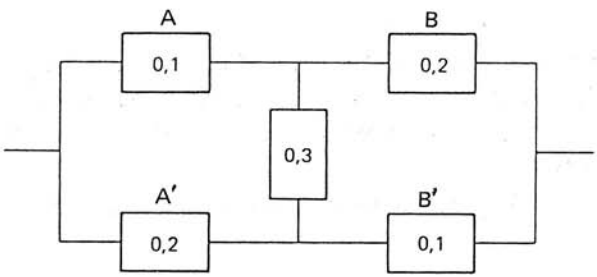
(b)

a. Hoe groot is $\lim_{R \to 1} \frac{R_a}{R_b}$?

b. Hoe groot is $\lim_{R \to 0} \frac{R_a}{R_b}$?

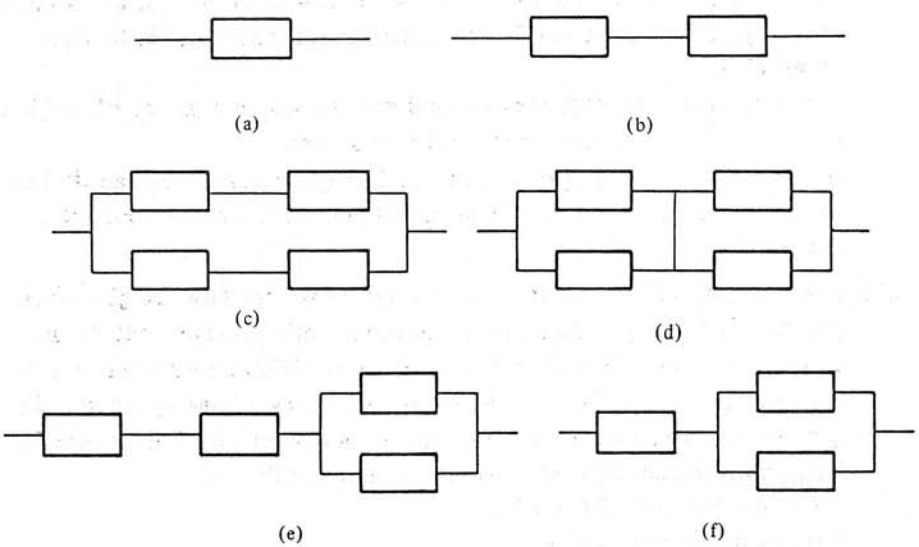
c. Schets $\frac{R_a}{R_b}$ voor n = 3 als functie van R.

6.6. a. Bereken de kans op falen van een systeem met het onderstaande catastrofale faalmodel. (In de blokken is de *faal*kans aangegeven; falen geschiedt stochastisch onafhankelijk.)



b. Levert het aanwezig zijn van de 'dwarstak' in het bovenstaande faalmodel altijd een verbetering van het systeem op? (De bijbehorende faalkans is altijd kleiner dan 1.)

6.7. Men beschikt over vier onderling identieke waterpompen, elk met bedrijfszekerheid R_o ($0 < R_o < 1$) en een opvoerhoogte van 5 meter. Deze pompen worden gebruikt in een systeem waarin het water 7 meter moet worden opgevoerd.
Van zes verschillende configuraties is hieronder het catastrofale faalmodel gegeven. Rangschik de configuraties naar opklimmende systeembedrijfszekerheid R_a, R_b, ..., R_f.



N.B. Elk blokje stelt één pomp voor.

6.8. Een redundant systeem zonder reparatie bestaat uit twee identieke units met een constante hazard rate λ.
a. Teken het Markov-diagram voor het geval dat het systeem *actief*-redundant is en voor het geval dat het systeem *passief*-redundant is.
b. Beredeneer aan de hand van beide Markov-diagrammen hoe groot de gemiddelde levensduur voor elk van bovenstaande systemen is.

6.9. Een computersysteem voor een procesregeling bestaat uit twee actief redundante computers die ieder voor zich in staat zijn het proces te regelen. De beide computers zijn aangesloten op het elektriciteitsnet. De volgende onafhankelijke fouten kunnen optreden in dit systeem:

Faalwijze	Failure rate
computer I faalt	λ_1
computer II faalt	λ_2
het elektriciteitsnet faalt	λ_N

Stel voor dit systeem het Markov-diagram op, waarbij is aangenomen dat er geen reparatie mogelijk is. Geef duidelijk aan wat de verschillende toestanden voorstellen en wat de begin- en 'down' toestand(en) is (zijn).

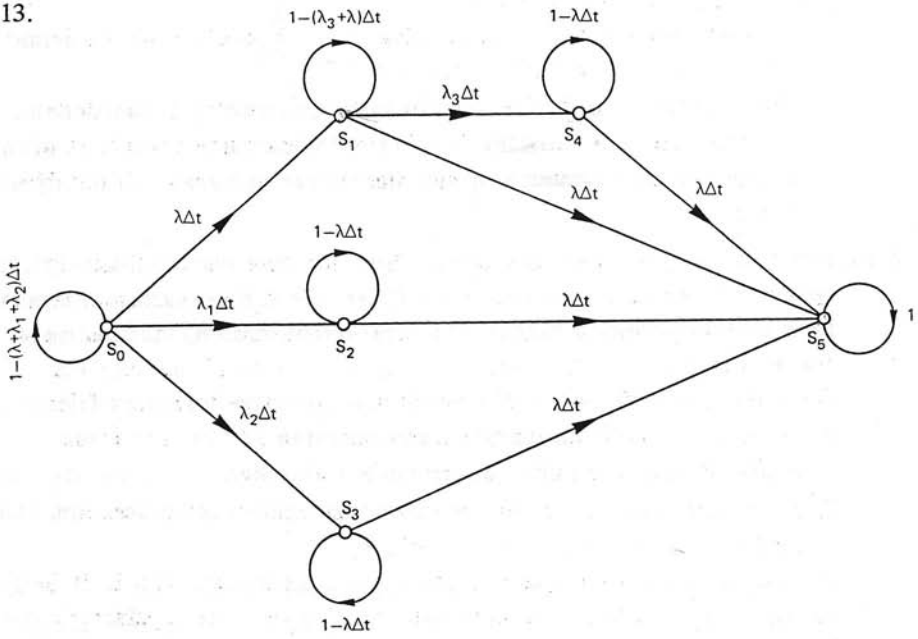
6.10. Een systeem bestaat uit n identieke units in serie die onafhankelijk van elkaar kunnen falen. Voor elke unit geldt K = f(R), waarin f een monotoon stijgende functie is (K = gegeneraliseerde kosten, R is bedrijfszekerheid).
Gevraagd wordt de bedrijfszekerheid van dit systeem groter of gelijk aan de waarde R_s te maken tegen minimale kosten.
Hoe groot is na deze optimalisatie de bedrijfszekerheid R_i van de i-de unit (i = 1,2,...,n) en wat zijn de totaal gemaakte kosten voor dit systeem?

6.11. Een stand-by redundant systeem is opgebouwd uit twee gelijke units. Een unit die geactiveerd is, heeft de failure rate λ_a. Een unit die in de stand-by mode staat, heeft, zolang zij in die stand-by mode staat, een failure rate λ_o. Het foutdetectie- en omschakelingsorgaan van dit systeem kan weigeren de tweede unit te activeren met failure rate λ_s. De gebeurtenissen zijn stochastisch onafhankelijk.
- Stel het Markov-diagram op.
- Definieer de toestanden.
- Geef de overgangswaarschijnlijkheden aan.
- Geef het eenvoudigste Markov-diagram van dit systeem aan (definieer hiervan ook de toestanden en geef de overgangswaarschijnlijkheden aan).

6.12. Om een bepaalde bedrijfszekerheid te kunnen garanderen blijkt het noodzakelijk een systeem tweevoudig redundant uit te voeren. Er kan gekozen worden uit slechts twee mogelijkheden, namelijk een twee-unit actief-redundant systeem of een twee-unit passief-redundant systeem. Bij de passief-redundante uitvoering is het noodzakelijk een schakelaar aan te brengen die het overschakelen naar de andere unit mogelijk maakt. Deze schakelaar heeft één faalwijze, namelijk dat hij weigert over te schakelen naar de andere unit (kleven). Als de failure rate van de actieve unit λ is, een passieve unit niet kan falen en de failure rate van de faalwijze van de schakelaar λ_s is, wat is dan de

minimale waarde van λ_s waarbij het actief-redundante systeem beter is dan het passief-redundante systeem?

6.13.



Een systeem zonder reparatie wordt beschreven door het bovenstaande Markov-diagram, waarin S_0 de begintoestand en S_5 de 'system down'-toestand is. Hoe groot is de gemiddelde levensduur (MTTF) van dit systeem? *Aanwijzing: vereenvoudig eerst het Markov-diagram zo ver mogelijk.*

6.14. Een bepaald technisch systeem is een 2-uit-3 actief-redundant systeem bestaande uit drie identieke units met failure rate λ. De units falen onafhankelijk van elkaar.
Gegeven is dat dit systeem 3 keer zo duur is als één unit en een gemiddelde levensduur heeft die slechts $\frac{5}{6}$ is van die van één unit. Weerleg de paradox dat dit systeem slechter is dan één unit; immers de kosten zijn drie keer hoger, de gemiddelde levensduur is korter en er moeten altijd minstens twee units werken, wil het systeem functioneren. Schets bij uw uitleg duidelijk de drie R(t)-curves van 1 unit, van 2 units in serie en van het 2-uit-3 systeem.

6.15. Een aandrijf-aggregaat levert een maximaal vermogen van 10 kW en heeft daarbij een failure rate van $\lambda_m = 4\times10^{-3}$/uur.
Als het aggregaat op zijn nominaal vermogen (7 kW) of daaronder bedreven wordt, heeft het een failure rate van $\lambda_n = 10^{-3}$/uur.

Een bepaalde toepassing vergt 10 kW; daartoe gebruikt men twee identieke aggregaten in een actief-redundante configuratie (*De units falen stochastisch onafhankelijk*).

a. Geef het bijbehorende Markov-diagram en bepaal hieruit de gemiddelde levensduur van dit systeem (MTTF).
b. Hoe groot is de bedrijfszekerheid van dit systeem en geef deze grafisch weer. Geef ook de bedrijfszekerheidscurve van het systeem als dat gerealiseerd zou zijn met slechts één aggregaat (in dezelfde figuur).

6.16. Een beveiligingssysteem bestaat uit drie monitoren aangesloten op één te bewaken proces. Het proces wordt terwille van de veiligheid telkens na een vaste periode afgeschakeld voor onderhoud. Het proces wordt tevens afgeschakeld als er een onveilige situatie wordt aangegeven.
De onderling identieke monitoren kunnen op twee manieren falen:

1. de monitor geeft ten onrechte een onveilige situatie aan (kans hierop is 0,05 gedurende de genoemde periode),
2. de monitor detecteert een onveilige toestand in het proces niet (kans 0,01 gedurende de genoemde periode).

De kosten van een niet-gedetecteerde onveilige situatie zijn f. 25.000,– per keer en van het ten onrechte afschakelen (en weer opstarten) van het proces f. 10.000,– per keer.
Neem aan dat de fouten stochastisch onafhankelijk zijn. Toon met behulp van een berekening aan welke van de volgende strategiën optimaal is:

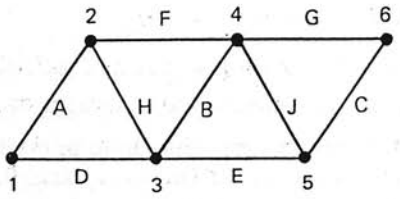
a. als er minstens één monitor een onveilige toestand aangeeft, wordt het proces afgeschakeld;
b. als er minstens twee monitoren een onveilige toestand aangeven, wordt het proces afgeschakeld;
c. pas als alle drie de monitoren een onveilige toestand aangeven, wordt het proces afgeschakeld.

6.17. Bij slurry-transport is het noodzakelijk dat het mengsel in de transportpijpen in beweging blijft, omdat anders verstopping optreedt. Daarom gebruikt men drie pompen in een 2-uit-3 passief-redundante configuratie. Om de benodigde capaciteit te halen is het noodzakelijk dat *twee* pompen functioneren. In het geval dat slechts één pomp functioneert wordt de capaciteit niet gehaald, maar er treedt dan geen verstopping in de pijpen op.
De pompen zijn identiek en ze falen stochastisch onafhankelijk. De failure rate λ is constant bij normaal gebruik; wanneer er nog slechts één pomp functioneert dan wordt de failure rate van deze pomp 2λ.

a. Wat is hiervan de MTTF, voor de fout dat de capaciteit niet bereikt wordt?

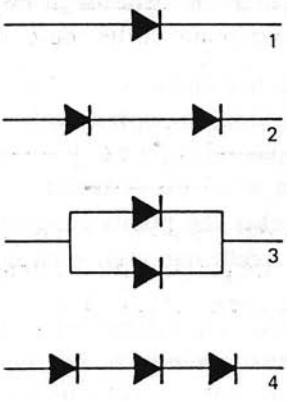
b. De tweede functie van het systeem is het in beweging houden van het mengsel. Hiervoor volstaat één pomp. Wat is de MTTF van deze functie bij bovenstaande configuratie?

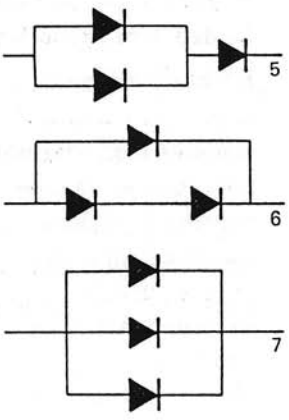
6.18. Zes computersystemen zijn met elkaar verbonden volgens het onderstaande netwerk. Elke lijn kan in beide richtingen worden gebruikt en heeft een onafhankelijke faalkans $p_0 = 0{,}1$. Bereken de *kans* dat er een succesvolle informatie-uitwisseling kan optreden tussen de computers 1 en 4. *Aanwijzing: vereenvoudig eerst het netwerk zoveel mogelijk en pas daarna de decompositiemethode toe.*



6.19. In een elektronische schakeling is een diodefunctie benodigd. Om de bedrijfszekerheid van de diodefunctie te verhogen wil men actieve redundantie toepassen waarbij echter niet meer dan drie dioden gebruikt mogen worden. De gebruikte dioden kunnen zowel open fouten als kortsluitfouten vertonen; de kansen hierop zijn:
- open fout $p_o = 0{,}02$;
- kortsluitfout $p_k = 0{,}01$.

De dioden falen stochastisch onafhankelijk. Geef aan voor welke van de onderstaande schakelingen de *bedrijfszekerheid maximaal* is en motiveer uw antwoord.



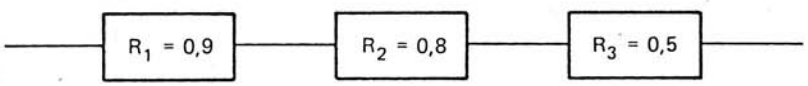


6.20. Een passief-redundant systeem bestaat uit twee units en een schakelaar, die alle onafhankelijk van elkaar kunnen falen. Zodra de eerste unit faalt wordt er overgeschakeld naar de tweede unit; beide units hebben een failure rate λ. De schakelaar kan falen op de volgende manieren:
- de schakelaar kan blijven kleven waardoor overschakelen niet meer mogelijk is. De failure rate voor deze gebeurtenis is λ_k.
- door stoorpulsen kan het schakelmechanisme geactiveerd worden waardoor de schakelaar, indien unit 1 nog functioneert, overschakelt naar de tweede unit. De failure rate waarmee deze stoorpulsen optreden bedraagt λ_s.

a. Teken het Markov-diagram. Geef duidelijk de overgangen en de toestanden aan.
b. Bereken de MTTF van het systeem.

6.21. Het onderstel van een vliegtuig wordt hydraulisch bediend. Wanneer de druk wegvalt doet een waarschuwingssysteem daarvan melding in de stuurhut. Enerzijds kan het waarschuwingssysteem weigeren het wegvallen van de druk te signaleren (met een kans 0,1) en anderzijds kan ten onrechte een waarschuwing gegeven worden (eveneens met een kans 0,1). Men wil niet-adaptieve meerderheidskeuzeredundantie toepassen waarbij het systeem maximaal viervoudig uitgevoerd mag worden; hierbij wordt in twijfelgevallen (evenveel fout- als goedmeldingen) geen alarm gegeven.
Wat is de beste systeemkeuze indien men een zekerheid van 94 % wenst te behalen dat het wegvallen van de druk gesignaleerd wordt? Motiveer uw antwoord duidelijk!

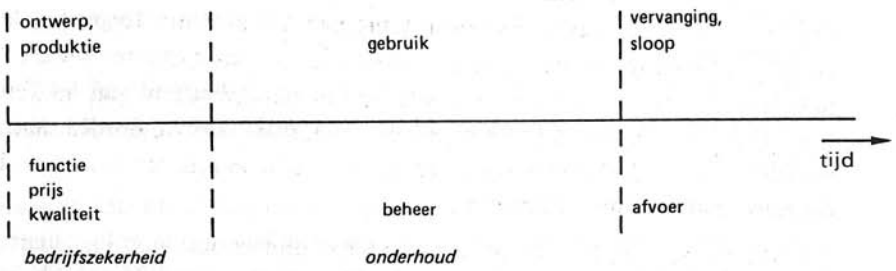
6.22. In de onderstaande figuur is een seriesysteem afgebeeld dat opgebouwd is uit drie componenten. De bedrijfszekerheden van de componenten staan in de blokjes vermeld. Men vindt de systeembedrijfszekerheid te laag, en wil deze opvoeren tot 0,8 of hoger tegen minimale investeringskosten. Om dit te bereiken past men actieve redundantie toe op componentniveau.



Als gegeven is dat alle componenten even duur zijn en dat het parallelschakelen van componenten geen extra kosten met zich meebrengt, bepaal dan de *optimale configuratie* (catastrofale faalmodel).

7. Onderhouden systemen

Zoals we reeds in paragraaf 6.1 hebben besproken is een onderhouden systeem onderhoudbaar en wordt ook metterdaad onderhouden. Dit onderhouden geschiedt door menselijk ingrijpen. Alvorens we verder ingaan op dit onderhoud is het zinvol een onderhouden systeem in een wat breder perspectief te bezien.
Zoals in figuur 7.1 is aangegeven, kan de totale *levenscyclus* van een systeem worden opgedeeld in een aantal fasen. Het 'leven' van een technisch systeem begint met het ontwerp en de fabricage van het systeem. Daarbij baseert men zich op de behoeften die bijvoorbeeld gebleken zijn uit een marktverkenning. In dit stadium worden belangrijke zaken vastgelegd: de functie wordt gespecificeerd, de prijs wordt bepaald, evenals de kwaliteit en de bedrijfszekerheid. Daarna begint de gebruiksfase, die tenslotte na een hopelijk lang en nuttig leven eindigt met de vervanging en het afvoeren van het systeem.



Figuur 7.1. De totale levenscyclus van een technisch systeem.

Nu zijn veel systemen zo kostbaar, dat wil zeggen de geïnvesteerde aanschaf kosten K_a uit figuur 6.9 zijn zo hoog, dat het economisch attractief is *onderhoud* te plegen tijdens de gebruiksduur van het systeem, omdat dan het geïnvesteerde kapitaal K_a over een langere periode kan worden afgeschreven. De keerzijde van de medaille is dat hier ook kosten (de onderhoudskosten K_o) aan verbonden zijn.
Onderhoud is vooral bij de complexere technische systemen arbeidsintensief en vraagt hooggeschoold en dus duur personeel (niet iedereen repareert zo maar even een videorecorder, laat staan een radarsysteem). De onderhoudskosten K_o gesommeerd over de totale gebruiksduur van het systeem kunnen dan ook zeer wel een veelvoud zijn van de vervangingswaarde van het systeem. Om de onderhoudskosten laag te houden, zal

het systeem onderhoudsbewust moeten zijn ontworpen. Dit kan onder andere door het systeem modulair op te bouwen, een goede toegankelijkheid van de systeemdelen te garanderen, automatische foutlocatie in te bouwen en testprogramma's en dergelijke mee te leveren.
Onderhoudsbewust ontwerpen is er op gericht de reparatie te vereenvoudigen en de reparatieduur te bekorten. Daarnaast komen ook nog andere aspecten naar voren. Men tolereert meestal wel enige fouten, als het maar veilige fouten zijn. 'Fail-safe'-concepties en de bijbehorende constructies en schakelingen moeten dus in de ontwerpfase al in het systeem zijn voorzien.
Om het systeem in de gebruiksfase zonder al te veel hinder te kunnen gebruiken, is een goed *gepland onderhoud* van belang. Er moeten voldoende reserve-onderdelen zijn, er moeten bekwame, met spoed inzetbare reparateurs aanwezig zijn, enzovoort. Zo'n planning kan bijvoorbeeld leiden tot *getrapt onderhoud*. Daarbij worden in het bedrijf zelf alleen modules vervangen door reserve-modules. Deze worden daarna verzonden om centraal gerepareerd te worden. De eerste trap is *vervanging*; deze kan snel en eenvoudig gebeuren. De tweede trap, de eigenlijke *reparatie*, duurt langer. Bovendien is hiervoor kostbare meetapparatuur en hooggeschoolde mankracht nodig.
Er zitten aan het onderhoud van een systeem dus duidelijk twee aspecten; een *ontwerpaspect* dat in de vormgeving van het systeem tot uiting komt, en een *beheersaspect*, waaraan de beheerder van het systeem tijdens de gehele levensduur aandacht moet besteden. In de navolgende paragrafen zullen wij ons vooral tot dit laatste aspect beperken. We zullen een aantal verschillende onderhoudsstrategieën die een systeembeheerder kan volgen op hun relatieve merites bezien.

Uit het bovenstaande valt op te maken dat onderhoud veel kan kosten, maar niet onderhouden kost nog meer. Het optimum zal liggen bij de laagste totaalkosten (aanschaf èn onderhoud) betrokken op de gehele levensduur van het systeem. Dit optimum wordt aangegeven met de term '*minimum life-cycle cost*'. In de praktijk treft men maar al te vaak uitersten aan. Aan de ene kant te dure systemen die ontworpen zijn onder het motto 'invest now, save later', en aan de andere kant te goedkope systemen die zo onderhoudsbehoeftig zijn dat het onderhoud bijna niet te betalen is. (Na-oorlogse woningbouw, civiele werken waarin veel hout en metaal is verwerkt in plaats van beton.)

7.1. Inleiding

Alle tot dusver behandelde modellen voor de bepaling van de bedrijfszekerheid van een systeem hadden gemeen dat ze geen menselijk ingrijpen

tijdens de gebruiksfase veronderstelden. Systemen waarbij onderhoud niet economisch verantwoord is, zijn hiervan één exponent.

Voorbeeld 7.1
In een tijd (1986) waarin de kosten van een reparateur fl. 50,– per uur bedragen, zal niemand denken aan reparatie van elektronische horloges van fl. 35,–.

Een tweede klasse van niet-onderhoudbare systemen is die waarbij onderhoud niet mogelijk is. Voorbeelden zijn: éénmalig gebruikte ruimtevoertuigen, meetapparatuur die in funderingen en dergelijke wordt ingebouwd of voorgoed in de oceaan wordt neergelaten.

De overige systemen zijn de zogenaamde onderhoudbare systemen.
Onderhoud (ook wel bewaking of 'maintenance' genoemd) is elke vorm van menselijk ingrijpen in een systeem met de bedoeling het systeem in een bruikbare toestand te houden *dan wel (na falen) weer in een bruikbare toestand te brengen.*
In deze omschrijving van wat wij zullen verstaan onder onderhoud valt een aantal zaken op:

- *Menselijk ingrijpen* is essentieel zoals we trouwens ook al in paragraaf 6.1 hebben gezien. Een systeem dat als het ware zichzelf repareert door inwendige redundante subsystemen in te schakelen is daarom nog niet noodzakelijkerwijs een repareerbaar of onderhoudbaar systeem.
- Het systeem, noch de vervangen component(en), behoeven na de reparatie weer 'als nieuw' te zijn. De aangebrachte componenten kunnen bijvoorbeeld door lang liggen in het magazijn slechter geworden zijn. Ook kan de reparateur fouten maken (te heet solderen, moeren te vast of te los aanzetten, en dergelijke) waardoor na de reparatie een tijdinterval met een verhoogde uitvalkans optreedt. Ook kan de reparateur het systeem weer gebruiksgereed hebben gemaakt, maar niet voor bijvoorbeeld alle functies van het systeem of voor de volledige capaciteit van het systeem.
- Naast het weer bruikbaar maken of het bruikbaar houden van een systeem heeft onderhoud ook tot doel de *veilige werking* van het systeem te waarborgen.

In de bovengegeven omschrijving behoeft het systeem niet altijd te falen. Immers, wanneer het een redundant systeem betreft, kan de redundantie meestal gerepareerd worden zonder verlies van de systeemfunctie. Men spreekt dan van *preventief onderhoud*. (Strikt genomen is in het juist genoemde geval het onderhoud preventief op systeemniveau, maar correctief op unit-niveau, daar men wacht tot minstens één van de redundante units heeft gefaald.)

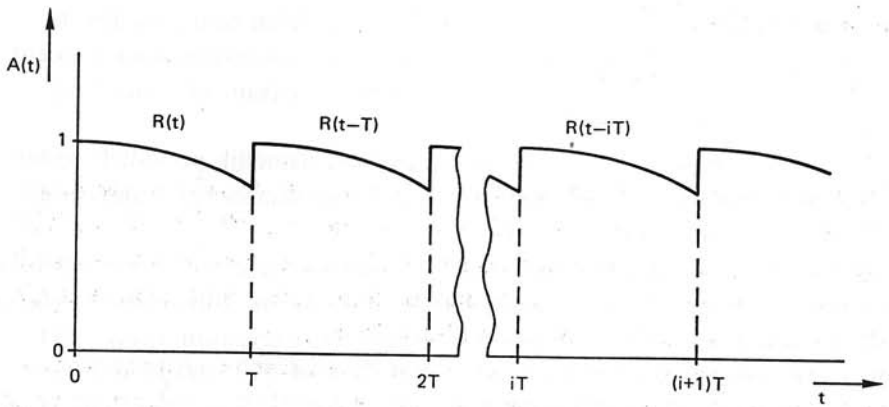
Preventief onderhoud is dus onderhoud vóórdat falen optreedt. Het is profylactisch onderhoud in de zin dat het voor toekomstig falen behoedt. Met dit soort onderhoud zal men niet kunnen volstaan: niet elke fout ziet men aankomen.
Er zijn twee categorieën preventief onderhoud, namelijk periodiek onderhoud en onderhoud dat afhangt van de conditie waarin het systeem verkeert.
Bij *periodiek onderhoud* (scheduled maintenance) geschiedt het menselijke ingrijpen volgens een van te voren vastgesteld schema. Bijvoorbeeld telkens na het verstrijken van een bepaald interval van de levensduurparameter. Een voorbeeld hiervan is het na elke 7 500 km of 500 bedrijfsuren vernieuwen van de olie en het oliefilter.
Bij '*condition-based maintenance*' wordt de onderhoudsbehoefte van een systeem gemeten. Op grond hiervan wordt ingegrepen. Bijvoorbeeld het olie verversen op basis van de verbrandingsprodukten in die olie; lagers vernieuwen op basis van het metaalslijpsel dat zich in de olie bevindt; een machine uitbalanceren wanneer het trillingsniveau te hoog wordt.
Op deze wijze wordt toekomstig onheil in de vorm van een systeemfout (en de daarbij optredende schade door vastlopen, breuk enzovoort) vermeden. Vereiste hiervoor is, dat er meettechnieken zijn voor de conditiedetectie en -bewaking.

7.2. Systemen met preventief onderhoud

We zullen in deze paragraaf veronderstellen dat er aan het beschouwde systeem uitsluitend preventief onderhoud wordt gepleegd. Tenslotte zal het systeem dan toch falen omdat preventief onderhoud geen waterdichte garantie biedt tegen falen van het systeem. We zullen verder de tijd die nodig is voor dit preventieve onderhoud verwaarlozen. We kunnen immers dit onderhoud (meestal) uitvoeren op een van te voren bekend tijdstip wanneer het systeem toch, om andere redenen, niet gebruikt wordt.

7.2.1. Periodiek onderhoud

We zullen, aan de hand van een eenvoudig periodiek onderhoudsmodel, het belang proberen aan te geven van de juiste keuze van het interval T dat ligt tussen opeenvolgende onderhoudsbeurten op t = iT.
Het model bestaat daaruit dat we aannemen dat we de onderhoudsbeurten op t = iT zo grondig (kunnen) doen dat het systeem na zo'n onderhoudsbeurt *als nieuw* is. De beschikbaarheid A(t) van zo'n systeem wordt dan gevormd door een periodieke herhaling in de tijd van het interval (0, T) van de bedrijfszekerheid R(t) van het systeem zonder periodiek onderhoud (zie figuur 7.2). We zijn nu benieuwd naar de gemiddelde levens-



Figuur 7.2. De beschikbaarheid van een systeem met periodiek onderhoud dat het systeem weer in de 'als nieuw'-toestand terugbrengt.

duur θ (tot de eerste fout optreedt). Deze levensduur noemen we ook wel Mean Time To First Failure (MTTFF):

$$\theta = \int_0^\infty R_S(t)\,dt.$$

Hierin is $R_S(t)$ de bedrijfszekerheid van het systeem *met* periodiek onderhoud. Voor het eerste tijdinterval (0,T) is $R_S(t)$ gegeven door:

$$R_S(t) = R(t), \qquad (0 \leqslant t < T).$$

Voor het (i + 1)-de tijdinterval moet het systeem de eerste i intervallen overleefd hebben en bovendien nog het tijdintervalletje (iT,t). We vinden daarom:

$$R_S(t) = R(T)^i R(t - iT), \quad (iT \leqslant t < (i+1)T).$$

We kunnen de levensduurintegraal splitsen in de som van de integralen over het onderhoudsinterval:

$$\theta = \lim_{n\to\infty} \sum_{i=0}^{n} \int_{iT}^{(i+1)T} R_S(t)\,dt.$$

De integraal $R_S(t)$ in aanmerking genomen, kunnen we dit schrijven als:

$$\theta = \lim_{n\to\infty} \sum_{i=0}^{n} \int_0^T R(T)^i R(t)\,dt.$$

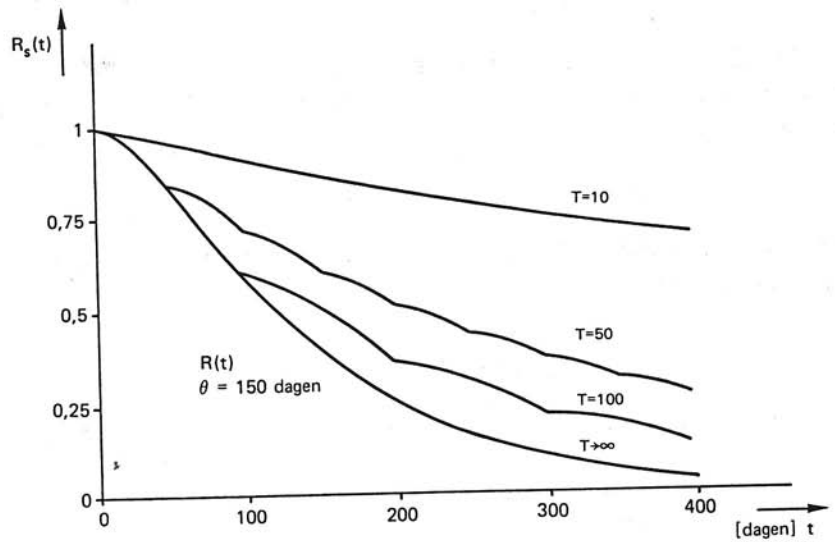
We mogen de constante $R(T)^i$ buiten de integraal halen en vinden dan met gebruik van:

$$\sum_{i=0}^{\infty} x^i = \frac{1}{1-x}$$

voor de MTTFF:

$$\theta = \frac{\int_0^T R(t)\,dt}{1 - R(T)}.$$

We weten reeds dat bij een systeem met een constante failure rate λ, dus een bedrijfszekerheid $R(t) = \exp(-\lambda t)$, periodiek onderhoud zinloos is. Immers alle nog niet gefaalde komponenten zijn als nieuw. De levensduur θ verandert dan ook niet door periodiek onderhoud en blijft gelijk aan $1/\lambda$. Dit volgt ook uit de bovenstaande uitdrukking.
We willen verder opmerken dat we in het bovenstaande geen enkele veronderstelling omtrent R(t) gedaan hebben: we hebben het algemene geval opgelost. In figuur 7.3 hebben we daarom $R_S(t)$ uitgezet voor verschillende onderhoudsperioden. We hebben dat gedaan voor een arbitrair gekozen R(t)-functie. Voor $T \to \infty$ krijgen we deze bedrijfszekerheidsfunctie terug.
Uit dit voorbeeld zien we dat het onderhoudsinterval T een grote invloed heeft op de bedrijfszekerheid $R_S(t)$. Vooral als het eerste onderhoudsinterval eindigt voorbij het vrijwel vlakke gedeelte van de R(t)-curve (lees: als de redundantie van het systeem vrijwel is uitgeput), heeft periodiek onderhoud nauwelijks nog zin. Men heeft te lang gewacht; het systeem is al te ver versleten; de redundantie is op.



Figuur 7.3. De bedrijfszekerheid $R_S(t)$ van een systeem met periodiek onderhoud (elke T dagen), waarna het systeem weer als nieuw is. R(t) is de bedrijfszekerheid van het systeem zonder onderhoud ($T \to \infty$).

Afsluitend nog een algemene opmerking over periodiek onderhoud: na een periodieke onderhoudsbeurt zal een systeem in de praktijk in het algemeen niet 'als nieuw' zijn. Theoretisch geldt dit alleen voor een (redundant) systeem bestaande uit units met een negatief-exponentiële faaldistributie.

Het gevolg van dit zogenaamde *niet perfecte periodieke onderhoud* is dat de curve van het systeem in figuur 7.2 op de tijdstippen iT (i = 1,2, . . .) niet gelijk is aan één, maar kleiner dan één blijft. Zonder reparatie zal de curve zelfs steeds kleiner worden voor toenemende i. Door één en ander zal de systeembedrijfszekerheid $R_S(t)$ dan ook sneller afvallen dan in figuur 7.3 is geschetst.

We kunnen nog op eenvoudige wijze iets over de kosten van periodiek onderhoud ten opzichte van reparatie zeggen. Stel dat de kosten van een periodieke onderhoudsbeurt gemiddeld K_P bedragen. Als men geen preventief onderhoud pleegt en het op reparatie laat aankomen, bedragen de reparatiekosten gemiddeld K_R. Duidelijk zal zijn dat:

$$K_P < K_R,$$

omdat het periodieke onderhoud 'gepland' kan worden, waardoor een betere onderhoudscapaciteitsbezetting mogelijk is. Bovendien sneuvelt er bij falen van een systeem meestal meer dan alleen de primair falende component.
Per eenheid van tijd zijn de kosten voor periodiek onderhoud met periode T dan K_P/T en voor reparatie $K_R/MTBF$.
Voeren we nu de verhouding η in:

$$\eta = \frac{K_P}{K_R} \frac{MTBF}{T},$$

dan is de eis voor (financieel) doelmatig periodiek onderhoud:

$$\eta < 1.$$

Voor een grote prijsverhouding tussen de beide vormen van onderhoud mag de onderhoudsperiode T dus niet (te) klein worden gekozen ten opzichte van de MTBF van het systeem. Al te grote T voert tot een lage bedrijfszekerheid en dus in de praktijk tot additionele reparatiekosten.

7.2.2. Op conditie gebaseerd onderhoud

In het voorgaande hebben we reeds gezien dat veel systemen de zogenaamde *run-to-break*-strategie (gevolgd door reparatie) niet toelaten. Deze zou te veel produktieverlies en onveilige situaties geven, of te kostbaar zijn doordat een machine bijvoorbeeld helemaal vastloopt.

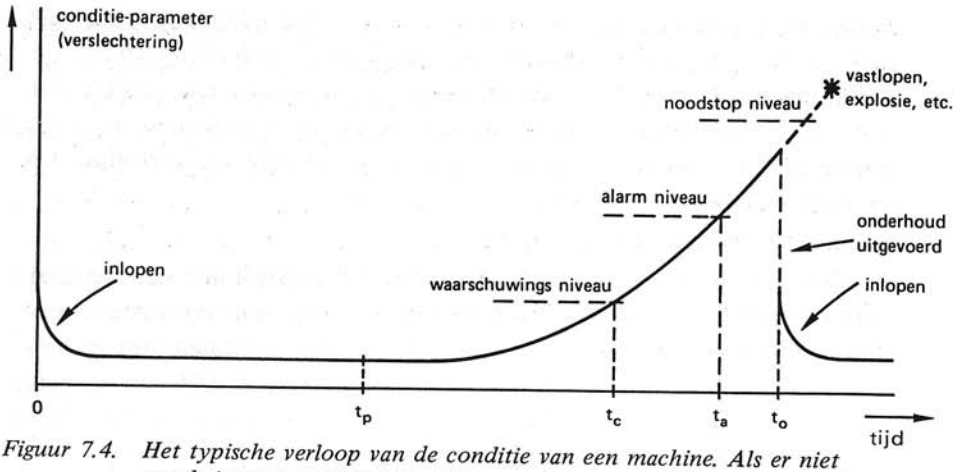
Daar waar we van een systeem (of delen daarvan) toekomstig falen reeds van te voren kunnen voorspellen, heeft preventief onderhoud zin. In de vorige paragraaf hebben we een speciale vorm daarvan, namelijk periodiek onderhoud, nader bezien. Bij *periodiek onderhoud* voorspellen we toekomstig falen gebaseerd op *statistische informatie* omtrent de levensduur van de komponenten.

Voorbeeld 7.2
Onder normale bedrijfsomstandigheden verwachten we met een bepaald type straalmotor moeilijkheden na 15 000 uur. Daarom inspecteren we iedere 5 000 uur met name het hete gedeelte van de straalmotor en vervangen alle verdachte componenten daarvan. Om de 10 000 uur reviseren we de hele motor, behalve de lagedrukcompressor en om de 30 000 uur houden we een volledige motorrevisie.

We zouden natuurlijk veel effectiever onderhoud kunnen doen als we *deterministische informatie* hadden over een toekomstig falen. Dan zouden we geen vaste tijdstippen voor het onderhoud meer nodig hebben maar het onderhoud kunnen aanpassen aan de onderhoudsbehoefte van het systeem. Deze informatie kunnen we (voor veel faalwijzen van een systeem) halen uit een aantal indicatieve parameters van zo'n systeem. Deze parameters zijn dan een maat voor de interne gezondheidstoestand (conditie) van het systeem. In plaats van *'time-based'-onderhoud* kunnen we dan overgaan op *'condition-based'-onderhoud*.
Helaas is het nooit volledig uit te sluiten dat een faalwijze aan de conditiemeting van een systeem ontsnapt. Daarom zal men dan ook meestal periodiek onderhoud en op conditie gebaseerd onderhoud samen uitvoeren.

Voorbeeld 7.3
De straalmotor uit het vorige voorbeeld heeft verschillende vormen van conditiebewaking (condition monitoring). Men meet tijdens bedrijf voortdurend motortemperaturen, brandstofgebruik en trillingsniveau's. Bovendien meet men bij het proefdraaien dat plaatsvindt tijdens een 'shop visit' nog meer indicatieve parameters. Mochten één of meer van deze parameters daar aanleiding toe geven, dan kan de motor tijdens de vlucht gestopt worden of op een lager vermogen worden gebruikt om onmiddelijk na de vlucht een extra onderhoudsbeurt te ondergaan tussen de hierboven geplande periodieke onderhoudsbeurten door.

De conditiemetingen worden in de praktijk verricht om na een fout verder onheil te voorkomen (automatic shut down), maar vooral ook om een fout van te voren te kunnen zien aankomen. Voor dat laatste is het nodig dat de *mate* van verslechtering van de conditie meetbaar is (zie figuur 7.4).

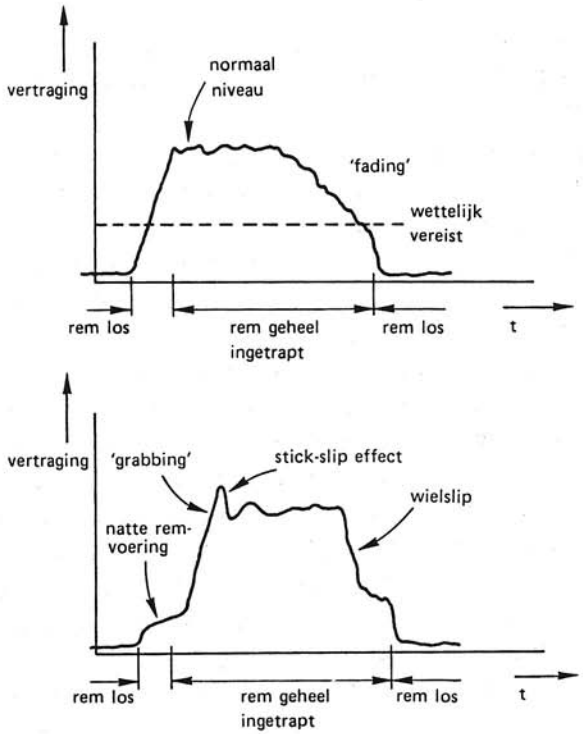


Figuur 7.4. Het typische verloop van de conditie van een machine. Als er niet wordt ingegrepen zal de machine na verloop van tijd totaal onbruikbaar zijn.

Als conditieparameters nemen we bijvoorbeeld het trillingsniveau van het huis van een grote waterkrachtturbine. Na een inloopperiode, waarin de machine-onderdelen op elkaar inslijten, blijft het trillingsniveau tamelijk constant. Als men (uitsluitend) periodiek onderhoud zou plegen, zou men in verband met een zekere veiligheidsmarge reeds bij t_p de machine moeten stilleggen voor onderhoud.
De machine wordt constant bewaakt (vanwege de grote schade die met falen gepaard gaat). Op t_c zal een waarschuwingssignaal gegeven worden, daar de trillingen door bijvoorbeeld schoepenbeschadiging of lagerslijtage zijn toegenomen tot boven normaal. Een nadere analyse van het frequentiespectrum van het trillingssignaal kan uitwijzen of het lagerslijtage dan wel schoepenbeschadiging betreft. Tenslotte wordt een alarmniveau overschreden. Daarboven mag de turbine bijvoorbeeld niet meer op vol vermogen draaien. Als niet door de operator zou worden ingegrepen, zou bij het noodstopniveau de turbine buiten bedrijf worden gesteld. Ware dit niet het geval dan zou waarschijnlijk tenslotte de trubine zichzelf en zijn fundering vernietigen.
We zien uit dit voorbeeld dat, als we aan de hand van de gemeten conditie van een machine, met tamelijk grote zekerheid de conditie kunnen extrapoleren naar de toekomst, er volstaan kan worden met een veel groter onderhoudsinterval t_o dan bij periodiek onderhoud (interval t_p). Dit geldt uiteraard alleen voor de fouten die gepaard gaan met voorboden van een toekomstig falen.

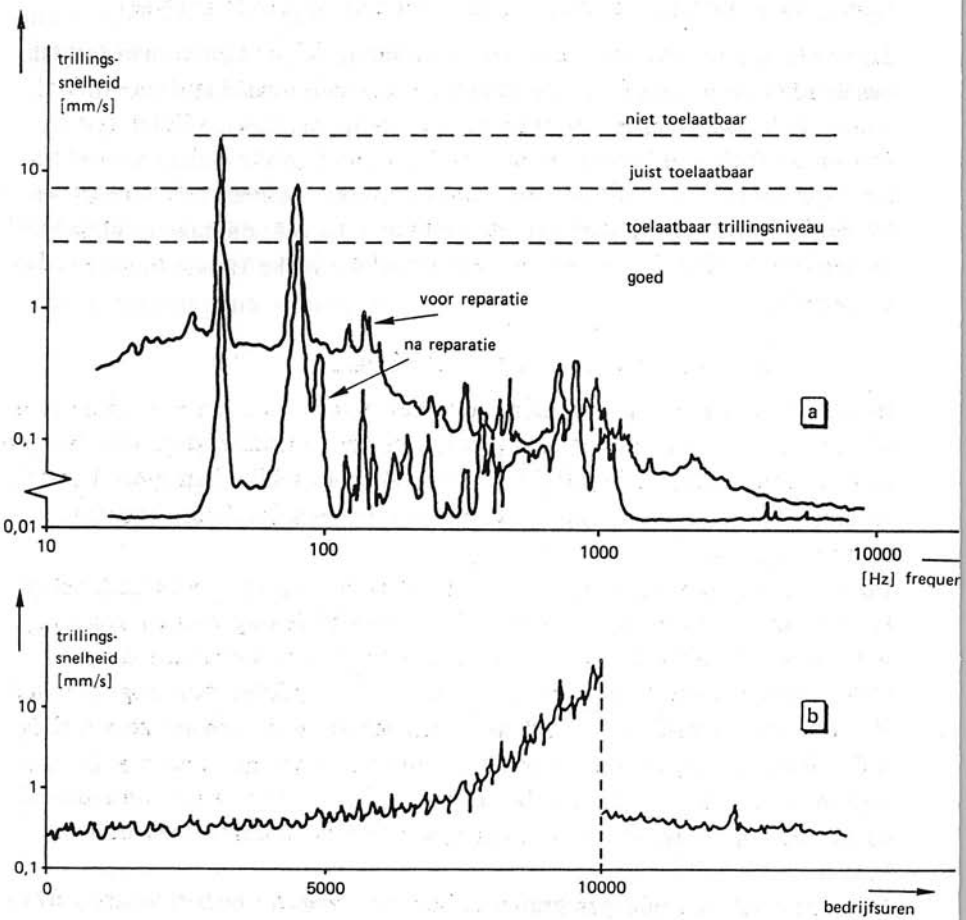
De grote moeilijkheid bij condition-based maintenance is de juiste indicatieve parameters te vinden die een toekomstig falen aangeven. Naast deze conditiemeting doet men dan ook wel zogenaamde '*performance*'-me-

tingen. Deze zijn zinvol als de gewenste functie van het systeem aan langzame degradatie (*graceful degradation*) onderhevig is. Een voorbeeld daarvan is gegeven in figuur 7.5. Met behulp van een versnellingsopnemer wordt de remvertraging van een voertuig gemeten. Aan de wijze van oplopen en afvallen van de vertraging kan men een globale indruk krijgen van het functioneren van het remsysteem. Op grond daarvan kan men de remvoeringen vervangen, remtrommels uitdraaien of schoonmaken, leidingen ontluchten enzovoort. Andere voorbeelden van zulke functiemetingen zijn: vollast-proeven, brandstofverbruiksmetingen, pomp- en transportcapaciteitsmetingen en dergelijke.



Figuur 7.5. Een functiemeting ('performance measurement') van het remsysteem van een zwaar voertuig.

Naast incidentele conditie of 'performance'-metingen kent men ook het bewaken van een systeem in de tijd om de trend van de conditie of de performance te volgen. Deze zogenaamde *trend monitoring* is van belang in complexe systemen om onregelmatigheden in het bedrijf van het systeem vroegtijdig te ontdekken en de oorzaak daarvan op te sporen.
In figuur 7.6 is daarvan een voorbeeld gegeven. Hier gaat het om een complexe tandwieloverbrenging. Uit een frequentieanalyse blijkt dat het



Figuur 7.6. (a) Het frequentiespectrum van de trillingssnelheid (effectieve waarde) van een hogesnelheidstandwielbak voor en na reparatie bij t = 10 000 uur (3% bandbreedte spectrum); (b) de trend van de trillingssnelheid (van 10–1 000 Hz, effectieve waarde) met de toename van het aantal bedrijfsuren.

grootste verschil in trillingsgedrag zit beneden 1 kHz. Derhalve is bij de trend monitoring gekozen voor een breedbandige meting (10 Hz – 1 kHz) van de effectieve waarde van de trillingssnelheid. Deze trend is in figuur 7.6b getoond.

Condition-based maintenance heeft vooral ingang gevonden bij onderhoud aan machines en dergelijke. Men meet daarbij onder andere corrosie (overgangsweerstandsmeting, visuele inspectie), temperaturen (thermografische verf, infra-rood thermografie), vermoeidheid (haarscheurtjes door middel van wervelstroomdetectoren, ultrasoon- en röntgenonderzoek), onbalans, slijtage, losse onderdelen (trillingsmetingen) en slijtage produkten (olie-

filters, koelwateranalyse, magnetische stoppen, spectrale analyse).

Bij elektronische systemen kan een toekomstig falen meestal niet voortijdig worden voorspeld (behalve natuurlijk bij redundante systemen). Dat komt omdat de meeste elektronische componenten geen slijtage-gedrag vertonen. Toch is periodiek onderhoud ook hier gewenst, bijvoorbeeld aan meetapparatuur die periodiek op onnauwkeurigheid moet worden gecontroleerd. Indien nodig moet het instrument opnieuw worden afgeregeld of dienen onderdelen die te ver uit de tolerantie zijn weggelopen, te worden vervangen.

7.3. Systemen met correctief onderhoud

In de volgende paragrafen zullen we nader ingaan op correctief onderhoud. We nemen dan dus aan dat een systeem of een essentieel deel van dat systeem faalt alvorens er ingegrepen wordt. Dit menselijke ingrijpen (herstel, reparatie) is er op gericht het systeem weer in een bruikbare toestand terug te brengen.
We veronderstellen eerst dat de tijd die daarvoor nodig is verwaarloosbaar klein is. Dit is (meestal) het geval bij een modulair opgebouwd systeem, waarbij we de gefaalde module slechts behoeven te vervangen door een ander, zonder deze te repareren. Vooral als de modulen ook nog voorzien zijn van een foutindicatie vergt het foutzoeken en -herstellen zeer weinig tijd. We mogen bij herstel door *vervanging* dan ook (meestal) wel de hersteltijddistributie zien als een *Diracfunctie*. Het herstel is dus onmiddelijk na de fout; de 'down-time' van het systeem is verwaarloosbaar of niet belangrijk.
In de daarop volgende paragrafen zullen we *reparatie* bezien waarbij foutrapportage, foutlocatie, onderdelen bestellen en repareren zoveel tijd kosten, dat we daar rekening mee moeten houden in de vorm van een *reparatietijddistributie.*

7.3.1. Vervanging

Onder de aannamen die we in het bovenstaande over vervanging van defecte modulen hebben gemaakt, is de beschikbaarheid A(t) van het systeem geen interessante grootheid meer, want:

$$A(t) = 1.$$

We nemen gemakshalve aan dat we ook te doen hebben met *ideale vervanging*. Dat houdt in dat de vervangen komponent 'als nieuw' is en niet geleden heeft onder het in- en uitbouwen. Daar vervanging een relatief simpele ingreep is, in tegenstelling tot reparatie, is deze veronderstelling meestal wel gewettigd.

Voorbeelden hiervan zijn de vervanging van smeltveiligheden in een huisinstallatie, de vervanging van gloeilampen in de verlichtingsinstallatie voor een auto of van prints in een computerinstallatie.
In de praktijk zal men nooit alle voorkomende systeemfouten alleen door vervanging van modulen kunnen corrigeren. Zelfs in een volledig modulair opgebouwd elektronisch systeem blijven dan toch nog kabelbreuken, connectorfouten en dergelijke over die gerepareerd moeten worden.

Stel dat f(t) de faalkansdichtheid is van het systeem zonder vervanging. Na vervanging zal het systeem weer falen. Stel dat de faalkansdichtheid van deze tweede fout $f_2(t)$ is, dan kunnen we $f_2(t)$ vinden uit:

$$f_2(t) = \int_0^t f(t - \tau)\, f(\tau)\, d\tau.$$

We nemen daarbij aan dat beide levensduren onafhankelijk zijn en op dezelfde wijze verdeeld zijn. Het tweede faaltijdstip is dan de som van de beide levensduren. Deze heeft de bovengegeven dichtheid $f_2(t)$. Het i-de vervangingstijdstip vinden we dan door een i-voudige convolutie van f(t) met zichzelf. Recursief genoteerd geeft dit:

$$f_i(t) = \int_0^t f(t - \tau) f_{i-1}(\tau)\, d\tau.$$

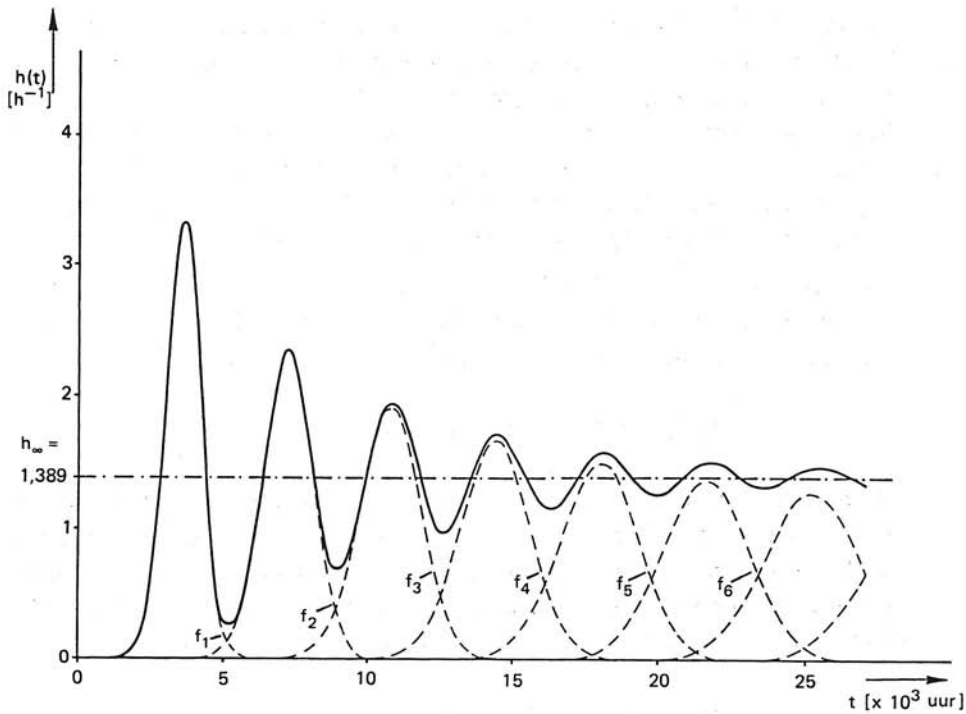
We voeren nu de *vervangingsdichtheid* (renewal density) h(t) in, waarbij $h(t)\Delta t$ de kans is dat er een vervanging plaatsvindt in het tijdinterval $(t, t+\Delta t]$. De waarde van h(t) vinden we dan eenvoudig met:

$$h(t) = \sum_{i=1}^{\infty} f_i(t).$$

We zullen hiervan een eenvoudig voorbeeld geven. We bezien daartoe een verzameling van een groot aantal identieke componenten N die een normaal verdeelde levensduur hebben met gemiddelde μ en spreiding σ. Alle uitgevallen componenten worden vervangen door nieuwe. In figuur 7.7 is hiervan een illustratie gegeven. We zien daaruit dat tenslotte de vervangingsdichtheid h(t) een constante waarde aanneemt die gegeven is door:

$$h_\infty = \lim_{t \to \infty} h(t) = \frac{N}{\mu}.$$

Ondanks het feit dat we uitgingen van een normale verdeling krijgen we tenslotte toch willekeurig in de tijd optredende vervangingen. Door de menging van oude en nieuwe componenten gaat het systeem zich tenslotte gedragen als of het door puur toeval uitvalt met een constant faaltempo. De piekbelastingen in het begin gaan de vervangingscapaciteit van de onderhoudsdienst te boven, of geven althans een weinig efficiënt gebruik van



Figuur 7.7. De vervangingsdichtheid voor een systeem bestaande uit 5000 (actieve) componenten die een normaal verdeelde levensduur hebben met een gemiddelde μ = 3600 uur en een spreiding σ = 600 uur.

het personeel (hollen en stilstaan). Hoe de *vervangingsstrategie* moet worden gewijzigd om meteen vanaf t ñ 0 de eindwaarde N/μ te krijgen is eenvoudig in te zien, evenals het feit dat we h(t) even goed de hazard rate z(t) van het systeem met vervanging zouden kunnen noemen.

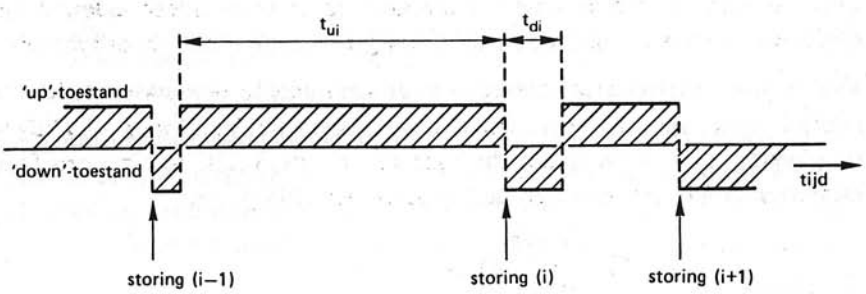
Voorbeeld 7.4

Een grote lichtreclame in Las Vegas wordt in gebruik genomen. De verlichting geschiedt geheel met gloeilampen met een gemiddelde brandduur μ = 1000 uur en een spreiding σ = 100 uur. De reclame bevat 1000 lampjes. We kunnen nu uitrekenen met figuur 7.7 dat de grootste piekbelasting voor de onderhoudsmensen komt na 1000 uur. Voor een normale verdeling ligt 63,8% binnen een ± 1 sigma-interval rond de gemiddelde waarde μ. Dus 638 lampen vallen uit in 200 uur tijds. Dit is zo'n drie lampen per uur. De eindwaarde, na oneindig veel vervangingen, is $N/\mu = 1$ lamp per uur. Men kan de onderhoudspiek in het begin afvlakken door reeds vanaf t = 0 te beginnen gemiddeld 1 lamp per uur te vervangen, ook al branden de te vervangen lampen nog. Dit levert evenwel een verspilling van nog goede lampen. Een meer optimale strategie is: met een gemiddeld tempo van 1 lamp per uur in elk geval alle kapotte lampen vervangen en de vervangen, nog goede lampen weer in het magazijn terugleggen. De lam-

pen die uit het magazijn gehaald worden, worden willekeurig gekozen: er wordt geen onderscheid tussen nieuwe en oude lampen gemaakt. Indien het verse deel van de magazijnvoorraad voldoende groot is kan men op deze manier, zonder verspilling, met een op nominale (maar reeds vanaf het begin) werkende onderhoudsdienst een vrijwel vlekkeloze lichtreclame bedrijven.
Dit probleem is van belang daar waar grote hoeveelheden nieuwe systemen blootgesteld worden aan gelijke aantallen bedrijfsuren, zodat ook de uitval grote correlatie zal vertonen.

7.3.2. Reparatie

In de volgende paragrafen nemen we aan dat een systeem gefaald heeft vóórdat er wordt ingegrepen. Voorts nemen we aan dat dit ingrijpen een zekere tijd $\underline{t}$ vergt. Hierin is $\underline{t}$ een niet-negatieve stochastische variabele, de *reparatie- of hersteltijd*, die verdeeld is volgens M(t), de *maintainability*. We nemen verder aan dat deze onderhoudsdistributie niet ontaard is zoals bij *vervanging* het geval was (de onderhoudskansdichtheid was dan immers een Diracfunctie).
De gebruiksfase (zie figuur 7.1) van zo'n repareerbaar systeem ziet er dan dus uit als aangegeven in figuur 7.8.



Figuur 7.8. Het al dan niet functioneren van een systeem of een unit in de tijd gezien (zie ook figuur 3.2).

De tijd t_{ui} stelt de i-de ononderbroken bedrijfsperiode voor, de tijd t_{di} de daarop volgende noodzakelijke herstelperiode.
Men moet het begrip 'bedrijfsperiode' hierin niet te eng interpreteren. Behalve de tijd waarin het systeem werkelijk naar behoren functioneert, wordt hiermee ook de tijd bedoeld waarin het systeem gebruiksgereed is, maar om welke redenen dan ook (andere dan defecten in het systeem) niet gebruikt wordt.

Het begrip bedrijfszekerheid zoals we in paragraaf 3.2 hebben gedefinieerd, heeft alleen betrekking op de eerste ononderbroken 'up'-toestand t_{u1} van het systeem. De kans dat deze toestand tot op het tijdstip t voortduurt is

R(t) en de gemiddelde tijd totdat de *eerste* systeemfout optreedt (Mean Time To First Failure) is daarom:

$$\text{MTTFF} = \int_0^\infty R(t)\,dt.$$

Het zal ook duidelijk zijn dat bij een systeem zoals aangegeven in figuur 7.8 de beschikbaarheid A(t) niet meer gelijk aan 1 is, zoals bij vervanging het geval was.
In paragraaf 3.2 hebben we de *beschikbaarheid A(t)* reeds gedefinieerd: A(t) is de kans dat het systeem op het tijdstip t in werkende (of bedrijfsgerede) toestand is, indien het over het interval [0,t] goed behandeld en bediend is.

N.B.: Wat opvalt is dat voor niet-repareerbare systemen, dus ook voor de tijd t_{ul} van een repareerbaar systeem, de begrippen *bedrijfszekerheid* R(t) en *beschikbaarheid* A(t) identiek zijn. We hadden dan ook kunnen volstaan met het invoeren van uitsluitend het algemenere begrip beschikbaarheid, ook voor niet-repareerbare systemen. In plaats van 'bedrijfszekerheid' hadden we dit boek dan ook 'beschikbaarheid' moeten noemen. Sommige auteurs doen dit dan ook consequent. Wij hebben echter gemeend, vanwege het essentiële verschil tussen onderhouden en niet-onderhouden systemen, ons te moeten aansluiten bij het algemeen gangbare woordgebruik.

Vaak is men slechts geïnteresseerd in de gemiddelde beschikbaarheid over relatief korte tijdintervallen. Dit is bijvoorbeeld het geval met vliegtuigen en schepen, die vooral tijdens hun missie (vlucht, vaart) niet mogen falen. Daarvoor definieert men dan de '*mission availability*' als:

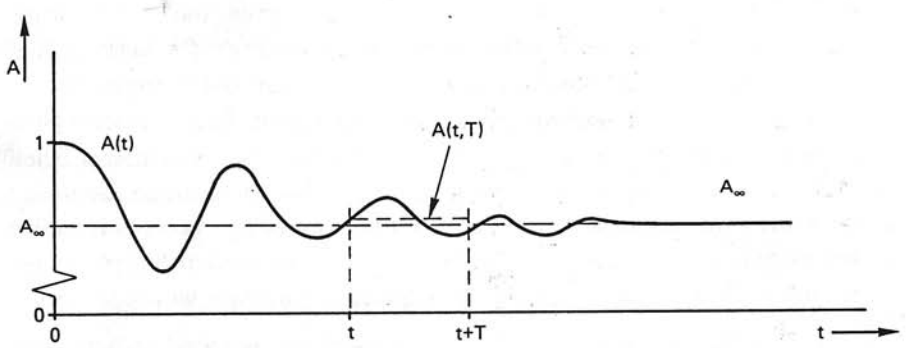
$$A(t, T) = \frac{1}{T} \int_t^{t+T} A(t)\,dt.$$

Deze grootheid geeft dus de fractie van de tijd aan dat het systeem (gemiddeld genomen) beschikbaar was gedurende het tijdinterval (t, t+T) dat nodig was voor het vervullen van de opdracht. In het algemeen is deze gemiddelde beschikbaarheid over de tijd T een functie van de absolute leeftijd t van het systeem; voor een oud systeem zal zij anders uitvallen dan voor een nieuw systeem.
In analogie aan de mission availability definieert men als *lange-termijnbeschikbaarheid*:

$$A_\infty = \lim_{t\to\infty} \frac{1}{t} \int_0^t A(t)\,dt.$$

De lange-termijnbeschikbaarheid A_∞ noemt men ook wel '*long-term avail-*

ability' of '*steady-state availability*'. De laatste uitdrukking komt voort uit het feit dat de beschikbaarheid A(t) van een systeem vlak na het ingebruiknemen van zo'n systeem nogal kan fluctueren, vooral als er grote aantallen componenten met (ongeveer) dezelfde levensduur toegepast zijn. Tenslotte evenwel, voor zeer grote t, is de leeftijdsopbouw van de componenten door de vele reparaties tamelijk uniform geworden. Hierdoor is de beschikbaarheid A(t) van praktische systemen voor zeer grote t vrijwel constant; het systeem heeft dan zijn 'steady-state availability' A_∞ bereikt. Een en ander is geïllustreerd in figuur 7.9. Opgemerkt dient te worden dat A_∞ slechts benaderd wordt na *zeer* vele reparaties. De meeste technische systemen benaderen tijdens hun gebruiksperiode daarom A_∞ nooit. Derhalve is het beter A_∞ te zien als een asymptotische waarde van de werkelijke A(t).



Figuur 7.9. Voorbeeld van de beschikbaarheid van een systeem als functie van de leeftijd t van het systeem.

We mogen voor de lange-termijnbeschikbaarheid ook schrijven:

$$A_\infty = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}}.$$

Hierin is de Mean (up-) Time Between Failures (MTBF):

$$\text{MTBF} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} t_{ui},$$

en de Mean (down-) Time To Repair (MTTR):

$$\text{MTTR} = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} t_{di}.$$

Als A(t) na voldoende grote, doch eindige tijd t willekeurig dicht de waarde A_∞ genaderd is, mogen we volstaan met de bovenstaande sommaties uit te voeren vanaf dat tijdstip. Het eerste deel waarin A(t) niet stationair

is, doet er dan niet meer toe. Men mag dus de MTBF en MTTR ook betrekken op alleen de 'steady-state'-toestand van een systeem.

N.B.: De MTBF en de MTTR zijn gemiddelden, zij zeggen niets over de verdeling. De down-time kan bijvoorbeeld opgebouwd zijn uit enkele zeer lange reparatietijden (die dominant zijn) en een groot aantal korte reparaties. Evenzo zegt een bepaalde lange-termijn beschikbaarheid (bijvoorbeeld $A_\infty = 0{,}99$) niets over het aantal storingen. Zij kan evengoed worden veroorzaakt door een zeer groot aantal kortdurende storingen als door een paar lange storingen.

Voor een kwantitatieve analyse van de beschikbaarheid van een systeem en de invloed van reparatie daarop is het zinvol de volgende indeling te maken:

A. *Systeem*	1. Configuratie
	2. Homogeniteit
	3. Beheersstrategie
B. *Units*	1. Faalwijzen
	2. Faaldistributies
C. *Reparatie*	1. Capaciteit
	2. Reparatiestrategie
	3. Reparatietijddistributies

De *configuratie* bepaalt de structuur van het systeem. De *homogeniteit* bepaalt of dit systeem al dan niet gemodelleerd kan worden als een configuratie bestaande uit statistisch identieke units. De *beheersstrategie* bepaalt zaken als het gebruik van redundantie in de actieve of de passieve vorm, het laten doordraaien van een systeem na een fout, of het volledig stilleggen na een opgetreden fout. In het laatste geval zullen tijdens de down-periode niet nòg meer fouten kunnen ontstaan. Meestal gaat echter het weer opstarten van een systeem met een tijdelijke verhoging van de hazard rate gepaard.

De units waaruit het systeem is opgebouwd, kunnen verschillende *faalwijzen* vertonen: catastrofaal, partieel, complementaire faalwijzen (open, kortgesloten), afhankelijke en intermitterende faalwijzen. De faalwijzen kunnen elk hun eigen *faaldistributie* hebben.

De *reparatiecapaciteit* wordt bepaald door het aantal ter beschikking staande *reparatiekanalen* en het aantal monteurs per kanaal. Een reparatiekanaal is daarbij gedefinieerd als een aantal monteurs (met reserve-onderdelen, meetapparatuur en gereedschap) dat samen aan het herstellen van één fout werkt. Dit aantal bepaalt de capaciteit van het desbetreffende reparatieka-

naal. Eén reparatiekanaal kan ook meerdere systemen bewaken; we spreken dan van *gedeelde reparatie* (shared repair). Ook kunnen twee reparatiekanalen, na elkaar, met hetzelfde systeem bezig zijn. Het tweede kanaal repareert dan de volgende fout als deze optreedt terwijl het eerste reparatiekanaal nog bezig is. De *reparatiestrategie* bepaalt welke vorm van reparatie wordt gekozen voor een systeem. Tenslotte heeft elke vorm van reparatie zijn eigen *reparatietijddistributie*.

We zullen verschillende configuraties bezien. We nemen daarbij een aantal dingen aan:

- Er is altijd minstens één reparatiekanaal aanwezig. Zo'n kanaal omvat de reparateur, zijn vakkennis, zijn gereedschappen, zijn meet- en testinstrumentarium en de onderdelen of modulen die hij voor het herstellen nodig heeft.
- De reparatie is ideaal. Dat wil zeggen: de gebruikte komponenten zijn 'als nieuw' en het systeem lijdt niet onder de reparatie; de reparatie introduceert geen nieuwe kinderziekten.
- Er is een oneindige voorraad reserve-onderdelen, tenzij anders vermeld.
- De tijd nodig voor reparatie is een stochastische variabele die negatief-exponentiëel verdeeld is en een gemiddelde waarde $1/\mu$ heeft. De parameter μ noemt men de *repair rate*. Dit is dus de tegenvoeter van de *failure rate* λ.

7.3.3. Repareerbare systemen zonder redundantie

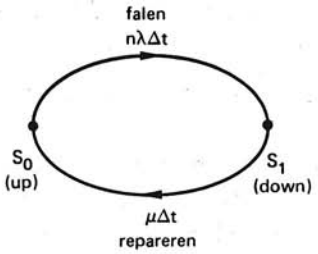
We zullen de wijze van benaderen van repareerbare seriesystemen demonstreren aan een systeem bestaande uit n units in serie die onderling stochastisch identiek zijn; een homogeen seriesysteem dus.
We bezien daartoe de eenvoudigste reparatiestrategie: één reparatiekanaal bestaande uit één monteur die onmiddelijk na een storing het systeem afschakelt en begint met repareren. Tijdens de reparatie kunnen er dus niet nog meer units falen. Onmiddelijk na het voltooien van de reparatie wordt het systeem weer ingeschakeld. De failure rate van de units is λ, de repair rate voor alle units μ.
We kunnen dit onderhoudbare systeem modelleren in een Markovmodel met slechts twee toestanden (zie figuur 7.10):

- De toestand S_0 waarin alle n eenheden functioneren en de monteur niets te doen heeft.
- De toestand S_1 waarin één unit heeft gefaald en de reparateur bezig is. De andere $n-1$ units kunnen dan niet falen!

Uit het Markovmodel kunnen we met behulp van de regels gegeven in paragraaf 5.3 rechtstreeks de differentiaalvergelijkingen opstellen:

$$\frac{dP_{S_0}(t)}{dt} = -n\lambda P_{S_0}(t) + \mu P_{S_1}(t),$$

$$\frac{dP_{S_1}(t)}{dt} = n\lambda P_{S_0}(t) - \mu P_{S_1}(t).$$



Figuur 7.10. Een toestandsmodel van een seriesysteem met n units, waarin tijdens een reparatie geen fouten kunnen optreden (de units staan dan afgeschakeld). De lussen die in S_0 en S_1 terugkeren zijn gemakshalve weggelaten.

Als we als beginvoorwaarden nemen $P_{S_0}(0) = 1$ en $P_{S_1}(0) = 0$ geeft Laplace-transformatie:

$$sP_{S_0}(s) - 1 = -n\lambda P_{S_0}(s) + \mu P_{S_1}(s),$$

$$sP_{S_1}(s) = n\lambda P_{S_0}(s) - \mu P_{S_1}(s).$$

De oplossing daarvan geeft voor $P_{S_0}(s)$:

$$P_{S_0}(s) = \frac{s + \mu}{s(s + n\lambda + \mu)}.$$

De beschikbaarheid A(t) vinden we door terugtransformeren van $P_{S_0}(s)$. We vinden dan:

$$A(t) = \frac{\mu}{n\lambda + \mu} + \frac{n\lambda}{n\lambda + \mu} e^{-(n\lambda + \mu)t}.$$

De gemiddelde beschikbaarheid A(t,T) (mission availability) over het interval (t, t+T) is dan:

$$A(t,T) = \frac{\mu}{n\lambda + \mu} - \frac{n\lambda e^{-(n\lambda + \mu)t}}{T(n\lambda + \mu)^2} \{e^{-(n\lambda + \mu)T} - 1\}.$$

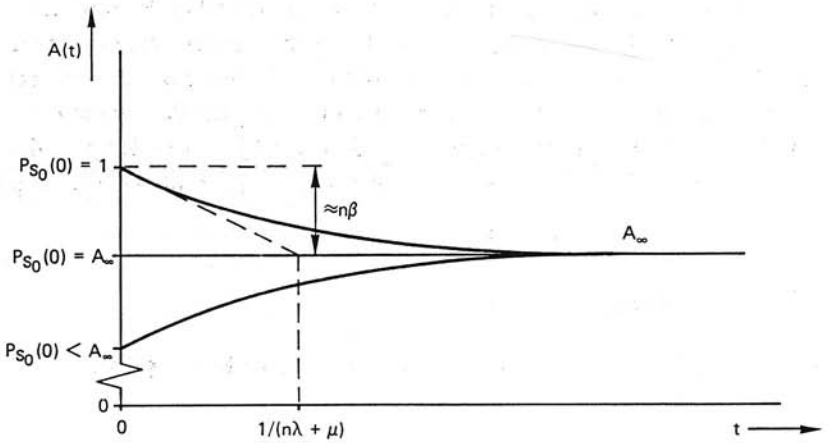
Voor de lange-termijnbeschikbaarheid A_∞ vinden we:

$$A_\infty = \frac{\mu}{n\lambda + \mu}.$$

Met de uitdrukking gegeven voor de lange-termijnbeschikbaarheid in paragraaf 7.3.2 hadden we de laatste uitdrukking direct op kunnen schrijven:

$$A_\infty = \frac{MTBF}{MTBF + MTTR} = \frac{1/n\lambda}{1/n\lambda + 1/\mu}.$$

In figuur 7.11 zijn A(t) en A_∞ weergegeven. Daarin is niet verondersteld dat $P_{S_0}(0) = 1$, maar zijn verschillende gevallen getekend. Het overgangsverschijnsel in de A(t)-curve treedt alleen op als $P_{S_0}(0) \neq A_\infty$.



Figuur 7.11. De beschikbaarheid van een homogeen seriesysteem bestaande uit n (identieke) units voor verschillende waarden van $P_{S_0}(0)$. Tijdens reparatie is het systeem afgeschakeld.

Opmerking: Men voert bij repareerbare systemen wel de verhouding β in:

$$\beta = \frac{\lambda}{\mu}.$$

Deze verhouding, die bij een gezond systeembeheer altijd zeer klein is, geeft dus aan hoeveel sneller een unit faalt dan hij gerepareerd wordt. We vinden dan de volgende benadering:

$$A_\infty = \frac{1}{1 + n\beta} \approx 1 - n\beta \qquad (\beta \ll 1)$$

De onbeschikbaarheid (unavailability) is:

$$\bar{A}_\infty = 1 - A_\infty \approx n\beta.$$

De *storingsdichtheid* (ook wel *renewal rate* genoemd) is het gemiddelde aantal storingen (en dus reparaties of vernieuwingen) per eenheid van tijd. De storingsdichtheid is:

$$h_\infty = n\lambda \frac{\mu}{\mu + n\lambda}.$$

Voor $n\beta \ll 1$ geldt dan:

$$h_\infty = n\lambda \frac{1}{1 + n\beta} \approx n\lambda(1 - n\beta).$$

De grootheid h_∞ bepaalt de noodzakelijke grootte van de reparatiecapaciteit, dus het aantal benodigde reparateur-uren.

We hadden voor de bepaling van A_∞ ook een snellere berekening kunnen kiezen dan die welke boven gegeven is. We hebben reeds gezien in paragraaf 7.3.2 dat A_∞ de 'steady-state'-waarde van de beschikbaarheid A(t) is. In deze stationaire toestand zullen de kansen P_{S_i} op de toestanden S_i (i = 1,2, . . . ,n) tijdonafhankelijk worden. De tijdafgeleiden van deze kansen zijn dus nul. Derhalve kunnen deze kansen gevonden worden uit:

$$-n\lambda P_{S_0} + \mu P_{S_1} = 0,$$

$$n\lambda P_{S_0} - \mu P_{S_1} = 0.$$

Daar het systeem altijd in één der toestanden S_i verkeert, geldt:

$$\sum_{i=0}^{n} P_{S_i} = 1.$$

Dit levert voor het n-unit homogene seriesysteem de oplossing:

$$A_\infty = P_{S_0} = \frac{\mu}{n\lambda + \mu}.$$

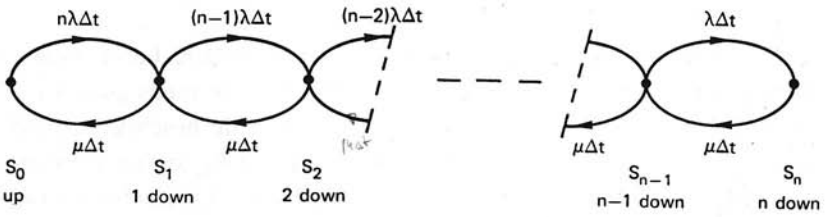
Na dit eenvoudige voorbeeld met één reparatiekanaal zullen we het effect bezien van het in bedrijf laten van de n – 1 nog functionerende units van het systeem tijdens de reparatie.
De afschakeling van het systeem tijdens reparatie is namelijk niet altijd wenselijk. Na het inschakelen is er opnieuw een opwarm- of aanlooptijd, die als het ware bij de reparatieduur komt. Bovendien is in- en uitschakelen van een systeem een vorm van foutversnellende stress waardoor de kans op uitval onmiddellijk na het inschakelen tijdelijk groter is. Daarom zullen we nu veronderstellen dat het systeem continu ingeschakeld blijft.

We nemen nu aan dat na één fout, dus gedurende de reparatie van een unit, wel degelijk andere fouten kunnen ontstaan. We nemen ook aan dat deze fouten met dezelfde failure rate λ optreden als onder normaal, ongestoord bedrijf.

We kunnen dan de navolgende inventaris van n+1 onderling disjuncte toestanden opstellen:

- S_0 : alle n units functioneren correct.
- S_i : $(n-i)$ units functioneren, één unit is in reparatie en $(i-1)$ units staan in de rij om gerepareerd te worden ($i = 1,2, \ldots ,n$).

Het toestandsmodel wordt dan als aangegeven in figuur 7.12.



Figuur 7.12. Een toestandsmodel van een homogeen seriesysteem met n units die kunnen falen tijdens een reparatie. Zie opmerking figuur 7.10.

Op basis van de inspectie van het toestandsmodel kunnen we de navolgende differentiaalvergelijkingen opstellen; met $\dot{P}(t) = dP/dt$:

$$\dot{P}_{S_0}(t) = -n\lambda P_{S_0} + \mu P_{S_1} = 0$$

$$\dot{P}_{S_1}(t) = +n\lambda P_{S_0} - [(n-1)\lambda + \mu]\, P_{S_1} + \mu P_{S_2} = 0$$

$$\dot{P}_{S_2}(t) = + (n-1)\lambda P_{S_1} - [(n-2)\lambda + \mu] P_{S_2} + \mu P_{S_3} = 0$$

Voor de verblijfskans in toestand S_i in de steady-state vinden we daaruit:

$$P_{S_i} = \binom{n}{i}\, i!\, \beta^i P_{S_0}, \qquad (i = 0,1, \ldots ,n).$$

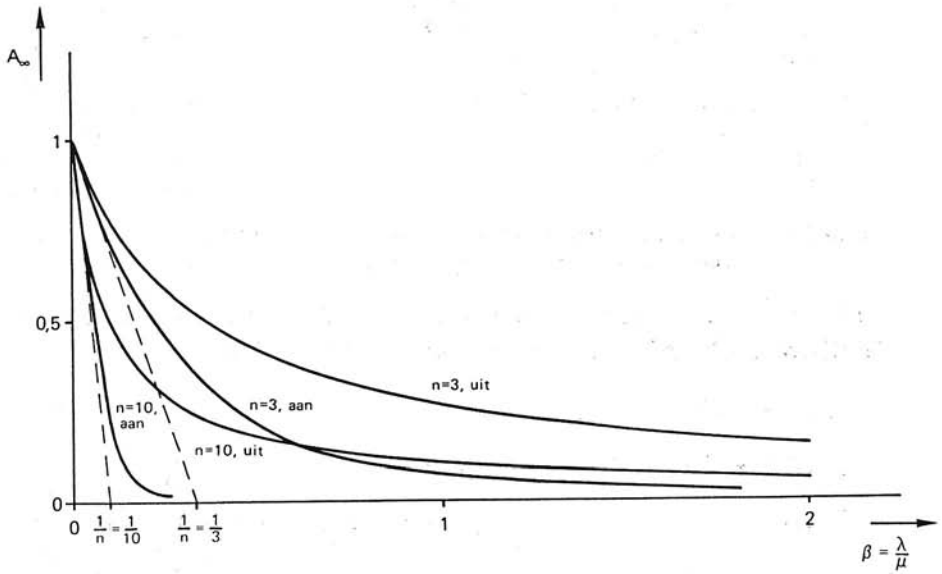
N.B.: We kunnen deze kansen ook opvatten als het gedeelte van de tijd dat het systeem (gemiddeld, over voldoende lange tijd) in de toestand S_i is. Daar de som van alle (n+1) verblijfskansen 1 is, vinden we voor de steady-state availability:

$$A_\infty = P_{S_0} = \frac{1}{n! \sum_{i=0}^{n} \frac{\beta^{n-i}}{i!}} = \frac{1}{n! \sum_{i=0}^{n} \frac{\beta^i}{(n-i)!}}.$$

Eenvoudig is in te zien dat:

$$\lim_{\beta \to 0} A_\infty = 1.$$

Voor $\beta \ll$ verschilt de situatie niet zo erg veel van die in figuur 7.11. Als de repair rate μ voldoende veel groter is dan de failure rate λ, brengt het niet afschakelen gedurende de reparatietijd slechts een hogere orde, kleine correctieterm aan in de beschikbaarheid A_∞. In figuur 7.13 is de long-term availability getekend versus de verhouding $\beta = \lambda/\mu$ voor een seriesysteem van drie en één van tien units met en zonder afschakeling van het systeem tijdens reparatie.

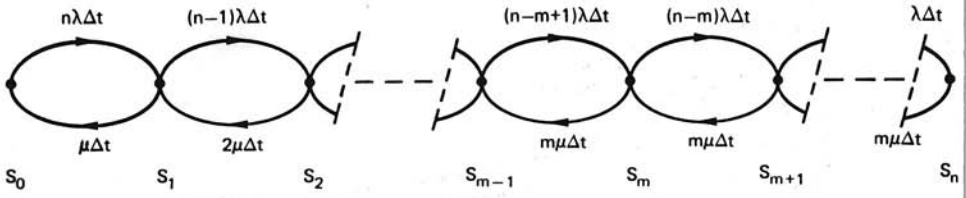


Figuur 7.13. De beschikbaarheid A_∞ van een n-voudig seriesysteem in het geval dat het in bedrijf blijft gedurende een reparatie (aan) en in het geval dat het systeem tijdens een reparatie wordt stilgelegd (uit), als functie van β.

We zien dat het, voor de kleine waarden van β die een gezond systeembeheer kenmerken, niet uitmaakt of het systeem al dan niet wordt afgeschakeld. Vaak is het dan ook zinvol het systeem aan te laten staan om nieuwe kinderziekten na de reparatie te voorkomen.
Let op: dit mag voor de reparateur geen gevaarlijke situaties met zich meebrengen, noch aanleiding geven tot langere reparatietijden wegens het omzichtig repareren door het gevaar dat voortvloeit uit het nog in bedrijf zijnde systeem.

Tot dusverre hebben we gewerkt met één reparatiekanaal bestaande uit één monteur. We willen nu bezien wat het effect is van meerdere reparatiekanalen, elk nog steeds bestaande uit één monteur. We laten tevens het homogene n-unit seriesysteem continu in bedrijf, waardoor meerdere fouten kunnen ontstaan. Na de eerste fout repareert één der aanwezige m re-

paratiekanalen ($m \leqslant n$) de unit. Sneuvelt tijdens deze reparatie een tweede unit, dan treedt het tweede reparatiekanaal in werking, enzovoort. Ook de reparatiekanalen zijn homogeen, allen hebben een repair rate μ.
In het Markovdiagram zal de i-de toestand S_i ($i = 0,1, \ldots ,n$) dan inhouden dat er i units defect zijn, waarvan er i in reparatie zijn als $i \leqslant m$ en waarvan er m in reparatie zijn als $i \geqslant m$. De overige $(n - i)$ units functioneren nog en kunnen falen. Het Markovdiagram is geschetst in figuur 7.14.



Figuur 7.14. Het Markovdiagram van een homogeen n-unit seriesysteem met m homogene reparatiekanalen en continubedrijf.

Als we dit diagram wat nader bezien merken we, reeds zonder berekening, een aantal dingen op. Als het systeem zich op $t = 0$ in de toestand S_0 bevindt zal door falen van één unit (n mogelijkheden) het systeem in de toestand S_1 geraken. Daaruit wordt het door een reparateur in het tempo μ teruggebracht naar S_0. De kans op nog een fout (S_2) is kleiner, er zijn maar $(n - 1)$ mogelijkheden daartoe. Bovendien is de kans op herstel van één van de twee units in het tijdintervalletje Δt twee keer groter, namelijk $2\mu\Delta t$. Deze redenatie voortzettend, komen we tot de conclusie dat het hoogst onwaarschijnlijk is dat de m-de reparateur iets te doen zal hebben. Deze kans neemt af naarmate m groter wordt (en is voor $m > n$ zelfs gelijk aan nul).

Voor $n = 2$, $m = 2$ en $\beta = \lambda/\mu$ wordt de steady-state availability:

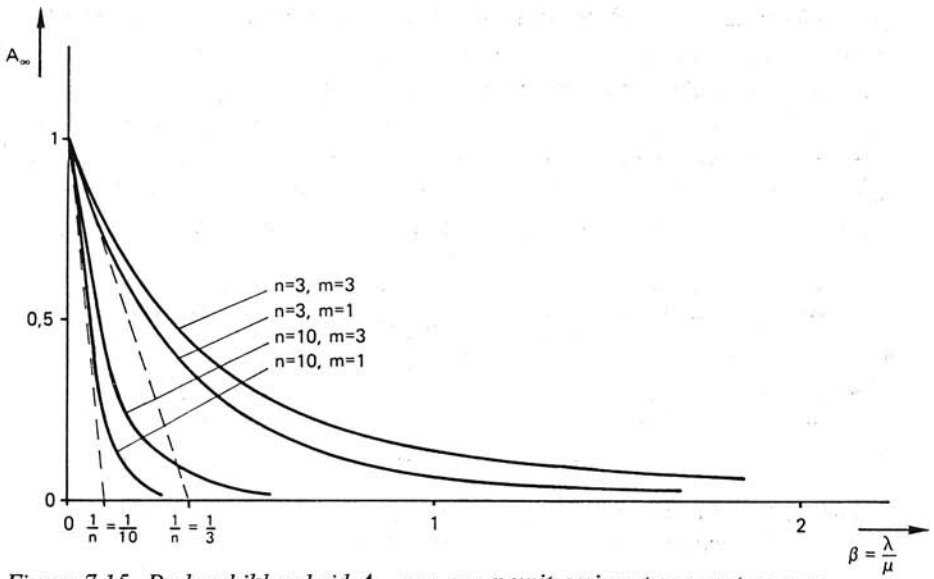
$$A_\infty = 1/(1 + \beta)^2,$$

en voor $\beta \ll 1$ geldt:

$$A_\infty \approx 1 - 2\beta.$$

Dit is dezelfde uitdrukking als die welke we vonden voor één reparateur. Kennelijk is de reparatietijd zo kort ten opzicht van de faaltijd van een unit dat de tweede reparateur vrijwel nooit werk heeft. In figuur 7.15 is dit nog eens voor een aantal gevallen geïllustreerd.

In het bovenstaande hebben we het effect van een aantal reparatiekanalen m op de beschikbaarheid van een n-unit seriesysteem bekeken. We



Figuur 7.15. De beschikbaarheid A_∞ van een n-unit seriesysteem met m reparatiekanalen.

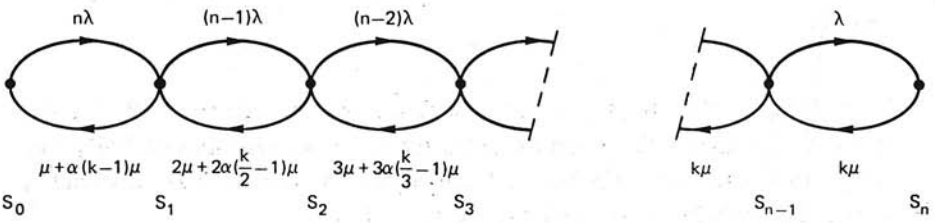
zullen nu slechts één kanaal veronderstellen, maar met meer dan één monteur. We nemen aan dat k monteurs binnen dat ene kanaal gelijktijdig actief bezig zijn met repareren. Als er slechts één unit defect is, zijn alle k monteurs hier gelijktijdig mee bezig. De reparatie zal dan ook sneller gaan, maar in het algemeen niet k keer sneller. We voeren een factor α in, zodanig dat de repair rate wordt:

$$\mu_{\text{effectief}} = \mu + \alpha(k-1)\mu, \quad 0 \leqslant \alpha \leqslant 1.$$

De factor α geeft dus de *inzetbaarheid* van de extra $(k-1)$ monteurs weer. Niet alle reparaties lenen zich namelijk even goed tot het inzetten van meer mensen. Denk maar aan het repareren van een mechanisch horloge enerzijds en het vervangen van doorgecorrodeerde pijpen in de procesindustrie anderzijds. We nemen bovendien het volgende aan:
Als er meerdere units defect zijn, splitst men de groep monteurs in een aantal reparatiekanalen, zodat er per kanaal altijd één defecte unit in reparatie is. Dit gaat zolang door tot er per kanaal één monteur aan één unit werkt. De kanalen zijn onderling onafhankelijk; zij werken immers aan verschillende units. De monteurs binnen één kanaal werken samen aan één unit.
De toestand S_i in het Markovdiagram wordt dan gekenmerkt door:
- n units waarvan er i defect zijn ($i \leqslant n$),
- k tot samenwerking bereide monteurs ($k \leqslant n$),

- i reparatiekanalen als $i \leqslant k$, $\mu_{eff} = \mu + \alpha(k/i - 1)\mu$;
- k reparatiekanalen als $i \geqslant k$, $\mu_{eff} = \mu$.

Het diagram is in figuur 7.16 weergegeven.



Figuur 7.16. Het Markovdiagram van een n-unit seriesysteem met k tot samenwerking bereide reparateurs. (De factoren Δt zijn hier weggelaten.)

Op basis van een inspectie van dit Markovdiagram zien we reeds dat (als voor $t = 0$: $P_{S_0} = 1$) de eerste sectie van het diagram, dus het gedeelte tussen S_0 en S_1 het belangrijkst is, vooral voor kleine waarden van $\beta = \lambda/\mu$. De verwachting is daarom dat we voor $\beta \ll 1$ mogen schrijven:

$$A_\infty = P_{S_0} \approx 1 - \frac{n\lambda}{\mu + \alpha(k-1)\mu} = 1 - \frac{n\beta}{1 + \alpha(k-1)}.$$

Dit is als volgt in te zien: bekijk uitsluitend de eerste twee toestanden in de steady-state. Als de inzetbaarheid α van de extra monteurs nul is, hebben we dus dezelfde situatie als met k onafhankelijke reparatiekanalen met elk één monteur; als $\alpha = 1$ dan is de reparatie k keer sneller en dientengevolge de beschikbaarheid groter.
Nu we enig inzicht in deze seriesystemen hebben gekregen kunnen we stellen dat we in plaats van de availability A_∞ beter de unavailability $\bar{A}_\infty$ kunnen bepalen. De benaderde uitdrukking voor $\beta \ll 1$ hiervoor kunnen we meteen opschrijven uit het Markovdiagram. Als $\beta \ll 1$ dan is de kans dat het systeem ooit in de toestanden S_2 en hoger komt namelijk te verwaarlozen. We hebben dan alleen met S_0 en S_1 te maken. Daarvoor schrijven we de onbeschikbaarheid zo op. Deze is namelijk het quotiënt van de faalovergangskans $(n\lambda\Delta t)$ en de reparatieovergangskans $[\mu + \alpha(k-1)\mu]\Delta t$, dus:

$$\bar{A}_\infty = 1 - A_\infty \approx \frac{n\lambda}{\mu + \alpha(k-1)\mu}.$$

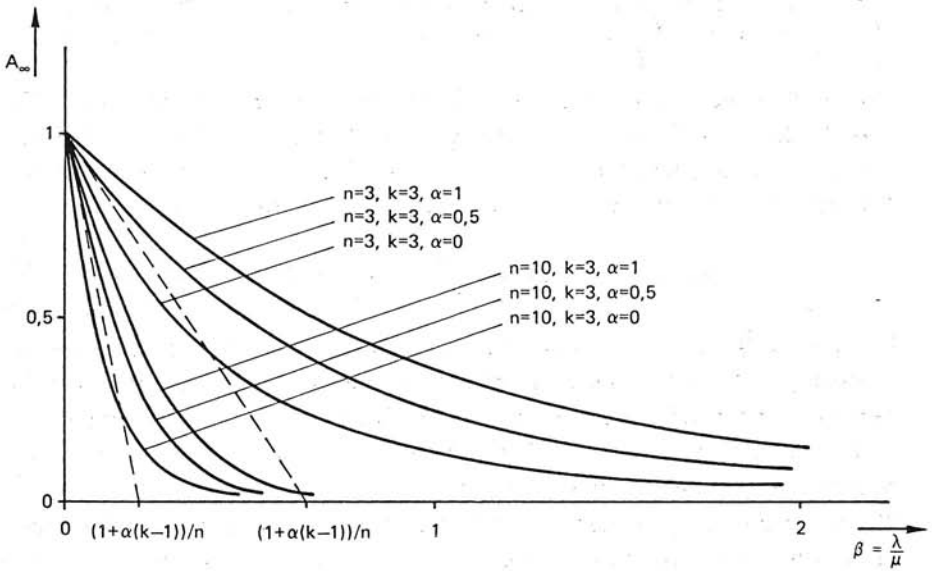
Voorbeeld 7.5
Stel dat $n = 2$ en $k = 2$ dan kunnen we met de eerder uitgelegde methode via de differentiaalvergelijkingen berekenen dat:

$$A_\infty = \frac{1 + \alpha}{1 + \alpha + 2\beta + \beta^2}.$$

Voor $\beta \ll 1$ kunnen we dit benaderen door:

$$A_\infty = 1 - \frac{2\beta}{1 + \alpha}.$$

De niet-beschikbaarheid (unavailability) $\bar{A}_\infty$ is dus ongeveer: $2\beta/(1 + \alpha)$. Door de inzetbaarheid α van de extra monteur is deze unavailability kennelijk met 100 % te veranderen; de gevoeligheid voor de inzetbaarheid is hoog. (Zie ook het voorbeeld van figuur 7.17).



Figuur 7.17. De beschikbaarheid van een n-unit homogeen seriesysteem met m reparateurs die een inzetbaarheid α hebben, als functie van de verhouding λ/μ.

Concluderend willen we deze paragraaf over onderhouden systemen zonder redundantie afsluiten met een aantal uitspraken:

- In een systeem met een gezond onderhoudsbeheer is $\beta \ll 1$ ($\beta = \lambda/\mu$).
- Het effect van het al dan niet afschakelen van zo'n systeem tijdens reparaties is klein. (Dit geldt niet voor systemen waarbij het aan- en afschakelen een stressor vormt. Zie hoofdstuk 2).
- Het inzetten van meerdere, onderling niet samenwerkende reparatiekanalen heeft weinig effect.
- In het geval van samenwerkende reparateurs (binnen één reparatiekanaal) is de verbetering van de beschikbaarheid van het systeem sterk afhankelijk van de inzetbaarheid α van de extra reparateurs.

7.3.4. Repareerbare systemen met redundantie

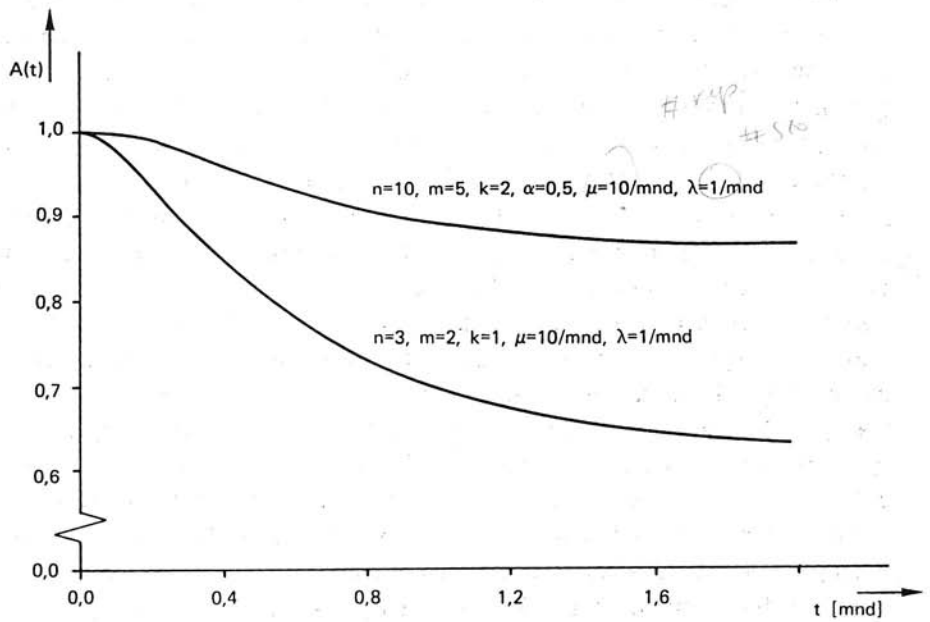
Het zal duidelijk zijn dat een zeer machtige combinatie van systeemonderhoud en -configuratie een redundante configuratie is, waaraan bovendien onderhoud wordt gepleegd. Het onderhoud begint reeds voordat alle systeemredundantie opgebruikt is. Op deze wijze is het mogelijk units die falen te repareren en terug in bedrijf te brengen voordat het systeem heeft gefaald en zonder dat het systeem daarvoor behoeft te worden stilgelegd. Naarmate de redundantiegraad η (zie paragraaf 6.3) groter is en naarmate de reparatie sneller verloopt, zal de kans op een systeemfout afnemen. Het systeem gaat immers slechts 'down' als alle redundantie reeds defect is en de reparatie voortduurt tot nà het tijdstip waarop de laatste unit faalt.

De reparatie van redundante units kan in het algemeen geschieden tijdens normaal systeembedrijf. Hoogstens is voor verwisseling van gefaalde redundante units een verwaarloosbaar korte onderbreking van de systeemfunctie nodig. We zullen in deze paragraaf dan ook een fout in een redundante unit en de reparatie daarvan niet als systeemfout opvatten zolang er tenminste nog voldoende goed functionerende units aanwezig zijn.
We zijn geïnteresseerd in een aantal grootheden van zo'n repareerbaar systeem met redundantie, te weten: de beschikbaarheid A_∞, de bedrijfszekerheid $R_S(t)$ en de gemiddelde tijd tot falen, de zogenaamde 'Mean Time To First *system* Failure' (MTTFF). Voor de bedrijfszekerheidsberekening en de MTTFF-bepaling nemen we aan dat de reparatie stopt als er een systeemfout optreedt. Dat zal zoals gezegd slechts kunnen gebeuren nadat alle redundante units hebben gefaald. We hebben dan dus een systeem met reparatie slechts zolang als de systeemfunctie nog ongestoord is; er is geen reparatie op systeemniveau. Deze aanname is uitsluitend gedaan om de begrippen $R_S(t)$ en MTTFF te kunnen hanteren; er is uiteraard niets op tegen om het gefaalde systeem toch te repareren.

We zullen in het navolgende het effect van reparatie onderzoeken op systemen met *actieve* en *passieve redundantie*. We nemen gemakshalve aan dat we met een homogeen systeem te doen hebben, bestaande uit units die onafhankelijk falen met failure rate λ. Ook de reparateurs zijn onafhankelijk met repair rate μ.

We gaan eerst actieve redundantie onderzoeken. We bepalen de beschikbaarheid van een n-unit systeem, afhankelijk van het aantal reparateurs k. Het Markovdiagram is dan erg eenvoudig. Het is namelijk precies hetzelfde als we in figuur 7.16 voor een seriesysteem hebben opgesteld. Het enige dat we nog moeten afspreken is de redundantiegraad η van het systeem; met andere woorden: hoeveel units mogen er defect zijn alvorens het systeem uitvalt. Nemen we aan dat we te maken hebben met een m-uit-n systeem (systeem goed zolang er nog minstens m units goed zijn), dan

hebben we het meest algemene geval beschreven. Het probleem is dan evenwel dat we niet meer tot hanteerbare analytische uitdrukkingen voor A_∞ kunnen komen. Voor een numerieke analyse met de computer is dit echter geen bezwaar zoals figuur 7.18 laat zien. Hierin is A(t) gegeven voor een aantal waarden van n, m, k, α, μ en λ.



Figuur 7.18. De beschikbaarheid van een m-uit-n (actief) redundant systeem opgebouwd uit units met een failure rate λ, met k samenwerkende reparateurs die een inzetbaarheid α hebben en een repair rate μ.

Terwille van de berekenbaarheid voeren we nu een aantal vereenvoudigingen in. We veronderstellen dat we evenveel reparateurs k hebben als het systeem groot is, dus k = n. Verder veronderstellen we dat de reparateurs niet samenwerken, maar k = n onafhankelijke reparatiekanalen vormen, dus $\alpha = 0$.
De beschikbaarheid is bij een m-uit-n systeem gelijk aan de som van de eerste $(n-m+1)$ toestandskansen P_{S_i}. In de steady-state toestand geldt:

$$A_\infty = \sum_{i=0}^{n-m} P_{S_i}.$$

Daar elke unit zijn eigen reparateur heeft en dus als onafhankelijk van de rest kan worden gezien, kunnen we het probleem ook anders formuleren. Immers elke combinatie van een unit plus reparateur heeft een beschikbaarheid:

$$A_\infty = \frac{\mu}{\mu + \lambda},$$

en een onbeschikbaarheid:

$$\bar{A}_\infty = \frac{\lambda}{\mu + \lambda}.$$

Voor P_{S_0} moeten er n units beschikbaar zijn, dus:

$$P_{S_0} = \binom{n}{n} \left(\frac{\mu}{\mu + \lambda}\right)^n.$$

Voor P_{S_1} moeten er $(n-1)$ units beschikbaar en één unit onbeschikbaar zijn:

$$P_{S_1} = \binom{n}{n-1}\left(\frac{\mu}{\mu + \lambda}\right)^{n-1}\left(\frac{\lambda}{\mu + \lambda}\right)^1;$$

zodat:

$$A_\infty = \sum_{i=0}^{n-m} \binom{n}{n-i}\left(\frac{\mu}{\mu + \lambda}\right)^{n-i}\left(\frac{\lambda}{\mu + \lambda}\right)^i.$$

Voorbeeld 7.6
Beschouw een actief redundant systeem bestaande uit twee units ($n = 2$, $m = 1$) met failure rate λ. Beide units hebben hun eigen monteur ($k = 2$). De monteurs werken niet samen ($\alpha = 0$). Op basis van het Markovmodel van figuur 7.16 berekenen we dat de steady-state availability is:

$$A_\infty = \frac{\mu^2 + 2\lambda\mu}{(\mu + \lambda)^2}.$$

Met $\beta = \lambda/\mu$ is de onbeschikbaarheid dus te schrijven als:

$$\bar{A}_\infty = \frac{\beta^2}{(1 + \beta)^2}.$$

In de vorige paragraaf hebben we gezien dat de onbeschikbaarheid van één enkele unit met reparatie $\bar{A}_\infty = \beta/(1 + \beta)$ bedroeg. De verbetering door toepassing van redundantie èn reparatie is dus een factor $1/\beta$. Afhankelijk van de grootte van μ ten opzichte van λ kan de verbetering dus enorm groot zijn.

Een ander eenvoudig, tamelijk algemeen geval is een zuiver redundant systeem met $\eta = 1$ (dus $m = 1$), bestaande uit n units die door slechts één reparateur hersteld worden ($k = 1$). We vinden dan voor de onbeschikbaarheid:

$$\bar{A}_\infty = \frac{1}{\sum_{i=0}^{n} \frac{1}{\beta^i i!}}.$$

Voorbeeld 7.7

Beschouw een actief redundant systeem bestaande uit twee units (n = 2, m = 1) met één reparateur (k = 1). Voor zo'n systeem kan worden berekend dat:

$$\bar{A}_\infty = \frac{2\lambda^2}{\mu^2 + 2\mu\lambda + 2\lambda^2} = \frac{2\beta^2}{1 + 2\beta + 2\beta^2}.$$

Voor een niet-redundant systeem met één reparateur gold:

$$\bar{A}_\infty = \frac{\beta}{1 + \beta},$$

zodat de onbeschikbaarheid gereduceerd is met de factor:

$$1 + \frac{1}{\beta(2 + 2\beta)} \approx \frac{1}{2\beta}, \qquad (\beta \ll 1).$$

De verbetering door het invoeren van redundantie is dus ongeveer een factor $1/(2\beta)$. Dit is slechts een factor 2 kleiner dan met twee reparateurs (zie het vorige voorbeeld).

We gaan nu de bedrijfszekerheid $R_S(t)$ en de gemiddelde tijd tot de eerste systeemfout (de MTTFF) van actief-redundante configuraties bepalen. We nemen daartoe aan dat in het algemene Markovdiagram van figuur 7.16 vanuit de toestand $S_{(n-m+1)}$ en hogere toestanden niet meer gerepareerd wordt. Verder blijft het diagram gelijk. Tussen de MTTFF en $R_S(t)$ bestaat het reeds eerder gegeven verband:

$$\text{MTTFF} = \int_0^\infty R_S(t)\,dt,$$

of, als we de Laplace-getransformeerde van $R_S(t)$ kennen:

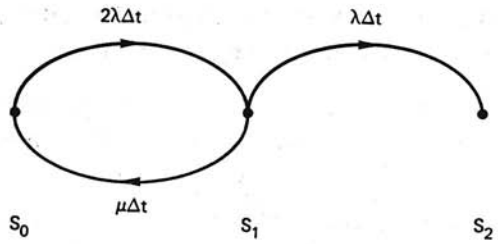
$$\text{MTTFF} = \lim_{s \to 0} R_S(s).$$

We zullen als voorbeeld van de berekeningswijze nu een eenvoudig systeem nemen zoals is geïllustreerd in figuur 7.19. De differentiaalvergelijkingen luiden voor dit homogene systeem:

$$\frac{dP_{S_0}(t)}{dt} = -2\lambda P_{S_0}(t) + \mu P_{S_1}(t)$$

$$\frac{dP_{S_1}(t)}{dt} = 2\lambda P_{S_0}(t) - (\lambda + \mu) P_{S_1}(t)$$

$$\frac{dP_{S_2}(t)}{dt} = \lambda P_{S_1}(t)$$



Figuur 7.19. Het Markovdiagram van een homogeen 1-uit-2 actief-redundant systeem met reparatie van de redundante units.

Met de beginvoorwaarden $P_{S_0}(0) = 1$ en $P_{S_1}(0) = P_{S_2}(0) = 0$ wordt de Laplace-getransformeerde van de bedrijfszekerheid:

$$R_S(s) = P_{S_0}(s) + P_{S_1}(s) = \frac{s + 3\lambda + \mu}{s^2 + (3\lambda + \mu)s + 2\lambda^2}.$$

De MTTFF wordt dus:

$$\text{MTTFF} = \lim_{s \to 0} R_S(s) = \frac{3\lambda + \mu}{2\lambda^2}.$$

Terugtransformeren van $R_S(s)$ naar het tijddomein levert:

$$R_S(t) = \frac{a e^{bt} - b e^{at}}{a - b}$$

waarin:

$$2a = -3\lambda - \mu + \sqrt{\lambda^2 + 6\lambda\mu + \mu^2},$$

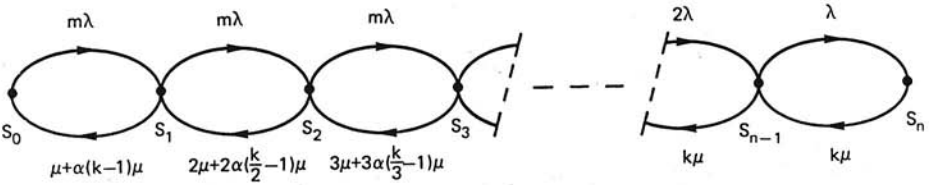
$$2b = -3\lambda - \mu - \sqrt{\lambda^2 + 6\lambda\mu + \mu^2}.$$

In het algemeen is terugtransformeren een complexe zaak. Men kan dan ook vaak met voordeel $R_S(s)$ benaderen met een eenvoudiger terug te transformeren uitdrukking. Met $\beta \ll 1$ blijkt een der polen van de uitdrukking voor $R_S(s)$ klein te zijn ten opzichte van de andere. Wat geeft dat voor benaderde uitdrukking voor $R_S(t)$? (Antwoord: $R_S(t) \approx e^{-t/\text{MTTFF}}$ voor $t \gg 0$).

De verbetering in gemiddelde levensduur door toepassing van reparatie is dus gelijk aan:

$$\frac{3\lambda + \mu}{3\lambda} \approx \frac{1}{3\beta}, \qquad \text{als } \beta = \lambda/\mu \ll 1.$$

We zullen in het volgende *passief-redundante configuraties* en het effect daarop van reparatie bekijken. We gaan daarbij uit van het Markovdiagram voor een m-uit-n passief-redundant homogeen systeem met k tot samenwerking bereide reparateurs die een inzetbaarheid α hebben. Voor dit meest algemene geval vinden we het diagram van figuur 7.20.



Figuur 7.20. Het Markovdiagram van een homogeen m-uit-n passief-redundant systeem met k samenwerkende reparateurs met inzetbaarheid α.

In de literatuur kan men voor de onbeschikbaarheid van zo'n systeem een aantal eenvoudige uitdrukkingen vinden, mits we het systeem iets minder algemeen maken. Veronderstellen we een redundantiegraad $\eta = 1$ (dus $m = 1$) en n onafhankelijke reparatiekanalen met elk één reparateur (dus $k = n$ en $\alpha = 0$) dan vinden we:

$$\bar{A}_\infty = \frac{1}{n! \sum_{i=0}^{n} 1/(i!\,\beta^{n-i})}.$$

Veronderstellen we, afwijkend van het bovenstaande, dat het aantal reparateurs niet gelijk is aan n maar aan 1 (dus $k = 1$) dan vinden we:

$$\bar{A}_\infty = \frac{1}{\sum_{i=0}^{n} 1/\beta^i}.$$

Voorbeeld 7.8
Voor $n = 2$, $m = 1$ en $k = 1$ vinden we:

$$\bar{A}_\infty = \frac{\lambda^2}{\lambda^2 + \lambda\mu + \mu^2} = \frac{\beta^2}{\beta^2 + \beta + 1}.$$

De verbetering ten opzichte van een soortgelijk systeem met actieve redundantie voor $\beta \ll 1$ is ongeveer gelijk aan 2.

Voor het uitrekenen van de bedrijfszekerheid $R_S(t)$ en de MTTFF van het passief-redundante systeem veronderstellen we k samenwerkende reparateurs met inzetbaarheid α die het werk neerleggen op het moment dat de eerste systeemfout optreedt. Hebben we te maken met een m-uit-n systeem,

dan treedt dat op als er $(n - m + 1)$ units defect zijn. Dat houdt in dat de reparatie-overgangskansen uitgaande van alle toestanden S_i in het Markov-diagram van figuur 7.20 nul zijn voor de toestanden $i = n - m + 1$ en hoger. Al deze toestanden kunnen dus gemakshalve worden samengenomen tot een toestand 'system down'.
Het is moeilijk de uitdrukkingen te geven voor het bovenomschreven algemene geval. We zullen hier volstaan met een eenvoudig voorbeeld, namelijk $n = 2$, $m = 1$ en $k = 1$. Hiervoor geldt:

$$R_S(s) = \frac{s + \mu + 2\lambda}{s^2 + (\mu + 2\lambda)s + \lambda^2}.$$

Derhalve wordt:

$$\text{MTTFF} = \lim_{s \to 0} R_S(s) = \frac{\mu + 2\lambda}{\lambda^2}.$$

Vergelijken we dit weer met het overeenkomstige actief-redundante geval, dan zien we dat het passief voorhanden houden van één unit (zoals verwacht) ons ongeveer een factor 2 betere MTTFF geeft. Na terugtransformeren vinden we:

$$R_S(t) = \frac{a e^{bt} - b e^{at}}{a - b},$$

waarin:

$$2a = -2\lambda - \mu + \sqrt{\mu^2 + 4\lambda\mu},$$

$$2b = -2\lambda - \mu - \sqrt{\mu^2 + 4\lambda\mu}.$$

Concluderend kunnen we nu een eenvoudige vergelijking maken tussen een enkelvoudig systeem $(n = 1)$ met één reparateur $(k = 1)$ en een tweevoudig systeem $(n = 2)$ met redundantie $(m = 1)$ dat door twee, niet samenwerkende reparateurs wordt hersteld $(k = 2, \alpha = 0)$ of dat door slechts één reparateur wordt hersteld $(k = 1)$. We onderscheiden daarbij actieve en passieve redundantie. Het resultaat is opgenomen in tabel 7.1.

7.3.5. Gedeelde reparatie

Onder gedeelde reparatie (*shared-repair facilities*) verstaan we de onderhoudssituatie waarbij één reparatiekanaal meerdere systemen moet bewaken. Als de capaciteit van het reparatiekanaal uit één monteur bestaat, moet deze ene monteur de fouten in n systemen opsporen en herstellen; n systemen delen één reparateur.
We hoeven voor de availability-berekening van deze situatie geen nieuw Markovmodel op te zetten. We kunnen het systeem immers bekijken als een

		Verbeteringsfactor			
	één unit	actieve redundantie n = 2, m = 1		passieve redundantie n = 2, m = 1	
	n = 1, k = 1	k = 2, α = 0	k = 1	k = 2, α = 0	k = 1
$\bar{A}_\infty$	$\frac{\beta}{1+\beta}$	$\frac{1}{\beta}$	$\frac{1}{2\beta}$	$\frac{2}{\beta}$	$\frac{1}{\beta}$
MTTFF	$\frac{1}{\lambda}$	$\frac{1}{2\beta}$	$\frac{1}{2\beta}$	$\frac{1}{\beta}$	$\frac{1}{\beta}$

(a)

	Verbeteringsfactor			
	zonder reparatie		met reparatie	
	actief	passief	actief	passief
MTTFF	$\frac{3}{2\lambda}$	$\frac{2}{\lambda}$	$\frac{1}{3\beta}$	$\frac{1}{2\beta}$

(b)

Tabel 7.1. Verbetering van een systeem door het invoeren van redundantie en reparatie.

homogeen seriesysteem bestaande uit n elementen die kunnen falen tijdens reparatie en die bewaakt worden door één reparateur. We krijgen dan ook het Markovmodel van figuur 7.12. De beschikbaarheid van één systeem is nu echter niet gelijk aan P_{S_0}, maar aan:

$$A_\infty = \sum_{i=0}^{n} \frac{(n-i)}{n} P_{S_i}.$$

Nu geldt ook:

$$P_{S_i} = \frac{n!}{(n-i)!}\beta^i P_{S_0},$$

$$P_{S_0} = \frac{1}{\sum_{i=0}^{n} \frac{n!}{(n-i)!}\beta^i}.$$

Voor de beschikbaarheid van een bepaald systeem vinden we dan:

$$A_\infty = \frac{\sum_{i=0}^{n} \frac{n-i}{n(n-i)!}\beta^i}{\sum_{i=0}^{n} \frac{1}{(n-i)!}\beta^i} = \frac{1}{n\beta}\left[1 - \frac{1}{\sum_{i=0}^{n} \frac{n!}{(n-i)!}\beta^i}\right].$$

We kunnen ook eenvoudig de kans P_b bepalen dat de reparateur bezig is met een systeem. Hij is bezig als er minstens één van de n elementen defect is dus:

$$P_b = \sum_{i=1}^{n} P_{S_i} = 1 - P_{S_0}.$$

De kans dat een systeem defect is en de reparateur er mee bezig is (dus het systeem staat *niet* op reparatie te wachten), is te schrijven als:

$$P_r = \frac{1}{n} \sum_{i=1}^{n} P_{S_i}.$$

Deze kans is berekend per systeem; vandaar de factor 1/n. Met deze uitdrukking en die voor A_∞ vinden we voor de kans dat een systeem op reparatie staat te wachten:

$$P_w = \sum_{i=2}^{n} \frac{(i-1)}{n} P_{S_i}.$$

We kunnen het bovenstaande ook anders formuleren. We nemen daartoe de *fractie* van de tijd dat een systeem functioneert (of kan functioneren) ρ_{up}, de fractie van de tijd dat het systeem op reparatie staat te wachten ρ_{wait} en de fractie van de tijd dat het systeem in de reparatie is ρ_{rep}. We krijgen dan:

$$\rho_{up} + \rho_{wait} + \rho_{rep} = 1.$$

Het zal duidelijk zijn dat het hier om gemiddelden gaat tijdens de steady-state van de onderhoudssituatie, dus na zeer veel reparaties. Dan is eenvoudig in te zien dat:

$$\rho_{up} = A_\infty,$$

$$\rho_{wait} = P_w,$$

$$\rho_{rep} = P_r.$$

We kunnen de bovenberekende kansen dus ook zien als (gemiddelde) tijdfracties (in de steady-state).
Het onderlinge verband tussen deze tijdfracties die op één systeem betrekking hebben is ook eenvoudig aan te geven. Namelijk:

$$\frac{\rho_{rep}}{\rho_{up}} = \frac{1/\mu}{1/\lambda} = \frac{\lambda}{\mu} = \beta.$$

Met de bovenstaande uitdrukkingen kunnen we dan eenvoudig de tijdfractie of kans bepalen dat de reparateur bezig is:

$$P_b = nP_r = n\rho_{rep} = n\beta\rho_{up} = n\beta A_\infty = 1 - \frac{1}{\sum_{i=0}^{n} \frac{n!}{(n-i)!}\beta^i}.$$

Voor verschillende waarden van n en β is de beschikbaarheid A_∞ en de bezettingsgraad van het reparatiekanaal P_b gegeven in tabel 7.2.

reparatietijd/faaltijd $\beta = \lambda/\mu$

	$\frac{1}{10}$		$\frac{1}{30}$		$\frac{1}{100}$	
n	P_b	A_∞	P_b	A_∞	P_b	A_∞
1	0,090	0,910	0,032	0,968	0,010	0,9999
2	0,180	0,902	0,064	0,967	0,020	0,9992
5	0,440	0,872	0,161	0,963	0,050	0,9897
10	0,790	0,785	0,319	0,956	0,099	0,9892
20	0,998	0,499	0,620	0,930	0,198	0,9879
30	1,000	0,333	0,868	0,868	0,296	0,9863
40	1,000	0,250	0,986	0,739	0,394	0,9840
50	1,000	0,200	1,000	0,600	0,491	0,9814
60	1,000	0,167	1,000	0,500	0,587	0,9775

Tabel 7.2. De beschikbaarheid A_∞ van een systeem en de bezettingsgraad P_b van het reparatiekanaal als het reparatiekanaal n systemen in onderhoud heeft als functie van $\beta = \lambda/\mu$: de verhouding van (gemiddelde) reparatietijd en faaltijd.

Ook de beschikbaarheid A_∞ kan eenvoudig in ρ_{wait} worden uitgedrukt:

$$A_\infty = \rho_{up} = \frac{1 - \rho_{wait}}{1 + \beta}.$$

N.B.: De beschikbaarheid van n systemen met gedeelde reparatie is kleiner dan die van één systeem met reparatie. De verslechtering is:

$$\frac{A_\infty(n)}{A_\infty(1)} = 1 - \rho_{wait}.$$

Deze uitdrukking is ook direct in te zien door de tijdintervallen gedurende welke een systeem op reparatie staat te wachten uit de tijdas weg te denken.

Gemiddeld zal $\rho_{wait} \ll 1$ zijn, zodat de beschikbaarheid nauwelijks achteruitgaat door een reparateur aan meerdere systemen toe te wijzen. Men kan dan een optimalere bezetting van de reparateur verwezenlijken. Als we de

tijdfractie dat de reparateur gemiddeld genomen bezig kan zijn op 75 % van zijn dagtaak stellen, dan kunnen we met de bovenstaande uitdrukkingen nagaan hoeveel systemen, met een gegeven β, we aan zo'n reparateur kunnen toevertrouwen en de daarbij behorende beschikbaarheid A_∞ van een systeem bepalen. Blijkt deze beschikbaarheid te laag, dan zullen we de capaciteit van het reparatiekanaal moeten verhogen, zodat β kleiner wordt. Dit maakt tevens dat het reparatiekanaal meer systemen aan zal kunnen. Op deze wijze kunnen we een kwantisering geven van de personele inzet die voor het onderhoud van een bepaald bedrijfsgebeuren nodig is en hoeveel mensen er direct beschikbaar moeten zijn bijvoorbeeld op het fabrieksterrein zelf.

Zijn de reparateurs niet direct beschikbaar dan hebben we te doen met een zogenaamde vertraagde reparatie. Als we de distributiefunctie van de vertragingstijd kennen, kunnen we weer grootheden als beschikbaarheid en MTTFF gaan bepalen. Meestal moet dit vanwege de complexiteit numeriek gebeuren.
Voeren we zo'n berekening uit voor een redundant systeem bestaande uit een actieve unit, een passieve redundante unit en een reparateur, dan krijgen we voor een constante wachttijd τ de eenvoudige uitdrukking:

$$\text{MTTFF} = \frac{2\lambda + 2\mu - \mu e^{-\tau\lambda}}{\lambda^2 + \lambda\mu - \lambda\mu e^{-\tau\lambda}}.$$

(De constante wachttijd kan bijvoorbeeld ontstaan door de aanvoertijd van onderdelen uit een centraal depot of de reistijd van een monteur die door de dealer wordt gezonden.) In de vorige paragraaf hebben we reeds s gegevonden dat voor $\tau = 0$ geldt:

$$\text{MTTFF} = \frac{\mu + 2\lambda}{\lambda^2}.$$

De verslechtering door het toelaten van een zekere constante wachttijd τ is dan bij benadering (de MTTFF voor $\tau \neq 0$ gedeeld door die voor $\tau = 0$):

$$\frac{1}{1 + \mu\tau}, \qquad (\tau\lambda \ll 1).$$

De laatste eis houdt in dat de wachttijd τ klein verondersteld wordt te zijn ten opzichte van de gemiddelde levensduur $1/\lambda$ van één unit uit het systeem. Als we deze veronderstelling maken blijkt men meestal (bij benadering) te kunnen rekenen met een effectieve reparatieduur $1/\mu_{\text{eff}}$ die gelijk is aan:

$$1/\mu_{\text{eff}} = 1/\mu + \tau = (1 + \mu\tau)/\mu.$$

De effectieve repair-rate μ_{eff} is dan juist de bovenstaande factor groter dan de repair rate μ:

$$\mu_{eff} = \frac{\mu}{1 + \mu\tau}.$$

Deze praktische benadering vereenvoudigt het rekenwerk drastisch; men kan met een (gecorrigeerde) $\mu = \mu_{eff}$ rekenen.

7.3.6. Inhomogene systemen

We hebben in de vorige paragrafen steeds aangenomen dat de systemen waarmee we te maken hebben homogeen waren. Dat wil zeggen dat we hebben aangenomen dat de units (modules, eenheden) van dat systeem onderling in statistische zin niet onderscheidbaar waren. Ze hadden dus dezelfde failure rate λ en de repair rate μ.
Het zal duidelijk zijn dat deze aanname niet altijd geoorloofd is. De units waarin een seriesysteem is op te splitsen verrichten verschillende operationele deeltaken; het zou dan wel heel toevallig zijn als ze dezelfde failure en repair rates hebben: het zijn immers verschillende units.
Zelfs al hebben we te maken met redundante units die dezelfde operationele (deel-) taak moeten vervullen als de primaire unit die op een bepaald moment geactiveerd is (passieve 1-uit-n redundantie), dan nog zal men de units veelal van verschillende fabrikanten betrekken en inwendig op verschillende wijze realiseren. Dit om afhankelijke fouten, die zoals we in paragraaf 6.4.1 hebben gezien een desastreus effect op de redundantie kunnen hebben, zoveel als maar mogelijk is te vermijden.
De conclusie moet dan ook zijn dat we in de praktijk te maken hebben met *inhomogene systemen*. Terwille van de eenvoud van het rekenwerk benadert men zulke systemen dan toch wel door een homogeen systeem. Wat gebeurt er in een inhomogeen systeem dat essentieel anders is als in een homogeen systeem? We hebben in de vorige paragrafen gezien dat de berekende functies R(t) en A(t) erg saaie functies waren. Dit is bij inhomogene systemen niet meer zo. Dat kunnen we het beste laten zien aan de hazard rate z(t) en aan de overeenkomstige functie a(t) bij een repareerbaar systeem. We hebben reeds gezien in paragraaf 3.2.1 dat geldt:

$$z(t) = \frac{f(t)}{R(t)} = \frac{-1}{R(t)} \cdot \frac{dR(t)}{dt}.$$

We definiëren overeenkomstig in het repareerbare geval:

$$a(t) = \frac{-1}{A(t)} \cdot \frac{dA(t)}{dt}.$$

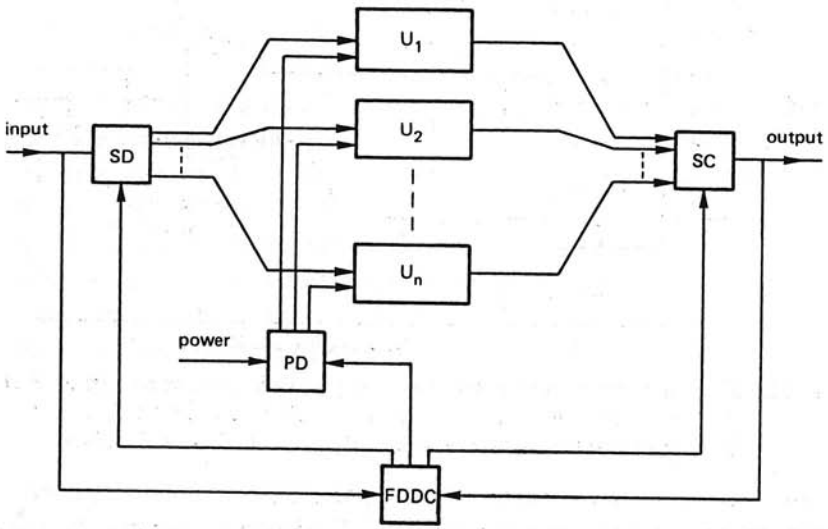
Wat houden deze twee grootheden nu in? Daartoe herschrijven we z(t) en a(t) als volgt:

$$z(t) = -\frac{\Delta R(t)/R(t)}{\Delta t},$$

$$a(t) = -\frac{\Delta A(t)/A(t)}{\Delta t}.$$

We zien dus dat deze grootheden de relatieve afname van R(t) respectievelijk A(t) per eenheid van tijd aangeven. Als er veranderingen in deze twee functies zijn waar te nemen, zullen deze veranderingen goed te zien zijn in z(t) en a(t). Deze beide functies zijn dus goed te gebruiken voor de analyse van de overgangssituatie na $t = 0$ en voordat de steady-state intreedt. In deze overgangssituatie doen zich namelijk de verschillen voor met een homogeen systeem zoals we in het navolgende zullen zien.

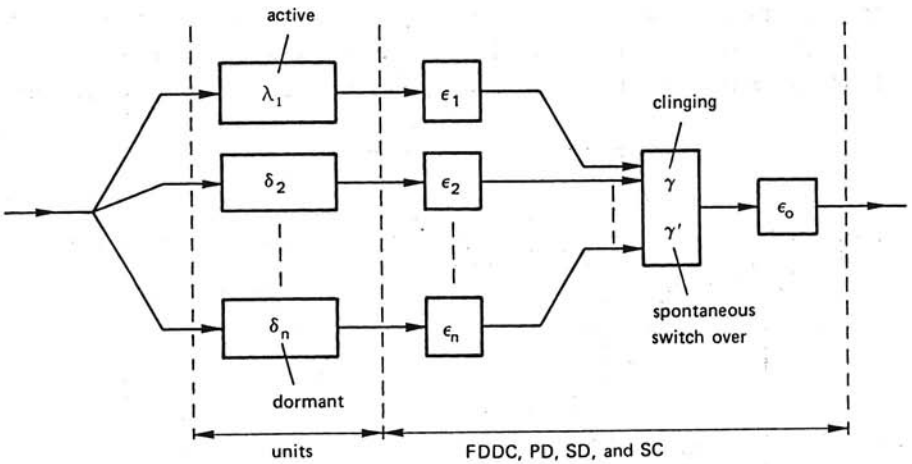
We zullen nu een voorbeeld geven van een inhomogeen systeem en dat systeem analyseren aan de hand van z(t) en a(t). Het systeem is afgebeeld in figuur 7.21. De ingangs- en uitgangssignalen in dit systeem worden omgeschakeld met respectievelijk SD en SC. Deze circuits voorkomen tevens dat een ingangsfout in één van de units (bijvoorbeeld kortsluiting naar aarde) of een uitgangsfout (bijvoorbeeld uitgang kortgesloten tegen de voedingsspanning) de systeemingang of -uitgang blokkeert en aldus een 'common-cause failure' zou vormen. Behalve voor *omschakelen* dienen deze circuits ook voor *foutisolatie*. Hetzelfde geldt voor de toevoer van voedings-



Figuur 7.21. Een algemeen functioneel model van een 1-uit-n redundant systeem. SD is een 'Signal Distributor' circuit, SC is een 'Signal Combination' circuit. PD is een 'Power Distributor' circuit en FDDC is een 'Fault Detection, Decision and Correction' circuit.

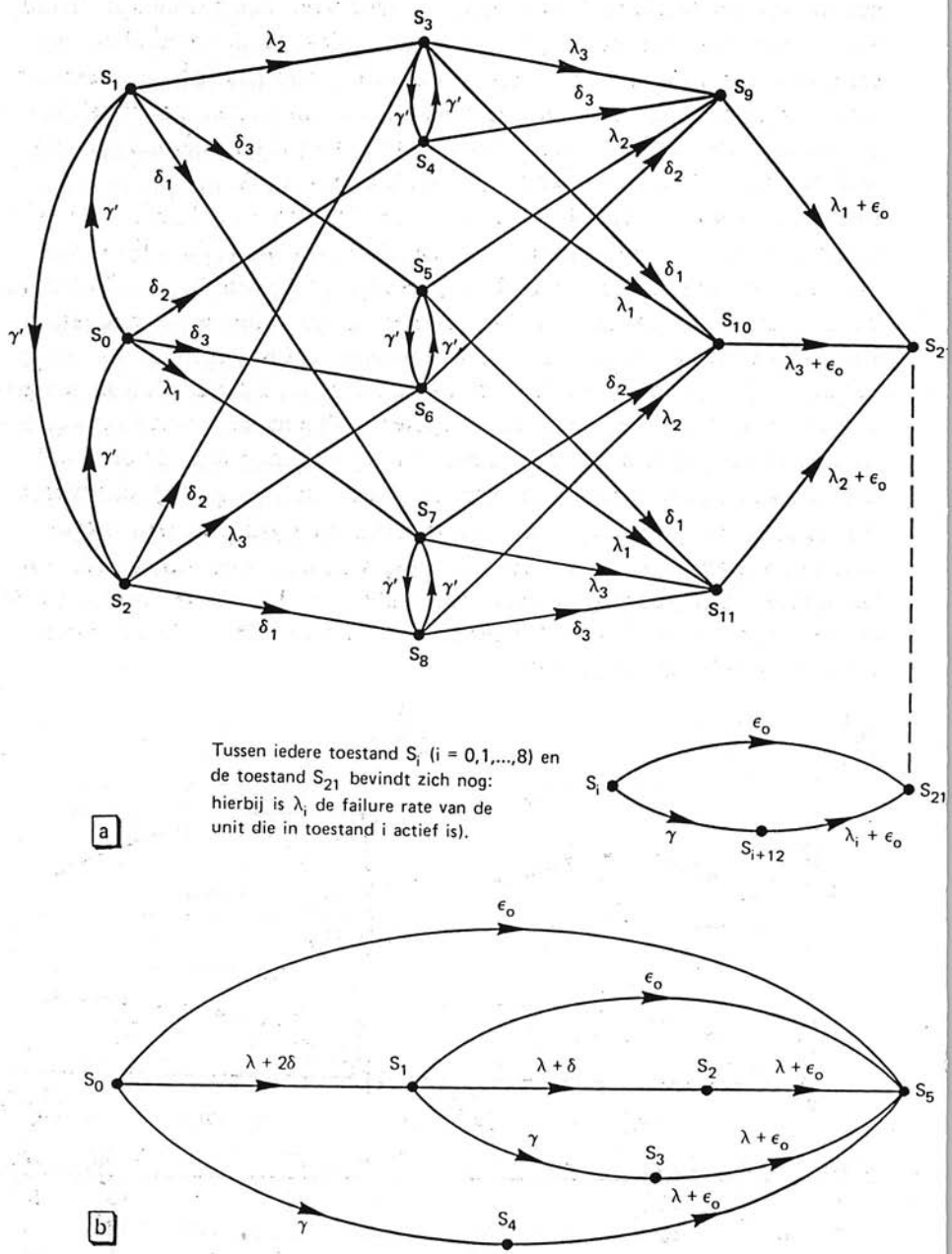
energie via PD. De circuits PD, SD en SC worden gestuurd vanuit FDDC. Dit circuit vergelijkt het ingangs- en uitgangssignaal van het systeem met elkaar en *detecteert* fouten in het functioneren van het systeem. Het circuit *beslist* welke actie moet worden ondernomen (afschakelen, aanschakelen, middelen over meerdere correct functionerende units, enzovoort). Verder *corrigeert* het circuit de fout in de vorm van stuursignalen voor PD, SD en SC.

In figuur 7.22 is het bedrijfszekerheidsmodel van dit systeem weergegeven. Als een unit ingeschakeld staat, is de failure rate λ_i, als hij afgeschakeld staat δ_i. De schakelfunctie van de FDDC kan falen door te blijven kleven op een reeds ingeschakelde unit (failure rate γ) en door ten onrechte spontaan over te schakelen naar een andere unit, terwijl de vorige nog goed was (γ'). De eerste fout merkt men pas wanneer de ingeschakelde unit faalt. De tweede fout verstoort alleen de volgorde van inschakelen. We nemen namelijk aan dat na de laatste unit weer de eerste wordt ingeschakeld in een poging toch nog een goede unit te vinden. Alle 'common-cause failures' zijn gemodelleerd in ϵ_0. De fouten ϵ_i ($i \neq 0$) zijn losse verbindingen, beslissingsfouten enzovoort.



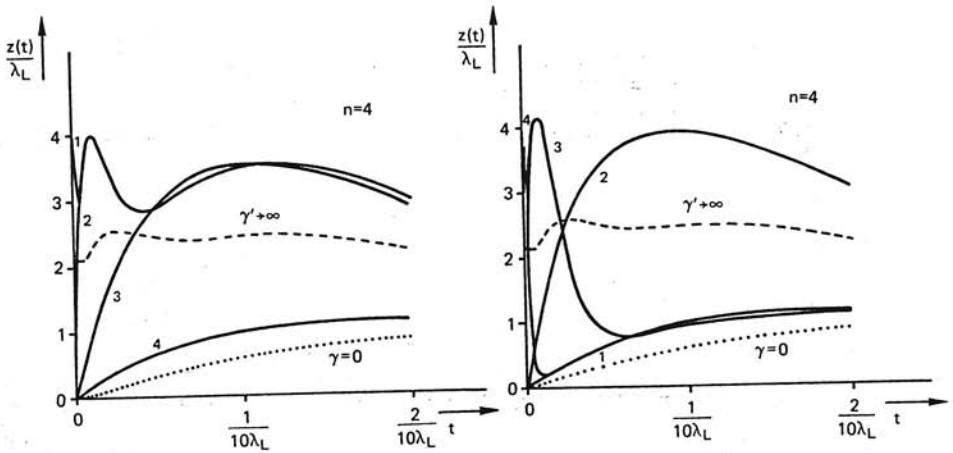
Figuur 7.22. Een algemeen bedrijfszekerheidsmodel van het systeem uit figuur 7.21. λ is de failure rate in actieve toestand, δ de niet-actieve toestand. De overige failure rates modelleren de FDDC-, PD-, SD- en SC-circuits.

In figuur 7.23 is het Markovmodel van figuur 7.22 gegeven. We hebben hier aangenomen dat het gaat om een 1-uit-3 redundant systeem. In de figuur eronder zien we hoe dit diagram zou reduceren als we homogeniteit zouden veronderstellen, dus als $\lambda_i + \epsilon_i = \lambda$ en $\delta_i = \delta$. De complexiteit van het inhomogene model is zo groot dat we onze toevlucht hebben genomen tot het numeriek oplossen met een computer van de differentievergelijkin-



Figuur 7.23. Het Markovdiagram van het systeem uit figuur 7.22, aannemende dat we met één-uit-drie redundantie te doen hebben; (b) het systeem zou heel eenvoudig worden als het homogeen verondersteld zou worden. λ_i en ϵ_i zijn samengenomen tot één λ_i.

gen die uit het Markovmodel volgen. De resultaten zijn vermeld in figuur 7.24. Deze resultaten zijn geplot voor een 1-uit-4 passief-redundant systeem (dus n = 4 en $\delta_i = 0$). In plaats van monotoon naar de eindwaarde te stijgen, zoals dat bij homogene systemen het geval is, kan z(t) tijdelijk groter worden dan de eindwaarde en kan z(t) één of meer maxima vertonen (dus pieken in de relatieve uitval per eenheid van tijd).
Het enige verschil tussen de acht genummerde curven uit figuur 7.24 is het verschil in de inschakelvolgorde. De vier gebruikte units zijn gelijkwaardig, maar hebben failure rates die onderling een factor 10 verschillen. We zien nu dat er maxima in z(t) ontstaan dordaat eerst slechte units worden ingeschakeld en bovendien de kleefkans van nul verschillend is. Dit heeft tot gevolg dat het systeem kan blijven 'hangen' op een slechte unit wat tijdelijk een grotere uitval geeft. Als er geen kleven optreedt tijdens de levensduur van deze unit kan het systeem blijven kleven op de volgende unit. Is deze unit ook slechter dan de beste, dan geeft dit weer een piek in z(t), enzovoort. Als de kans op spontaan, onterecht overschakelen groot is, wordt elke unit vele malen tijdens zijn levensduur ingeschakeld waardoor de z(t) van het systeem zich gedraagt als het gemiddelde van de overige curven. Dit is de gestreepte curve $\gamma' \to \infty$. De gestippelde curve geeft de situatie weer voor een kleefkans nul ($\gamma = 0$).

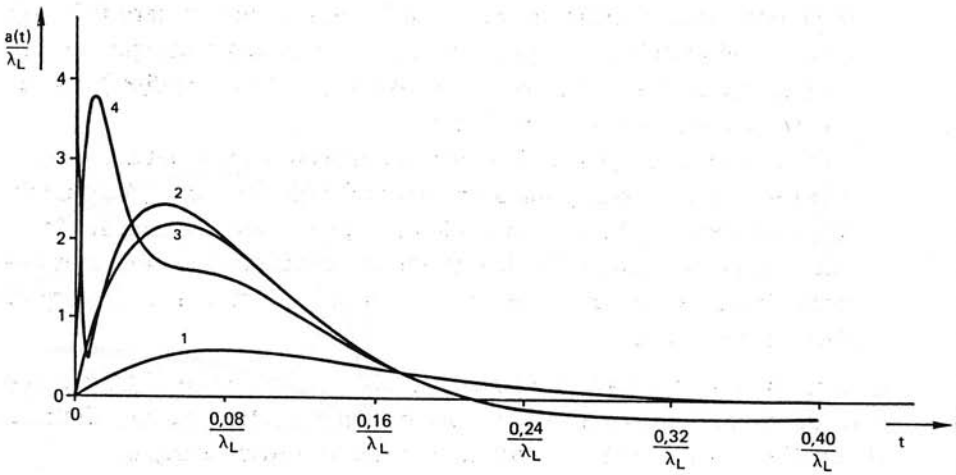


Curve	λ_1/λ_L	λ_2/λ_L	λ_3/λ_L	λ_4/λ_L
1	10^3	10^2	10	1
2	10^2	10	1	10^3
3	10	1	10^3	10^2
4	1	10^3	10^2	10

Curve	λ_1/λ_L	λ_2/λ_L	λ_3/λ_L	λ_4/λ_L
1	1	10	10^2	10^3
2	10	10^2	10^3	1
3	10^2	10^3	1	10
4	10^3	1	10	10^2

Figuur 7.24. De hazard rate z(t) van een inhomogeen 1-uit-4 passief-redundant systeem met een imperfecte inschakeling van redundante units. λ_L is de failure rate van de beste unit. Spontaan overschakelen komt niet voor ($\gamma' = 0$). De schakelaar kleeft met $\gamma = 10\lambda_L$. Er treden geen common-cause failures op ($\epsilon_0 = 0$).

We zullen nu reparatie in het systeem van figuur 7.21 invoeren en dan de functie a(t) met de computer bepalen. We kunnen verschillende reparatiestrategieën volgen. Zo kunnen we bijvoorbeeld een defecte unit meteen gaan repareren met repair rate μ_i (i = 1,2, . . . ,n). Het repareren van een klevende schakelaar is wat lastiger omdat deze fout pas manifest wordt als de bijbehorende unit faalt. Voor detectie van zulke kleeffouten moet de reparateur het systeem dus opzettelijk verstoren, zodat een nieuwe unit wordt ingeschakeld. Is dit altijd toelaatbaar en kan een defecte schakelaar altijd zonder het systeem uit te zetten worden gerepareerd? Waar moet minstens voor gezorgd worden om het systeem door deze bewust geïntroduceerde verstoring niet te laten uitvallen?
In het algemeen blijven zulke fouten als kleeffouten vaak ongedetecteerd; de *coverage* van een systeeminspectie is niet 100 %; er blijven gemaskeerde fouten in het systeem achter. We zullen derhalve veronderstellen dat het systeem mag uitvallen en we na systeemuitval met de repair rate μ alle defecte komponenten weer herstellen, waardoor het systeem na reparatie weer als nieuw is. Wat betekent dit voor het Markovdiagram? In figuur 7.25 is a(t) getekend voor verschillende situaties. Verklaar zelf de vorm van de gegeven curven.



Curve	λ_1/λ_L	λ_2/λ_L	λ_3/λ_L	λ_4/λ_L
1	1	10	10^2	10^3
2	10^3	10^2	10	1
3	10^2	10	10^3	1
4	10^3	10	10^2	1

Figuur 7.25. De a(t)-functie van een inhomogeen passief-redundant systeem met reparatie: repair rate μ = 10, n =4, γ =10 en γ' = 0.

7.4. Onderhoudsaspecten

In deze paragraaf zullen we een aantal belangrijke aspecten van de instandhouding van technische systemen door één of meer vormen van onderhoud aan de orde stellen. Deze instandhouding omvat natuurlijk niet alleen het in stand houden van de *functie* van het systeem (*auto*: transportfunctie, *telefoon*: communicatiefunctie), maar ook de *veiligheid* van dat systeem (*auto*: versleten veiligheidsgordels vervangen, *telefoon*: reparatie van de twee anti-parallelle dioden over de microtelefoon om gehoorbeschadiging door stoorpieken te voorkomen).
We zullen eerst een aantal onderhoudsstrategieën bespreken.

7.4.1. Onderhoudsstrategieën

In het begin van hoofdstuk 7 hebben we reeds benadrukt dat het enige wat de gebruiker bij een kant en klaar systeem nog kan doen om de beschikbaarheid te vergroten is zijn onderhoudsstrategie te optimaliseren. Door zijn (onderhoudsbewuste) ontwerp heeft het systeem inherent meegekregen van de fabrikant een tweetal eigenschappen:

- *onderhoudsarmheid*. Voorbeelden zijn: onderhoudsvrije accu's (nikkel-cadmium) die niet zoals gewone accu's moeten worden bijgevuld, zelfsmerende gesloten lagers die voor hun levensduur met smeermiddel zijn gevuld, zelf-nastellende koppeling en remmen in een auto, gebruik van constructiematerialen die geen conservering (verf en dergelijke) behoeven zoals aluminium en kunststoffen;
- *onderhoudsvriendelijkheid*. Voorbeelden hiervan zijn: modulair opgebouwde systemen met gemakkelijk toegankelijke en vervangbare modulen, systemen opgebouwd uit slechts een gering aantal verschillende units (grote aantallen onderling gelijke en uitwisselbare units). Automatische foutindicatie, controle-lampjes, testprogramma's met uitgebreide foutdiagnoses, enzovoort.

Gegeven deze eigenschappen kan de gebruiker (daarin meestal geadviseerd door de systeemontwerper of -producent) een bepaalde onderhoudsstrategie uitstippelen op basis van kosten- en veiligheidsoverwegingen.
We hebben ook reeds gezien dat we correctief en preventief onderhoud kennen. *Correctief onderhoud* is vaak duur door de gevolgschade (verlies van produktiecapaciteit, produktie van defecte produkten, het 'vastdraaien' van machines, enzovoort). Met *preventief onderhoud* alleen komt men er niet, er zal altijd een zekere kans op het onverwacht uitvallen van het systeem zijn. (Voorbeeld: kapotte autoruit.) Men heeft altijd nog correctief onderhoud nodig.
Een zeer lichte vorm van preventief onderhoud, dat meestal door het laagste onderhoudsniveau (de gebruiker zelf) wordt verricht, is het zogenaam-

de *verzorgende onderhoud*. Dit omvat eenvoudige controles, inspecties en bij- en afstelhandelingen. Voorbeelden hiervan zijn: het schoonmaken van de koppen van een cassetterecorder met een wattenstaafje met alcohol, het testen van een aardlekschakelaar, het smeren van eenvoudige constructies, enzovoort. Bij *periodiek onderhoud* vervangt men alle verdachte componenten (ingebrande weerstanden) of kapotte componenten (redundantie) na het verlopen van een bepaald aantal bedrijfsuren, het overschrijden van een bepaalde geaccumuleerde belasting of een bepaald aantal afgelegde kilometers. Bij *op conditie gebaseerd onderhoud* grijpt men in als de gemeten conditie van het systeem daartoe aanleiding geeft.
Men kent *direct* en *getrapt onderhoud*. Het directe onderhoud gebeurt locaal op de plek waar het systeem zich bevindt, meestal door eigen personeel. Bij getrapt onderhoud vervangt men delen van het systeem en zendt deze delen op voor reparatie in een centrale werkplaats, bijvoorbeeld bij de dealer of fabrikant. Voorbeelden: lekke autoband, defecte meetapparatuur.
Er zit aan onderhoud ook een *logistiek aspect*. Men moet namelijk over voldoende *reserve-onderdelen* kunnen beschikken. Daartoe kan men een locale voorraad aanleggen ter plaatse van het systeem (voorbeeld: smeltveiligheden). Men kan ook gebruik maken van een centraal magazijn (voorbeeld: gangbare elektronische componenten) of de reserve-onderdelen bestellen bij de fabrikant (voorbeeld: elektromotor van een schijfgeheugen). Men vertrouwt er daarbij op dat de fabrikant een voldoende grote voorraad van alle onderdelen van vroeger geproduceerde systemen gedurende voldoende lange tijd aanhoudt. Daar dit een enorme kapitaalinvestering inhoudt wordt door sommige fabrikanten met deze naleverbaarheid wel eens de hand gelicht. Het is daarom verstandig om voor strategische systeemdelen een 'second source' leverancier te hebben.
Een gelijksoortig logistiek probleem doet zich voor als het *onderhoudspersoneel* van de ene plaats naar de andere moet reizen voor het plegen van onderhoud (voorbeeld: computeronderhoud middels een onderhoudsabonnement afgesloten met de fabrikant).
Systeemuitval is een stochastisch proces waarin grote uitschieters kunnen voorkomen. Als door toevallig grote uitval de *reparatiecapaciteit* van de *onderhoudsdienst* wordt overschreden, heeft men te maken met een extra wachttijd.
Men kan veel van deze problemen verlichten door systemen met *redundantie* toe te passen en door de *gebruiker* of *operator* van het systeem zelf *eenvoudige correctiehandelingen* te laten plegen. Eventueel wordt het systeem door deze handelingen niet geheel teruggebracht tot zijn nominale functie maar kan het toch nog een *deeltaak* uitvoeren om de tijd tot professionele reparatie te overbruggen.

Het zal duidelijk zijn dat alle genoemde aspecten tezamen voor een bepaald systeem de onderhoudsstrategie bepalen. Men geraakt tot deze strategie door registratie van storingsgegevens, door ervaringen opgedaan met vroegere systemen, door adviezen van de fabrikant en 'last but not least' door het 'engineering judgement' van de systeemgebruiker zelf. Het is daarbij van belang voor het onderhoudspersoneel dat men duidelijk maakt welke serviceverlening wordt verlangd. Men onderscheidt wel de navolgende 'repair policies':

1. First come, first served (first in, first out).
2. Last come, first served (last in, first out).
3. Random service sequence (sequential in, random out).
4. Priority service discipline.

De eerste 'policy' treedt automatisch op door het pijplijneffect van een reparatiekanaal met een te lage capaciteit. Bij de tweede manier van werken spreekt men af dat men per karwei een korte tijd ter beschikking heeft; langer durende klussen worden doorgeschoven. De derde manier van werken is er een die door ontaarding ontstaat. Deze treedt namelijk op als men hobbyistisch te werk gaat. Men vindt sommige onderhoudswerkzaamheden leuker dan andere; de 'leukere' krijgen voorrang. Bij de vierde manier van werken heeft men verschillende klanten (of systemen) die ieder hun eigen prioriteiten hebben; men werkt volgens dit prioriteitenlijstje.

7.4.2. Voorraad reserve-onderdelen

Voorraden reserve-onderdelen vergen een zekere kapitaalinvestering. Zo'n investering geeft dus een zekere rentelast. Aan de ene kant is het derhalve wenselijk zo weinig mogelijk reserve-onderdelen in voorraad te hebben. Aan de andere kant moeten we er voldoende van hebben zodat het onderhoud niet geblokkeerd zal raken. Het probleem is nu hoeveel *reserve-onderdelen* (*spare parts*) moeten we in voorraad houden om met de kans P_S over het tijdinterval (0,T) geen blokkering van het onderhoud te krijgen. Dit is het zogenaamde '*spare-parts provisioning*'-probleem.
Laten we aannemen dat we te doen hebben met een seriesysteem van n componenten. Gemakshalve stellen we dat de componenten onderling identiek zijn. Verder hebben we M reserve componenten. Het aantal fouten op het tijdstip T in het seriesysteem is N(T). Dit aantal is dus juist gelijk aan het aantal vervangen componenten, mits de voorraad groot genoeg is. We zijn nu geïnteresseerd in de oplossing van:

$$P\,(N(T) \leqslant M) \geqslant P_S.$$

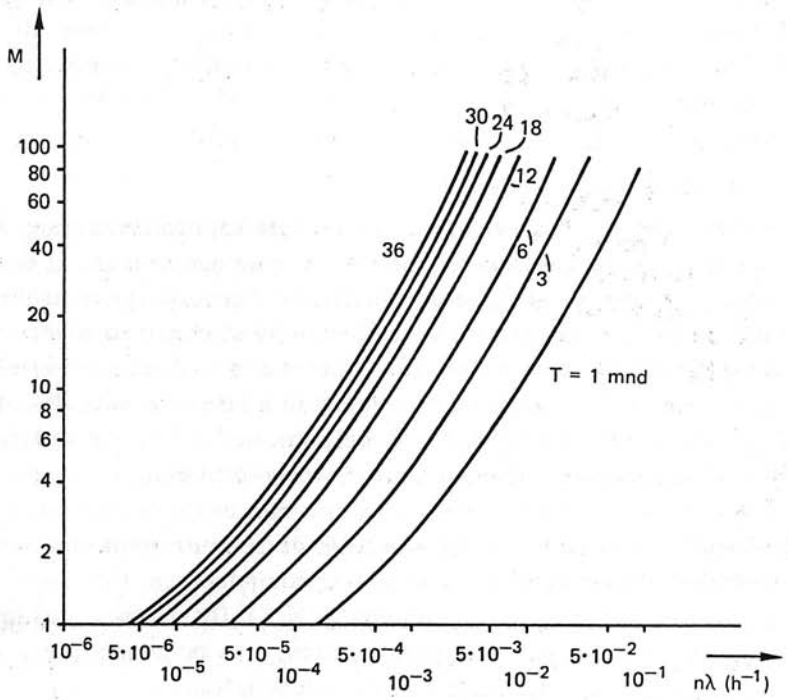
Als we aannemen dat de failure rate van de individuele componenten λ is, dan vinden we:

$$P(N(T) \leqslant M) = \sum_{i=0}^{M} \frac{(n\lambda T)^i e^{-n\lambda T}}{i!}.$$

Deze uitdrukking is gemakkelijk op te stellen. We hebben immers te doen met een seriesysteem met een failure rate $n\lambda$, waaraan in passieve redundantie M componenten parallel staan. De uitdrukking voor een R(T) van dit systeem hebben we reeds in paragraaf 6.4 gegeven. Deze is juist gelijk aan de bovenstaande uitdrukking.
Uit de bovenstaande uitdrukkingen kunnen we bij gegeven n, λ, T en P_S het aantal reserve-onderdelen M bepalen, immers:

$$P_S = e^{-n\lambda T} \sum_{i=0}^{M} \frac{(n\lambda T)^i}{i!}.$$

In figuur 7.26 is deze uitdrukking grafisch weergegeven voor $P_S = 0{,}9$. Voor verschillende bedrijfsuren T en effectieve failure rate $n\lambda$ is daaruit het vereiste aantal reserve-onderdelen M te bepalen dat nodig is om met een kans van 0,9 geen blokkering van het onderhoud te krijgen.



Figuur 7.26. Het aantal reserve-onderdelen M dat benodigd is bij verschillende bedrijfsduren T als functie van de effectieve failure-rate $n\lambda$, waarbij de kans Ps om geen uitputting van de voorraad te verkrijgen gelijk is aan 0,9.

Opgaven

7.1. Wat verstaat men in de bedrijfszekerheidstechniek onder een onderhoudbaar systeem en wat onder een onderhouden systeem?

7.2. Wat verstaat men in de bedrijfszekerheidstechniek onder preventief onderhoud en waaraan moet de hazard rate z(t) van een systeem voldoen opdat preventief onderhoud zinvol is?

7.3. Welke kosten omvat de optimalisatie van de '*life cycle cost*' van een systeem?

7.4. Een systeem bestaat uit twee actief redundante units, ieder met een failure rate λ. De twee units falen stochastisch onafhankelijk.
   a. Hoe groot is de MTTF?
   b. Als er periodiek onderhoud wordt gepleegd, met een tijdinterval T, hoe groot is dan de MTTFF? (*Het onderhoud kost geen tijd en het systeem is na een onderhoudsbeurt als nieuw.*)

7.5. Aan een systeem met een bedrijfszekerheid $R(t) = 1 - \frac{1}{2}t$ op het interval $0 \leqslant t \leqslant 2$ wordt perfect periodiek onderhoud gepleegd met een periodeduur $T = 1$.
   a. Schets het verloop van de bedrijfszekerheid $R_S(t)$ van dit systeem versus de tijd t.
   b. Hoe groot is de gemiddelde levensduur θ van dit systeem (dus de MTTFF)?

7.6. Van een machinepark, bestaande uit n identieke machines, is het noodzakelijk dat allen functioneren voor het correct functioneren van een proces. Bij het falen van één of meer machines laat men de andere machines tijdens de reparatie in bedrijf. Voor iedere machine is een monteur aanwezig. De monteurs werken niet samen aan een machine. De repair rate is μ per monteur, de failure rate is λ per machine en de machines falen stochastisch onafhankelijk.
   a. Geef het Markovdiagram van het bovenstaande onderhoudbare systeem.
   b. Bepaal aan de hand van dit Markovdiagram een uitdrukking voor de steady-state availability A_∞ van dit systeem.

7.7. Teken het Markovdiagram van een homogeen 2-uit-3 passief redundant systeem met twee samenwerkende reparateurs met inzetbaarheid α. (De repair rate is μ per reparateur, de failure rate is λ per unit.)

7.8. Een onderzeeër beschikt voor de voortstuwing over twee identieke elektromotoren die elk afzonderlijk voldoende capaciteit hebben om op kruissnelheid te kunnen varen. De motoren falen onafhankelijk van elkaar en hebben altijd een failure rate λ_m. In normaal bedrijf zijn

beide motoren actief. De benodigde elektrische energie wordt opgewekt door een dieselgenerator met failure rate λ_g. Indien de dieselgenerator uitvalt dan wordt de energievoorziening overgenomen door een accu-batterij, die niet kan falen zolang deze geen energie levert. De accu-batterij kan slechts voor een beperkte tijd stroom leveren. De (tijdafhankelijke) hazard rate van de accubatterij bedraagt $z_a(t-t_0)$, waarbij t_0 het tijdstip voorstelt waarop de accu-batterij ingeschakeld wordt. Het gehele systeem faalt indien de voortstuwing wegvalt.
Teken het Markovdiagram dat bij dit systeem hoort en geef *duidelijk* de betekenis van de toestanden, de overgangen en de begin- en eindtoestanden aan.

7.9. Teken het Markovdiagram van een homogeen 2-uit-4 passief redundant systeem met twee niet-samenwerkende reparateurs (inzetbaarheid $\alpha = 0$), als gegeven is dat de reparateurs pas gaan repareren als minstens twee units gefaald hebben en daarna doorgaan tot alle units weer gerepareerd zijn. (De repair rate is μ per reparateur, de failure rate is λ per unit en het systeem wordt niet uitgeschakeld tijdens de reparatie.)

7.10. Een telefoonkabel heeft drie lijnen; langs elke lijn kan één gesprek gevoerd worden. De gespreksaanvragen komen onafhankelijk van elkaar binnen met een gemiddelde frequentie λ.
Als er geen vrije lijn is wordt een gespreksaanvraag geweigerd.
Als verder gegeven is dat de gespreksduur negatief-exponentiëel verdeeld is met gemiddelde $1/\mu$, bereken dan de steady-state beschikbaarheid van deze kabel (dat wil zeggen de kans op één of meer vrije lijnen).

7.11. De bedrijfszekerheid van een systeem wordt gegeven door

$$R(t) = \frac{\tau}{t+\tau}, \text{ met } 0 \leqslant t \leqslant \infty \text{ en } \tau > 0.$$

Men besluit periodiek onderhoud op dit systeem te gaan toepassen met een periodetijd T. De tijd nodig voor dit periodieke onderhoud wordt verwaarloosbaar klein verondersteld en het systeem is na onderhoud als nieuw.

a. Hoe groot is de gemiddelde levensduur (MTTFF) van dit systeem voor $T = \tau$, en voor $T = 3\tau$?
b. Voor welke van deze twee waarden van T is de gemiddelde levensduur het grootst, en hoe is dat te verklaren?

7.12. Een systeem bestaat uit twee units in actieve redundantie. De units hebben een constante failure rate λ van 10^{-3} per uur en falen stochastisch onafhankelijk.

a. Indien geen correctief onderhoud op unit niveau wordt gepleegd,

hoe groot is dan de MTTFF?

b. Hoe groot wordt de MTTFF als er wel op unit niveau wordt gerepareerd indien de repair rate μ 10^{-1} per uur bedraagt?

c. Hoe groot is in het geval b de aanspreekfrequentie van het reparatiekanaal als we mogen stellen dat geldt $\lambda \ll \mu$?

d. De reparatiekosten van een unit bedragen fl. 500,– per keer. Als het systeem echter 'down' gaat dan bedragen de kosten, mede door het optredende produktieverlies, fl. 5 000,– per keer. Bepaal op basis van de uitkomsten van a, b en c of het economisch verantwoord is correctief onderhoud te plegen op unitniveau.

7.13. Een klep kan op twee wijzen falen, namelijk hij kan open blijven staan of gesloten blijven. De 'open' failure mode heeft een constante failure rate λ_1 en repair rate μ_1. Evenzo heeft de 'gesloten' failure mode een failure rate λ_2 en een repair rate μ_2.
Hoe groot is de steady-state availability van deze klep?

7.14. Een sleepboot moet een booreiland verslepen van Noorwegen naar de Golf van Mexico. Voor het goed functioneren van het communicatiesysteem is het noodzakelijk dat zowel de zend- als ontvangstapparatuur goed functioneren. Beide hebben een failure rate van 10^{-3} per uur en kunnen tijdens de reis niet gerepareerd worden: slechts vervanging is mogelijk. De reis duurt 6 weken (1000 uur) zonder dat er gebunkerd kan worden.
Hoeveel reserve zenders en ontvangers moeten er meegenomen worden opdat de kans dat het communicatiesysteem niet meer goed functioneert tijdens de reis kleiner is dan 2 %, als er verder gegeven is dat zender en ontvanger onafhankelijk van elkaar falen en dat een zender of ontvanger in reserve niet kan falen?

N.B.: De terugtransformatie van $\frac{a^i}{(s+a)^{i+1}}$ is $\frac{(at)^i}{i!} e^{-at}$.

7.15. a. Een fotozetmachine bestaat uit een mechanisch en een elektronisch deel. Het elektronische deel is dubbel uitgevoerd in de vorm van actieve redundantie. Het mechanische deel heeft een failure rate λ_m, terwijl ieder van de twee elektronische units een failure rate λ_e heeft. Het falen geschiedt stochastisch onafhankelijk.
Teken het catastrofale faalmodel van het hierboven beschreven systeem en bereken hieruit de bedrijfszekerheid.

b. Men besluit onderhoud te gaan plegen aan de fotozetmachine van a. Hiervoor zijn twee reparateurs nodig: één voor het mechanische deel en één voor het elektronische deel.

De repair rate voor het mechanische gedeelte is μ_m en de repair rate voor ieder van de elektronische units is μ_e.
De machine wordt tijdens de reparatie niet uitgeschakeld.
Daar de twee monteurs niet gelijktijdig aan de machine kunnen werken, is de volgorde van reparatie als volgt vastgelegd:

- De hoogste prioriteit heeft het functioneren van één van de beide elektronische units, daar hiermee het functioneren van het mechanische deel getest kan worden.
- Daarna komt het functioneren van het mechanische gedeelte, daar de fotozetmachine na reparatie hiervan weer correct kan functioneren.
- De laagste prioriteit voor reparatie heeft de redundante elektronische unit.

Stel het Markovdiagram op voor het systeem met een dergelijke onderhoudsstrategie en specificeer de daarin gebruikte toestanden en geef de begin- en de 'system-down'-toestand(en) aan.

c. We nemen nu aan dat bij de onderhoudsstrategie van b het systeem wordt uitgeschakeld tijdens de reparatie, zodra het systeem niet meer kan functioneren (dus als het mechanische deel gefaald heeft of als de twee elektronische units gefaald hebben). Verder nemen we aan dat de systeemdelen die op dat moment nog goed zijn tijdens deze afschakeling niet kunnen falen. Als we veronderstellen dat het systeem weer wordt ingeschakeld zodra dit weer kan functioneren (dus minimaal moet het mechanische deel en één elektronische unit goed functioneren), wat is dan de steady-state availability A_∞ van dit systeem, gegeven dat $\lambda_e/\mu_e = 0{,}1$ en $\lambda_m/\mu_m = 0{,}01$?

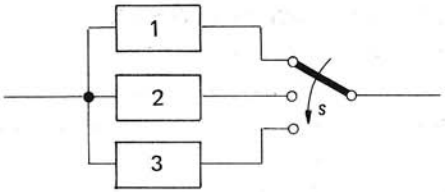
7.16. Verklaar waarom een aantal van de in figuur 7.25 getekende functies a(t) negatief worden.

7.17. Een drukkerij werkt met een drukpers met een faaldistributie die voor tijdsintervallen kleiner dan 10^5 uur benaderd kan worden door:

$$F(t) = 50 \cdot 10^{-12}\, t^2.$$

Om het verlopen van de afstelling van de drukpers en om plaatselijke slijtage te corrigeren wordt er periodiek onderhoud gepleegd, waarna de pers weer als nieuw is. De tijdsduur van de onderhoudsbeurten kan verwaarloosd worden.

a. Bereken en schets de beschikbaarheid A(t) voor het geval dat eens per $50 \cdot 10^3$ uur onderhoud gepleegd wordt.
b. Bereken de gemiddelde beschikbaarheid A(t) van de drukpers voor het interval $[0,\infty)$.



7.18. Een passief redundant systeem bestaat uit drie identieke units en een schakelaar (zie figuur). Steeds wanneer de geactiveerde unit faalt wordt er overgeschakeld naar de volgende unit. In stand drie kan er natuurlijk niet meer verder geschakeld worden.

De schakelaar kent twee fouten:

- Een 'kleeffout' waardoor overschakelen niet meer mogelijk is. De failure rate is $\lambda_k = 1$.
- Een intermitterende fout veroorzaakt door stoorpulsen uit het lichtnet die de schakelaar (onterecht) een stap verder laten schakelen. De tijd tussen twee opeenvolgende stoorpulsen is negatief exponentieel verdeeld met $\lambda_s = 1$.

Zodra het systeem faalt wordt er gerepareerd totdat alles weer functioneert. Gedurende de reparatie kan er niets falen. Als gegeven is dat de units een failure rate $\lambda = 2$ hebben en dat de repair rate van het systeem $\mu = 100$ bedraagt bereken dan de MTTFF en de steady-state availability.

7.19. Een ertstrein, bestaande uit 20 wagons en 3 diesellocomotieven kan rijden indien minstens 2 locomotieven èn alle gebruikte koppelingen correct functioneren.

In het geval dat alle locomotieven correct functioneren hebben ze een failure rate λ_1. Bij één gefaalde locomotief hebben de overige een failure rate λ_2. Indien het systeem down is (de trein staat stil) kunnen goede componenten niet falen. Er geldt: $\lambda_1 < \lambda_2$. Alle gebruikte koppelingen van de wagons en van de locomotieven, die tijdens het rijden kunnen falen, hebben een failure rate λ_k.

Zowel de locomotieven als de koppelingen kunnen gerepareerd worden, maar men begint pas met repareren als het systeem gefaald heeft, waarna men doorgaat totdat alles gerepareerd is. Er is één reparateur beschikbaar voor de locomotieven, met een repair rate μ_L. Een tweede monteur repareert de koppelingen met een repair rate μ_K.

Teken het Markovdiagram en geef daarin duidelijk de overgangskansen en de (down-)toestanden aan.

8. Evaluatiemethoden

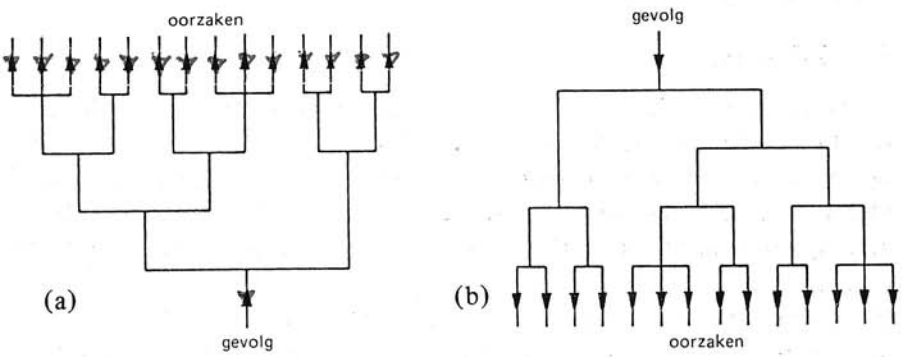
In het begin van de jaren 60 is men evaluatiemethoden gaan ontwikkelen voor de analyse van de beschikbaarheid en de veiligheid van complexe technische systemen. Met deze methoden is men in staat in een vroegtijdig stadium ontwerpfouten aan te tonen, zodat men niet in een later stadium geconfronteerd wordt met kostbare ontwerpwijzigingen of zelfs wijzigingen van het reeds geproduceerde systeem.
Een voorbeeld hiervan is het door de fabrikant terugroepen van auto's voor een wijziging van de stuur- of reminrichting.
Deze evaluatiemethoden worden ook wel achteraf gebruikt om de meest waarschijnlijke foutoorzaak op te sporen als het systeem zelf niet bereikbaar is of verloren is gegaan. Door een evaluatie achteraf heeft men bijvoorbeeld aan kunnen tonen dat de oorzaak voor het tuimelen van de Surveyor-2 het niet willen starten van motor nr. 3 van de stuurinrichting van het aandrijfsysteem was.

8.1. Inleiding

De evaluatiemethoden bestaan uit een grafische representatie van de oorzakelijke samenhang tussen de gebeurtenissen die kunnen leiden tot het optreden van een bepaalde ongewenste gebeurtenis. De representatie vindt plaats in de vorm van georiënteerde grafen met een boomstructuur. De knooppunten stellen gebeurtenissen voor, de overgang daartussen het optreden van zo'n gebeurtenis.
De evaluatiemethoden die hierna zullen worden besproken zijn dus *gebeurtenis-georiënteerd* in tegenstelling tot de *bedrijfszekerheidsmodellen* die we in hoofdstuk 5 hebben gebruikt voor de evaluatie van een systeem en die *structuur-georiënteerd* zijn. Met die bedrijfszekerheidsmodellen kan men fouten te lijf (hardware-fouten) die aanleiding geven tot een verstoring van de structuur van het systeem (bijvoorbeeld een open fout in een connector) die op haar beurt leidt tot het buiten de specificaties vallen van de functie van dat systeem.
Met de bovenbedoelde *gebeurtenis-georiënteerde evaluatiemethoden* zijn niet alleen hardware-fouten te modelleren maar ook ongewenste situaties die ontstaan door fouten in programmatuur, bediening of onderhoud en ook ongewenste situaties teweeggebracht door de omgeving van het

systeem. Deze evaluatiemethoden zijn dus veel machtiger dan de evaluatie aan de hand van bedrijfszekerheidsmodellen. Alle evaluaties met bedrijfszekerheidsmodellen zoals beschreven in hoofdstuk 5 kunnen ook met de hierna beschreven evaluatiemethoden worden gedaan.

Er bestaan twee essentieel verschillende groepen van gebeurtenis-georienteerde evaluatiemethoden. In de ene groep worden de relaties tussen oorzaak en gevolg doorlopen in de *causale richting*. Dus eerst de veroorzakende gebeurtenis en daarna (en daardoor) de gevolggebeurtenis. Men noemt zulke evaluatiemethoden dan ook '*forward methods*'. Uitgegaan wordt van mogelijke faalgebeurtenissen in de komponenten van een systeem (dat zijn er dus vele) en geëindigd wordt met de gebeurtenis dat het systeem faalt (dat is er dus één). Men krijgt bij de grafische presentatie daarvan dan ook een diagram dat breed begint en smal eindigt (zie figuur 8.1a). Men noemt zo'n evaluatie dan ook wel een '*bottom-up*'-*evaluatie*. Een andere benaming stamt uit de logische redenering '*inductie*' waarbij men van het bijzondere (of van het detail) tot het algemene (of het globale) besluit. Daar de afleiding door inductie ten grondslag ligt aan deze groep van evaluatiemethoden worden deze ook wel *inductieve methoden* genoemd.



Figuur 8.1. De structuur en de oriëntatie van grafen gebruikt voor de evaluatie van de bedrijfszekerheid van systemen.
(a) inductief, forward of bottom-up;
(b) deductief, backward of top-down.
De pijlen geven de redenatierichting aan.

De tweede groep van evaluatiemethoden kenmerkt zich daardoor dat de er aan ten grondslag liggende redenering *anti-causaal* is: men begint met het gevolg en speurt de mogelijke oorzaken op. Na het hiervoor besprokene zal duidelijk zijn dat deze methoden (zie figuur 8.1b) ook wel aangeduid worden als '*backward*'-, '*top-down*'- of *deductieve methoden*.

In het navolgende zullen we van elke groep de belangrijkste evaluatiemethodiek bespreken.

8.2. Causale evaluatie

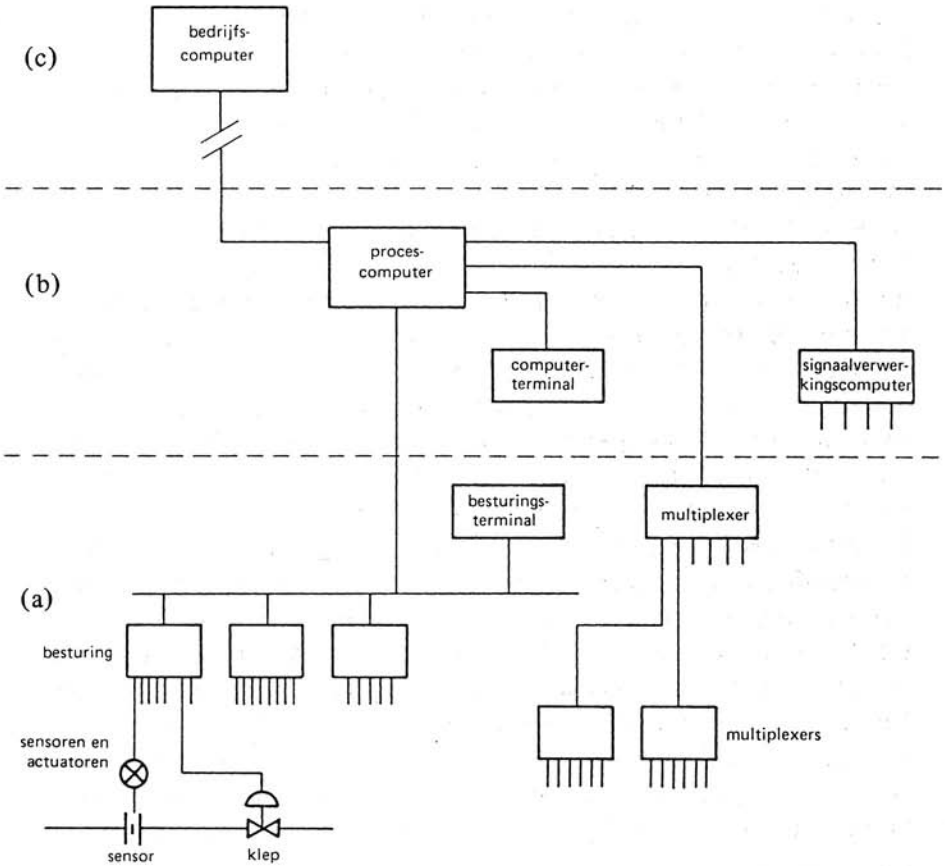
Een causale evaluatie is een systematische evaluatie van een systeem of een subsysteem die begint met elementaire gebeurtenissen die plaatshebben op het laagst zinvolle systeemniveau.
Voorbeelden hiervan zijn: een bepaalde las in een pijp lekt ..., een verstopping in de olietoevoer van een bepaald glijlager waardoor ..., het falen van de overtemperatuurbeveiliging waardoor ... .
Een nadeel van deze methodieken is dat men het betreffende systeem reeds in zijn kleinste detail moet kennen alvorens men causale evaluatie kan starten. Gedurende het ontwerpen van een systeem begint men meestal eerst met de overall-specificaties die weer leiden tot specificaties van subsystemen. Pas als men het ontwerp op de hogere complexiteitsniveaus van het systeem gereed heeft, vult men de details in. Dus het ontwerp van units en modulen gebeurt pas in laatste instantie. Toch heeft men deze detailgegevens nodig voor een causale evaluatie. In de ontwerpfase gebruikt men dan ook meestal een anti-causale evaluatiemethode die het ontwerp als het ware vanaf de top op de voet volgt.
De causale evaluatie gebruikt men meestal voor gevaar- en risicoanalyse en identificatie van gevaarlijke bottlenecks in een systeem, zoals single-point failures (dit zijn die fouten in een komponent of module die het gehele systeem uitschakelen). Men kan namelijk, als men op het laagste niveau begint heel gemakkelijk alle faalwijzen van elke zelfstandige eenheid (komponent, module, unit) van een systeem en de gevolgen daarvan opschrijven. Men komt dus gemakkelijk tot een *volledige* inventarisatie waarbij er geen gebeurtenissen over het hoofd worden gezien. Dat is bij een anti-causale methode veel moeilijker.

8.2.1. FMECA analyse

Als belangrijkste voorbeeld van een causale evaluatiemethode zullen we nu kort de zogenaamde 'Failure Mode, Effect and Criticality Analysis' (FMECA) bespreken. We zullen deze voorwaartse methode aan de hand van een kwalitatief voorbeeld nader uitleggen.

Voorbeeld
Een petrochemische industrie vergt investeringen van vele honderden miljoenen guldens. Door relatief korte produktie-onderbrekingen kan zo'n industrie dan ook miljoenen guldens per jaar verliezen. De eis is hier dan ook een beschikbaarheid die zeer dicht bij 100% ligt. In zo'n industrie voor

de vervaardiging van plastics en rubbers uit aardolieprodukten neemt de procesregeling een sleutelpositie in. Deze procesregeling maakt intensief gebruik van computers, terminals, multiplexers, regelaars, transmitters, stuurorganen en dergelijke. In figuur 8.2 is hiervan een voorbeeld gegeven.

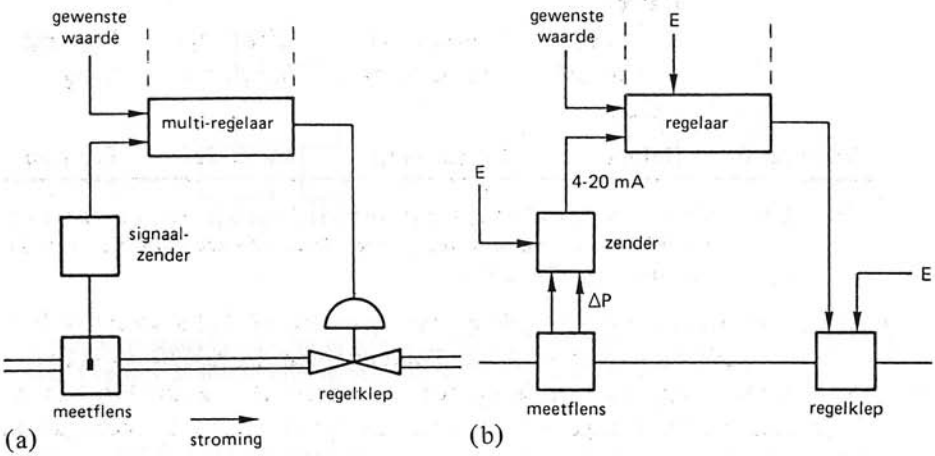


Figuur 8.2. Een voorbeeld van computerhiërarchie in de petrochemische industrie. Niveau A is het niveau met de hoogste beschikbaarheid, niveau C dat met de laagste.

Het met A aangeduide niveau moet het meest bedrijfszeker functioneren daar de instrumenten op dit niveau het dichtst bij het proces staan en zij gegevens voor de hogere niveaus moeten doorgeven. Deze instrumenten zijn in hoge mate modulair opgebouwd en gestandaardiseerd zodat ze onderling uitwisselbaar zijn. Op kritieke punten zijn deze instrumenten dan ook redundant uitgevoerd. Niveau B, dat van de procesregelingscomputer, kan volstaan met een lagere bedrijfszekerheid. De organen op niveau A

kunnen namelijk (gedurende niet te lange tijd) ook zelfstandig werken. Het proces verloopt dan echter inefficiënter. De procescomputer combineert namelijk gegevens vanuit verschillende delen van het proces en rekent die om in stuurgegevens voor de instrumenten op niveau A. Verder zijn belangrijke functies voor deze computer de zogenaamde 'data logging' en 'reporting'. Ook op niveau B wordt daarom modulaire opbouw en redundantie nagestreefd. De veel grotere complexiteit op dit niveau drukt echter de beschikbaarheid. Op het niveau C is uitval meer hinderlijk dan dat het aanleiding tot katastrofale gevolgen zou kunnen geven. De beschikbaarheid mag hier dan ook lager zijn dan op niveau B.
We zullen ons nu bepalen tot één regelkring op het meest kritische niveau A. Deze is in figuur 8.2 reeds aangegeven. Voor de FMECA van deze regelkring gaan we als volgt te werk:

- Stel een functioneel schema op waarin *alle* relevante onderdelen voorkomen (zie figuur 8.3).
- Catalogiseer *alle* onderdelen en geef *alle* faalwijzen van deze onderdelen aan (zie tabel 8.1).
- Bepaal uit de relatie van één onderdeel tot de rest van het systeem het *gevolg* van een bepaalde wijze van falen en hoe *kritiek* dit gevolg is.
- Bepaal hoe *vaak* de faalwijze *voorkomt*.



Figuur 8.3. De regelkring van figuur 8.2 nader uitgewerkt:
(a) functionele representatie;
(b) elektrische regelkring (E = voedingsenergie).

We kunnen deze FMECA-methode opgebouwd denken uit een 'Failure Mode Analysis' (FMA) en een 'Failure Effect Analysis' (FEA) die uitgebreid is met een 'Failure Criticality Analysis' (FCA).

Komponent	Faalwijze	Effect	Hoe kritiek	Frequentie
Meetflens	Vervuiling	Verkeerd gedoseerde flow	Kritiek	Hoog
	Bijna verstopt	Instabiliteit	Marginaal	Erg laag
Drukzender	Uit calibratie	Verkeerd gedoseerde flow	Kritiek	Laag
	Nulpuntsfout	"	Kritiek	Laag
	Sluiting	Regeling stopt	Verwaarloosbaar	Erg laag
Regelaar	Geen set point	Regeling stopt	Verwaarloosbaar	Erg laag
	Versterking:			
	- te hoog	Neiging tot instabiliteit	Marginaal	Erg laag
	- te laag	Traag	Verwaarloosbaar	Erg laag
	Sluiting	Proces stopt	Marginaal	Erg laag
Regelklep	Blijft hangen	Regeling stopt	Verwaarloosbaar	Laag
	Defect:			
	- vol open	Ontploffing	Catastrofe	Erg laag
	- helemaal dicht	Proces stopt	Marginaal	Laag
Voeding E	Defect	Proces stopt	Marginaal	Erg laag

Tabel 8.1. Matrix van de faalwijze, het gevolg van falen, de mate van risico bij het falen en de relatieve faalfrequentie van de komponenten van de regelkring van figuur 8.3.

- FMA: We dienen *alle* belangrijke komponenten van het systeem te bekijken en *alle* faalwijzen van deze komponenten. In het voorbeeld zojuist gegeven zijn niet alle faalwijzen opgegeven. Doorgaans krijgt men te maken met veel uitgebreidere matrices dan in tabel 8.1 weergegeven. De computer kan dan een zeer nuttig hulpmiddel zijn.
- FEA: Bij deze deelanalyse wordt het gevolg op het systeem nagegaan van het falen op een bepaalde (faal-) wijze van de komponenten van het systeem. Opgemerkt moet worden dat het systeem kennelijk al goed ontworpen is, dat wil zeggen *fail-safe*. Immers bij volle flow treedt een ontploffing op. Dit moet vermeden worden. Als de voeding E wegvalt gaat daarom de regelklep (onder invloed van een veer) helemaal

dicht. Als een ingang van de regelaar wegvalt houdt deze de klep in de laatst ingestelde stand. Als de regelaar uitvalt gaat de regelklep ook dicht, enzovoort.

- FCA: De mate van risico van falen is een belangrijke grootheid. Falen mag immers geen dure of gevaarlijke gevolgen hebben voor de mens, het milieu en andere technische systemen. We onderscheiden daarom verschillende *criticality levels*: verwaarloosbaar, marginaal, kritiek en catastrofaal. In het voorbeeld kan een verkeerde flow-dosering tot een overdosering leiden die gevaarlijk wordt. Dit is derhalve beoordeeld met kritiek. We zullen op de veiligheid en het risico van systemen terugkomen in paragraaf 8.4.

De FMECA is ook een bruikbare techniek voor het vaststellen van de onderhoudsbehoefte van een systeem. In het voorbeeld van tabel 8.1 moet bijvoorbeeld de meetflens regelmatig (met stoom) worden schoongespoeld om een ontoelaatbare vervuiling te voorkomen. Aangezien deze vervuiling leidt tot een kritieke fout moet hier periodiek onderhoud worden gepleegd volgens een strak schema. Verder zou, gezien de hoge frequentie van de vervuiling ook een extra bewakingscircuit hiervoor adviseerbaar zijn. (Door bijvoorbeeld de turbulenties in de flow te meten tengevolge van het aankoeken van olie- en teerprodukten op de meetflens.) Verder moet ook de drukzender regelmatig afgeregeld worden en moet de regelklep op gangbaarheid gecontroleerd worden.
Men kan dus op deze wijze al tijdens het ontwerp van een systeem onderhoudsschema's opstellen.

In het bovenstaande voorbeeld hebben we slechts één regelkring op het laagste complexiteitsniveau van de procesregeling in figuur 8.2 met de FMECA-methode in beeld gebracht. Het zal duidelijk zijn dat als we de gevolgen van het falen van de komponenten uit deze regelkring weer als ingangsgebeurtenissen zien voor een hogere FMECA, er een (gigantisch) voorwaarts diagram ontstaat dat eigenlijk nog slechts met de computer is op te stellen en te evalueren.

8.3. Anti-causale evaluatie

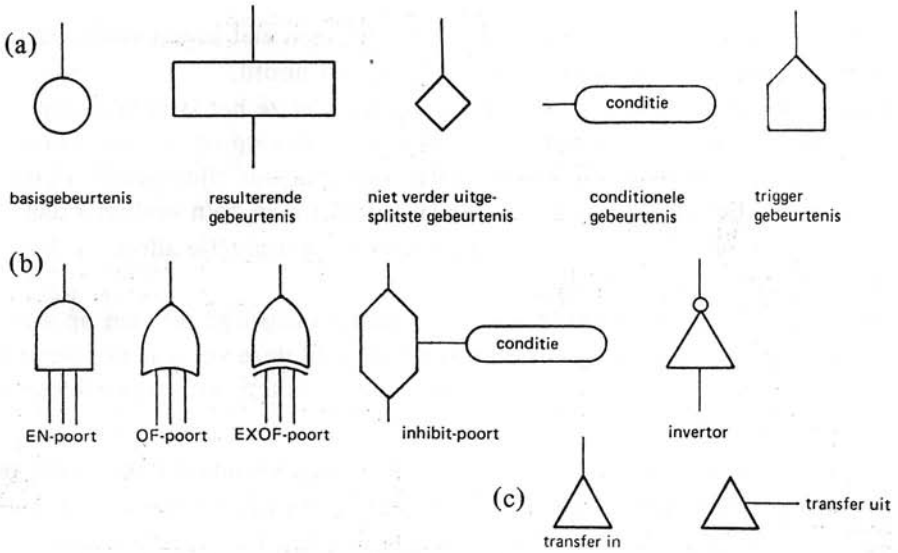
Zoals we reeds hebben gezien begint een anti-causale evaluatie van de beschikbaarheid van een systeem met de meest complexe gebeurtenis die men wil analyseren. Voorbeelden zijn: het leven van de astronaut is in gevaar. Maar ook: de zonnepanelen van een ruimtevaartuig ontvouwen zich niet.
Deze 'top'gebeurtenis wordt deductief opgesplitst in *alle* andere gebeurtenissen die tot deze topgebeurtenis kunnen leiden. Hier heeft men meteen

een zwak punt van een anti-causale evaluatie: men ziet gemakkelijk een oorzaak voor het topgebeuren (gevolg) over het hoofd.
Een sterk punt van deze evaluatiemethoden is dat ze het (van systeemniveau naar komponentniveau) voortschrijdende ontwerp op de voet kunnen volgen. Ook deze evaluatie kan bij complexe systemen tijdrovend en ingewikkeld worden. Bij complexe systemen verricht men zo'n evaluatie dan ook meestal met de computer of men betrekt de evaluatie alleen op het meest kritische subsysteem.
Zoals we reeds gezien hebben kan de evaluatie vastgelegd worden op grafische wijze met gestandaardiseerde symbolen. In deze vorm is het een grote hulp voor ontwerpers, gebruikers en beheerders om ontwerpwijzigingen of onderhoudsstrategieën door te spreken.

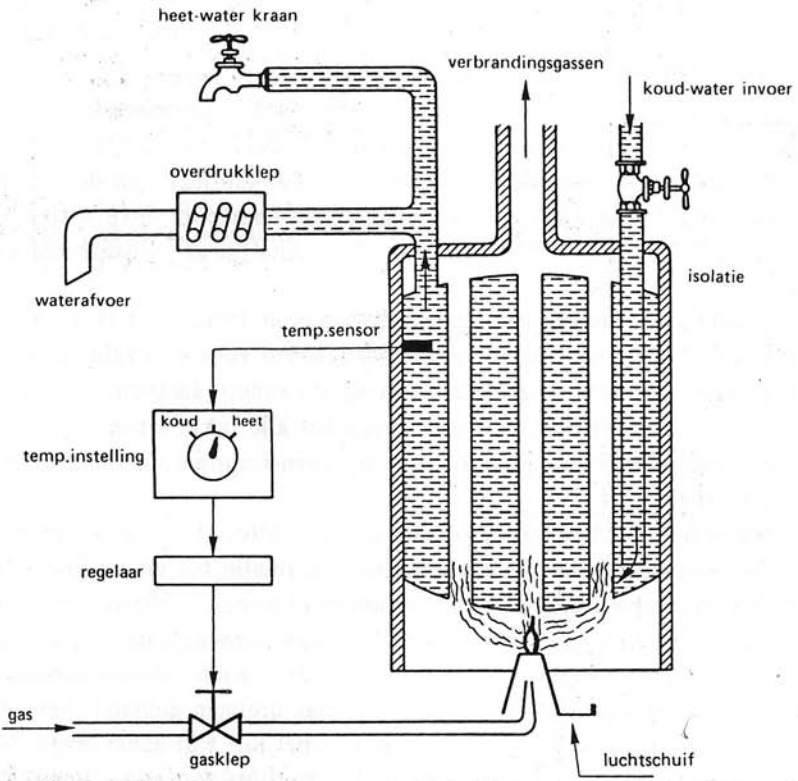
Hebben we van de causale evaluatiemethoden een kwalitatief voorbeeld gegeven, we zullen van de anti-causale evaluaties een kwantitatief voorbeeld geven. Het is namelijk ook mogelijk om bijvoorbeeld de beschikbaarheid te bepalen uit zo'n evaluatie.
We zullen slechts de meest belangrijke anti-causale evaluatiemethode bespreken.

8.3.1. Faalboom analyse

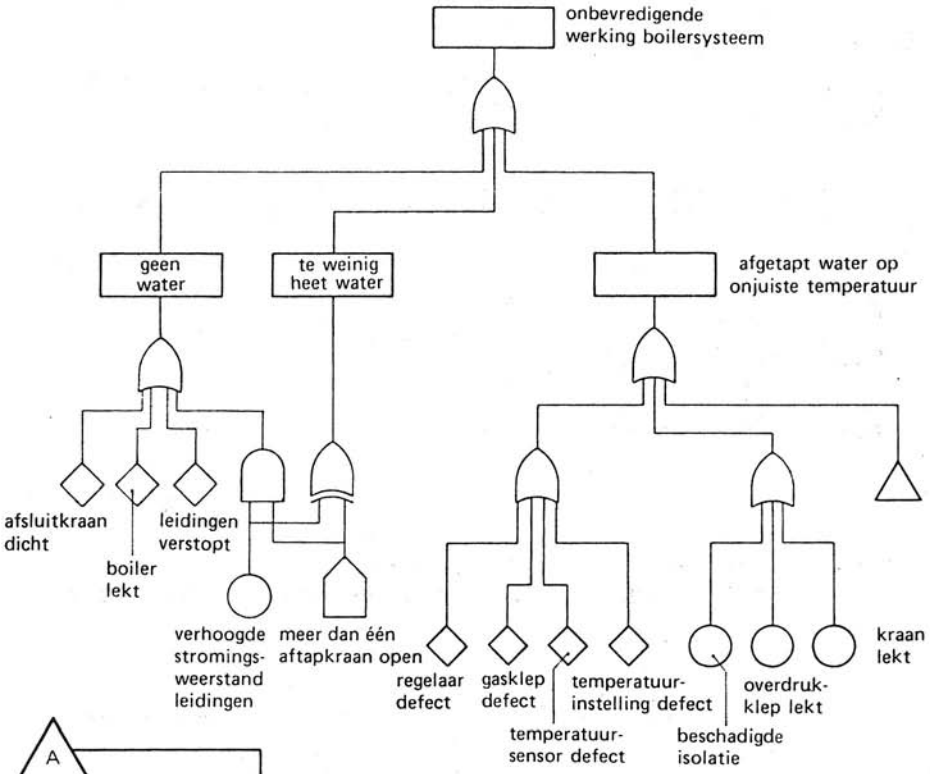
De 'Fault Tree Analysis' (FTA, faalboomanalyse) is de bekendste anti-causale evaluatietechniek geworden, voornamelijk door standaardisatie van de gebruikte symbolen, waardoor iedereen de FTA kan lezen en door het gemak waarmee de mate van detail (uitsplitsing) voor complexe systemen door de opsteller kan worden gekozen. Deze analyse is wijdverbreid aanvaard.
De evaluatie door middel van een faalboom is in 1962 door H.A. Watson van de 'Bell Telephone Laboratories' ontwikkeld voor de evaluatie van de beschikbaarheid van raketlanceerbewakingssystemen (Launch Control Systems). Zij is sedertdien doorgedrongen tot alle takken van industrie en techniek: ruimtevaart, telecommunicatie, (kern-) energiecentrales, vervoerssystemen, enzovoort.
Zoals we al hebben besproken bestaat de evaluatie uit een georiënteerde graaf die oorzaak- en gevolggebeurtenissen in relatie tot elkaar grafisch weergeeft. De gebeurtenissen (of toestanden) kunnen veelomvattend zijn, zoals: het vrijkomen van radioactiviteit uit een kerncentrale, maar ook heel gedetailleerde gebeurtenissen of toestanden, zoals: alarmwaarschuwingslamp 3 heeft gefaald. Het in relatie tot elkaar brengen gebeurt met de gestandaardiseerde logische symbolen die in tabel 8.2 zijn aangegeven. Verder geeft figuur 8.4b een voorbeeld van de structuur van een (kleine) faalboom.



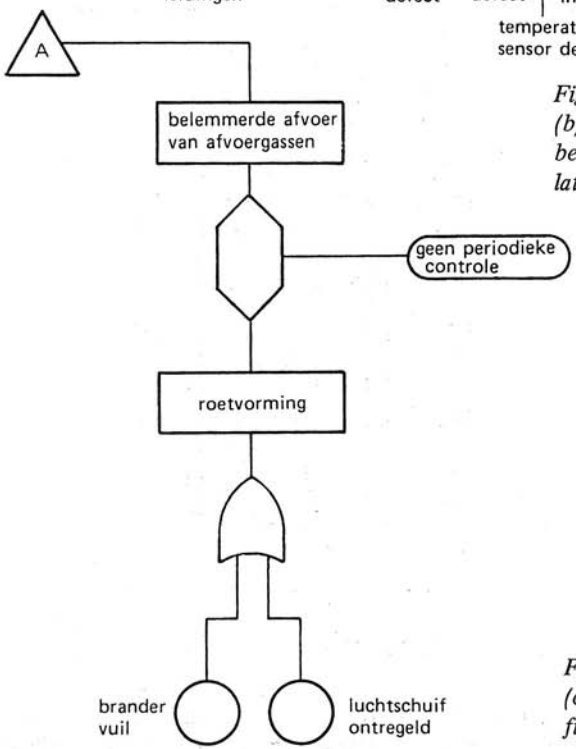
Tabel 8.2. Gestandaardiseerde faalboomsymbolen.
(a) Gebeurtenissymbolen; (b) Poortsymbolen; (c) Transfersymbolen.



Figuur 8.4. (a) Een doorsnede van een gasgestookte heetwaterboiler. (De waakvlam en de vlam-uit-beveiligingsinstallatie zijn niet getekend. Meestal is dit een extra gasklep in serie die door de thermospanning van een thermokoppel element in de waakvlam tegen een veer in wordt opengehouden.)



Figuur 8.4.
(b) De structuur van de faalboom behorende bij de heet-water installatie van figuur 8.4a.

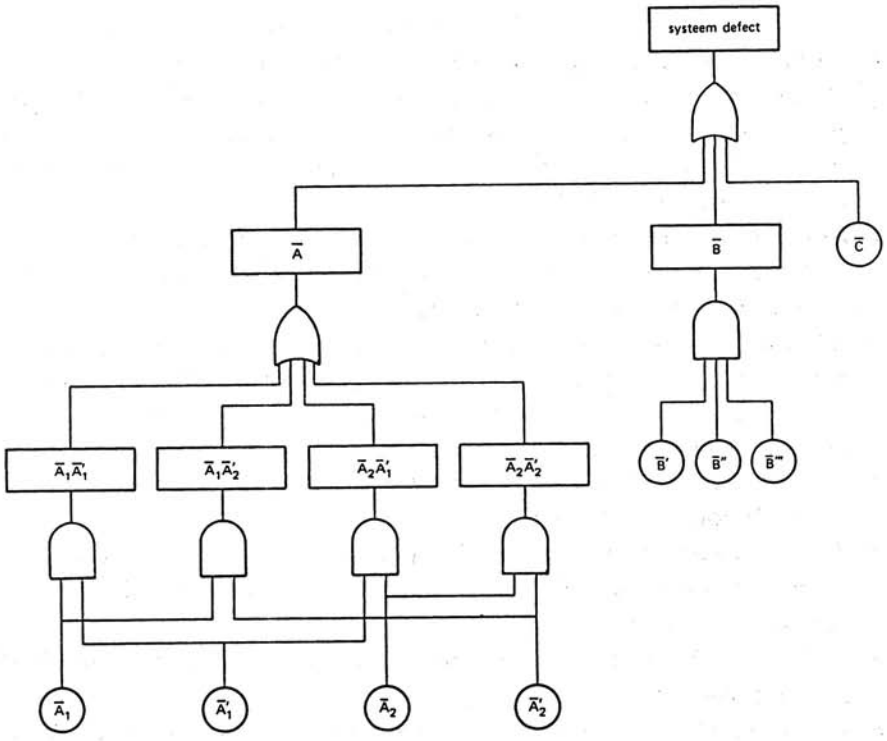


Figuur 8.4.
(c) Sub-faalboom behorende bij figuur 8.4b.

De betekenis van de in tabel 8.2 gebruikte symbolen is als volgt:

- *Basisgebeurtenis.* Dit symbool geeft een eindpunt van de faalboom aan. De cirkel geeft een basisstoring aan: het falen van een elementaire komponent, een omgevingsfout, of een menselijke fout (bediening, reparatie). Hierbij wordt aangegeven de kans op het optreden van deze gebeurtenis of de kansdistributie daarvan.
- *Resulterende gebeurtenis.* De rechthoek geeft een gebeurtenis aan aan de uitgang van een poort die resulteert uit een combinatie van gebeurtenissen aan de ingang van de poort.
- *Niet-uitgesplitste gebeurtenis.* Het diamantsymbool geeft een gebeuren aan waarvan de oorzaken niet volledig zijn nagegaan. Deze gebeurtenis zou verder ontwikkeld kunnen worden als de informatie en de interesse daarin aanwezig is.
- *Conditionele gebeurtenis.* De ellips geeft een conditie of restrictie aan die geldt voor een bepaalde poort.
- *Triggergebeurtenis.* Het huissymbool geeft een gebeurtenis aan die bij normaal gebruik verwacht wordt of juist niet verwacht wordt en als trigger voor een aantal andere gebeurtenissen werkt.
- *EN-poort.* De uitgangsgebeurtenis treedt op dan en slechts dan als alle ingangsgebeurtenissen optreden.
- *OF-poort.* De uitgangsgebeurtenis treedt op als één of meer van de ingangsgebeurtenissen optreden.
- *Exclusive OF-poort.* De uitgang treedt niet op tenzij één en slechts één ingang optreedt.
- *Inhibit-poort.* De uitgang treedt niet op als er aan de conditie wordt voldaan.
- *Invertor.* De uitgangsgebeurtenis is de inverse van de ingangsgebeurtenis.
- *Transfer.* Wordt gebruikt om herhaling van delen van een faalboom te vermijden. Een driehoeksymbool verbindt bijvoorbeeld delen van faalbomen die zich uitspreiden over meerdere pagina's met elkaar.

Men kan op deze wijze, te beginnen bij de (top-) gebeurtenis die men wil analyseren, een faalboom steeds verder detailleren tot men vastloopt op basisgebeurtenissen die niet verder uitsplitsbaar zijn.
We zullen nu een eenvoudig voorbeeld geven van een faalboom. We nemen daartoe het systeem van figuur 6.8a uit paragraaf 6.7.
We zien hieruit dat de gebeurtenis $\overline{C}$ een zogenaamde *single-point failure* geeft, omdat deze basisgebeurtenis rechtstreeks naar de topgebeurtenis doorspreekt via een of meer of-poorten. We zien verder dat de seriesystemen kennelijk aanleiding geven tot of-poorten en parallelsystemen tot en-poorten.
We hebben in de faalboom van figuur 8.5 kennelijk de ontwikkeling afgebroken op unit-niveau en het falen van een unit als basisgebeurtenis opge-



Figuur 8.5. De faalboom die behoort bij figuur 6.8a.

vat. Als we ook de kans P waarmee een unit faalt, de faaldistributie F(t) of de onbeschikbaarheid (1 − A(t)) van de basisgebeurtenissen weten, kunnen we de kans, faaldistributie of onbeschikbaarheid van de topgebeurtenis bepalen. Een faalboom is dus ook een geschikt middel voor de bepaling van de bedrijfszekerheid of de beschikbaarheid, evenals de bedrijfszekerheidsmodellen van figuur 6.8.
We zullen de berekening een keer uitvoeren aan de hand van de faalboom van figuur 8.6. Voor de gebeurtenis $\bar{A} \cup \bar{B}$ geldt:

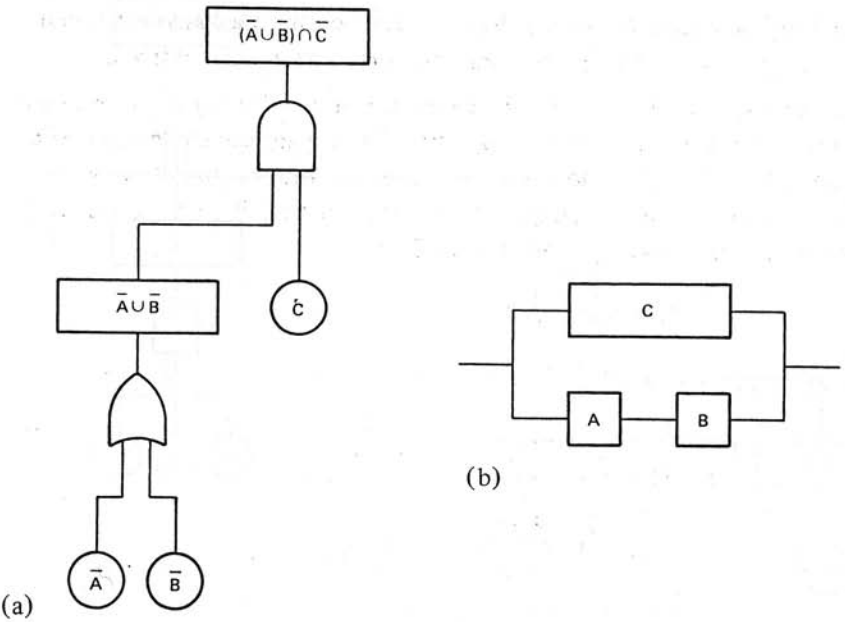
$$P(\bar{A} \cup \bar{B}) = P(\bar{A}) + P(\bar{B}) - P(\bar{A} \cap \bar{B}).$$

Als de gebeurtenissen 'A faalt' en 'B faalt' disjunct zouden zijn (wat doorgaans niet het geval is), mogen we schrijven:

$$P(\bar{A} + \bar{B}) = P(\bar{A}) + P(\bar{B}).$$

De kans op de doorsnede kunnen we met het theorema van Bayes schrijven als:

$$P(\bar{A}\bar{B}) = P(\bar{A})\,P(\bar{B}|\bar{A}) = P(\bar{B})\,P(\bar{A}|\bar{B}).$$



Figuur 8.6. (a) De faalboom en (b) het bedrijfszekerheidsmodel van een bepaald systeem.

Dus als de gebeurtenissen $\bar{A}$ en $\bar{B}$ stochastische onafhankelijk zijn geldt:

$$P(\bar{A}\bar{B}) = P(\bar{A})\,P(\bar{B}).$$

Substitueren levert dan:

$$P(\bar{A} + \bar{B}) = P(\bar{A}) + P(\bar{B}) - P(\bar{A})\,P(\bar{B}).$$

Meestal zijn de faalkansen erg klein. Dan mogen we het produkt in het rechterlid van de bovenstaande uitdrukking verwaarlozen en geldt:

$$P(\bar{A} + \bar{B}) \approx P(\bar{A}) + P(\bar{B}).$$

De tweede stap die in de faalboom van figuur 8.6 nodig is om tot de top-gebeurtenis te komen levert geen nieuwe gezichtspunten op. Onder welke aanname geldt dat de uitgangskans van een en-poort (ongeveer) gelijk is aan het product van de ingangskansen? We vinden dan:

$$P_{top} = P((\bar{A} \cup \bar{B}) \cap \bar{C}) \approx [P(\bar{A}) + P(\bar{B})]\,P(\bar{C}),$$

(mits $P(\bar{A})$, $P(\bar{B}) \ll 1$ en $\bar{A}$, $\bar{B}$ en $\bar{C}$ stochastisch onafhankelijk zijn).

Conclusie: we kunnen, onder de beide boven gemaakte aannames, de kans

op de topgebeurtenis eenvoudig bepalen door de ingangskansen van een of-poort op te tellen en die van een en-poort te vermenigvuldigen.

We nemen nu aan dat de basisgebeurtenissen in een faalboom negatief-exponentieel verdeeld en onafhankelijk zijn. De uitgangsgebeurtenissen van de of-poorten in de faalboom zijn dan weer negatief-exponentieel verdeeld met een failure rate gelijk aan de som van de failure rates van de n ingangsgebeurtenissen (seriesysteem). Dus:

$$z_{of}(t) = \lambda_{of} = \sum_{i=1}^{n} \lambda_i .$$

Voor een en-poort geldt:

$$z_{en}(t) = \frac{\sum_{i=1}^{n} \lambda_i(\alpha_i - 1)}{[\prod_{i=1}^{n} \alpha_i] - 1}$$

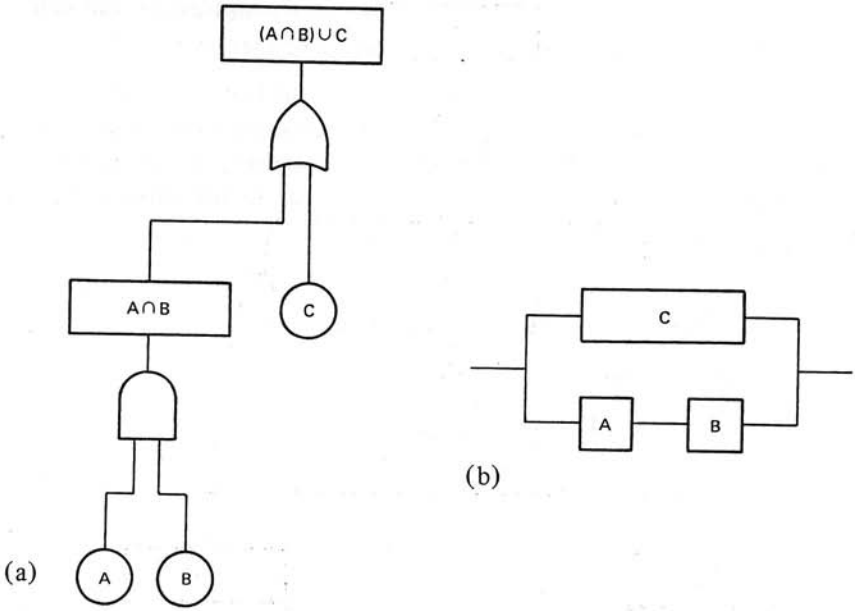
waarin:

$$\alpha_i = 1/(1 - e^{-\lambda_i t}).$$

De faalboom is een tamelijk 'negatieve' benadering van het bedrijfszekerheidsprobleem waarbij het juist om *niet* falen gaat. Deze foutgebeurtenis georiënteerde evaluatie kan evenwel gemakkelijk in een succesgebeurtenis-georiënteerde evaluatie worden omgezet. De *faalboom* wordt dan vervangen door zijn *duale vorm* de *succesboom*. Met behulp van een aantal eenvoudige omzettingen kan men een boom in zijn duale vorm omzetten:
- Vervang alle en-poorten door of-poorten en, eveneens, alle of-poorten door en-poorten in de oorspronkelijke boom.
- Vervang alle gebeurtenissen door hun complementaire gebeurtenis.

Dit is uitgevoerd voor de faalboom van figuur 8.6. Het resultaat is weergegeven in figuur 8.7.

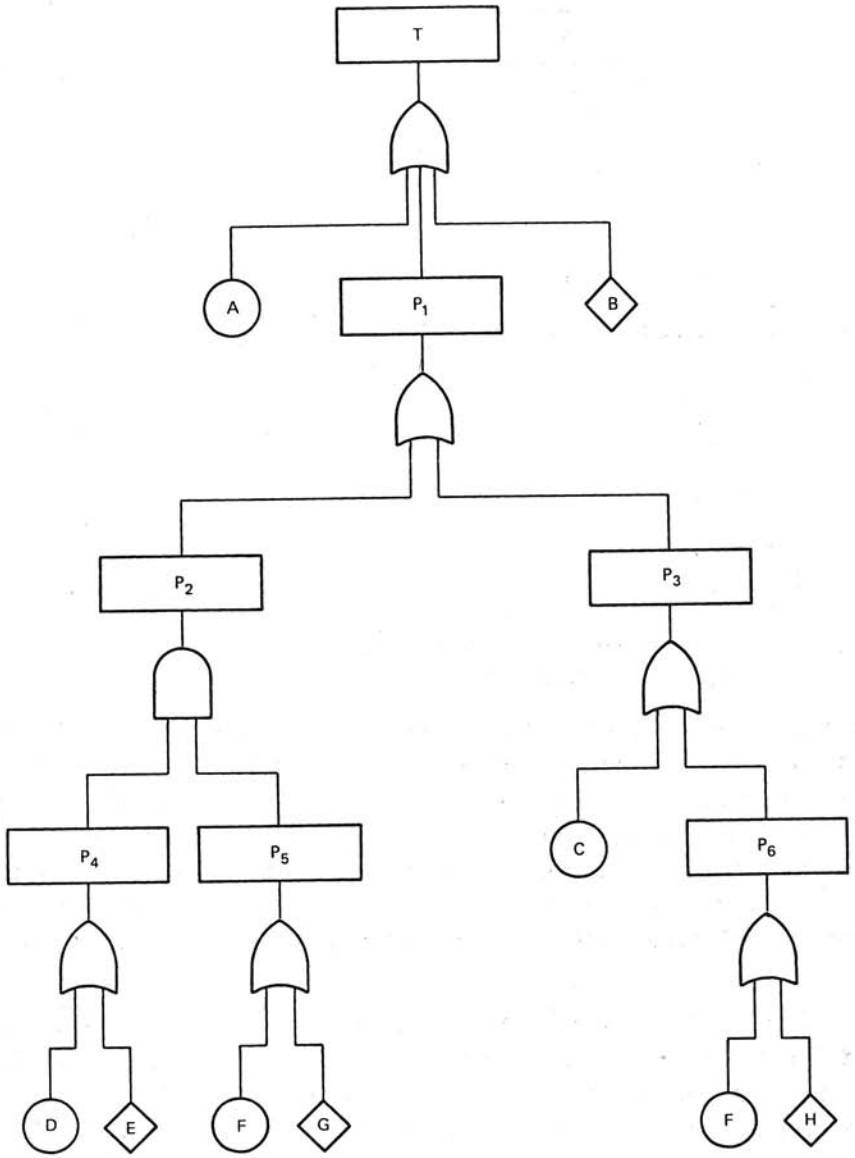
De faalboom die men opmaakt aan de hand van een praktisch systeem kan meestal drastisch gereduceerd worden. Dit doet men door bijvoorbeeld de rekenregels voor samengestelde gebeurtenissen toe te passen die we ook in paragraaf 6.9 hebben toegepast.
Een andere methode voor de kwantitatieve evaluatie van een faalboom is die welke we in paragraaf 6.9.2 reeds hebben leren kennen. In de termen van een faalboom is een *snede* elke verzameling van basisgebeurtenissen waarvan het gezamenlijk optreden de topgebeurtenis teweeg brengt. Een *minimumsnede* is een snede die niet verder te reduceren is en toch nog juist de topgebeurtenis veroorzaakt. Een lijst van minimumsneden van een



Figuur 8.7. (a) De succesboom en (b) het bedrijfszekerheidsmodel van een bepaald systeem. (Zie ook figuur 8.6).

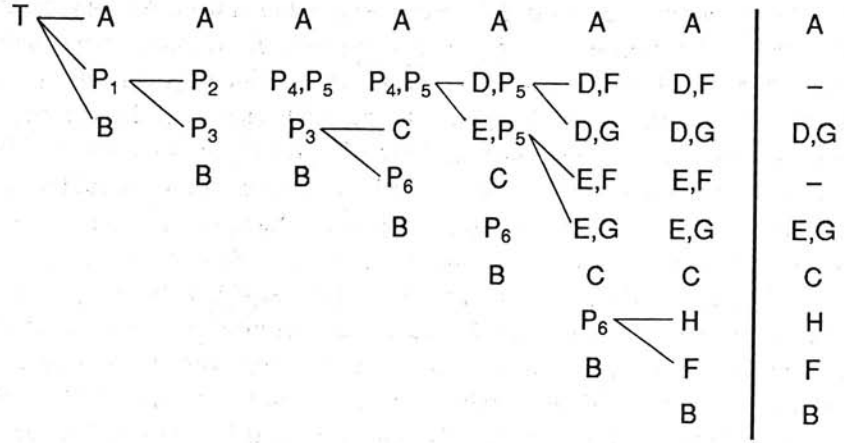
systeem is erg belangrijk voor ontwerpdoeleinden om de zwakste schakels van het systeem te identificeren. In grotere faalbomen kan men deze minimumsneden niet meer door een eenvoudige inspectie van de faalboom vinden. Wij zullen derhalve een algoritme aangeven (het Fussel-Vesely algoritme) om deze minimumsneden te bepalen. Het algoritme is gebaseerd op de waarneming dat een en-poort in een faalboom altijd de *grootte* van een snede doet toenemen, terwijl een of-poort altijd het *aantal* sneden doet toenemen.

We zullen het algoritme uitleggen aan de hand van de faalboom van figuur 8.8. We gaan van boven naar beneden door de faalboom en leggen daarbij een lijstmatrix aan die we na het passeren van elke poort bijstellen. Het idee daarbij is de uitgangsgebeurtenis van elke poort die we tegenkomen te vervangen door de ingangsgebeurtenissen van die poort. Daarmee gaan we door tot we een lijstmatrix hebben gekregen die uitsluitend nog basisgebeurtenissen bevat. Als de poort een *of-poort* is, wordt de uitgangsgebeurtenis in de lijst vervangen door een *kolom* bestaande uit de ingangsgebeurtenissen van die poort. Bij een *en-poort* wordt de uitgangsgebeurtenis vervangen door de *rij* van ingangsgebeurtenissen van die poort. Dit houdt dus in dat we verticaal in een kolom hebben staan de vereniging van alle gebeurtenissen die tot de topgebeurtenis kan leiden. Horizontaal

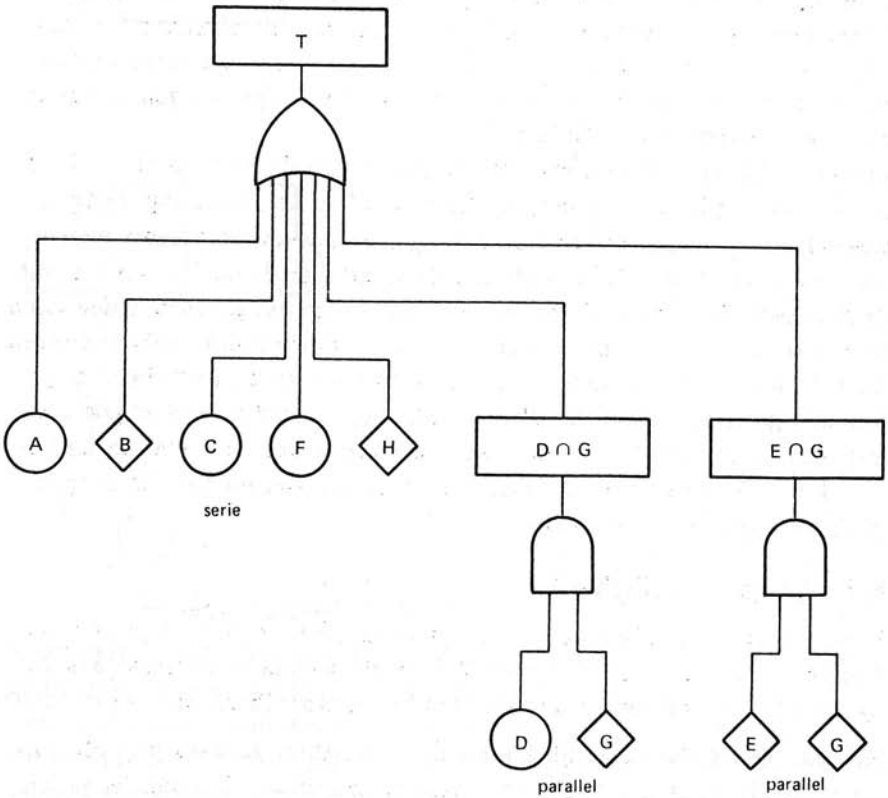


Figuur 8.8. Een faalboom als voorbeeld voor het minimum snede-algoritme.

in elke rij staat de doorsnede van de gebeurtenissen die tot de topgebeurtenis leidt. Als deze gebeurtenissenlijstmatrix tenslotte nog uitsluitend basisgebeurtenissen bevat, hebben we op elke rij een minimumsnede staan als geen der basisgebeurtenissen meerdere malen voorkomt. Is dit wel het geval dan moeten we uit de eindlijst de niet-minimumsneden nog elimineren om alleen minimumsneden over te houden.



Figuur 8.9. Lijstmatrices van gebeurtenissen die tot de topgebeurtenis T leiden in de faalboom van figuur 8.8.



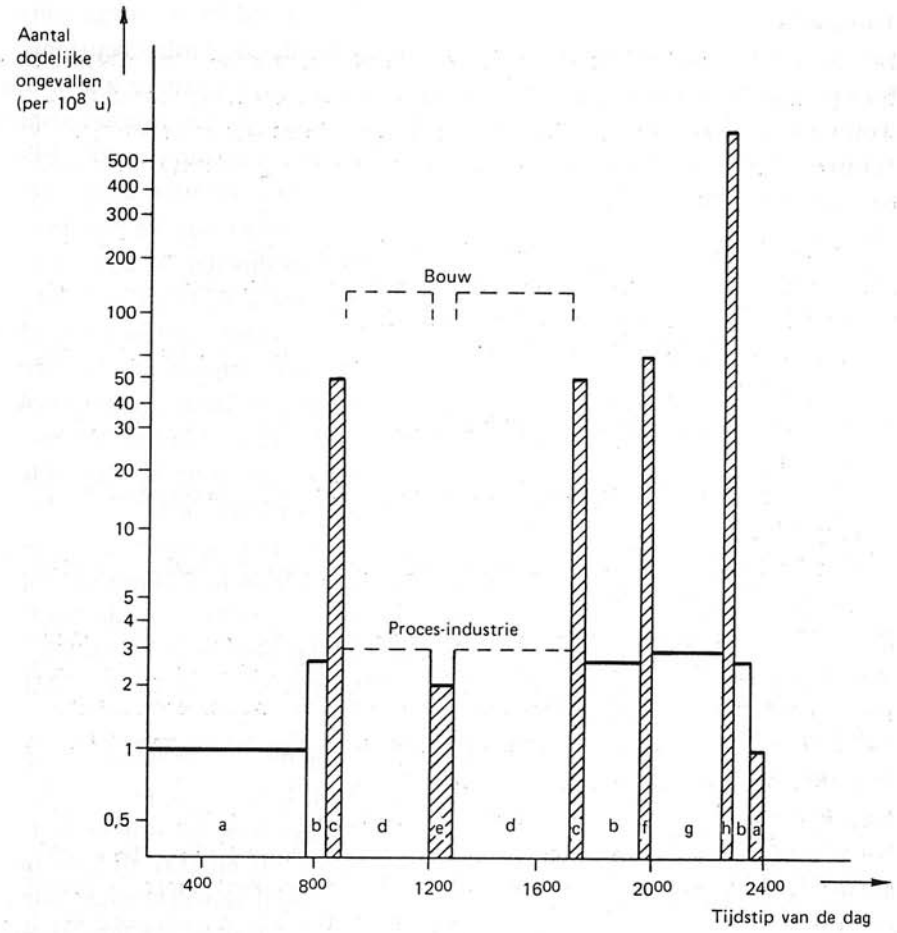
Figuur 8.10. De faalboom uit figuur 8.8 gereduceerd door middel van de minimum-sneden methode als geïllustreerd in figuur 8.9.

Voor de faalboom van figuur 8.8 vinden we, beginnend bij de topgebeurtenis, dan de lijstmatrices van figuur 8.9. We zien dat de basisgebeurtenis F twee keer voorkomt. De rijen van de laatst gevonden lijstmatrix zijn dus niet allen minimumsneden. We weten zeker dat F alleen een minimumsnede vormt, derhalve zijn de doorsneden DF en EF geen minimumsneden. Elimineren we deze, dan vinden we als minimumsneden alle rijen achter de verticale lijn in figuur 8.9. We kunnen op grond hiervan ook de *gereduceerde faalboom* van figuur 8.10 opstellen. We zien dus dat A, B, C, F en H elk afzonderlijk storing kunnen veroorzaken, terwijl D, G en E,G dat alleen samen kunnen doen. Als de gebeurtenissen in deze faalboom zouden slaan op het falen van komponenten uit een systeem kunnen we dus denken in de termen 'serie' en 'parallel'. In een faalboom kunnen echter ook menselijke fouten zoals bedieningsfouten en verkeerd onderhoud als gebeurtenis worden gebruikt, evenals fouten veroorzaakt door de omgeving van het systeem (bijvoorbeeld: er treedt condensvorming op).
In de faalboom van figuur 8.10 zijn A, B, C, F en H zogenaamde *single-point failures.* Dat zijn fouten of gebeurtenissen die in hun eentje de topgebeurtenis kunnen veroorzaken. Bijvoorbeeld het uitvallen van de koeling van een systeem. In een bedrijfszeker systeem moeten deze fouten zoveel mogelijk vermeden worden. Dit kan door ze gedwongen te combineren met andere gebeurtenissen.
Bijvoorbeeld: het systeem valt slechts dan uit als de hoofdkoeling uitvalt en ook de hulpkoeling uitvalt, èn dat bovendien de systeemoperator de waarschuwingslichten dat de hulpkoeling niet meer voor gebruik gereed was, genegeerd heeft. Men heeft dan de situatie zoals bij D,G en E,G uit de faalboom dat slechts de doorsnede van een aantal gebeurtenissen falen kan veroorzaken. Nu kan men verder nog de kans op deze gebeurtenissen klein houden. Dit kan men bewerkstelligen door goede materialen te gebruiken, goed onderhoud te plegen en het bedienend personeel goed te instrueren. Men heeft dan een grotere zekerheid dat falen niet zal optreden dan bij een single-point faalgebeurtenis waarvan men de kans op optreden laag probeert te houden.

8.4. Risico en veiligheid

In paragraaf 3.2 hebben we de begrippen risico en veiligheid reeds gedefinieerd. Het risico is de kans op een fout die schade veroorzaakt aan het systeem of zijn omgeving; veiligheid is het aanvaardbaar zijn van dit risico.

Nu gaat helaas elk menselijk ingrijpen in de natuur gepaard met een van nul verschillend risico; 100% veiligheid bestaat niet! Ook elk technisch gebeuren, hoe simpel ook, gaat met risico gepaard. Vergelijk maar eens



Figuur 8.11. Een voorbeeld van het verloop van het risico op een dodelijk ongeval met het tijdstip van de dag.
(a) slapen; (b) thuis eten, wassen en aankleden; (c) autorijden van en naar het werk; (d) risico tijdens het werk; (e) lunchpauze; (f) rijden naar avondafspraak in het donker; (g) visite, cafebezoek, recreatie; (h) rijden in donker met een glaasje op.

het gebruik van een ladder. In figuur 8.11 is het risico met het verlopen van de dag aangegeven. Een *risicoanalyse* heeft tot doel de aard van de risico's te onderkennen en de grootte van de risico's af te schatten. Daarnaast leidt een risicoanalyse tot het treffen van maatregelen om het risico te verkleinen, zodanig dat het resterende risico aanvaardbaar is, gelet op technische, economische, sociale, psychologische en juridische factoren.

N.B.: Deze opsomming is in willekeurige volgorde en wil geen prioriteiten aangeven!

Voorbeeld

Het wonen in een land beneden de zeespiegel (technische verworvenheid) brengt risico's met zich mee. Deze risico's kunnen aanvaardbaar gemaakt worden door waterstaatkundige voorzieningen: hoge dijken, slaper- en wakerdijken en door tijdige alarmering van de bevolking voorafgaande aan een noodzakelijke evacuatie.

Naarmate de mens op grotere schaal gebruik maakt van technische systemen wordt ook het risico groter, als er tenminste geen adequate tegenmaatregelen getroffen worden. Dit komt doordat:

- de mens meer afhankelijk wordt van zijn systemen (pacemaker, vliegtuigelektronica);
- er gevaarlijkere processen worden toegepast (kernreactor, chemische procesindustrie);
- de procesvoering kritischer wordt (hogere drukken, temperaturen en dergelijke);
- er schaalvergroting toegepast wordt (grotere proceseenheden waardoor gevolgen groter zijn).

Door deze oorzaken worden de potentiële gevaren van een verdergaande industrialisatie en een intensiever gebruik van technische systemen steeds groter (vliegrampen door botsing of falen van grote passagierstoestellen, radioactieve uitstoot van kernreactoren, maar ook gevolgen van defecten in aardlekschakelaars, pacemakers enzovoort).

Naast de analyse van de grootte van het risico dat het gebruik van een bepaald technisch systeem met zich meebrengt, zal de risicoanalyse ook antwoord (moeten) geven op de aard van het risico; met name de *gevolgen* van een onveilige fout. We willen graag weten hoe kritisch een bepaalde fout is ten aanzien van de *gevolgschade*. Deze schade kan *aan het systeem zelf* toegebracht worden (functieverlies, schade of zelfs verwoesting) maar ook *aan de omgeving* (milieu-overlast, hinder, verwoesting) en *aan de mens* (levensgevaar, gezondheidsrisico, verwonding, demotivatie, enzovoort).

Een dergelijke analyse noemt men wel '*Criticality Analysis*' (*CA*). Zo'n analyse kan op natuurlijke wijze gecombineerd worden met de in paragraaf 8.2.1 beschreven FMEA tot een FMECA. Globaal genomen gaan we daarbij als volgt te werk:

- Omschrijving en inventarisatie van het systeem.
- Opsporen van risico's van het systeem.
- Kwantificeren van de kans op falen.
- Bepalen van de mate van kritisch zijn van het gevolg van een fout.

Als we ook tegenmaatregelen gaan nemen wordt deze analyse uitgebreid met:

- Alternatieven opstellen ter verkleining van de risico's.
- Resultaten van de voorgestelde alternatieven.
- Voorspellen (door de bovenstaande vier stappen toe te passen op de alternatieven).
- Keuze maken uit de alternatieven.
- Controle van het gekozen alternatief.

Een paar opmerkingen zijn hierbij op zijn plaats. Bij het bepalen van de gevolgen van fouten in technische systemen moet men rekening houden met materiële en immateriële schade. De moeilijkheid daarbij is dat sociale, ecologische en psychologische gevolgen vrijwel niet kwantitatief te benaderen zijn.

Bij de keuze van een alternatieve oplossing wordt de systeemontwerper geconfronteerd met de moeilijke vraag of het bijbehorende risiconiveau al dan niet acceptabel is. Is het bijvoorbeeld acceptabel dat in Nederland in het verkeer (transportsysteem) jaarlijks duizenden doden vallen?

		Risico		
		per uur ($\times 10^{-8}$)	blootstelling per leven [uren]	per leven ($\times 10^{-3}$)
Werk:	proces-industrie (1970)	3	2500 x 40	3
	industrie (1970)	2	2500 x 40	2
	industrie (1930)	60	2500 x 40	60
	bouw (1960)	120	2500 x 40	120
	mijnbouw (1970)	150	1600 x 30	72
Vrijwillig:	reizen per trein	6	600 x 50	1,8
	reizen per vliegtuig	9	100 x 50	0,45
	reizen per auto	50	600 x 50	15
	sigaretten roken	10	?	–
	sportvliegen	100	? 1000.	2,07
	motorracen	350	?	–
Onvrijwillig:	natuurramp	0,2	10000 x 70	1,4
	brand	0,5	10000 x 70	3,5
	ziekte	1	10000 x 70	7

Tabel 8.3. Voorbeeld van de kans op een dodelijk ongeval (risico) per uur blootstelling en per mensenleven.

Als de wetgever bepalingen stelt wordt veelal aangenomen dat een risico beneden de door de wet aangegeven grenzen acceptabel is. Een voorbeeld hiervan is het gebruik van spanningen beneden 50 V in een vochtige omgeving. De overige risico's kan men indelen in werkrisico's, vrijwillige en onvrijwillige risico's (zie tabel 8.3). Globaal kan men spreken van een verwaarloosbaar risico door een technisch systeem veroorzaakt als dit risico verwaarloosbaar is ten opzichte van de toch al aanwezige risico's als het systeem niet gebruikt zou worden. Denk er hierbij aan dat de blootstelling sterk kan variëren! (Omwonenden, systeemoperator.)

Bij een analyse achteraf (*case history*) van grote calamiteiten is een aantal lerenswaardige dingen gebleken:

- Bij een ernstig ongeluk blijken meestal talloze regels en voorschriften gelijktijdig niet te zijn nageleefd; het is zelden of nooit één overtreding die tot een ongeluk leidt (de ontwerper, de gebruiker en degene die het onderhoud pleegt maken allen fouten).
- Na een ernstig ongeluk worden de veiligheidsregels streng nageleefd. Geleidelijk verslapt de discipline echter, totdat het volgende ongeluk of bijna-ongeluk ('near miss') optreedt.

Men dient er daarom voor te waken tijdens de:

- ontwerpfase,
- gebruiks- en onderhoudsfase,
- afdankfase,

dat de regels (voor ontwerpen, gebruiken, onderhouden en afdanken) niet alleen *redelijk* gehouden worden (het bijna onmogelijke wordt toch niet gedaan), maar dat tevens wordt nagegaan hoe redelijk het is om ze onder praktische omstandigheden te overtreden. In dit verband moet worden opgemerkt dat: 'zien overtreden, doet overtreden'. Vooral wanneer er geen sancties op staan of als de overtreder er zelfs nog voordeel van heeft (sneller klaar is, eerder naar huis kan en dergelijke) is dit erg verleidelijk. We dienen ons goed te realiseren in verband met het aspect 'veiligheid' dat we te doen hebben met mensen die, hoewel van goede wil, in de dagelijkse praktijk toch de neiging tot het nemen van de weg van de minste weerstand niet altijd kunnen onderdrukken. Dit geldt zowel voor de ontwerper (te weinig doordacht ontwerp dat snel klaar moest), de gebruiker (de bedieningshandleiding niet gelezen), de reparateur (andere dan de voorgeschreven materialen of onderdelen gebruikt) als de verschrotter (met het huisvuil meegegeven kwikbatterijen die sterk milieuvervuilend zijn).

Gewenning is een zeer veel voorkomende oorzaak van 'sloppy' procedures (*familiarity breeds contempt*). Langzamerhand licht men meer en meer de hand met de op veiligheidsgronden voorgeschreven procedures. Met na-

me werknemers die langere tijd in dienst zijn zien de mogelijke gevaren niet meer; het is immers tot nog toe nog steeds goed gegaan. Verder hebben druggebruik (zelfs van sommige medicijnen) en alcoholmisbruik ook al geschieden deze buiten werktijd, een grote invloed op de alertheid en het beslissingsvermogen van de werkers.
Veel voorkomende 'human errors' worden gemaakt in de navolgende gebieden:

- verkeerde etiketten op flessen (chemicaliën) en handboeken (onvindbaar, slecht leesbaar);
- het overvullen, vullen met te hoge druk, en vullen met verkeerde inhoud van flessen, tanks, cylinders en dergelijke;
- lekkage van pijpen, slangen, koppelstukken, maar ook van elektrische kabels (elektrocutie);
- dampen en stof die bij bepaalde handelingen vrijkomen kunnen explosies en brand veroorzaken;
- verkeerde stand van schakelaars, kleppen, enzovoort;
- geen aandacht (meer) bestedenaan alarmen die 'toch meestal ten onrechte afgaan'.

Al met al factoren die bij risico-bewust handelen meestal wel onderkend worden, maar in de dagelijkse praktijk door slordigheid en dergelijke tot soms catastrofale ongevallen aanleiding kunnen zijn.

Een belangrijke analyse die men meestal uitvoert is de *gevolgenanalyse* van een technisch incident. De gevolgenanalyse is gebaseerd op:

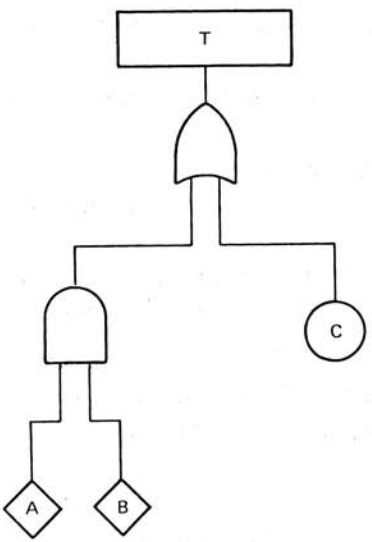
$$S = P \cdot E,$$

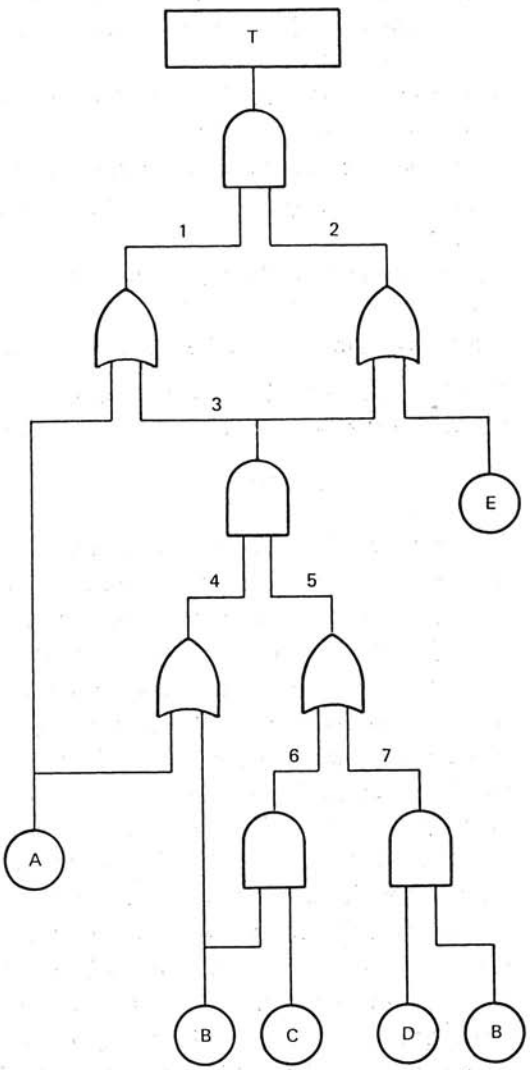
waarin S de schade is, P de kans van optreden van het betreffende incident en E het effect dat het incident teweegbrengt. De zwakke schakel in de gevolgenanalyse (zwak in die zin dat zij voor de meeste mensen moeilijk emotioneel te aanvaarden is) is dat het in de gevolgenanalyse niet uitmaakt of er bij een verkeersongeluk per jaar 2000 mensen zouden omkomen of dat er bij 2000 verkeersongelukken elk één mens omkomt. Dit hangt nauw samen met de *aanvaardbaarheid,* dit is de *subjectieve* beleving van het risico en de toelaatbaarheid daarvan. Zo kan men stellen dat een grote ramp (per eenheid van tijd) minder aanvaardbaar is dan een groot aantal kleine 'rampjes' in dezelfde tijd. Bij vrijwillige blootstelling 'pikt' men grotere risico's dan bij verplichte, beroepsmatige blootstelling (denk aan sporten zoals ski-races, zweefvliegen, motorraces). Aan de andere kant is men als werknemer in een fabriek bereid grotere risico's te aanvaarden dan een toevallige omwonende van die fabriek. Men zou kunnen stellen dat de werknemer er baat bij heeft, terwijl de blootstelling van de omwonende opgelegd is (zonder dat hij er baat bij heeft).

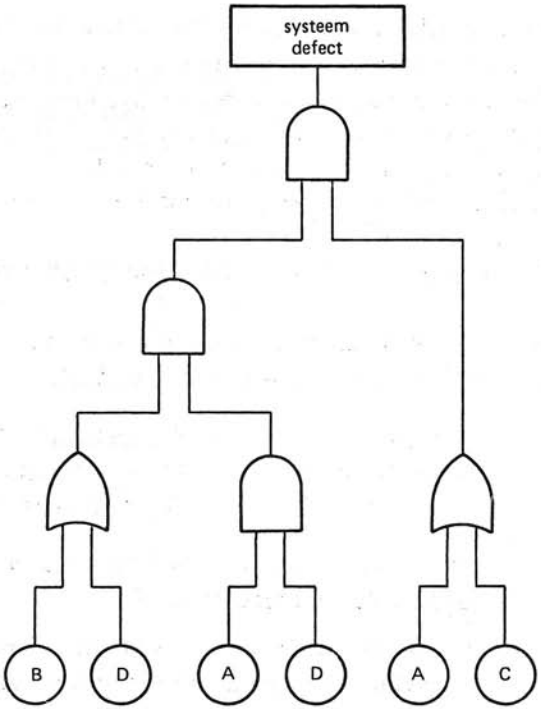
Opgaven

8.1. Bestaan er naast faalbomen ook succesbomen? Indien uw antwoord op deze vraag bevestigend is, zet dan de links onderstaande faalboom met faalgebeurtenissen A, B, C en T om in een succesboom met de overlevings- of succesgebeurtenissen A′, B′, C′ en T′.
Wat is het bijbehorende catastrofale faalmodel?

8.2. Bepaal met behulp van het Fussel-Vesely algoritme de gereduceerde faalboom van de rechts onderstaande faalboom.







8.3. a. Bepaal van de bovenstaande faalboom met behulp van het Fussel-Vesely algoritme de minimumsneden en geef de gereduceerde faalboom.

b. Als gegeven is dat de gebeurtenissen A, B, C en D stochastisch onafhankelijk zijn en dat de failure rates behorende bij deze gebeurtenissen respectievelijk λ_A, λ_B, λ_C en λ_D zijn, wat is dan de faalkans van dit systeem op tijdstip t?

8.4. Een viermotorig vliegtuig kan desnoods nog met twee motoren blijven vliegen, ongeacht de plaats van deze motoren. De motoren falen stochastisch onafhankelijk.

a. Indien de bedrijfszekerheid van elke motor gedurende de vlucht 90% bedraagt, hoe groot is dan de kans dat het vliegtuig behouden aankomt?

b. Als nu bovendien nog vereist is, dat in het geval dat er nog twee motoren werken, deze zich aan weerszijde van de romp dienen te bevinden, (dus aan iedere vleugel één), geef dan de faalboom van dit systeem.

c. Hoe groot is in geval (b) de kans dat het vliegtuig behouden aankomt als de bedrijfszekerheid per motor 90% bedraagt?

d. Als de failure rate van de motoren λ is, hoe groot is dan in geval (b) de 'mission reliability' als de vluchtduur T is?

8.5. Een solo-zeiler die de Atlantische Oceaan wil oversteken neemt twee radio zend/ontvangst installaties mee. Eén daarvan is de normale zend/ontvanger die op het 24 V accunet van de boot aangesloten kan worden. Het tweede toestel is voor noodgebruik en kan zowel op het 24 V net als op een 'battery pack' van 6 V aangesloten worden.
Beide radiotoestellen bestaan uit een zendgedeelte en een ontvangstgedeelte die *apart* kunnen falen.
Voor een goede communicatie moet zowel gezonden als ontvangen kunnen worden.

a. Stel de faalboom op voor de gebeurtenis dat geen goede communicatie mogelijk is. Gebruik hiervoor de volgende notaties.

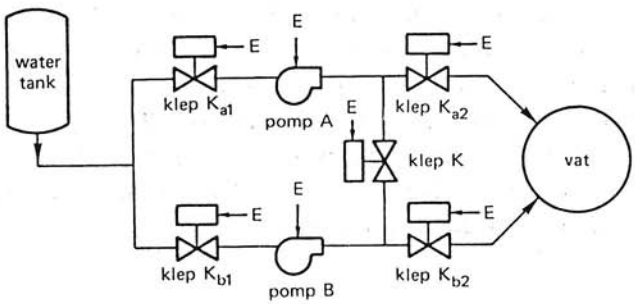
N = net	B = battery pack
Z_1 = zender 1	O_1 = ontvanger 1
Z_2 = zender 2	O_2 = ontvanger 2

b. Indien alle onderdelen van de installatie een faalkans van 0,1 hebben, bereken dan de kans op de topgebeurtenis.

8.6. Het 'low-pressure injection system' van een kernreactor bestaat uit een watertank waaruit met behulp van een actief redundant uitgevoerde pomp water naar een koelvat gepompt wordt. Om onderhoud aan de pompen mogelijk te maken tijdens bedrijf kan een pomp van het circuit geïsoleerd worden door de kleppen K_{a1}, K_{a2} en K, respectievelijk K_{b1}, K_{b2} en K dicht te zetten. De kleppen en de pompen zijn aan hetzelfde elektriciteitsnet E gekoppeld. Een klep kent slechts één faalmode, namelijk ten onrechte dicht. De pompen kunnen falen en bovendien kan het elektriciteitsnet uitvallen waarbij alle kleppen automatisch dichtgaan en de pompen stilvallen.

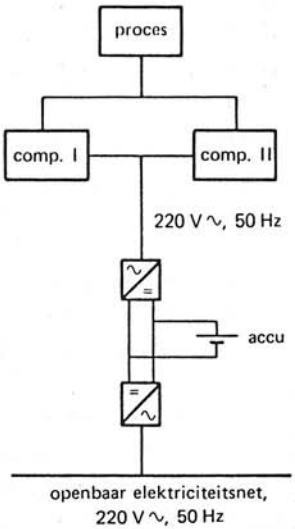
a. Bepaal met behulp van de padenmethode de bedrijfszekerheid van dit systeem als gegeven is dat de bedrijfszekerheid van een klep R_K, van een pomp R_P en van het elektriciteitsnet R_E is.

b. Geef een faalboom van dit systeem met als topgebeurtenis dat het koelvat geen water toegevoerd krijgt.



8.7. Een computersysteem voor een procesregeling bestaat uit twee redundante computers die ieder voor zich in staat zijn het proces te regelen. Om korte netstoringen te overbruggen is een elektrisch circuit tussen het openbare net en de net-aansluting van de computers aangebracht, waarin o.a. een accu is opgenomen die in staat is de benodigde energie te leveren aan *beide* computers gedurende één uur.
Dit houdt dus in dat als de netstoring na 1 uur nog niet verholpen is, de procesregeling zal stoppen. Verder kunnen nog de volgende vier onafhankelijke fouten in dit systeem optreden:
- computer I faalt;
- computer II faalt;
- de accu is stuk;
- het openbaar net valt uit.

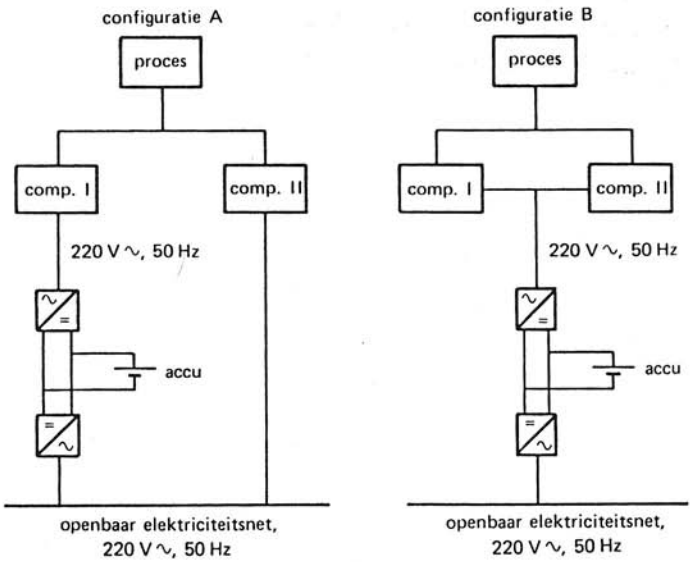
Stel voor dit systeem een faalboom op waar al de bovenstaande gegevens in verwerkt zijn. (De topgebeurtenis is dat het proces niet meer geregeld wordt.)



8.8. Een computersysteem voor een procesregeling moet gedurende 1 000 uur onafgebroken correct functioneren. Het systeem bestaat uit twee redundante computers die ieder voor zich in staat zijn het proces te regelen. Om korte netstoringen te overbruggen is een elektrisch circuit tussen het openbare net en de net-aansluiting van één (configuratie A) of van beide computers (configuratie B) aangebracht. In dit elektrisch circuit is een accu opgenomen die in staat is de benodigde energie te leveren aan de aangesloten computer(s) gedurende twee uur voor configuratie A en gedurende één uur voor configuratie B. Dit houdt in dat

als een netstoring na respectievelijk twee en één uur niet verholpen is, de procesregeling stopt.
Verder kunnen nog de volgende vier onafhankelijke fouten in dit systeem optreden waarbij de kans dat deze fout optreedt gedurende de bovenstaande 1 000 uur achter de fout is vermeld:
- computer I faalt (0,01);
- computer II faalt (0,01);
- de accu is stuk (0,01);
- het openbare net valt uit (0,1).

Verder is nog gegeven dat de kans dat het openbare net niet gerepareerd is binnen één uur 0,1 en niet binnen twee uur 0,01 is. Bepaal met behulp van de respectievelijke faalbomen welk van de twee configuraties de hoogste bedrijfszekerheid geeft.



8.9. Geef de definitie van *risico*.

8.10. We beschouwen een rookdetectiesysteem in een bepaalde ruimte. Hierin wordt gebruik gemaakt van een sensor die het alarm doet afgaan bij een bepaalde hoeveelheid rook. Deze sensor kan echter op de volgende wijzen falen: (met erachter de kans)
- Signaleert rook als er geen rook aanwezig is (0,1);
- signaleert geen rook als er wel rook aanwezig is (0,15).

Dit systeem is duidelijk niet bedrijfszeker genoeg en daarom besluit men drie van deze sensoren toe te passen.

a. Bij welke toestand van de drie sensoren moeten we het alarm laten afgaan opdat de detectiewaarschijnlijkheid van rook maximaal is?
b. Hoe groot is dan deze detectiekans?

c. Hoe groot is dan de kans op een vals alarm?
d. De optimale beslissingsstrategie is die waarbij het produkt (detectiekans × (1 − vals-alarm-kans)) het dichtst tot 1 nadert. Welke is dit in het bovenstaande geval en hoe groot is dan dit produkt?

8.11. Veiligheidseisen gebieden dat liftkabels viervoudig uitgevoerd worden. Elke kabel op zich is in staat om de lift op en neer te bewegen. Bovendien moet de lift nog voorzien zijn van veiligheidshaken die zich vastgrijpen in de wanden van de liftkoker zodra een bepaalde daalsnelheid overschreden wordt. Dit beveiligingssysteem kan falen met een failure rate λ_b, waardoor het systeem niet meer zal aanspreken als de maximaal toegelaten daalsnelheid overschreden wordt.
Als verder gegeven is dat de (identieke) kabels kunnen breken met failure rate λ_k, teken dan het bij deze lift behorende Markovdiagram. Geef duidelijk aan wat de toestanden voorstellen en wat de begin- en faaltoestand(en) is (zijn).

9. Bedrijfszekerheid van computerprogrammatuur

Het gebruik van computers is in de loop der tijd sterk toegenomen. Niet alleen voor wetenschappelijke en administratieve doeleinden (reken- en computercentra) maar ook voor technische (meetinstrumentatie computers) en industriële doeleinden (procesregeling) worden computers op grote schaal gebruikt. Dit gebruik strekt zich uit van zeer kritische toepassingen (vliegtuig- en scheepsbesturing, navigatie, beveiliging en bewaking) tot speelse, alledaagse toepassingen (spelletjes). In paragraaf 1.2 hebben we de noodzaak van een hoge bedrijfszekerheid besproken van zulke technische systemen die nauw met ons alledaagse leven verweven zijn.

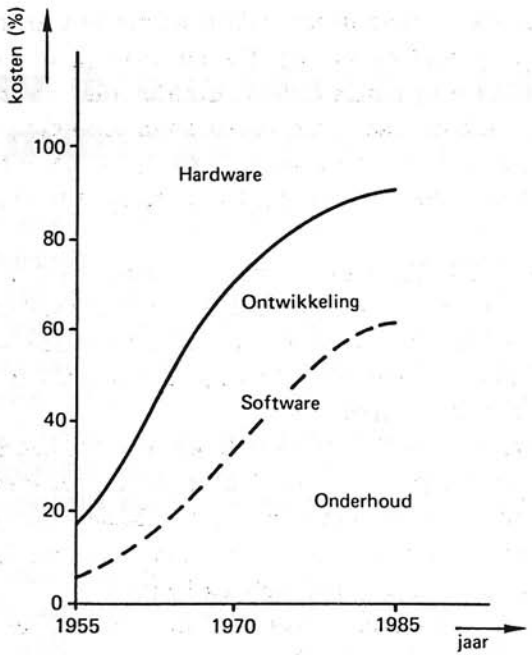
Men kan computertechniek ruwweg opdelen in de kant die te maken heeft met de fysische implementatie (de logische systemen, de communicatiewegen, de gegevensopslag, enz.) en de kant die te maken heeft met de besturing van de binaire processen die zich in de computer afspelen. Deze dichotomie wordt aangeduid met 'hardware'- en 'software'-computertechniek. Wat de bedrijfszekerheid van de hardware-kant van de computer betreft; deze is niet verschillend van wat we tot nu toe hebben behandeld. Het is juist de software-kant die een aparte benadering vraagt. Dit is voornamelijk vanwege het feit dat het falen van software veroorzaakt wordt door menselijke ontwerpfouten bij het schrijven van de software. Deze menselijke fouten zijn moeilijker voor mathematische behandeling toegankelijk dan de hardware fouten, die door allerlei fysische degeneratie-processen worden veroorzaakt.

De laatste jaren heeft de software reliability engineering sterke aandacht gekregen. Dit ligt onder andere aan het feit dat gigantische kosten gemoeid zijn met de ontwikkeling, de verificatie, de validatie, het onderhoud en de documentatie van programmatuur (zie figuur 9.1).

Dit is evenwel niet de enige reden. Ook de toepassing van computers in kritische systemen waarvan het uitvallen veel kosten, produktieverlies en ergernis met zich mee kan brengen, ja zelfs mensenlevens kan kosten, heeft er voor gezorgd dat de bedrijfszekerheid van computerprogrammatuur veel aandacht krijgt.

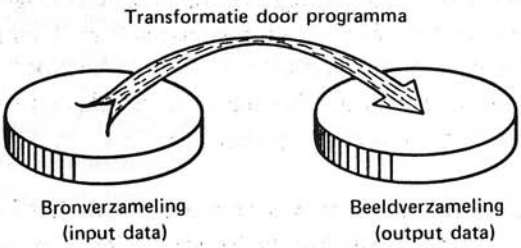
9.1. Inleiding

Een correct lopend computerprogramma kan gezien worden als een trans-



Figuur 9.1. De verhouding van de totale 'hardware' kosten en de 'software' kosten voor meetcomputersystemen. Deze grafiek heeft betrekking op de totale 'cost of ownership'.

formatie die de elementen van een bronverzameling (*input data set*) afbeeldt op elementen van een beeldverzameling (*output data set*), zoals in figuur 9.2 aanschouwelijk is voorgesteld.



Figuur 9.2. Programmatuur beeldt elementen van een bronverzameling (input data) af op elementen van een beeldverzameling (output data).

Nu kan het programma op een bepaalde deelverzameling van alle mogelijke geldige input-data blijven steken, een foutmelding geven of een fout resultaat produceren. Dit betekent niet dat deze fout op het ogenblik dat de fout veroorzakende opdracht wordt geëxecuteerd ook inderdaad ontstaat: deze fout bevond zich reeds in het programma (*dormant failure*) en werd opgeroepen door de toevallige combinatie van ingangsdata die het pro-

gramma een executiepad deden volgen waarin een tot op dat ogenblik verborgen gebleven fout voorkwam. De remedie is, althans in theorie, erg simpel: test het programma (*alle* opdrachten die het programma kan uitvoeren) voor alle mogelijke combinaties van ingangsgegevens. Het zal duidelijk zijn dat dit zeker voor complexe programmatuur praktisch ondoenlijk is (het zou in sommige gevallen een testtijd van ettelijke jaren betekenen).

In de software reliability engineering kan men een drietal onderverdelingen aanbrengen: het schrijven (ontwerpen) van bedrijfszekere programma's, het testen en verifiëren van programma's en het modelleren van de programmatuur-bedrijfszekerheid. We zullen op elk van deze zaken in een aparte paragraaf wat nader ingaan.

Algemeen kan men stellen dat, om te geraken tot bedrijfszekere programma's, men strikt logisch en consistent te werk moet gaan. Men dient daarbij in het oog te houden dat er een aantal belangrijke verschillen is met de bedrijfszekerheid van hardware-systemen zoals we die in de voorgaande hoofdstukken van dit boek hebben besproken:

- Software fouten worden uitsluitend door de ontwerper gemaakt. Bij de produktie (het kopiëren) van software worden geen fouten geïntroduceerd.
- Programmatuur kent geen slijtagegedrag, noch kent het driftfouten; een fout treedt op of treedt niet op.
- Fouten in de software geven geen voorboden (*precursors*) van een op handen zijnd toekomstig falen. Ze treden plotseling op. Na jarenlang sluimerend geweest te zijn worden ze manifest door een bepaalde combinatie van opdrachten en ingangsgegevens die het programma een weg laten doorlopen waarop één of meer voetangels en klemmen voorkomen.
- Reparaties, dus programmawijzigingen, kunnen hier ook nieuwe, onvermoede fouten met zich meebrengen, vooral als ze in de haast worden uitgevoerd (het 'even snel' werkend maken van het programma!).
- Oudere en langer gebruikte programmatuur wordt (als het regelmatig wordt verbeterd) hoe langer hoe bedrijfszekerder. Het faalgedrag in de tijd van software-paketten is analoog aan dat van hardware met kinderziekten.
- De bedrijfszekerheid van software is onafhankelijk van de fysische omgeving (trillingen, vocht, temperatuur, en dergelijke). Wel is het afhankelijk van de machine-omgeving (het type computer, de configuratie en het operating system).
- Redundant executeren van hetzelfde programma heeft geen zin, eventuele fouten zijn volledig afhankelijk. Het redundant executeren van

door een ander team ontwikkelde software zou kunnen, maar heeft weinig effect daar de redundantie dan op een zeer hoog niveau van complexiteit wordt uitgevoerd.

- Volledig correcte software faalt niet meer.
- Theoretisch kan software volledig getest worden en nooit meer fouten geven.

9.2. Schrijven van bedrijfszekere programma's

Zoals we reeds gezien hebben worden de fouten in software bij het ontwerp (dus het schrijven) van de programmapakketten gemaakt. Om de kans op fouten klein te maken is het een vereiste dat de ontwerper zowel de 'taal' als de 'omgeving' waarin het programma gebruikt gaat worden goed kent. Complexe programmatuur wordt doorgaans door teams geschreven. Van groot belang is daarbij een goede coördinatie tussen de teamleden (*reliability management*). Verder is van groot belang het ontwikkelen van software zoveel mogelijk langs weldoordachte lijnen uit te voeren en bovendien de ontwikkelde software op een bepaalde manier te structureren (*structured programming*). De gemeenschappelijke noemer van 'structured programming'-technieken is een *top-down*-ontwerp dat *opgebouwd* is *uit modules* die apart en in hun onderlinge samenhang getest kunnen worden.

In het 'top-down'-ontwerp start men met de software-specificatie: wat moet de programmatuur doen? Daarna wordt de architectuur bepaald, de modulaire structuur, de grootte van de modules, het gebruik van vaste subroutines, enzovoort. De kern van het programma wordt eerst geschreven, voorlopig met dummy subprogramma's op het volgende, lagere niveau. Deze subprogramma's worden daarna op gelijksoortige wijze verder ontwikkeld. Hierbij worden ongestructureerde sprongopdrachten zoals de beruchte 'goto' instructie vermeden, niet omdat deze inherent bedrijfsonzeker zouden zijn, maar omdat ze de executievolgorde kunnen wijzigen waardoor de programmaloop moeilijk traceerbaar wordt. Dit heeft tot gevolg dat het programma moeilijk leesbaar is en dus moeilijk op fouten te onderzoeken is.

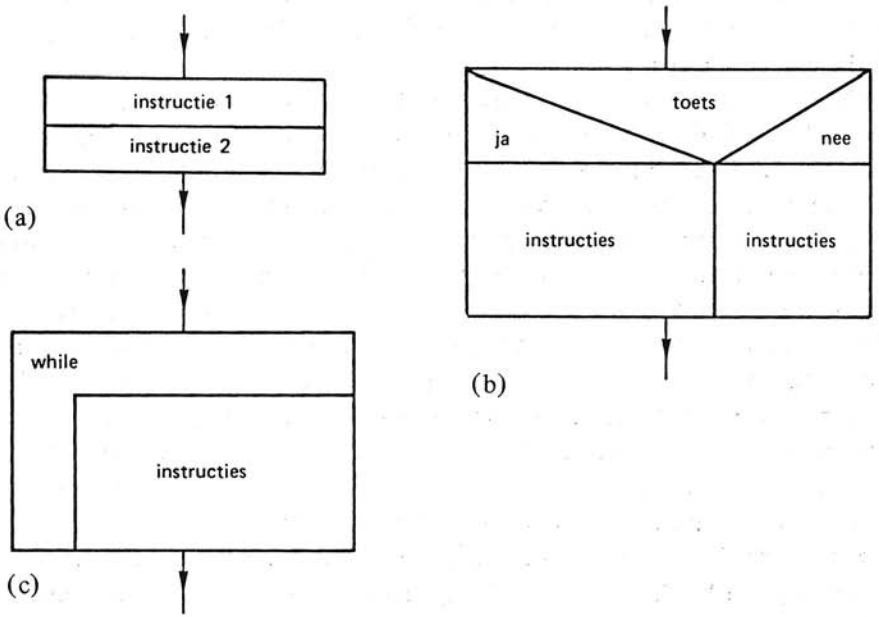
Het gehele programma-ontwerp dient als onderdeel van het bedrijfszeker programmeren goed gedocumenteerd te worden. Dit houdt onder meer in een *functionele beschrijving* van het geheel en van iedere module (subroutine, procedure). Deze beschrijving dient te bestaan uit een omschrijving van:

- de naam van de betreffende module;
- de datum, het versienummer en de naam van de ontwerper;
- de functie van de betreffende module;
- de vereiste invoerparameters;

- de vereiste uitvoerparameters;
- alle modulen of routines waardoor de betreffende module wordt aangeroepen;
- alle modulen of routines die de betreffende module zelf aanroept.

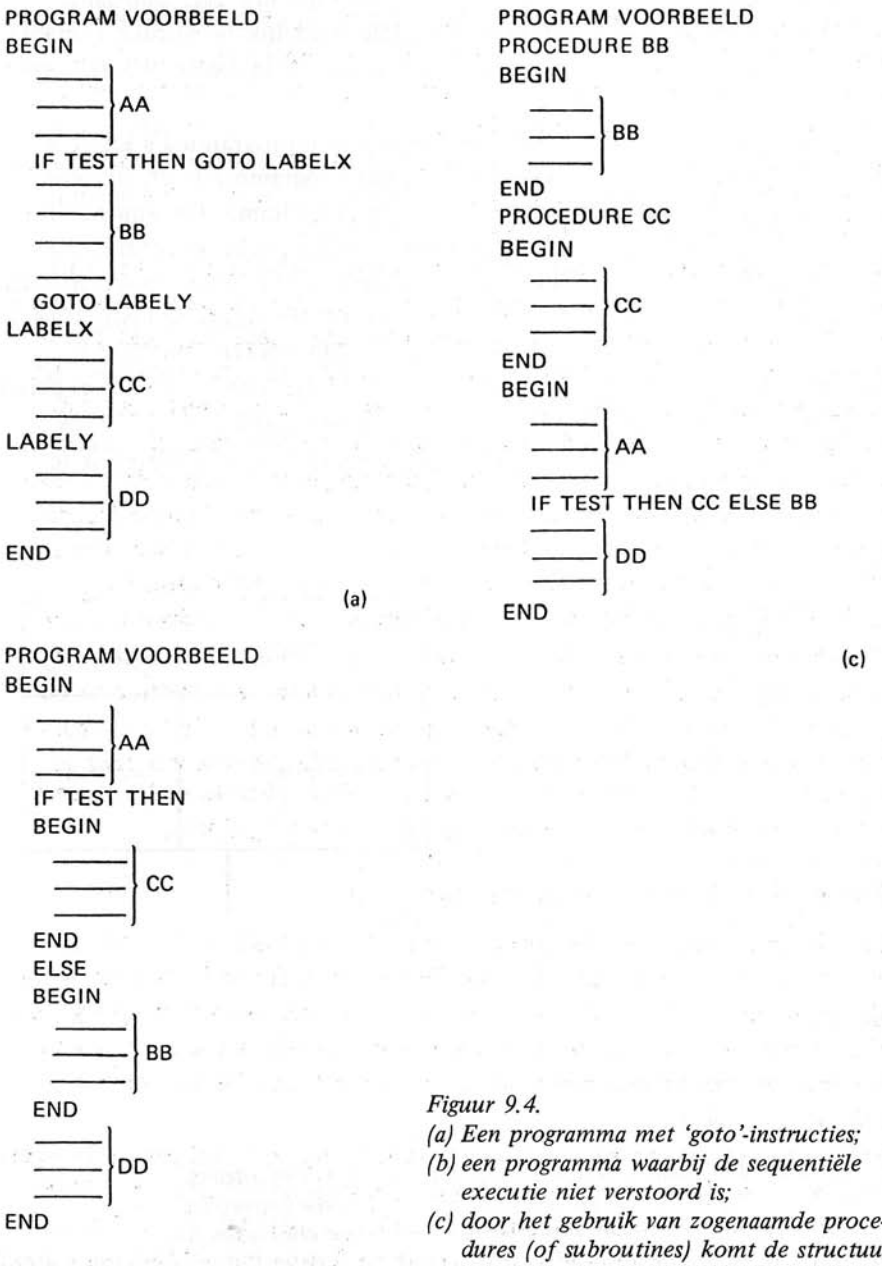
Verder dient de structuur van iedere module duidelijk te worden gemaakt, bijvoorbeeld met behulp van diagrammen zoals die in figuur 9.3 zijn weergegeven.

Het is eenvoudig in te zien dat men transparante programma's krijgt als de volgorde waarin men de instructies in het programma leest, overeenkomt met de volgorde van executie van dat programma. Dit kan bereikt worden door het programma op de bouwen uit logische structuren die slechts één ingang, slechts één uitgang en slechts één functie hebben. Men dient zich verder in het gebruik te beperken tot de volgende instructies: 'sequence', 'IF THEN ELSE', 'DO WHILE', 'DO UNTIL', en 'CASE'. Het gebruik van 'GOTO' of 'JUMP' statements die 'control transfer' geven naar een willekeurig ander programmadeel hoort hierin dus niet thuis. Dat het relatief eenvoudig is 'goto'-vrije programma's te schrijven is te zien in figuur 9.3.



Figuur 9.3. Programma structuren met één ingang en één uitgang.
(a) Het na elkaar sequentieel uitvoeren van instructies.
(b) De logische structuur van de 'if then else' instructie.
(c) Bij de while .. do instructie worden de instructies in het blok steeds opnieuw uitgevoerd indien er aan de voorwaarde voldaan wordt.

Met het gebruik van zulke instructies kan men het programma sequentieel afwerken. Dat dit voor de lezer aanzienlijk beter te overzien is is aangegeven in figuur 9.4.



Figuur 9.4.
(a) Een programma met 'goto'-instructies;
(b) een programma waarbij de sequentiële executie niet verstoord is;
(c) door het gebruik van zogenaamde procedures (of subroutines) komt de structuur van een programma duidelijk naar voren.

9.3. Testen op bedrijfszekerheid

Het doel van het testen van software is dat het programma functioneert zoals gespecificeerd en dat er geen fouten meer in voorkomen. Dit testen kan op verschillende wijzen geschieden. Het verdient aanbeveling het testen te laten doen door andere mensen dan de betrokken programma-ontwerpers. Een eerste stap is het zorgvuldig nagaan van de geschreven 'code' (*manual code walk throughs*). Een tweede stap is het gebruik van speciaal gereedschap (software) om de geschreven software te controleren. Deze hulpmiddelen geven naast een foutsignalering soms ook een numerieke maat voor de grondigheid waarmee getest is.

Het te testen programmamoduul in zijn oorspronkelijke vorm (de zogenaamde source code) wordt omgezet in een zogenaamd geïnstrumenteerd moduul, waarin sensor- en counterinstructies zijn toegevoegd aan het te testen moduul zonder dat dit de functie van het moduul verandert. Het toevoegen van deze diagnostische instructies noemt men instrumentatie. Het geïnstrumenteerde moduul wordt daarna geschikt gemaakt om het uit te voeren met test-input data. Na executie geeft dit naast de normale output een verzameling instrumentatie-data. Daarna wordt deze instrumentatie data en het oorspronkelijke programma van het geïnstrumenteerde moduul toegevoerd aan een zogenaamd analysemoduul. Dit analyseprogramma produceert dan een rapport over het gedrag van het geteste moduul gedurende het verwerken van de aangeboden test invoer. Deze gerapporteerde informatie geeft vertrouwen in de structuur en de gebruikte instructies door te verzekeren dat iedere tak in het programma minstens één maal is doorlopen. Een testmethode die ook wel eens gebruikt wordt is de software op een geheel andere wijze te realiseren, de beide programma's te draaien en de resultaten te vergelijken.

9.4. Faalmodellen voor programmatuur

We hebben reeds gezien dat software faalt door menselijke fouten. Dit maakt dat een deterministische modellering van softwarefouten onmogelijk is: de mens is moeilijk in een model te vangen. Toch kunnen we ook hier weer stellen dat, als het gaat om complexe softwarepakketten waar veel mensen aan hebben meegewerkt, er in stochastische zin zeker nog iets over te zeggen valt.

Het primaire doel van een software reliability model is het gedrag te voorspellen van de programmatuur zodra deze operationeel is. De bedrijfszekerheid van systeemprogrammatuur verandert drastisch met de tijd, daar het programma voortdurend getest wordt en fouten hersteld worden door herprogrammering. De bedrijfszekerheid en de MTTF nemen in het alge-

meen toe naarmate de geaccumuleerde computertijd toeneemt. Daarom zijn modellen die gebaseerd zijn op de geaccumuleerde executietijd veel nauwkeuriger dan modellen die op de kalendertijd zijn gebaseerd. De actueel gebruikte processortijd is een goede praktische maat voor de foutinducerende stress waaraan het programma blootstaat. We zullen in het navolgende *computertijd model* daarom de programmatuur-bedrijfszekerheid (*software reliability*) bepalen als functie van de totaal geaccumuleerde computertijd voor een programma. Opgemerkt dient te worden dat dit model zich alleen uitspreekt over de tijdsperiode gedurende welke het programma wordt getest en ontdaan wordt van fouten (*debugging*). Als het programma na beëindiging van de testperiode niet meer onderhouden wordt, hangt de bedrijfszekerheid alleen nog af van de tijd waarover het programma gebruikt wordt: de modelparameters veranderen niet meer.

Het aantal fouten N dat bij het testen wordt *gedetecteerd* en wordt *gecorrigeerd* is een exponentiële functie van de totale CPU-tijd, geaccumuleerd tijdens het testen. Deze CPU-tijd zullen we aanduiden met τ.
We krijgen dan:

$$N = N_0(1 - e^{-\tau C/M_0 T_0}).$$

Hierin is N_0 het initiële aantal fouten in de programmatuur na de systeemintegratie. C is een versnellingsfactor die aangeeft hoe zwaar het testen het programma belast ten opzichte van het gebruik van het programma onder normale omstandigheden. M_0 is het totale aantal fouten dat mogelijk is gedurende de duur van het testen en het corrigeren en is gelijk aan het aantal fouten dat geconstateerd zal worden wanneer het programma zolang getest wordt dat alle fouten verwijderd zijn. T_0 tenslotte is de MTTF bij het starten van de testprocedure.
Verder zal niet elke geconstateerde fout succesvol hersteld worden; een foutieve correctie kan zelfs andere, extra fouten introduceren. Als we aannemen dat per geconstateerde fout gemiddeld B fouten uit het programma verwijderd worden ($0 < B < 1$) dan geldt:

$$N_0 = B \cdot M_0$$

en natuurlijk ook:

$$N = B \cdot M,$$

waarbij M het aantal gedetecteerde fouten voorstelt. Dit maakt dat het aantal geconstateerde fouten eveneens een negatief-exponentiële functie is van de geaccumuleerde computertijd:

$$M = M_0(1 - e^{-\tau C/M_0T_0}).$$

Hieruit volgt dat de MTTF op het tijdstip τ onder normale gebruikscondities voldoet aan :

$$MTTF(\tau) = \frac{C}{dM(\tau)/d\tau} = T_0\, e^{\tau C/M_0T_0}.$$

De bedrijfszekerheid voor een operationele periode $(\tau, \tau+\Delta\tau)$ is dan:

$$R(\Delta\tau) = e^{-\Delta\tau/MTTF(\tau)}.$$

Als men zich bij het testen een minimum MTTF van T_{min} ten doel heeft gesteld, heeft men nog ΔM geconstateerde fouten te gaan en moet men nog $\Delta\tau$ testtijd investeren, als de huidige MTTF = T ($T \leqslant T_{min}$):

$$\Delta M = M_0T_0(\frac{1}{T} - \frac{1}{T_{min}}),$$

$$\Delta\tau = \frac{M_0T_0}{C} \ln(\frac{T_{min}}{T}).$$

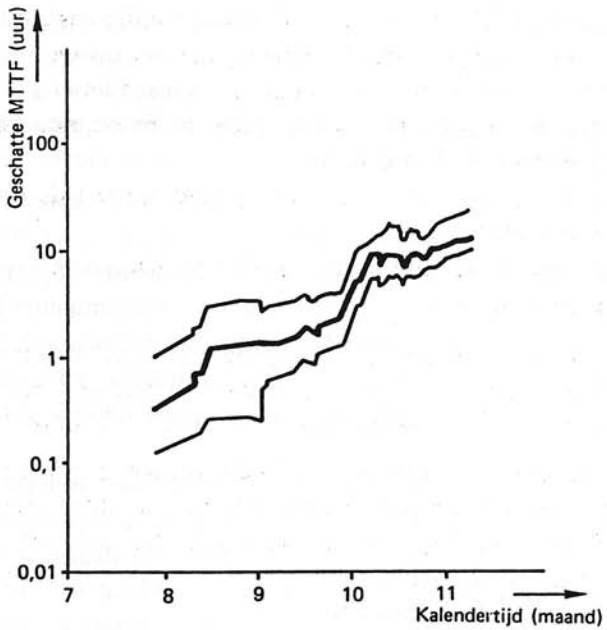
Tot op heden hebben we alles in CPU-tijd uitgedrukt. Als we weten welke fractie van de kalendertijd deze CPU-tijd is, dus als we weten voor welk gedeelte van de tijd er getest wordt, kunnen we dit model omrekenen in kalendertijd. De fractie CPU-tijd hangt af van de toekenning van CPU-tijd voor het testen en hoelang het vinden en corrigeren van een fout duurt. In het algemeen kan men stellen dat in het begin de gemiddelde tijd tussen twee fouten bij het testen zo kort is, dat men van tijd tot tijd het testen moet stoppen om de programmeurs de tijd te geven de geconstateerde fouten te herstellen. Bij verder testen wordt de intervaltijd tussen twee opeenvolgende fouten steeds groter: nu wordt de foutcorrectie niet meer begrensd door de snelheid waarmee de programmeurs fouten kunnen herstellen, maar door de snelheid waarmee het testteam de testprocedure kan uitvoeren en faaldata kan analyseren. Tenslotte wordt voor nog spaarzamer voorkomende fouten de capaciteit van de rekenfaciliteit de beperkende factor.

Drie modelparameters zijn nodig om het model vast te leggen: C, M_0 en T_0. De versnellingsfactor C wordt bepaald door de testomgeving, terwijl M_0 en T_0 door het programma (en de ontwerpers daarvan) bepaald worden. Deze laatste parameters kunnen initieel geschat worden en gedurende het testen nauwkeuriger bepaald worden naarmate er meer gegevens beschikbaar zijn. De initiële schatting gaat als volgt:

N_0 wordt vooral door de complexiteit van het programma bepaald en bedraagt ongeveer 5 fouten per 1000 instructies voor programma's geschreven in zogenaamde assemblertaal.
De foutreductiefactor B hangt af van de grondigheid waarmee men tewerk gaat ($0 < B < 1$). M_0 kan nu worden berekend. De parameter T_0 kan voorspeld worden uit:

$$T_0 = \frac{1}{f \cdot k \cdot N_0},$$

waarin de executiefrequentie f van het programma bepaald wordt door het aantal aangeboden instructies in het programma en de gemiddelde executietijd per instructie. De foutblootstellingsfactor k is het quotiënt van de gemiddelde executietijd van het programma en de gemiddelde geaccumuleerde executietijd tussen twee manifestaties van dezelfde fout. Of, anders gezegd, k geeft de gemiddelde fractie van het totaal aantal programma-executies waarin een bepaalde fout optreedt.
Tenslotte is in figuur 9.5 een voorbeeld gegeven hoe op basis van dit computertijdmodel de geschatte MTTF (met voortdurend aangepaste waarden voor C, M_0 en T_0) er uitziet als functie van de kalendertijd die verloopt bij het testen. De beide buitenste curves markeren het 75 % betrouwbaarheidsinterval rondom de uit metingen geschatte waarde (middelste curve).



Figuur 9.5. De geschatte 'huidige' MTTF van een softwarepakket gedurende de testperiode, geschat op basis van het CPU-tijd model.

Opgaven

9.1. In een computerprogramma geschreven in BASIC komt de volgende sequentie van instructies voor:

```
400 IF A > 0 THEN GOTO 420
410 GOTO 430
420 IF B > 0 THEN GOTO 450
430 LET D = -C
440 GOTO 460
450 LET D = C
460 PRINT D
```

Herschrijf dit deel van het programma zonder gebruik te maken van GOTO opdrachten.

9.2. Toon aan dat de MTTF van een programma na een geaccumuleerde computer-testtijd τ, gelijk is aan $T_0 \, e^{\tau C / M_0 T_0}$, waarin T_0 de initiele MTTF is en M_0 het initiële totale aantal fouten is dat kan optreden tijdens het testen en corrigeren. C is de versnellingsfactor voor het optreden van fouten gedurende de testprocedure ten opzichte van het optreden van fouten tijdens normaal gebruik van het programma.

9.3. Men eist van een programma dat een chemisch proces moet controleren een MTTF van 10^6 uur. Het programma bestaat uit 100.000 instructies, waarbij voor de aanvang van het testen mag worden aangenomen dat er 600 fouten in zitten. De reductiefactor B is 0,3; de executiefrequentie f is 5 per seconde; de blootstellingsfactor k is 10^{-2} en de versnellingsfactor is 2.

a. Hoeveel computer-testtijd is benodigd om aan de bovenstaande eis te voldoen?
b. Hoeveel initiële fouten zijn er daarna gemiddeld nog aanwezig in het programma?

9.4. Zoals uit figuur 9.1 blijkt krijgen de kosten voor programmatuurontwikkeling en -onderhoud een steeds groter aandeel in de totale kosten van computersystemen. Geef hiervoor een aantal oorzaken.

9.5. Hoofddoel bij het streven naar bedrijfszekere programmatuur is het voorkómen van programmafouten in een zo vroeg mogelijk stadium van de ontwikkeling. Bedenk een aantal oorzaken voor het ontstaan van programmafouten:

a. tijdens de *specificatiefase*;
b. tijdens de *realisatiefase*;
c. in de *test-* en *gebruiksfase.*

9.6. Het vinden en corrigeren van programmafouten wordt beduidend lastiger naarmate het programma in een later stadium van ontwikkeling verkeert. Bedenk een aantal richtlijnen voor het voorkomen van programmeerfouten.

Uitgewerkte opgaven

1. Inleiding

1.1. Bedrijfszekerheid is de *kans* dat een bepaald *systeem* nauwkeurig *gespecificeerde functies* uitvoert gedurende een bepaald interval van een *levensduurvariabele* mits het systeem bedreven wordt binnen een bepaald *omgevingsgebied.*

1.2. Betrouwbaarheid is niet hetzelfde als bedrijfszekerheid; de term betrouwbaarheid is afkomstig uit de statistiek en is gereserveerd voor de kans dat de werkelijke waarde van een stochastische parameter ligt binnen een zeker interval rondom een op basis van een eindige steekproef geschatte waarde.

1.3. Door een gelijkmatige verdamping stijgt de weerstand van een uniforme gloeidraad ook gelijkmatig (uniform). Bij voeding uit een constante spanningsbron daalt dan de dissipatie ($P = U^2/R$) waardoor de temperatuur zal dalen en de verdamping steeds verder afneemt tot deze uiteindelijk zal stoppen.

1.4. Bij temperaturen lager dan 0° C en hoger dan 50° C voldoet de versterker blijkbaar niet meer aan de overige specificaties. Opslag van deze versterker is bij deze temperaturen nog wel mogelijk zonder blijvende schade.

1.5. De deterministische bedrijfszekerheidstechniek houdt zich bezig met het bestuderen van de fysische aftakelingsprocessen (bijvoorbeeld corrosie) die tot falen leiden.

1.6. Voor het vervaardigen van een bedrijfszeker produkt zijn alle facetten van de realisatie van zeer groot belang: het ontwerp, de keuze van de toe te passen componenten, het testen, het verzamelen van uitvalgegevens, het berekenen van de te verwachten bedrijfszekerheid, het analyseren van de fysische aftakelingsprocessen en de (constante) kwaliteit van de produktie. Doorgaans zal het toezicht op al deze taken onmogelijk door één persoon uitgevoerd kunnen worden en daarom dient een multi-disciplinair gezelschap (*reliability group*) geformeerd te worden waarvan elk lid een deeltaak toegeschoven krijgt. Zonder een goede taakverdeling en een terugkoppeling van faalgegevens zal zo'n gezelschap nooit optimaal kunnen functioneren en daarom is een goede organisatie zeer gewenst.

1.7. Voorbeelden van omgevingselementen die voor geïntegreerde circuits invloed zouden kunnen hebben op verouderingsprocessen zijn: vocht, damp, de temperatuur, een aggressief chemische milieu (zuur, basisch, oplossend), mechanische trillingen en spanningen, elektrische belasting (spanning, stroom, elektrische lading).

2. Deterministische bedrijfszekerheid

2.1. Voor de Mean Time To Failure (MTTF) geldt voor de drie verschillende temperaturen het model van Arrhenius:
$MTTF(T_1) = t_0 \exp[E_A/kT_1] = 6{,}5 \cdot 10^3$ uur met $T_1 = 373$ K,
$MTTF(T_2) = t_0 \exp[E_A/kT_2] = 2{,}4 \cdot 10^4$ uur met $T_2 = 258$ K,
$MTTF(T_3) = t_0 \exp[E_A/kT_3]$ met $T_3 = 298$ K.
Uit de eerste twee vergelijkingen kan de activeringsenergie E_A bepaald worden volgens:

$$E_A = \frac{k}{(1/T_2 - 1/T_1)} \ln\left[\frac{MTTF(T_2)}{MTTF(T_1)}\right] = 1 \text{ eV}.$$

$MTTF(T_3)$ wordt dan gevonden als:

$$MTTF(T_3) = MTTF(T_1) \cdot \exp\left[\frac{E_A}{k}\left(\frac{1}{T_3} - \frac{1}{T_1}\right)\right] = 1{,}66 \cdot 10^7 \text{ uur}.$$

2.2. Sterkstroomgeleiders hebben een veel kleinere stroomdichtheid (A/m^2) dan de zeer kleine gemetalliseerde paden in halfgeleiders (die enkele µm breed en dik zijn), waardoor elektromigratie niet of slechts nauwelijks voorkomt. De geleiders zijn bij sterkstroominstallaties relatief veel dikker omdat de maximaal toegestane temperatuur in verband met isolatie van hoge spanningen veel lager is.

2.3. Men past kathodische bescherming toe waarbij in de buurt van de dure scheepsschroef een metaal aangebracht wordt dat gemakkelijker oplost dan het metaal van de schroef, dat hierbij gespaard blijft.

2.4. Het dominante faalmechanisme van een auto waarvan de olie nooit ververst wordt is een sterke slijtage van de te smeren onderdelen. Eén van de mogelijke gevolgen (één van de mogelijke faalwijzen) is het stukgaan van de motorlagers.

2.5. Het beproeven van *alle* produkten voorafgaand aan de aflevering met het doel zwakke en kapotte componenten te verwijderen wordt 'screening' genoemd. Wanneer de overgebleven componenten niet merkbaar verzwakt zijn door de beproeving, dan zal de afgeleverde groep produkten gemiddeld een hogere bedrijfszekerheid bezitten dan de oorspronkelijke groep.

2.6. Early failures (kinderziekten) treden op vlak na de ingebruikname. Ze vinden hun oorzaak in een produktieproces dat produkten aflevert die niet geheel gelijkwaardig zijn. Sommige produkten hebben daardoor zwakke plekken die ze snel doen uitvallen. Indien een produkt het kinderziekte-gebied (de garantieperiode) overleeft dan kan men aannemen dat het goed gefabriceerd was.

3. Statistische bedrijfszekerheidstechniek

3.1. De hazard rate is de conditionele faalkansdichtheid en is gedefinieerd als:

$$z(t) = \frac{f(t)}{R(t)} = -\frac{dR(t)}{R(t)}\,\frac{1}{dt},$$

ofwel de *relatieve* afname van de hoeveelheid overgebleven componenten.

3.2. Zie bladzijde 39.

3.3. Zie bladzijde 39.

3.4. De bedrijfszekerheid R(t) is gegeven door $R(t) = \exp\{-\int_0^t z(t)dt\}$.

Daar er verder moet gelden $\lim_{t\to\infty} R(t) = 0$, volgt uit de formule voor R(t) direct dat

$$\lim_{t\to\infty} \int_0^t z(t)dt = \infty$$

3.5. $\lim_{t\to\infty} tR(t) = 0$, zie bladzijde 42.

3.6. De hazard rate is gedefinieerd als $z(t) = \frac{f(t)}{R(t)}$. Verder geldt $f(t) = -\frac{\Delta R}{\Delta t}$.
We kunnen z(t) dus schrijven als

$$z(t) = -\left(\frac{\Delta R(t)}{R(t)}\right)\frac{1}{\Delta t}.$$

Hier volgt dus uit dat z(t) gelijk is aan de relatieve afname van de bedrijfszekerheid per tijdseenheid.

3.7. De bedrijfszekerheid R(t) is gegeven door

$$R(t) = \exp\{-\int_0^t z(t)dt\}$$

en de hazard rate z(t) door

$$z(t) = \frac{f(t)}{R(t)}.$$

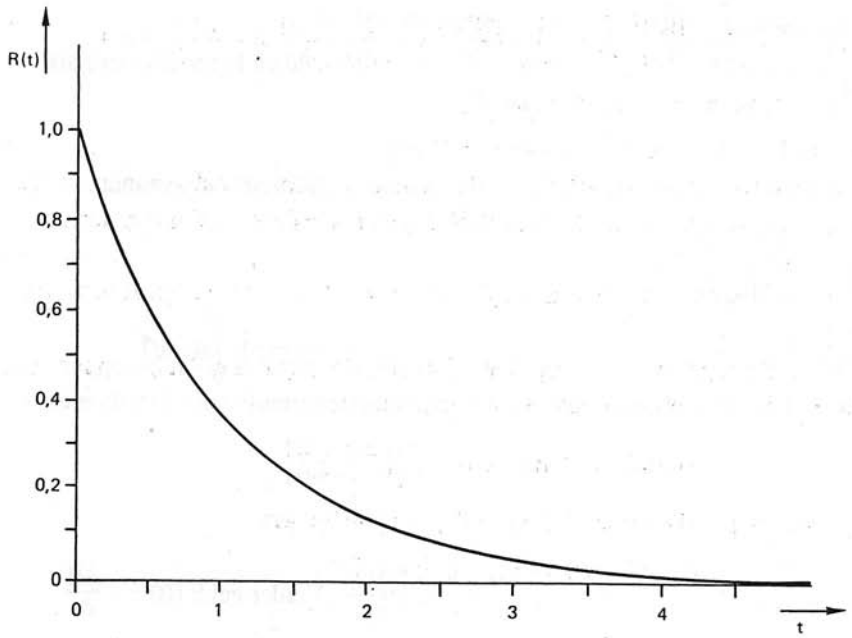
Hieruit volgt $f(t) = z(t)\exp\{-\int_0^t z(t)dt\}$.

3.8. a. Zie figuur. De bedrijfszekerheidsfunctie moet aan de volgende eisen voldoen:

- $0 < R(0) \leq 1$;
- monotoon dalend op $[0,\infty)$;
- $\lim_{t\to\infty} R(t) = 0$.

b. De bedrijfszekerheid is gegeven door:

$$R(t) = R(0)\exp\{-\int_0^t z(t)dt\}.$$



R(t) zal alleen monotoon dalen als de integraal in het argument van de exponentiële functie monotoon toeneemt met t. Dit houdt dus in dat voor z(t) moet gelden: $z(t) \geq 0$ in $[0,\infty)$. Uit het feit dat R(t) naar nul moet gaan als t naar oneindig gaat, volgt als eis voor z(t):

$$\lim_{t\to\infty} \int_0^t z(t)dt = \infty.$$

R(t) moet gelijk zijn aan R(0) voor t = 0. Dus moet voor z(t) ook gelden

$$\lim_{t\downarrow 0} \int_0^t z(t)dt = 0, \text{ ofwel } \lim_{t\downarrow 0} t\,z(t) = 0.$$

3.9. De eisen waaraan z(t) moet voldoen hebben we gevonden in opgave 3.8b. Aan deze voorwaarden wordt voldaan indien geldt $A \geq 0$ en $B \geq 0$. Verder moet de dimensie van A zijn: tijdseenheid^{-1} en voor B: tijdseenheid^{-2}.
In opgave 3.7 hebben we voor f(t) gevonden:

$$f(t) = z(t)\exp\{-\int_0^t z(t)dt\}.$$

Substitueren van $z(t) = A + Bt$ levert op:

$$f(t) = (A + Bt)\exp\{-(At + \frac{Bt^2}{2}\}.$$

3.10. $S_t^R = \lim_{\Delta t \to 0} \frac{\Delta R(t)}{R(t)} \frac{1}{\Delta t} = \frac{1}{R(t)} \frac{dR(t)}{dt} = -\frac{1}{R(t)} \frac{dF(t)}{dt} = -\frac{f(t)}{R(t)} = -z(t).$

$-S_t^R$ is dus gelijk aan de hazard rate z(t).

3.11. a. R (1000 uur) = $\exp(-10^{-3}) \approx 0{,}999$.

b. De faalkans is $1 - \exp(-10^{-3}) \approx 0{,}001$. Als er 10.000 van zulke apparaten zijn dan is het te verwachten aantal dat zal falen gedurende deze 1000 uur gelijk aan $0{,}001 \times 10.000 = 10$.

c. De gemiddelde levensduur is gelijk aan $1/\lambda = 10^6$ uur. De bedrijfszekerheid is dan gelijk aan $e^{-1} \approx 0{,}37$.

d. De overlevingskans voor nog eens 1000 uur, als gegeven is dat het apparaat de eerste 1000 uur heeft overleefd, wordt gegeven door

$$P(2000 \text{ uur} \mid 1000 \text{ uur}) = \frac{P(2000 \text{ uur})}{P(1000 \text{ uur})}$$

en voor de negatief exponentiële verdeling is dit gelijk aan

$$P(1000 \text{ uur}) = \exp(-10^{-3}) \approx 0{,}999.$$

3.12. $R(t) = R(0) \exp\{-\int_0^t z(t)dt\} = R(0) \exp\{-\int_0^t z(t)dt - \int_{t_1}^t \lambda dt\} =$

$= R(t_1) \exp\{-\lambda(t - t_1)\}.$

3.13. $R(1000) = \exp(-10^4 \cdot 1000) = 0{,}905$.

3.14. a. $R(t) = \exp(-\frac{a^2}{2}t^2)$; $z(t) = at$.

b. $T_1 = 10$ uur; $\exp(-\frac{a^2}{2}T_1^2) = \frac{4700}{5000}$ (300 gefaald);

$T_2 = 20$ uur; $\exp(-\frac{a^2}{2}T_2^2) = \{\exp -\frac{a^2}{2}T_1^2\}^4 = (\frac{47}{50})^4 \rightarrow \approx 1096$ gefaald.

In het tijdsinterval van 10 tot 20 uur falen er naar verwachting 796.

4. Faalgedrag van systeemcomponenten

4.1. a. $R(t) = \sum_{i=0}^{1} \frac{(\lambda t)^i}{i!} e^{-\lambda t} = (1 + \lambda t)e^{-\lambda t}$.

Hieruit volgt de hazard rate volgens:

$$z(t) = -\frac{1}{R(t)} \frac{dR(t)}{dt} = \frac{-1}{(1+\lambda t)e^{-\lambda t}} \cdot (-)\lambda^2 t e^{-\lambda t} = \frac{\lambda^2 t}{1+\lambda t}.$$

b. De gevonden functie is monotoon niet-dalend waarbij voor $t \rightarrow \infty$ geldt dat deze nadert tot $z(\infty) = \lambda$; het is zeer onwaarschijnlijk dat er nog geen eenheid gefaald heeft. Indien het systeem dan nog functioneert dan staat de laatste eenheid inge-

schakeld en zal de hazard rate van het systeem gelijk zijn aan de failure rate van deze eenheid: $z_{max} = z(\infty) = \lambda$.

4.2. De componenten hebben een constante failure rate. Dat houdt in dat deze componenten willekeurig falen en dat deze faalgebeurtenissen dus volgens Poisson verdeeld zijn. Poisson zegt dat als er gemiddeld m keer in een tijdsinterval T een bepaalde willekeurige gebeurtenis optreedt, dan de kans op geen optreden van deze gebeurtenis in het tijdsinterval T gelijk is aan exp(–m). In ons geval is de willekeurige gebeurtenis het falen van een transistor, waarbij het te verwachten aantal fouten in de geaccumuleerde testuren T (de zogenaamde componenturen) λT is, waarin λ de te bepalen failure rate is. We willen nu een oplossing voor λ waarbij de kans slechts 10 % is dat λ te laag geschat wordt. Uit $e^{-m} = 0{,}1$ volgt dat $m = 2{,}3$, zodat de kans dat λT ligt tussen 2,3 en ∞ gelijk aan 10 % is. De kans is dus 90 % dat λT ligt tussen 0 en 2,3. Uit $\lambda T = 2{,}3$ en $T = 10^4$ componenturen, vinden we dus $\lambda = 2{,}3 \times 10^{-4}$/uur. De failure rate ligt dus met een betrouwbaarheidsinterval van 90 % tussen 0 en $2{,}3 \times 10^{-4}$/uur.

4.3. Een afnemende hazard rate betekent dat de systemen zich nog in de kinderziektefase van hun levensduur bevinden en dat voornamelijk de reeds zwakke componenten uitvallen.

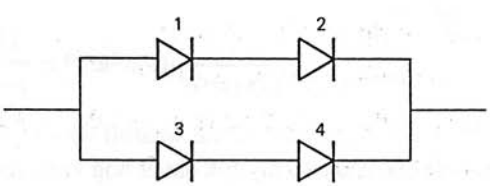
4.4. $$\lim_{t\to\infty} z(t) = \lim_{t\to\infty} \frac{f(t)}{R(t)} \overset{\text{L'Hopital}}{=} \lim_{t\to\infty} -\frac{f'(t)}{f(t)} = \lim_{t\to\infty} \frac{t-\theta}{\sigma^2} \to \infty.$$

4.5. Bij versnelde levensduurexperimenten worden de te testen systemen blootgesteld aan een verhoogde stress waardoor bepaalde faalmechanismen versneld worden. Op deze wijze hoopt men sneller over voldoende uitvalsgegevens te beschikken om een uitspraak te kunnen doen over de bedrijfszekerheid onder normale condities. Hiervoor moet aan de volgende voorwaarden voldaan worden:

- de versnellingsfactor moet bekend zijn;
- de hogere stress mag geen *nieuwe* faalmechanismen introduceren;
- de hogere stress mag geen andere faalmechanismen maskeren.

5. Statistische bedrijfszekerheidsmodellen

5.1. *Schakeling A.*

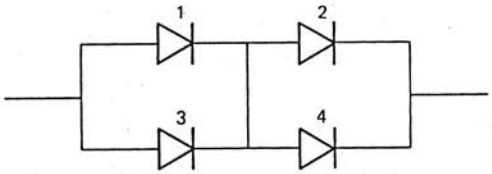


De kans op een open fout is: $a_o = 4q_o^2 - 4q_o^3 + q_o^4$.

De kans op een kortsluitfout is: $a_k = 2q_k^2 - q_4^k$.

De totale faalkans is dus: $a = a_o + a_k$.

Schakeling B.



De kans op een open fout is: $b_o = 2q_o^2 - q_o^4$.

De kans op een kortsluitfout is: $b_k = 4q_k^2 - 4q_k^3 + q_k^4$.

Het verschil van de faalkansen bedraagt:

$$a - b = q_o^2[2 - 4q_o + 2q_o^2] - q_k^2[2 - 4q_k + 2q_k^2].$$

We kunnen nu drie gebieden onderscheiden:

- $q_o < q_k \Rightarrow a < b$: beter geen tussenverbinding;
- $q_o = q_k \Rightarrow a = b$: geen voorkeur;
- $q_o > q_k \Rightarrow a > b$: beter wel tussenverbinding.

5.2. Twee disjuncte gebeurtenissen met ieder een kans van optreden die niet nul is, kunnen niet onafhankelijk zijn: het feit dat het optreden van één gebeurtenis het optreden van de ander uitsluit maakt de gebeurtenissen afhankelijk.

5.3.
$$\left.\begin{aligned} R(t) &= 1 - F(t) = 1 - \frac{t}{L} \\ F(t) &= \int_0^t \frac{1}{L}\,dt = \frac{t}{L} \\ z(t) &= \frac{f(t)}{R(t)} = \frac{1}{L-t} \end{aligned}\right\} 0 \le t \le L \qquad t > L \begin{cases} R(t) = 0 \\ F(t) = 1 \\ z(t) = \text{onbepaald} \end{cases}$$

5.4. a. Bij een constante failure rate is de bedrijfszekerheid gegeven door

$$R(t) = \exp(-t/MTTF).$$

De faalkans gedurende een vlucht van vier uur is dus:

$$F(4) = 1 - \exp(-\frac{4}{1140}) = 3{,}5 \times 10^{-3}.$$

b. Laten we aannemen dat de vlucht tijd T duurt: $\exp(-T/MTTF) \ge 0{,}99$.

$$T \le -MTTF \ln 0{,}99 = 11{,}5 \text{ uur}.$$

De maximale duur van de vlucht is dus 11,5 uur.

5.5. a. $R(t) = 1 - \int_0^t \{at \exp(-\frac{a}{2}t^2)\}dt = \exp(-\frac{a}{2}t^2)$

$z(t) = f(t)/R(t) = at.$

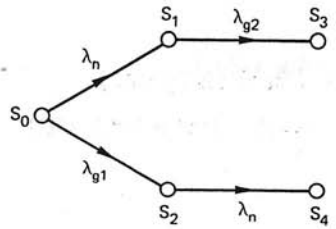
b. Na 10 uur is de bedrijfszekerheid $\frac{4700}{5000} = \exp(-\frac{a}{2}T_1^2)$, met $T_1 = 10$ uur.

Na 20 uur ($T_2 = 2T_1$) is de bedrijfszekerheid $\exp(-\frac{a}{2}T_2^2) = \{\exp -\frac{a}{2}T_1^2\}^4 = (\frac{47}{50})^4$.

Dan hebben dus naar verwachting $\{1 - (\frac{47}{50})^4\} \times 5000 = 1096$ units gefaald.
In het tijdsinterval van 10 tot 20 uur falen dus naar verwachting 796 units.

5.6. Zie figuur 5.5. η is de verhouding van de gemiddelde sterkte y en de gemiddelde belasting x.

5.7.



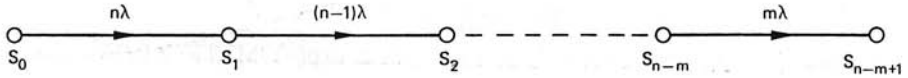
S_0 = net goed en generator goed
S_1 = net uitgevallen en generator goed
S_2 = net goed en generator gefaald (en kan dus niet meer opstarten)
S_3 = net uitgevallen en generator gefaald
S_4 = net uitgevallen en generator gefaald
S_3 en S_4 zijn de faaltoestanden voor dit systeem.

6. Niet-onderhouden systemen

6.1. 'Afhankelijk' is het verschijnsel dat het optreden van een bepaalde gebeurtenis het optreden van andere gebeurtenissen meer of minder waarschijnlijk maakt. Voorbeelden zijn common-cause failures (bijvoorbeeld netuitval) en secondary-failures (zoals het vastlopen van een lager door olielekkage).

6.2. Het Markovdiagram voor een actief m-uit-n systeem is gegeven in onderstaande figuur. De gemiddelde tijd voor de overgang van S_0 naar S_1 is $1/n\lambda$; voor de overgang van S_1 naar S_2 $1/(n-1)\lambda$; enzovoort. De MTTF is de gemiddelde tijd voor de overgang van S_0 naar S_{n-m+1} en is dus gelijk aan

$$MTTF = \frac{1}{n\lambda} + \frac{1}{(n-1)\lambda} + \ldots + \frac{1}{m\lambda} = \frac{1}{\lambda}\sum_{k=m}^{n}\frac{1}{k}.$$



6.3. $\lambda_{eff} = (\frac{1}{4} \times 4 \cdot 10^{-8} + \frac{3}{4} \times 4 \cdot 10^{-9})/k = 1{,}3 \times 10^{-8}/k.$

6.4. a. Het systeem faalt als alle n units gefaald hebben. De kans dat een unit faalt is $1 - \exp(-\lambda t)$. De kans dat het systeem faalt is dus $\{1 - \exp(-\lambda t)\}^n$. De bedrijfszekerheid van dit systeem is dus

$$R(t) = 1 - \{1 - \exp(-\lambda t)\}^n = \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{1} \exp(-\lambda i t).$$

b. $\theta = \int_0^\infty R(t)dt = \frac{1}{\lambda} \sum_{i=1}^{n} (-1)^{i+1} \binom{n}{i} \frac{1}{i}$.

De gemiddelde levensduur kunnen we ook vinden met behulp van de Markovmethode. Het Markovdiagram is hetzelfde als bij opgave 6.2 met m = 1. We vinden dan voor de gemiddelde levensduur:

$$\theta = \frac{1}{\lambda} \sum_{i=1}^{n} \frac{1}{i}.$$

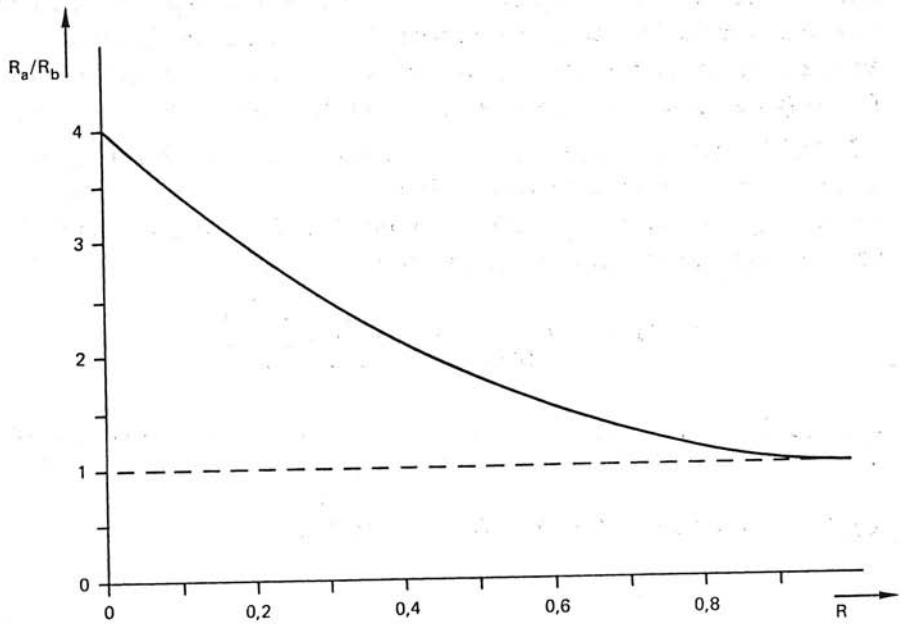
(Alhoewel de twee oplossingen verschillend lijken is dit niet het geval!)

6.5. a. $R_a = \{1 - (1 - R^n)^2\}^n = R^n(2 - R)^n$; $R_b = 1 - (1 - R^n)^2 = R^n(2 - R^n)$

$$\lim_{R \to 1} \frac{R_a}{R_b} = 1.$$

b. $\lim_{R \to 0} \frac{R_a}{R_b} = 2^{n-1}$.

c. Zie figuur.



6.6. De kans op falen van het gegeven systeem kan bepaald worden met behulp van de padenmethode of de decompositiemethode. De oplossing met behulp van de padenmethode is grafisch weergegeven in figuur 6.12. De bedrijfszekerheid van het systeem is weergegeven door

$$R = \sum_{i=0}^{n} (-1)^i R_i,$$

waarin n het maximale aantal lussen en R_i de som van de bedrijfszekerheden van alle subgroepen met i lussen is:

$$\begin{aligned} R = {} & P(A)P(B) + P(A')P(B') + P(A)P(B')P(C) + P(A')P(B)P(C) + \\ & + P(A)P(B)P(B')P(C) - P(A)P(A')P(B)P(B') - P(A)P(A')P(B')P(C) + \\ & - P(A)P(A')P(B)P(C) - P(A')P(B)P(B')P(C) + 2P(A)P(A')P(B)P(B')P(C). \end{aligned}$$

Met $P(A) = P(B') = 0{,}9$; $P(A') = P(B) = 0{,}8$ en $P(C) = 0{,}7$ vinden we $F = 1 - R = 0{,}05124$. Het is duidelijk dat bij deze oplossingsmethode de kans op fouten groot is. Een betere methode is daarom de decompositiemethode. Deze is grafisch weergegeven in figuur 6.13. De bedrijfszekerheid is gegeven door:

$$R = P(C)P(S/C) + P(\bar{C})P(S/\bar{C}),$$

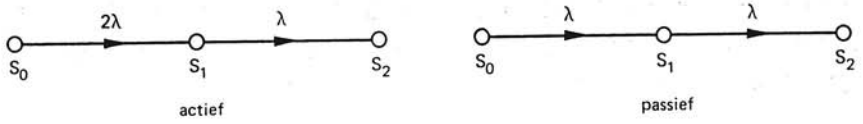
met

$$\begin{aligned} R(S/C) &= \{1 - P(A)P(A')\}\{1 - P(B)P(B')\} = 0{,}9604 \\ R(S/\bar{C}) &= 1 - \{1 - P(A)P(B)\}\{1 - P(A')P(B')\} = 0{,}9216 \\ F &= 1 - R = 0{,}05124. \end{aligned}$$

Een catastrofaal faalmodel zoals in deze opgave beschreven ontstaat als een systeem bestaat uit een 1-uit-2 actief redundant systeem waarbij elk kanaal gedacht kan worden te bestaan uit twee verschillende sub-eenheden en waarbij, indien in een kanaal een sub-eenheid faalt en in het andere kanaal de andere, verschillende sub-eenheid gefaald is, er een omschakeleenheid is die de twee ongelijke, nog functionerende sub-eenheden met elkaar kan verbinden. Een voorbeeld van zo'n systeem is een computersysteem bestaande uit twee centrale processors en twee geheugeneenheden in een actief redundante configuratie. Als een van de twee processors en een van de twee geheugens gefaald heeft het systeem altijd nog kan functioneren indien de overschakeleenheid niet gefaald is. De dwarstak levert dus een verbetering op ten opzichte van het systeem zonder dwarstak.

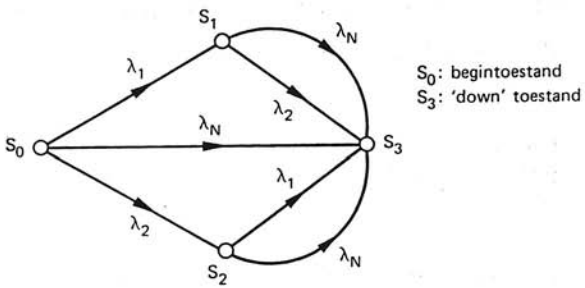
6.7. $0 = R_a < R_e < R_b < R_f < R_c < R_d$. Dit is als volgt in te zien. Configuratie a geeft $R_a = 0$, daar een enkele pomp niet in staat is het water 7 meter omhoog te brengen. Configuratie b levert $R_b = R_o^2$. Voor c vinden we $R_c = 1 - (1 - R_o^2)^2 = R_o^2(2 - R_o^2)$ en voor de $R_d = \{1 - (1 - R_o)^2\}^2 = R_o^2(2 - R_o^2)$. e resulteert in $R_e = R_o^2\{1 - (1 - R_o)^2\} = R_o^3(2 - R_o)$ en f in $R_f = R_o^2(2 - R_o)$. Uit $0 < R_o < 1$ volgt dan de bovenstaande volgorde.

6.8. a. Zie de figuur.



b. Actief: de gemiddelde tijd voor de overgang van S_0 naar S_1 is $1/(2\lambda)$. De gemiddelde tijd voor de overgang van S_1 naar S_2 is $1/\lambda$. De gemiddelde levensduur van het systeem is dus $3/(2\lambda)$.
Passief: met dezelfde methode als hierboven vinden we $2/\lambda$.

6.9. Vanuit de begintoestand S_0 zijn er drie overgangen uit deze toestand mogelijk, namelijk het net kan falen, computer I kan falen (overgang naar toestand S_1) of computer II kan falen (overgang naar toestand S_2). Als het net faalt is het systeem 'down' (toestand S_3). Bij de andere twee overgangen functioneert het systeem nog steeds. Vanuit toestand S_1 zal het systeem falen als óf het net óf computer II faalt. Een en ander is weergegeven in het onderstaande Markovdiagram.



6.10. De units zijn identiek. Dit houdt in dat de bedrijfszekerheid van het gehele systeem wordt gegeven door:

$$R_s = R_{totaal} = R^n.$$

De bedrijfszekerheid van een seriesysteem is altijd lager dan die van één enkele unit; de bedrijfszekerheid van één unit wordt hier dus gegeven door

$$R = \sqrt[n]{R_s}$$

en de totale kosten door

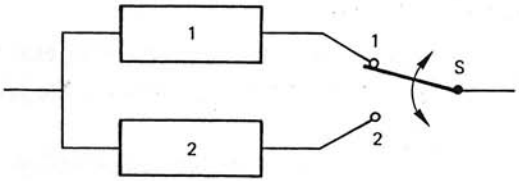
$$K_{totaal} = nKf(\sqrt[n]{R_s}).$$

6.11. In toestand S_0 kunnen drie dingen falen:

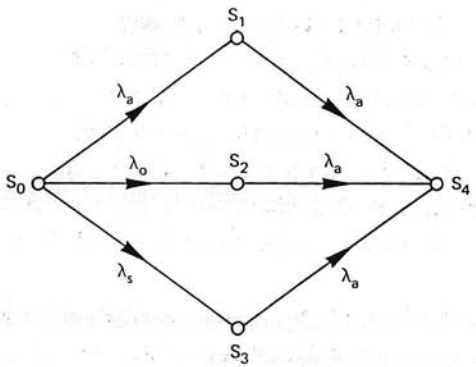
- de actieve unit kan falen (overgang naar toestand S_1);
- de stand-by unit kan falen (overgang naar toestand S_2);
- het foutdetectie- en omschakelingsorgaan kan falen (overgang naar toestand S_3).

(Maak hier niet de fout te denken dat deze fout pas optreedt als de actieve unit faalt

en er overgeschakeld moet worden: dan zul je inderdaad pas bemerken dat het foutdetectie- en omschakelingsorgaan gefaald is; dit falen is echter vóór het falen van de actieve unit gebeurd en moet als dusdanig ook in het Markovdiagram weergegeven worden.)

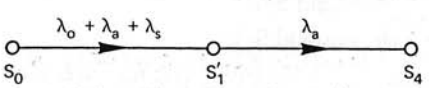


In zowel toestand S_1 als in toestand S_2 zou alsnog het omschakelingsorgaan kunnen falen waardoor niet meer overgeschakeld kan worden. Daar in S_1 de redundante unit reeds ingeschakeld is zodat niet meer overgeschakeld behoeft te worden en in toestand S_2 de redundante unit reeds gefaald is zodat overschakelen zinloos is, zal het falen van het omschakelingsorgaan in deze twee toestanden de kans op 'system down' niet veranderen en kan deze extra overgang vanuit deze twee toestanden weggelaten worden. Zo zal ook het falen van de redundante unit als het systeem zich in toestand S_3 bevindt geen invloed hebben op de 'system down' kans, ofwel op de bedrijfszekerheid van het systeem.



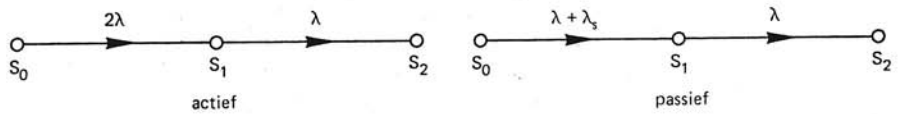
S_0: alles goed; S_1 alleen 1 defect
S_2: alleen 2 defect (terwijl S in 1)
S_3: alleen S defect in stand 1
S_4: systeem faalt.

Aangezien de kans om naar de toestand S_4 over te gaan voor de toestanden S_1, S_2 en S_3 gelijk is (λ_a), kunnen deze toestanden samengenomen worden tot één toestand (S_1'), die dan een kans λ_a heeft om over te gaan naar de toestand S_4. De binnenkomende takken van S_1, S_2 en S_3 worden dan eveneens samengenomen en de kans op de overgang van S_0 naar deze samengenomen toestand S_1' is de som van de overgangskansen van S_0 naar S_1, S_2 en S_3.



S_0: alles goed;
S_1': alleen de ingeschakelde component (1 of 2) is nog bruikbaar
(de samenvoeging van S_1, S_2 en S_3);
S_3: systeem faalt.

6.12. Het Markovdiagram heeft voor beide configuraties dezelfde vorm. Om te bepalen welke de grootste bedrijfszekerheid heeft, hoeven we dus enkel naar de overgangskansen te kijken. Hieruit volgt dat als $\lambda_s > \lambda$ actieve redundantie de hoogste bedrijfszekerheid heeft, terwijl voor $\lambda_s < \lambda$ de actieve redundantie de kleinste bedrijfszekerheid heeft.



6.13. $\text{MTTF} = \frac{1}{\lambda} + \frac{1}{\lambda + \lambda_1 + \lambda_2}$.

Deze MTTF kan gevonden worden door van het Markovdiagram de bijbehorende differentiaalvergelijkingen op te lossen met behulp van de Laplace-transformatie. De MTTF is dan gegeven door

$$\text{MTTF} = \sum_{i=1}^{4} \lim_{s \to 0} P_{S_i}(s).$$

Het zal duidelijk zijn dat dit voor het gegeven Markovdiagram nogal tijdrovend zal zijn en gauw zal resulteren in vergissingen. Daarom moeten we altijd eerst proberen het Markovdiagram te vereenvoudigen. Twee regels zijn hierbij belangrijk:

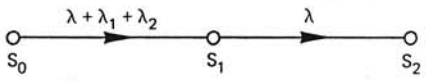
- toestanden die een overgang hebben naar dezelfde toestand met dezelfde overgangswaarschijnlijkheid kunnen samengenomen worden tot één gecombineerde toestand mits vanuit de samengenomen toestanden geen overgang(en) naar nog een andere toestand mogelijk is (zijn), uitgezonderd onderlinge overgangen. De overgangswaarschijnlijkheid van de gecombineerde toestand naar de gemeenschappelijke toestand is gelijk aan de oorspronkelijke overgangswaarschijnlijkheid.

Bovenstaande regel is eenvoudig in te zien bij het gegeven Markovdiagram. Als je vanuit toestand S_5 kijkt naar toestand S_1 en toestand S_4, dan is als gegeven is dat het systeem zich in toestand S_1 óf in toestand S_4 bevindt, de overgangskans van de gecombineerde kans $S_{1,4}$ naar toestand S_5 natuurlijk nog steeds $\lambda\Delta t$.
Verder kunnen we de toestand $S_{1,4}$ combineren met toestand S_2 en toestand S_3 tot de nieuwe toestand $S_{1,2,3,4}$.

- Als vanuit een bepaalde toestand meerdere overgangen mogelijk zijn naar een andere zelfde toestand dan kunnen deze overgangen gecombineerd worden tot één overgang met een overgangswaarschijnlijkheid gelijk aan de som van de afzonderlijke overgangswaarschijnlijkheden.

Deze laatste regel spreekt eigenlijk vanzelf. Als we deze regel toepassen op het diagram dat het resultaat is na de vereenvoudigingen met behulp van regel 1, dan

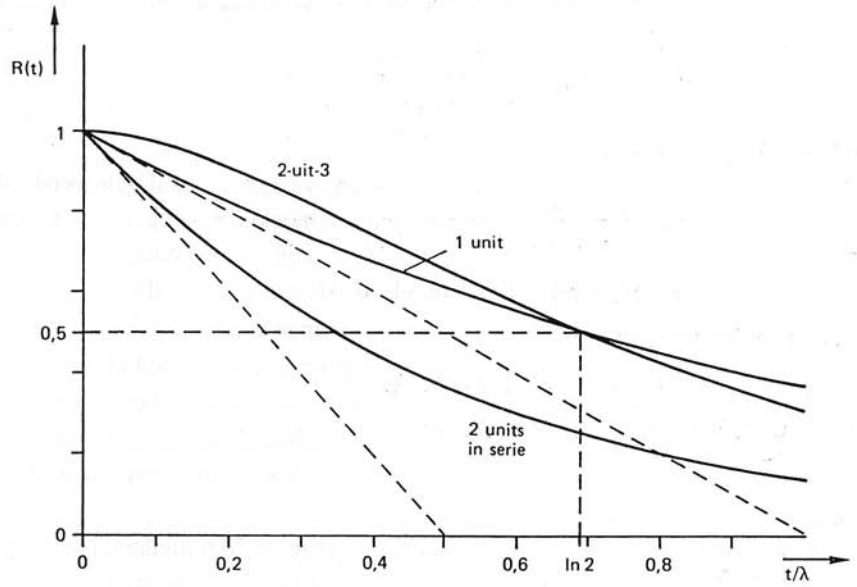
resulteert het diagram als in onderstaande figuur. Hieruit volgt direct de MTTF.
Opmerking. Het gegeven Markovdiagram beschijft het systeem zoals gegeven in opgave 6.11. U ziet dat de MTTF van dit relatief ingewikkelde systeem gevonden kan worden zonder iets uit te rekenen!



6.14. Voor een 2-uit-3 actief redundant systeem geldt:

$$R(t) = (3 - 2e^{-\lambda t})e^{-2\lambda t} \text{ (zie paragraaf 6.5).}$$

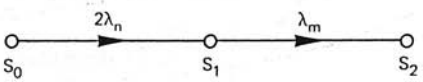
Voor één unit geldt: $R(t) = e^{-\lambda t}$.
Voor twee units in serie geldt: $R(t) = e^{-2\lambda t}$.
De bovenstaande bedrijfszekerheden zijn weergegeven in de figuur.



Hier volgt direct uit dat voor $t < (1/\lambda) \ln 2$ het redundante systeem een hogere bedrijfszekerheid heeft dan bij één unit. Hier zien we dus weer dat de gemiddelde levensduur alléén geen informatie geeft over de bedrijfszekerheid van het systeem.

6.15. a. Uit het Markovdiagram volgt direct:

$$\text{MTTF} = \frac{1}{2\lambda_n} + \frac{1}{\lambda_m} = 750 \text{ uur.}$$



(a)

b. Uit het Markovdiagram volgen de differentiaalvergelijkingen:

$$\frac{dP_0}{dt} = -2\lambda_n P_0$$

$$\frac{dP_1}{dt} = 2\lambda_n P_0 - \lambda_m P_1$$

$$\frac{dP_2}{dt} = \lambda_m P_1.$$

De Laplace-transformatie geeft:

$$P_0 = \frac{1}{s + 2\lambda_n}$$

$$P_1 = \frac{2\lambda_n P_0}{s + \lambda_m} = \frac{2\lambda_n}{(s + \lambda_m)(s + 2\lambda_n)}$$

$$R = P_0 + P_1 = \frac{s + \lambda_m + 2\lambda_n}{(s + \lambda_m)(s + 2\lambda_n)}.$$

Terugtransformatie levert:

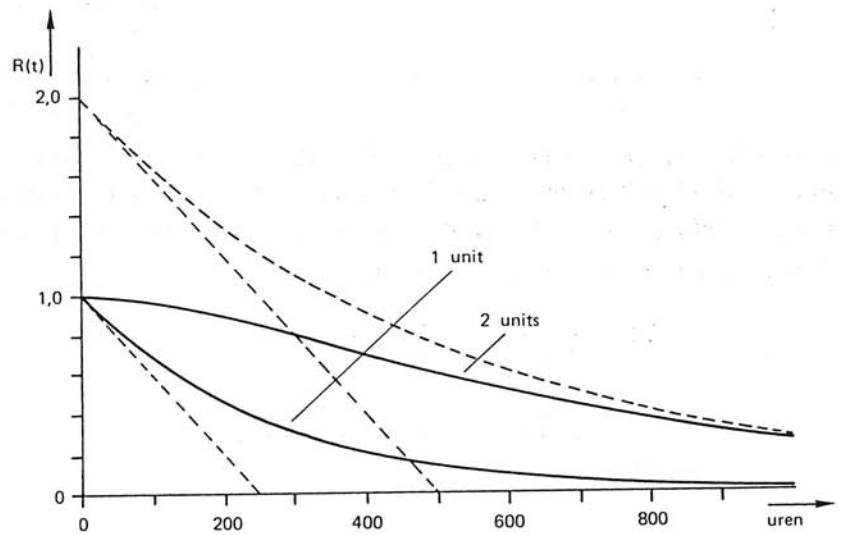
$$R(t) = \frac{\lambda_m}{\lambda_m - 2\lambda_n} e^{-2\lambda_n t} - \frac{2\lambda_n}{\lambda_m - 2\lambda_n} e^{-\lambda_m t} =$$

$$= 2\exp(-2\cdot 10^{-3}t) - \exp(-4\cdot 10^{-3}t).$$

Voor één unit vinden we:

$$R(t) = e^{-\lambda_m t} = \exp(-4\cdot 10^{-3}t).$$

Een en ander is weergegeven in de figuur.



6.16. Voor het bepalen van de optimale strategie zullen we voor de drie gevallen de gemiddelde kosten per periode moeten uitrekenen. Voor strategie a vinden we:

$$(1 - 0{,}95^3) \times f\ 10.000 + 0{,}01^3 \times f\ 25.000 = f\ 1426{,}28.$$

Voor strategie b:

$$(3 \times 0{,}05^2 \times 0{,}95 \times 0{,}05^3) \times f\ 10.000 + (3 \times 0{,}01^2 \times 0{,}99 + \\ + 0{,}01^3) \times f25{,}000 = f\ 79{,}95.$$

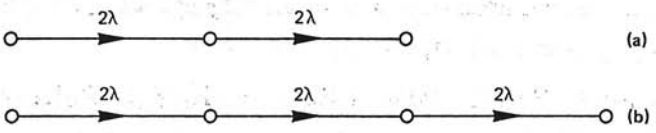
Voor strategie c:

$$(0{,}05^3 \times f\ 10.000 + (1 - 0{,}99^3) \times f\ 25.000 = f\ 743{,}78.$$

De optimale strategie is dus b.

6.17. a. Twee pompen moeten gelijktijdig actief zijn. Faalt er één dan wordt de passieve pomp ingeschakeld. Faalt er daarna nog een pomp dan wordt de benodigde capaciteit niet gehaald en is voor deze functie het systeem dus 'down'. Dit is weergegeven in het bovenste Markovdiagram. De MTTF van de benodigde capaciteit is dus

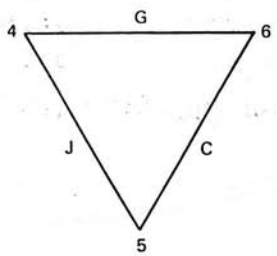
$$\text{MTTF} = \frac{1}{2\lambda} + \frac{1}{2\lambda} = \frac{1}{\lambda}.$$



b. Als er twee pompen gefaald hebben dan zal de laatste pomp het mengsel in beweging houden. De failure rate van deze pomp is dan 2λ. Als deze laatste pomp faalt is het systeem 'down'. Dit is weergegeven in het onderste Markovdiagram. De MTTF van de stromingsfunctie is dus:

$$\text{MTTF} = \frac{1}{2\lambda} + \frac{1}{2\lambda} + \frac{1}{2\lambda} = \frac{3}{2\lambda}.$$

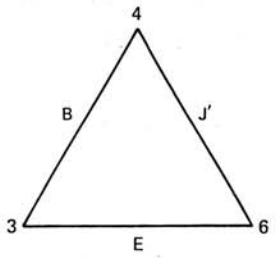
6.18. Reduceer eerst



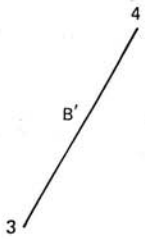
tot

met faalkans $p_j' = 0{,}019$.

Reduceer vervolgens

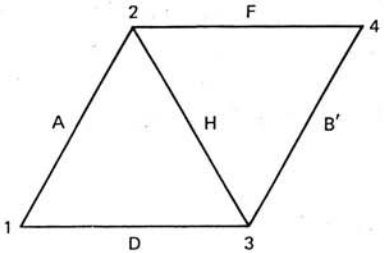


tot



met faalkans $p_{B'} = 0{,}01171$.

Er blijft nu een brugstructuur over.



Met de decompositiemethode kunnen we dit als volgt oplossen (S = systeem):

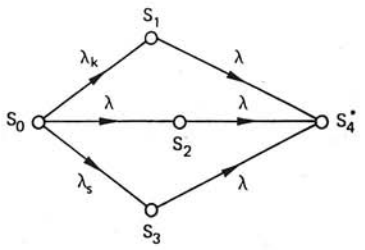
$$R_S = P(H)\cdot P(S|H) + P(H)^{\circ}\cdot P(S|H)$$
$$= R_h\cdot[(1 - F_aF_d)(1 - F_fF_{b'})] + F_h[1 - (1 - R_aR_f)(1 - R_{b'}R_d)] = 0{,}988.$$

6.19. We moeten bij deze opgave bedenken dat een serieschakeling van dioden redundant is voor kortsluitfouten terwijl een parallelschakeling redundant is voor open fouten. We kunnen dan de volgende tabel van faalkansen opstellen:

schakeling	open fout	kortsluitfout	totaal
1	$p_o = 0{,}02$	$p_k = 0{,}01$	0,03
2	$\approx 2p_o = 0{,}04$	$p_k^2 = 10^{-4}$	0,0401
3	$p_o^2 = 4\cdot10^{-4}$	$\approx 2p_k = 0{,}02$	0,0204
4	$\approx 3p_o = 0{,}06$	$p_k^3 = 10^{-6}$	0,060001
5	$\approx p_o + p_o^2 = 0{,}0204$	$\approx 2p_k^2 = 2\cdot10^{-4}$	0,0206
6	$\approx 2p_o^2 = 8\cdot10^{-4}$	$\approx p_k^2 + p_k = 0{,}0101$	0,0109
7	$p_o^3 = 8\cdot10^{-6}$	$\approx 3p_k = 0{,}03$	0,03

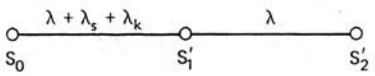
We zien hieruit dat bij de gegeven kansen van diodefouten ($p_o = 0{,}02$ en $p_k = 0{,}01$) schakeling 6 optimaal is.

6.20. a. Markovdiagram:



S_0: alles goed.
S_1: de schakelaar kleeft en unit 1 is ingeschakeld.
S_2: 1 unit kapot; de tweede unit is ingeschakeld.
S_3: schakelaar ten onrechte in stand 2 en dus is de tweede unit actief.
S_4: het systeem faalt.

b. Bovenstaand Markovdiagram kan vereenvoudigd worden tot:



(Het maakt immers niet uit of we in toestand S_1, S_2 of S_3 zitten. Het systeem faalt voor al deze toestanden met failure rate λ). De gemiddelde levensduur is dan de gemiddelde tijd die nodig is om van S_0 naar S_1' te komen plus de gemiddelde tijd om van S_1' naar S_2' te komen, oftewel:

$$\text{MTTF} = \frac{1}{\lambda + \lambda_s + \lambda_k} + \frac{1}{\lambda}.$$

6.21. Het wegvallen van de druk wordt goed gesignaleerd als vooraf geen meerderheid alarm geeft en na het wegvallen van de druk wel een meerderheid alarm geeft.

1. enkelvoudig: $P_{sign} = 0{,}8$;
2. tweevoudig: $P_{sign} = 0{,}8^2(2g) + 2\cdot0{,}8\cdot0{,}1(1g,1o) = 0{,}8$;
3. drievoudig: $P_{sign} = 0{,}8^3(3g) + 3\cdot0{,}8^2\cdot0{,}1(2g,1w) + 3\cdot0{,}8^2\cdot0{,}1(2g,1o) +$
   $+ 6\cdot0{,}8\cdot0{,}1\cdot0{,}1(1g,1w,1o) = 0{,}944$;
4. viervoudig: $P_{sign} = 0{,}8^4(4g) + 4\cdot0{,}8^3\cdot0{,}1(3g,1w) + 4\cdot0{,}8^3\cdot0{,}1(3g,1o) +$
   $+ 6\cdot0{,}8^2\cdot0{,}1^2(2g,2o) + 12\cdot0{,}8^2\cdot0{,}1\cdot0{,}1(2g,1o,1w) +$
   $+ 12\cdot0{,}8\cdot0{,}1^2\cdot0{,}1(1g,2o,1w) = 0{,}934.$

Het drievoudige systeem is dus de beste keus.

6.22. In de onderstaande tabel zijn de bedrijfszekerheden van de drie blokjes gegeven voor verschillende aantallen parallel geschakelde componenten.
De eerste stap is heel duidelijk: om een totale bedrijfszekerheid van 0,8 te bereiken

moeten alle blokjes een hogere bedrijfszekerheid hebben. We gaan dan uit van de configuratie:

$$R_1(1\times), R_2(2\times), R_3(3\times)$$

die een bedrijfszekerheid heeft van:

$$R_s = R_1 \cdot R_2^2 \cdot R_3^3 = 0{,}756$$

hetgeen nog niet voldoende is.

	$comp_1$	$comp_2$	$comp_3$
1×	0,9	0,8	0,5
2×	0,99	0,96	0,75
3×	0,999	0,992	0,875
4×	0,9999	0,9984	0,9375

Het toevoegen van een extra component aan één van de blokjes levert de volgende verbeteringsfactoren op voor de systeembedrijfszekerheid.

$$\frac{R_s'}{R_s} = \frac{0{,}99}{0{,}9} = 1{,}1 \text{ voor blokje 1 } (R_s' = 0{,}832);$$

$$\frac{R_s'}{R_s} = \frac{0{,}992}{0{,}96} = 1{,}0333 \text{ voor blokje 1 } (R_s' = 0{,}7812);$$

$$\frac{R_s'}{R_s} = \frac{0{,}9375}{0{,}875} = 1{,}0714 \text{ voor blokje 1 } (R_s' = 0{,}81).$$

Hieruit volgt de optimale configuratie $R_1(1\times), R_2(2\times), R_3(3\times)$.

7. Onderhouden systemen

7.1. Een onderhoudbaar systeem is een systeem dat nadat het gefaald heeft weer door menselijk ingrijpen kan worden teruggebracht in een werkende toestand.

7.2. Preventief onderhoud wordt uitgevoerd voordat het systeem gefaald heeft en is bedoeld om het systeem voor toekomstig falen te behoeden. De hazard rate z(t) van een systeem moet monotoon stijgen opdat preventief onderhoud zinvol is. Het systeem komt dan na onderhoud van een hoge hazard rate terug in een toestand met een lagere hazard rate. Zou de hazard rate afnemen met de tijd dan komt het systeem met een bepaalde hazard rate terecht in een toestand met een hogere hazard rate na onderhoud waardoor het juist eerder zal falen (hetgeen meestal niet de bedoeling is).

7.3. Bij optimalisatie van de 'life cycle cost' van een systeem wordt met de volgende kosten gerekend:

- de initiële investeringskosten;
- de onderhouds- en exploitatiekosten;
- de eventuele ontmantelingskosten.

7.4. a. MTTF = $3/2\lambda$ (zie opgave 6.8).

b. Uit het Markovdiagram bij de oplossing van opgave 6.8 is eenvoudig af te leiden dat voor het systeem zonder periodiek onderhoud de bedrijfszekerheid R(t) gegeven wordt door

$$R(t) = 2\exp(-\lambda t) - \exp(-2\lambda t).$$

Voor een systeem met periodiek onderhoud met een tijdsinterval T geldt:

$$\text{MTTFF} = \frac{\int_0^t R(t)dt}{1 - R(T)} = \frac{3}{2\lambda}\,\frac{1 - \frac{1}{3}\exp(-\lambda T)}{1 - \exp(-\lambda T)}.$$

Opmerking. Als we T gelijk kiezen aan de gemiddelde levensduur van één unit (= $1/\lambda$) dan wordt de MTTFF gelijk aan $1{,}39 \times 3/2\lambda$. We zien hier uit dat periodiek onderhoud dan slechts een verbetering van de gemiddelde levensduur geeft ten opzichte van het systeem zonder periodiek onderhoud met een factor 1,39. Periodiek onderhoud is dus alleen zinvol als T voldoende klein gekozen wordt ten opzichte van de gemiddelde levensduur van één unit.
De MTTF nadert voor zeer kleine T tot $1/\lambda^2 T$, zodat deze dan zeer groot wordt ten opzichte van $1/\lambda$.

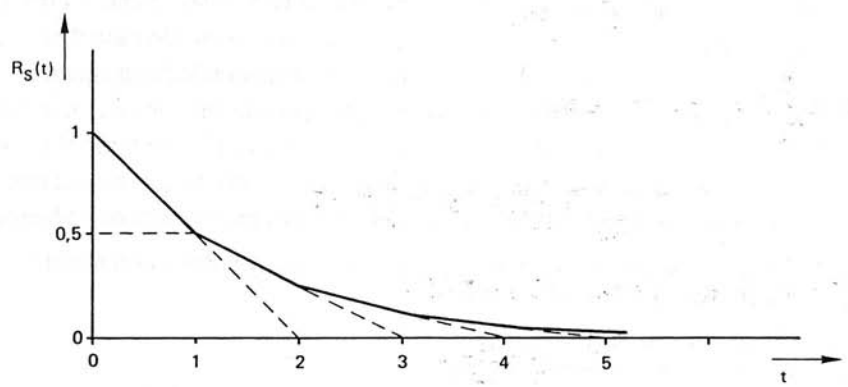
7.5. a. De bedrijfszekerheid van een systeem met periodiek onderhoud is gegeven door:

$$R_s(t) = R(T)^i R(t - iT) \qquad (iT \le t < (i+1)T).$$

Met $R(t) = 1 - \frac{1}{2}t$ wordt dit:

$$R_s(t) = (\tfrac{1}{2})^i\{1 - \tfrac{1}{2}(t - i)\} \qquad (i \le t < i+1).$$

Deze $R_s(t)$ is uitgezet in onderstaande figuur.



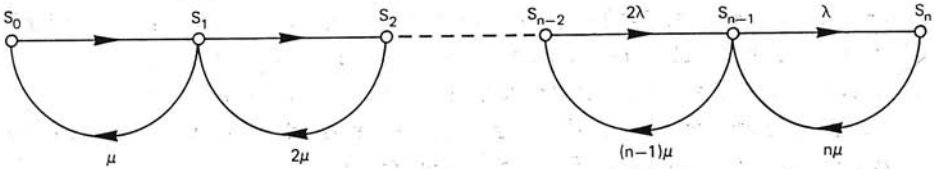
b. De gemiddelde levensduur is het oppervlak onder de $R_s(t)$-functie:

$$\frac{3}{4} + \frac{3}{8} + \frac{3}{16} + \ldots = \frac{3}{2}.$$

Deze gemiddelde levensduur kan ook gevonden worden met

$$\text{MTTFF} = \frac{\int_0^t R(t)dt}{1 - R(T)} = \frac{3}{2}.$$

7.6. a. Het Markovdiagram van het beschreven systeem is weergegeven in de figuur. Alleen in toestand S_0 functioneert het systeem correct: alle andere toestanden zijn 'system down'-toestanden.



b. Voor de steady-state availability moeten alle toestanden in balans zijn: de kans op een overgang naar een toestand is even groot als de kans op een overgang vanuit die toestand. Voor toestand S_n moet dus gelden

S_n: $\quad n\mu P_n = \lambda P_{n-1}$

S_{n-1}: $\quad (n-1)\mu P_{n-1} = 2\lambda P_{n-2}$

$\vdots \qquad\qquad \vdots$

S_2: $\quad 2\mu P_2 = (n-1)\lambda P_1$

S_1: $\quad \mu P_1 = n\lambda P_0.$

Hier volgt direct uit:

$$P_i = \binom{n}{i}\left(\frac{\lambda}{\mu}\right)^i P_0.$$

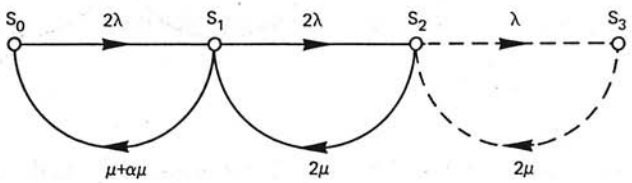
Met $\sum_{i=0}^{n} P_i = 1$ vinden we dan

$$P_0\{\sum_{i=0}^{n} \binom{n}{i}\left(\frac{\lambda}{\mu}\right)^i\} = P_0(1 + \frac{\lambda}{\mu})^n = 1.$$

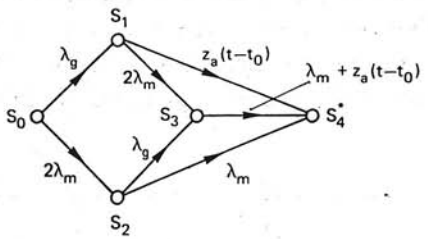
Voor de steady-state availability geldt dus

$$A_\infty = P_0 = (1 + \frac{\lambda}{\mu})^{-n}.$$

7.7. Het Markovdiagram van een homogeen 2-uit-3 passief redundant systeem met twee samenwerkende reparateurs met inzetbaarheid α is weergegeven in de onderstaande figuur. S_2 en S_3 zijn hierbij de faaltoestanden.



7.8. Het Markovdiagram ziet er als volgt uit:



Toestanden

S_0: Dit is de begintoestand; de dieselgenerator en beide motoren zijn ingeschakeld en kunnen dus falen.

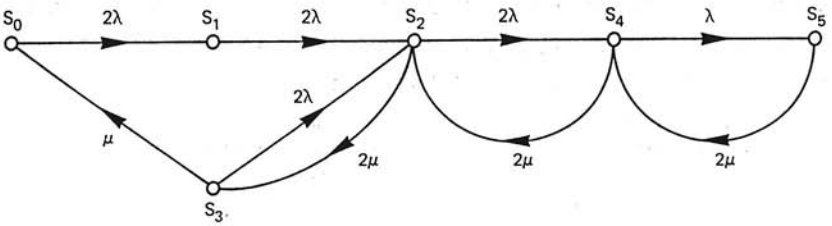
S_1: De dieselgenerator heeft gefaald en de stroomvoorziening is overgenomen door de accu. Zowel de accu als beide motoren kunnen in deze toestand falen.

S_2: Eén van de motoren heeft gefaald. In deze toestand kunnen de overgebleven motor en de dieselgenerator uitvallen.

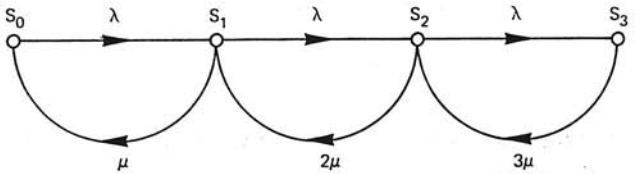
S_3: De dieselgenerator en één motor zijn uitgevallen. De overgebleven motor wordt gevoed vanuit de accu. Zowel de accu als de motor kunnen nu nog falen.

S_4: Dit is de eindtoestand van het systeem. Er is nu geen voortstuwing meer mogelijk.

7.9. In toestand S_1 van het bijgaande Markovdiagram heeft pas één unit gefaald en komen de reparateurs dus nog niet in actie. In toestand S_2 hebben twee units gefaald en komen beide reparateurs in actie (tak naar S_3). In toestand S_3 is één unit gerepareerd en daar de reparateurs niet samenwerken blijft slechts één reparateur aan het werk (tak naar S_0). Daar ook in toestand S_3 twee units kunnen falen is er ook een tak van S_3 terug naar S_2 waarin beide reparateurs weer aan het werk zijn. In toestand S_2 kunnen uiteraard ook twee units falen hetgeen een overgang naar S_4 oplevert. In de toestand S_4 kan er nog slechts één unit falen. Vanuit S_4 en S_5 zijn beide reparateurs actief waardoor de overgangen van S_5 naar S_4 en van S_4 naar S_2 doorlopen kunnen worden. Daar in toestand S_4 drie units gefaald hebben zijn S_4 en S_5 'down'-toestanden.



7.10. In toestand S_0 zijn er drie lijnen vrij. De kans op een gespreksaanvraag, dus op een overgang van toestand S_0 naar S_1 is $\lambda\Delta t$. In toestand S_1 is één lijn bezet en is de kans op een overgang terug naar S_0 gelijk aan $\mu\Delta t$. Er is echter ook een kans op het binnenkomen van nog een gespreksaanvraag, dus op een overgang naar S_2. De overgangskans van S_2 (twee lijnen bezet) naar S_1 (één lijn bezet) is nu $2\mu\Delta t$. De rest van het diagram spreekt voor zich. In toestand S_3 zijn geen vrije lijnen meer beschikbaar.



Met de methode gegeven in opgave 7.6 vinden we

$$\lambda P_2 = 3\mu P_3$$

$$\lambda P_1 = 2\mu P_2 = \frac{6\mu^2}{\lambda} P_3$$

$$\lambda P_0 = \mu P_1 = \frac{6\mu^3}{\lambda} P_3$$

$$P_0 + P_1 + P_2 + P_3 = 1$$

$$\overline{A}_\infty = P_3 = \frac{1}{1 + \frac{3\mu}{\lambda} + \frac{6\mu^2}{\lambda^2} + \frac{6\mu^3}{\lambda^3}}.$$

Voor de steady-state availability vinden we dus

$$A_\infty = \frac{\frac{3\mu}{\lambda} + \frac{6\mu^2}{\lambda^2} + \frac{6\mu^3}{\lambda^3}}{1 + \frac{3\mu}{\lambda} + \frac{6\mu^2}{\lambda^2} + \frac{6\mu^3}{\lambda^3}}.$$

7.11. a. De gemiddelde levensduur (MTTFF) van het systeem wordt gegeven door

$$\text{MTTFF} = \frac{\int_0^T R(t)dt}{1 - R(T)} = \frac{T + \tau}{T}\tau \ln\left(\frac{T + \tau}{\tau}\right).$$

Bij periodiek onderhoud met periodetijd $T = \tau$ vinden we dan:

$$\text{MTTFF} = 2\tau \ln 2$$

en voor $T = 3\tau$:

$$\text{MTTFF} = \frac{8}{3}\tau \ln 2.$$

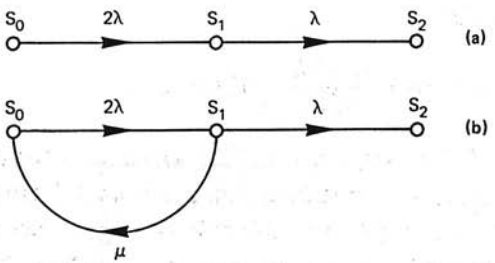
b. Voor $T = 3\tau$ vinden we de grootste gemiddelde levensduur; dus voor periodiek onderhoud waarbij de periodetijd T het grootst is! De verklaring is eenvoudig te vinden door de hazard rate z(t) te bepalen:

$$z(t) = \frac{1}{t+\tau}.$$

Dit is een monotoon dalende functie. Door periodiek onderhoud breng je het systeem telkens weer terug van een lage hazard rate naar een hogere en dus minder gunstige hazard rate. Dit verlaagt de gemiddelde levensduur en de afname wordt groter naarmate de frequentie van het onderhoud toeneemt. De conclusie moet dus zijn dat dit systeem niet geschikt is voor periodiek onderhoud.

7.12. a. Indien geen correctief onderhoud wordt gepleegd vinden we Markov-diagram a. Hieruit is eenvoudig de MTTFF te bepalen:

$$\text{MTTFF} = \frac{1}{2\lambda} + \frac{1}{\lambda} = \frac{3}{2\lambda} = 1500 \text{ uur}.$$



b. Als we de MTTFF willen bepalen als er op unit-niveau gerepareerd wordt dan moeten we uitgaan van een Markovdiagram waarbij wordt aangenomen dat als het systeem 'down' gaat er geen reparatie meer verricht wordt. Dit is aangegeven in het diagram b. We kunnen nu de MTTFF bepalen door eerst $R_s(t)$ te bepalen met behulp van de differentiaalvergelijkingen en de Laplace transformatie, en door daarna van $R_s(t)$ de tijdintegraal van 0 tot oneindig te bepalen. Dit is echter een omslachtige methode. We zullen hier een eenvoudiger methode demonstreren.

De MTTFF is gedefinieerd als

$$\text{MTTFF} = \int_0^\infty R_s(t)\,dt = \int_0^\infty P_0(t)\,dt + \int_0^\infty P_1(t)\,dt.$$

De differentiaalvergelijkingen van het Markovdiagram zijn

$$\frac{dP_0}{dt} = \mu P_1 - 2\lambda P_0;$$

$$\frac{dP_1}{dt} = 2\lambda P_0 - (\mu + \lambda)P_1;$$

$$\frac{dP_2}{dt} = \lambda P_1.$$

Integreer nu alles in de tijd van nul tot oneindig:

$$-1 = \mu\int_0^\infty P_1 dt - 2\lambda\int_0^\infty P_0 dt;$$

$$0 = 2\lambda\int_0^\infty P_0 dt - (\mu + \lambda)\int_0^\infty P_1 dt;$$

$$1 = \lambda\int_0^\infty P_1 dt.$$

Hieruit volgt:

$$\int_0^\infty P_1 dt = \frac{1}{\lambda};\ \int_0^\infty P_0 dt = \frac{\mu + \lambda}{2\lambda^2}.$$

De MTTFF wordt dus:

$$\text{MTTFF} = \frac{\mu + 3\lambda}{2\lambda^2} \approx 50.000 \text{ uur}.$$

Opmerking. Voor de bepaling van de MTTFF kan de stap met de differentiaalvergelijkingen in principe overgeslagen worden. Voor de begintoestand wordt dP_0/dt vervangen door -1. (Voor $t = 0$ is de kans op goed functioneren gelijk aan 1). Voor de eindtoestand ($t \to \infty$) vervangen we dP_n/dt door $+1$. (De units hebben voor $t \to \infty$ een faalkans 1). Voor alle andere toestanden wordt dP_i/dt gelijk aan 0. Alle andere kansen worden vervangen door de tijdintegraal van die kans.
Uit deze vergelijkingen zijn eenvoudig de tijdintegralen van alle kansen te bepalen. De MTTFF is nu gelijk aan de som van de tijdintegralen van alle kansen waarvan de bijbehorende toestand een nog correct functionerende toestand is.

c. Indien geldt $\lambda \ll \mu$ behoeven we van het Markovdiagram alleen de eerste loop in ogenschouw te nemen. De gemiddelde tijd om van toestand S_0 naar toestand S_1 te

komen is $1/2\lambda$. De gemiddelde tijd om van S_1 naar S_0 terug te komen is $1/\mu$. De gemiddelde tijd om de loop te doorlopen is dus

$$\frac{1}{2\lambda} + \frac{1}{\mu}.$$

De aanspreekfrequentie van het reparatiekanaal wordt dus

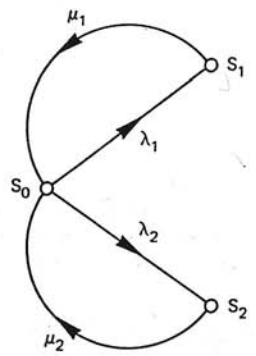
$$f = \frac{1}{\frac{1}{2\lambda} + \frac{1}{\mu}} \approx 2\lambda = 2 \times 10^{-3}/\text{uur}.$$

d. Als we geen reparatie op unit-niveau verrichten dan worden de kosten per tijdseenheid: f 5000/1500 uur = f 3,33 / uur.
Als we wel reparatie op unit-niveau verrichten vinden we voor de kosten per tijdseenheid:

$$\frac{2 \times 10^{-3} \times 50.000 \times f\ 500 + f\ 5000}{50.000} = f\ 1{,}10 / \text{uur}.$$

De conclusie is dus dat reparatie op unit-niveau economisch verantwoord is.

7.13. Het Markovdiagram van dit probleem is weergegeven in bijgaande figuur.



Voor toestand S_1 en S_2 geldt:

$$\mu_1 P_1 = \lambda_1 P_0$$
$$\mu_2 P_2 = \lambda_2 P_0$$

Verder geldt:

$$P_0 + P_1 + P_2 = 1.$$

Hier volgt direct uit

$$A_\infty = P_0 = \frac{1}{1 + \frac{\lambda_1}{\mu_1} + \frac{\lambda_2}{\mu_2}}.$$

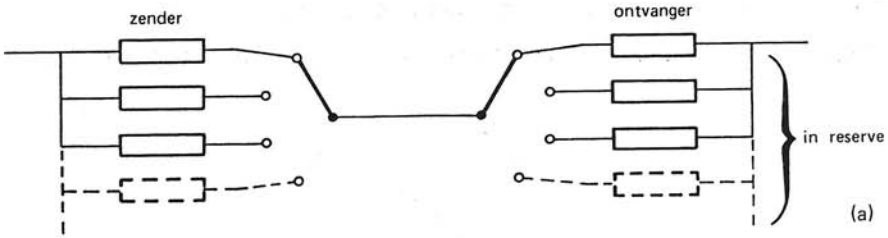
7.14. In onderstaande figuur (a) is de configuratie schematisch weergegeven. We nemen aan dat we M reservezenders en M reserveontvangers mee moeten nemen. (Omdat zenders en ontvangers statistisch gezien even snel falen ligt het voor de hand om de aantallen gelijk te kiezen). Daar de bedrijfszekerheid van het geheel gelijk is aan het produkt van de bedrijfszekerheid van de zenderconfiguratie en de ontvangerconfiguratie kunnen we ons beperken tot de bepaling van de bedrijfszekerheid van één van de twee. Het Markovdiagram (b) voor enkel de zenderconfiguratie is eenvoudig te bepalen. We vinden dan:

$$\frac{dP_0}{dt} = -\lambda P_0;$$

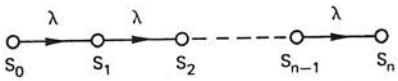
$$\frac{dP_1}{dt} = \lambda P_0 - \lambda P_1;$$

$$\vdots$$

$$\frac{dP_{n+1}}{dt} = \lambda P_M.$$



(a)



(b)

Met Laplace:

$$P_0 = \frac{1}{s + \lambda};$$

$$P_1 = \frac{\lambda}{(s + \lambda)^2};$$

$$P_2 = \frac{\lambda^2}{(s + \lambda)^3};$$

$$\vdots$$

$$P_M = \frac{\lambda^M}{(s + \lambda)^{M+1}}.$$

Voor de bedrijfszekerheid van de zenderconfiguratie vinden we dan:

$$R_z(s) = \sum_{i=0}^{M} \frac{\lambda^i}{(s+\lambda)^{i+1}}.$$

Terugtransformatie levert:

$$R_z(t) = \sum_{i=0}^{M} \frac{(\lambda t)^i}{i!} e^{-\lambda t}.$$

(Dit is de Erlang-verdeling, zie paragraaf 4.1.5). Voor de ontvangerconfiguratie vinden we dezelfde bedrijfszekerheid. Voor de bedrijfszekerheid van het geheel na tijd T vinden we dus:

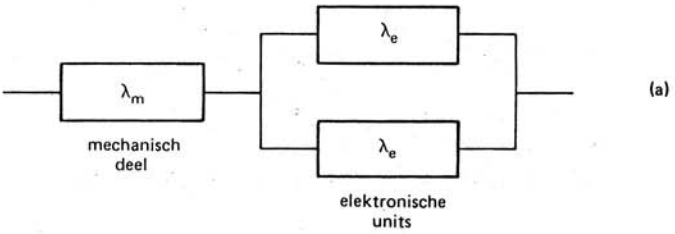
$$R = e^{-2\lambda T} \left\{ \sum_{i=0}^{M} \frac{(\lambda t)^i}{i!} \right\}^2.$$

Met $R \geq 98\ \%$, $\lambda = 10^{-3}$ en $T = 1000$ uur vinden we voor het aantal reservezenders en -ontvangers $M = 4$. R is dan gelijk aan 0,9927. Een aantal van 3 reservezenders en 5 -ontvangers (of omgekeerd) zou voldoen aan de bedrijfszekerheidseis, maar deze keuze is niet optimaal (R is dan gelijk aan 0,980) omdat de faalkansen voor beiden even groot zijn.

7.15. a. Het systeem faalt als het mechanische deel faalt of als beide elektronische units falen. Het catastrofale faalmodel hiervan is hieronder gegeven. De bedrijfszekerheid is gelijk aan het produkt van de bedrijfszekerheid van het mechanische deel en het elektronische deel:

$$R(t) = \exp(-\lambda_m t)[1 - \{1 - \exp(-\lambda_e t)\}^2] =$$

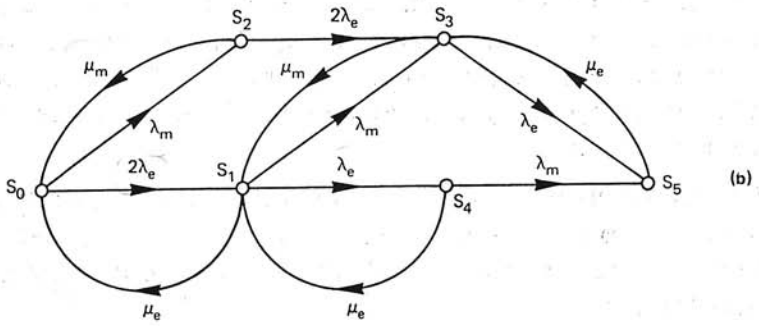
$$= \{2 - \exp(-\lambda_e t)\} \exp\{-(\lambda_m + \lambda_e)t\}.$$



(a)

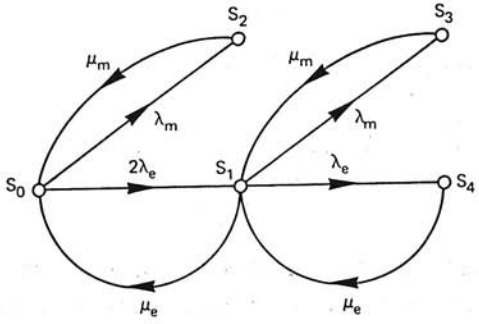
b. Om het Markovdiagram te construeren nemen we eerst aan dat er geen reparatie is. In begintoestand S_0 kunnen twee dingen gebeuren: een elektronische unit faalt (overgang naar S_1) of de mechanische unit faalt (overgang naar S_2). In toestand S_1 kunnen ook twee dingen gebeuren: de tweede elektronische unit kan falen (overgang naar S_4) of de mechanische unit faalt (overgang naar toestand S_3). In toestand

S_4 kan alleen nog de mechanische unit falen en in toestand S_3 alleen nog de tweede elektronische unit (overgang naar S_5). Het zal duidelijk zijn dat toestanden S_2, S_3, S_4 en S_5 'system down'-toestanden zijn.
Nu kunnen we reparatie gaan invoeren. Daar er telkens slechts één reparateur aan het werk kan zijn, zal er uit iedere toestand (behalve de begintoestand S_0) slechts één tak terugleiden. Waar deze heen gaat wordt bepaald door de reparatiestrategie: in toestand S_5, waarin alles heeft gefaald, zullen we eerst een elektronische unit repareren, dus een tak naar S_3, waarin de mechanische unit en de tweede elektronische unit nog gerepareerd moet worden. In toestand S_3 zullen we eerst de mechanische unit repareren daar dan het systeem weer kan functioneren (overgang naar S_1). In S_1 is alleen nog een elektronische unit die gerepareerd moet worden en dat geeft dus een tak naar S_0. In S_4 zijn beide elektronische units in reparatie en dat geeft een tak naar S_1. In S_2 is de mechanische unit in reparatie en dat geeft een tak naar S_0. Nu is het Markovdiagram compleet.



(b)

c. Als we het systeem afschakelen als het systeem niet meer kan functioneren vinden we met bovenstaande methode (we gaan nu niet verder dan een 'system down' toestand) het onderstaande Markovdiagram.



(c)

We kunnen hieruit met de bekende methode de steady-state availability A_∞ bepalen:

$$\mu_e P_4 = \lambda_e P_1$$

$$\mu_m P_3 = \lambda_m P_1$$

$$\mu_m P_2 = \lambda_m P_0$$

$$\mu_e P_1 = 2\lambda_e P_0$$

$$P_0 + P_1 + P_2 + P_3 + P_4 = 1$$

$$A_\infty = P_0 + P_1$$

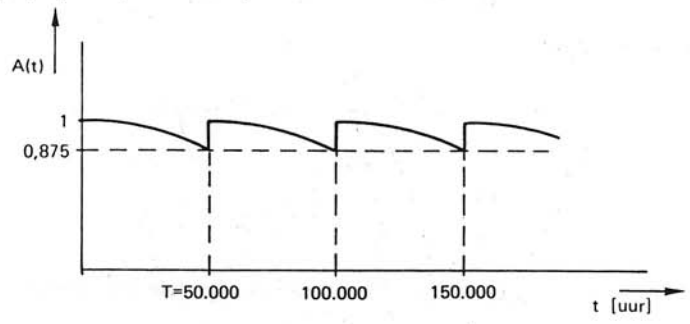
$$A_\infty = \frac{1}{1 + \beta_m + \dfrac{2\beta_e^2}{1 + 2\beta_e}} \approx 0{,}974$$

$$(\beta_m = \frac{\lambda_m}{\mu_m} \text{ en } \beta_e = \frac{\lambda_e}{\mu_e}).$$

7.16. Als de beste unit (met $\lambda = \lambda_L$) als eerste ingeschakeld wordt, dan zal de schakelaar wegens een grotere hazard rate ($10\lambda_L$) een grotere kans heben om eerder te falen dan de unit. Het overgangsverschijnsel in de A(t)-functie zal daarom een kalm en monotoon verloop hebben totdat de steady-state-waarde bereikt wordt. Indien echter met de slechtere units begonnen wordt dan bestaat er een kans dat de goede unit niet meer ingeschakeld kan worden door het falen (kleven) van de schakelaar. De uitval is dan in eerste instantie hoger dan het reparatiekanaal kan verwerken. Omdat verder in de tijd de gemiddelde uitval beduidend lager ligt (de goede unit komt dan wel aan bod) zal de reparatie-achterstand gedeeltelijk kunnen worden weggewerkt. De availability A(t) neemt dan langzaam toe tot de steady-state waarde A_∞; dit houdt dus in dat de relatieve afname a(t) van de availability A(t) tijdelijk negatief wordt.

7.17. Omdat er alleen periodiek onderhoud gepleegd wordt en het systeem na elke onderhoudsbeurt weer als nieuw is, zal het begin van de bedrijfszekerheidscurve steeds herhaald worden. Dus:

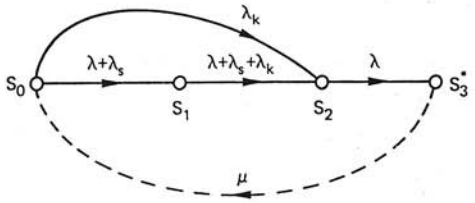
a. $A(t) = R(t - iT) = 1 - F(t - iT) = 1 - 50 \cdot 10^{-12}(t - iT)^2$ voor $iT \leq t < (i + 1)T$ met $i = 0, 1, 2, \ldots$ $(T = 50 \cdot 10^3)$.



b. De gemiddelde beschikbaarheid is dan

$$A_{gem} = \frac{1}{T}\int_0^T A(t)\,dt = 0{,}958.$$

7.18. Markovdiagram:



Voor het berekenen van de MTTFF moeten de takken in het Markovdiagram die vanuit de downtoestand(en) vertrekken genegeerd worden (het systeem wordt immers slechts beschouwd *tot* de downtoestand, wanneer de gebruiker pas merkt dat het niet meer te gebruiken is). Door de differentiaalvergelijkingen links en rechts van het '='-teken te integreren over $[0,\infty)$ worden de volgende vergelijkingen verkregen:

$$\left.\begin{aligned} -1 &= (\lambda + \lambda_s + \lambda_k)\theta_0 \\ 0 &= (\lambda + \lambda_s)\theta_0 - (\lambda + \lambda_s + \lambda_k)\theta_1 \\ 0 &= \lambda_h\theta_0 + (\lambda + \lambda_s + \lambda_k)\theta_1 - \lambda\theta_2 \\ 1 &= \lambda\theta_2 \end{aligned}\right\} \text{ met } \theta_i = \int_0^\infty P_{S_i}(t)\,dt.$$

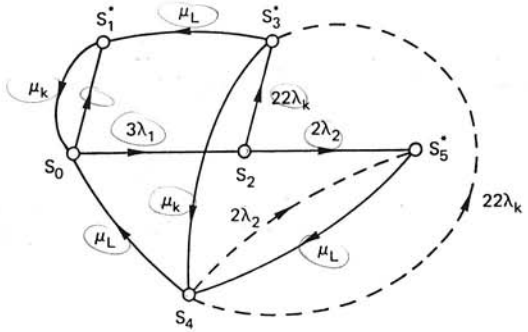
Hieruit volgt:

$$\text{MTTFF} = \theta_0 + \theta_1 + \theta_2 = \frac{1}{4} + \frac{1}{2} + \frac{3}{16} = \frac{15}{16} = \text{MTBF}.$$

De steady-state availability bedraagt dan:

$$A_\infty = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}} = \frac{15/16}{15/16 + 1/10} = 0{,}904.$$

7.19. Markovdiagram:



Toestanden

S_0: Alles functioneert; de drie locomotieven hebben ieder een failure rate λ_l en de koppelingen hebben ieder een failure rate λ_k.

S_1: Er is één koppeling kapot. De trein staat stil en de koppeling is in reparatie, terwijl de overige componenten niet kunnen falen.

S_2: Er is één locomotief kapot. De beide andere locomotieven hebben nu een failure rate λ_2. Omdat de trein nog steeds kan rijden wordt er nog niet gerepareerd.

S_3: Er is één locomotief en één koppeling kapot. Beide zijn in reparatie.

S_4: Dit is een tussentoestand in het reparatieproces. Er is nu alleen nog maar één locomotief kapot (en in reparatie). De trein kan weer rijden en alle andere componenten kunnen weer falen. De nog defecte locomotief wordt gerepareerd aangezien het systeem down is geweest (in S_3 of S_5). Als de trein blijft stilstaan totdat alle componenten gerepareerd zijn, dan ontbreken de gestreepte takken vanuit S_4 naar S_3 en naar S_5.

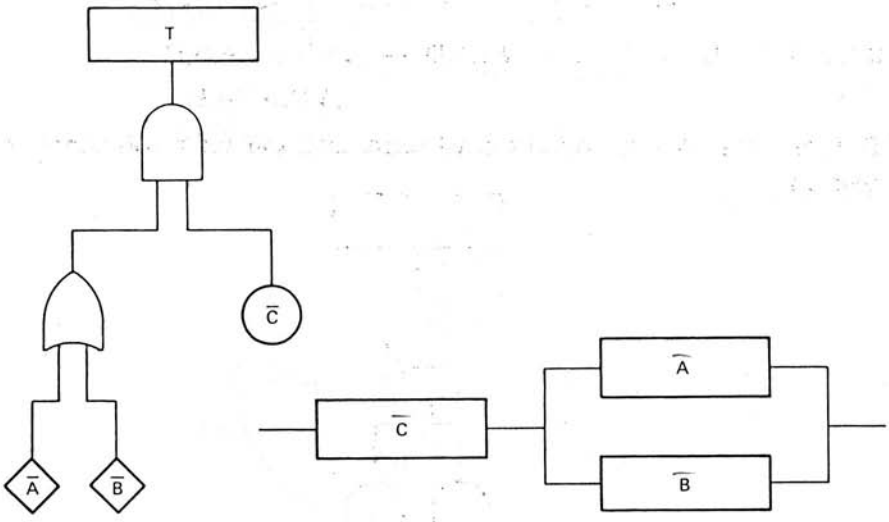
S_5: Er zijn twee locomotieven kapot waardoor het systeem faalt. Eén van de kapotte locomotieven is in reparatie. De overige componenten kunnen niet falen.

8. Evaluatiemethoden

8.1. Ja, natuurlijk is het mogelijk in plaats van faalbomen succesbomen te gebruiken. Om deze succesboom op te zetten kunnen we uitgaan van de uitdrukking voor de topgebeurtenis van de gegeven faalboom $T = A \cdot B + C$. Voor het niet optreden van de topgebeurtenis volgt dan:

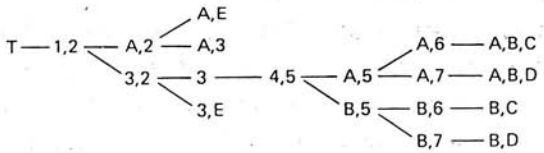
$$T = \overline{A \cdot B + C} = \overline{A} \cdot \overline{B} \cdot \overline{C} = (\overline{A} + \overline{B}) \cdot \overline{C}.$$

Dit is weergegeven in de onderstaande succesboom.

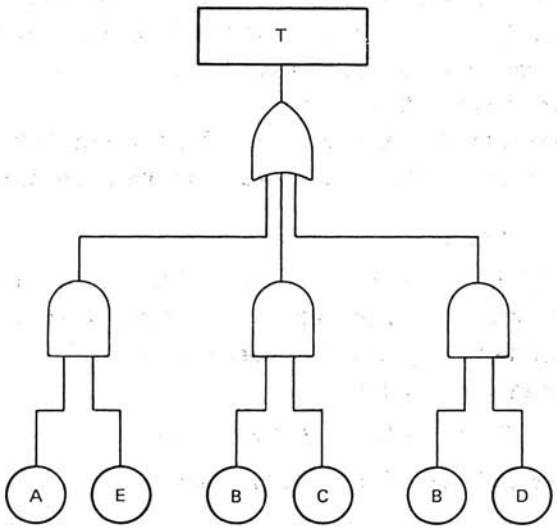


De topgebeurtenis T treedt dus op als A en/of B succes heeft *en* C succes heeft. Ook het catastrofaal faalmodel is hier eenvoudig uit te bepalen en is in de figuur weergegeven.

8.2. a. Uit figuur a blijkt dat de minimum snedes zijn: A,E; B,C en B,D.

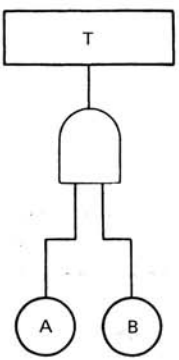


b. De gereduceerde faalboom is weergegeven in figuur b.



8.3. a. T — 1,2 — 2,3,4 — 2,3,A,D — 3,A,D — A,B,D
3,A,C,D
A,D

De minimum snede is dus A,D. De gereduceerde faalboom wordt zoals hieronder gegeven.

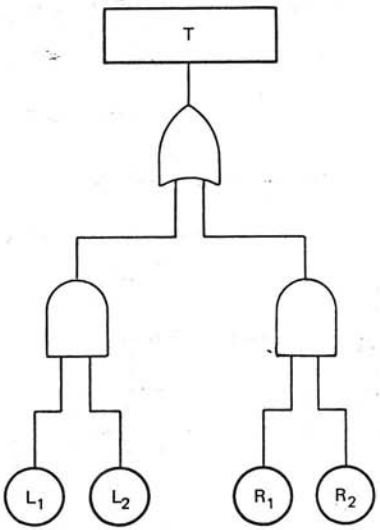


b. Het systeem zal falen als beide gebeurtenissen A en D optreden. De faalkans wordt dus

$$F(t) = \{1 - \exp(-\lambda_A t)\}\{1 - \exp(-\lambda_D t)\}.$$

8.4. a. De kans dat alle vier motoren de vlucht overleven is gelijk aan $\binom{4}{0}(0,9)^4$. De kans dat drie motoren de vlucht overleven is $\binom{4}{1}(0,9)^3(0,1)$, terwijl de kans dat slechts twee motoren de vlucht overleven gelijk is aan $\binom{4}{2}(0,9)^2(0,1)^2$. In ieder van deze gevallen komt het vliegtuig behouden aan. De kans hierop is de som van bovenstaande kansen en is gelijk aan 0,9963.

b. Het geval dat zich minstens aan iedere vleugel een werkende motor moet bevinden maakt dat het vliegtuig niet behouden aankomt als beide linker motoren falen en/of beide rechtermotoren falen. Dit geeft onderstaande faalboom weer.



c. De kans dat het vliegtuig niet behouden aankomt is gelijk aan de kans op de topgebeurtenis T. Uit bovenstaande figuur volgt voor T:

$$P(T) = P(L_1)P(L_2) + P(R_1)P(R_2) - P(L_1)P(L_2)P(R_1)P(R_2).$$

De kans dat het vliegtuig wel aankomt is dan

$$1 - P(T) = 0,9801.$$

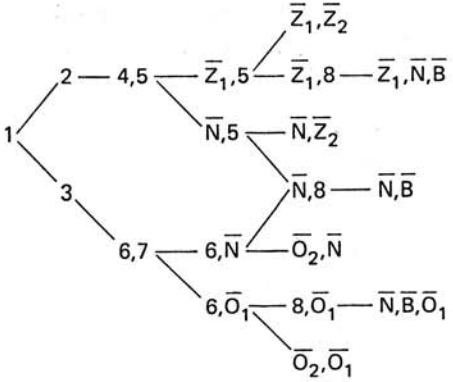
d. De bedrijfszekerheid R van een motor voor een vluchtduur T is $\exp(-\lambda t)$. De faalkans van een motor voor deze vluchtduur is $1 - R$. Als we dit substitueren in de uitdrukking onder c, dan vinden we voor de 'mission reliability':

$$\exp(-2\lambda T)\{2 - \exp(-\lambda T)\}^2.$$

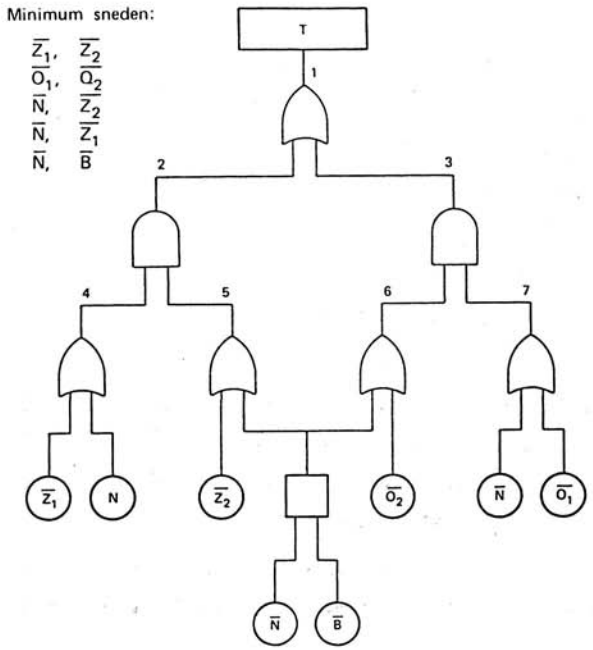
8.5. a. Voor het opzetten van de faalboom voor dit probleem kunnen we het best eerst beschouwen wanneer de zenders niet meer gebruikt kunnen worden. De nor-

male zender kan niet meer gebruikt worden als òf de zender gefaald heeft òf het net gefaald heeft. De noodzender kan niet meer gebruikt worden als de noodzender gefaald heeft en/of er geen voedingsspanning meer is. Er is geen voedingsspanning meer voor de noodzender als zowel het 24 Volt net als de 'battery pack' gefaald hebben. Dit resulteert in het linkerdeel van de onderstaande faalboom. Ditzelfde kunnen we opzetten voor het ontvangstgedeelte. Dit resulteert in het rechtergedeelte. Als de beide zenders en/of beide ontvangers buiten gebruik zijn dan resulteert de topgebeurtenis: er is geen communicatie meer mogelijk.

b. Met behulp van het Fussel-Vesely algoritme kunnen we nu de minimumsneden bepalen:



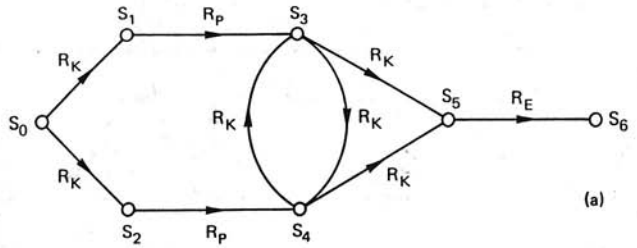
De minimumsneden zijn gegeven in de figuur.



De kans op de topgebeurtenis wordt gegeven door:

$$P_1 = P(Z_1)P(Z_2) + P(O_1)P(O_2) + P(W)P(Z_2) + P(N)P(O_2) + P(N)P(O_2) + P(N)P(B) - \{P(Z_1)P(Z_2)P(O_1)P(O_2) + \ldots \text{ alle tweevoudige doorsneden}\} + + \{\text{alle drievoudige doorsneden}\} - \text{enzovoort}\ldots = 0{,}04471.$$

8.6. a. De bedrijfszekerheidsgraaf is weergegeven in onderstaande figuur. Het zal duidelijk zijn dat voor de bedrijfszekerheid klep $K_{a.1}$ en pomp A in serie staan. Dit geldt ook voor klep $K_{b.1}$ en pomp B. Daar klep K water kan doorlaten in beide richtingen moeten in de graaf beide takken opgenomen worden. In het bedrijfszekerheidsmodel moet het elektriciteitsnet in serie staan met de rest van het systeem daar het systeem zal falen als het elektriciteitsnet faalt.



De bedrijfszekerheid van het systeem zonder de tak met R_E kan nu opgelost worden met de methode zoals gegeven bij de oplossing van opgave 6.6 ($R_A = R_{A'} = R_K P_P$ en $R_B = R_{B'} = R_C = R_K$).

Voor de totale bedrijfszekerheid moet de hierboven gevonden bedrijfszekerheid vermenigvuldigd worden met de bedrijfszekerheid van het net (R_E). We vinden dan:

$$R = R_E(R_K + R_P)\{2R_K(1 + R_K - R_K^2) + R_K^2(2R_K - 3)(R_K + R_P)\}.$$

b. De faalboom behorend bij dit systeem is eenvoudig te vinden en is op bladzijde 275 weergegeven.

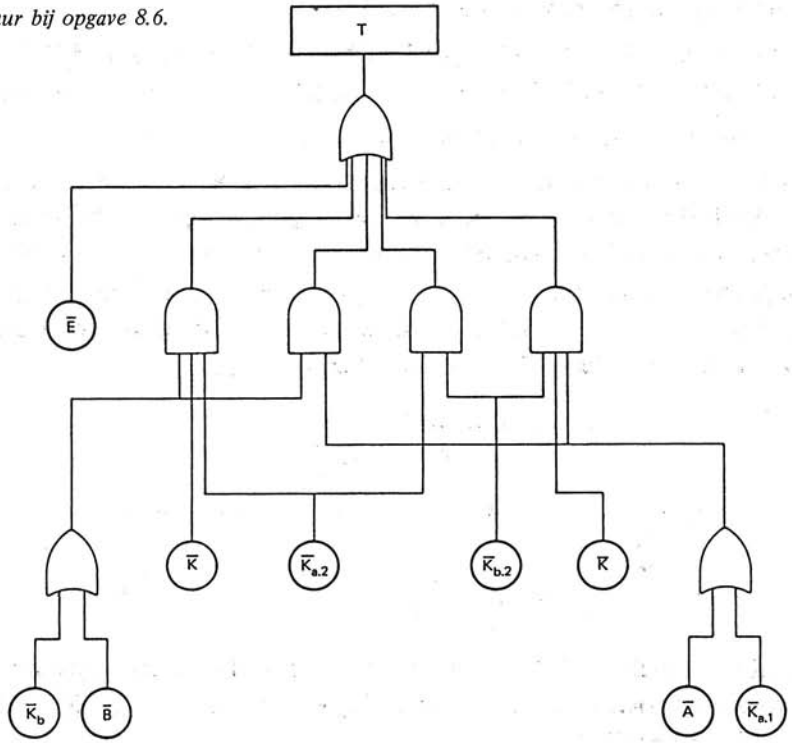
8.7. De faalboom behorende bij het gegeven probleem staat op bladzijde 276. Hierin zijn de basisgebeurtenissen:

A: computer I faalt;
B: computer II faalt;
C: het openbaar elektriciteitsnet valt uit;
D: de accu is stuk;
E: reparatie van het openbaar net duurt langer dan 1 uur.

De resulterende gebeurtenissen zijn:

F: accu leeg;
G: accu faalt;
H: voeding computers faalt;

Figuur bij opgave 8.6.



I: redundantie kanaal I faalt;
J: redundantie kanaal II faalt.

De topgebeurtenis is:

T: procesregeling stopt.

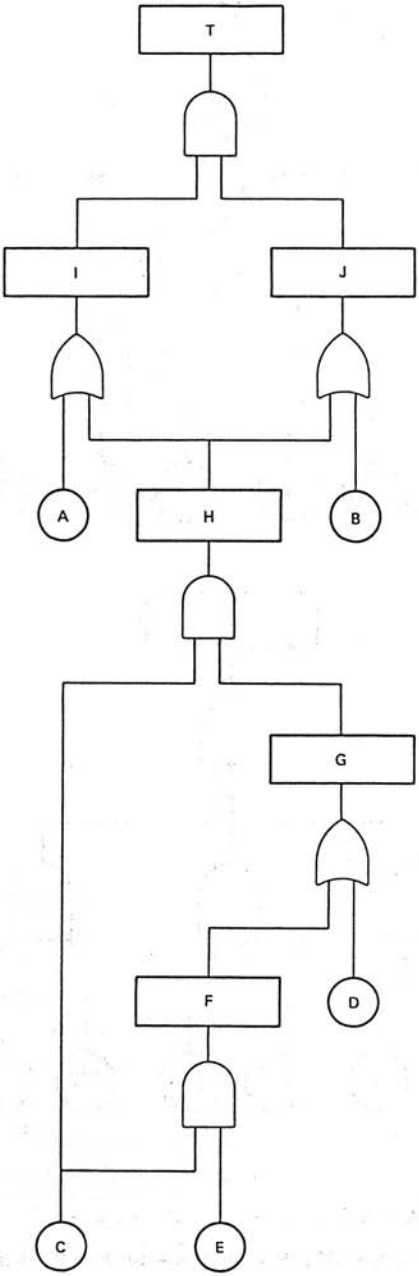
Natuurlijk is het ook mogelijk een andere configuratie te vinden voor de faalboom. Deze faalboom is correct als de topgebeurtenis gelijk is aan

$$(A \cap B) \cup (C \cap D) \cup (C \cap E).$$

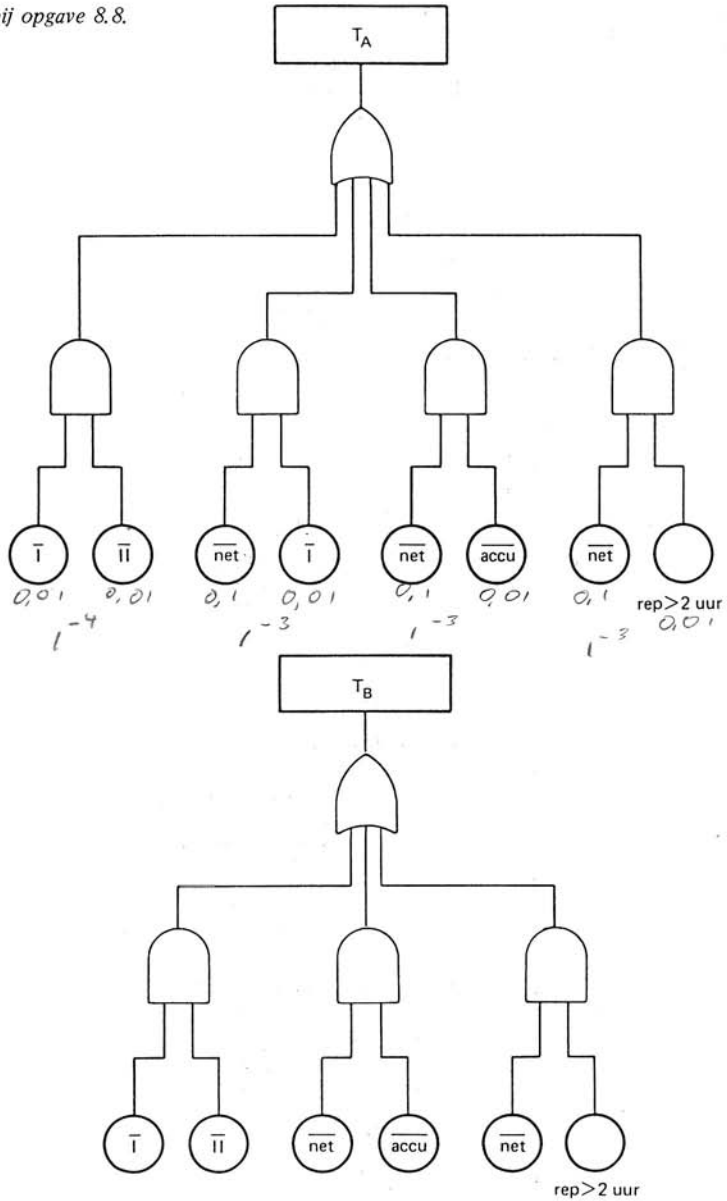
8.8. De gereduceerde faalbomen voor beide configuraties zijn hieronder weergegeven, samen met de berekening van de kans op de topgebeurtenis.
Configuratie A geeft dus de hoogste bedrijfszekerheid. Uit dit praktijkvoorbeeld blijkt duidelijk dat bij gegeven units en componenten voor een systeem de bedrijfszekerheid in hoge mate bepaald kan worden door de keuze van de configuratie van dat systeem.

8.10. a. Natuurlijk is de detectiewaarschijnlijkheid van rook maximaal als het alarm afgaat als één of meer sensoren rook signaleren.
b. Er wordt geen rook gedetecteerd terwijl er wel rook is, als geen van de drie

Figuur bij opgave 8.7.



Figuur bij opgave 8.8.



$$P(T_A) = \bar{I}\cdot\bar{II} + \bar{I}\cdot\bar{N} + \bar{N}\cdot\bar{A} + \bar{N}\cdot\bar{R} - \bar{I}\cdot\bar{II}\cdot\bar{N} - \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{A} - \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{R} - \bar{I}\cdot\bar{N}\cdot\bar{A} - \bar{I}\cdot\bar{N}\cdot\bar{A} - \bar{I}\cdot\bar{N}\cdot\bar{R} +$$
$$- \bar{N}\cdot\bar{A}\cdot\bar{R} + \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{A} + \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{R} + \bar{I}\cdot\bar{N}\cdot\bar{A}\cdot\bar{R} + \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{A}\cdot\bar{R} - \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{A}\cdot\bar{R} = 0{,}0030601$$

$$P(T_B) = \bar{I}\cdot\bar{II} + \bar{N}\cdot\bar{A} + \bar{N}\cdot\bar{R} - \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{A} - \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{R} - \bar{N}\cdot\bar{A}\cdot\bar{R} + \bar{I}\cdot\bar{II}\cdot\bar{N}\cdot\bar{A}\cdot\bar{R} = 0{,}01099891$$

detectoren rook signaleert. De kans hierop is $(0{,}15)^3$. De kans dat de rook wel gedetecteerd wordt is $1 - (0{,}15)^3 = 0{,}997$.

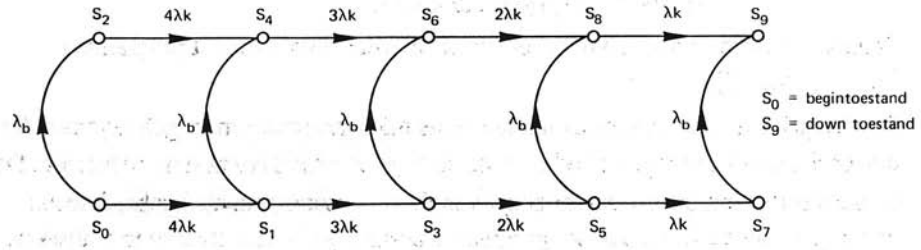
c. De kans op vals alarm is 1 – kans op geen vals alarm = $1 - (0{,}9)^3 = 0{,}27$.

d. Als twee of meer sensoren rook signaleren moet het alarm afgaan. Het produkt {detectiekans × (1 – vals alarm kans)} is dan:

$$\{\binom{3}{1}(0{,}85)^2 0{,}15 + (0{,}85)^3\} \times \{1 - \binom{3}{1}(0{,}1)^2 0{,}9 - (0{,}1)^3\}(1 - 0{,}028) = 0{,}913.$$

Voor het geval dat het alarm afgaat als minstens één sensor rook signaleert vinden we voor het produkt 0,723. En in het geval dat alle drie sensoren rook moeten signaleren voordat het alarm afgaat vinden we $(0{,}85)^3(1 - (0{,}1)^3) = 0{,}614$.

8.11. Het Markovdiagram is als in onderstaande figuur.



Vanuit de begintoestand S_0 kan één van de vier kabels breken (overgang naar toestand S_1) of kan het beveiligingssysteem, waarbij bij een vrije val veiligheidshaken zich in de wanden zouden vastgrijpen, falen (overgang naar S_2).
In toestand S_1 kan één van de drie overblijvende kabels breken (naar S_3) of kan het beveiligingssysteem falen (naar S_4). Zo kunnen we het hele diagram nalopen.
Als het systeem in toestand S_7 terecht komt dan is het systeem in principe 'down', daar alle vier kabels gebroken zijn. Uit het oogpunt van veiligheid heeft het systeem echter nog niet gefaald: in de toestand S_7 heeft het beveiligingssysteem immers gewerkt. De lift hangt nu ergens vast. Toestand S_9 is niet alleen bedrijfszekerheidstechnisch maar ook letterlijk een 'down'-toestand: het is de vlugste edoch fatale manier om beneden te komen.

9. Bedrijfszekerheid van computerprogrammatuur

9.1.
```
400 IF A > 0 AND B > 0 THEN D = C ELSE D = -C
401 PRINT D
```

9.2. Tijdens het uitvoeren van het programma zullen de fouten willekeurig optreden. Dit houdt in dat de gemiddelde tijd tot het optreden van een fout (de MTTF) omgekeerd evenredig zal zijn met het aantal aanwezige fouten. Dit betekent dat het produkt van de MTTF en het aantal mogelijke fouten constant is en gelijk is aan M_0T_0. Na een testtijd τ zijn er nog $M_0e^{-\tau C/M_0T_0}$ mogelijke fouten, zodat de MTTF(τ) gelijk is aan $T_0e^{\tau C/M_0T_0}$.

9.3. a. Het totale aantal fouten dat mogelijk is gedurende de duur van de test en het corrigeren is het aantal programmafouten N_0 gedeeld door de reductiefactor B, dus $M_0 = 2000$. De initiële MTTF T_0 wordt gegeven door $(fKN_0)^{-1} = 1/30$ s. De testtijd τ wordt nu gegeven door

$$\tau = \frac{M_0 T_0}{C} \ln \frac{MTTF(\tau)}{T_0} = 847 \text{ s.}$$

b. Het aantal gedetecteerde initiële fouten wordt gegeven door

$$N = N_0[1 - \exp(-\tau C/M_0 T_0)].$$

Het resterende aantal initiële fouten is dus

$$N_0 \exp(-\tau C/M_0 T_0) = 5{,}6 \times 10^{-9}.$$

Praktisch volgt hieruit dat om aan bovenstaande eis te voldoen het programma foutloos moet zijn.

9.4. De prijzen van basiscomponenten zoals microprocessoren en geheugens dalen drastisch terwijl de mogelijkheden en de bedrijfszekerheid ervan sterk toenemen. De tendens is daarom om zoveel mogelijk van deze basiscomponenten gebruik te maken en de vereiste functie onder programmabesturing (in de software) te realiseren. De te gebruiken programmatuur verschilt echter per toepassing en zal in hoge mate de systeembedrijfszekerheid bepalen. Voor een goede bedrijfszekerheid dient de programmatuur niet alleen modulair, overzichtelijk (gestructureerd) en transparant opgebouwd te worden, maar dient ook extra geld uitgetrokken te worden voor het testen en corrigeren van de software en het schrijven van goede documentatie.

9.5. a. Mogelijke foutoorzaken bij het ontwikkelen van programmatuur in de specificatiefase zijn:

- misverstanden en onduidelijkheden in de probleemstelling;
- onvoldoende aandacht voor randvoorwaarden van het systeem zoals processorcapaciteit, geheugenruimte, rekentijd en in- en uitvoermogelijkheden;
- een niet-eenduidige definitie van interfaces en communicatieprotocollen;
- overschatting van het begripsvermogen of het opleidingsniveau van de gebruiker.

b. Mogelijke foutoorzaken in de realisatiefase zijn:

- onvolledige of onduidelijke detailspecificaties;
- foutieve interpretatie van specificaties;
- tegenstrijdigheden binnen de algoritmen;
- onjuiste initialisering;
- onduidelijkheden over programmastructuur.

c. Foutoorzaken in de test- en gebruiksfase kunnen zijn:

- het bij programmaverbetering introduceren van nieuwe programmafouten door onzorgvuldigheid;
- onduidelijke of onvolledige documentatie;
- verandering van de hardware- of de software-omgeving;
- capaciteitsgebrek ('overlopen' van een buffer, gebrek aan geheugenplaatsen).

9.6. Enige richtlijnen ter voorkoming van programmatuurfouten zijn:

- het vooraf en schriftelijk vastleggen van richtlijnen en werkmethoden waarin kwaliteitskenmerken en de te volgen procedures in voorkomen;
- de detailspecificaties dienen de programmastructuur in acht te nemen en zo nauwkeurig mogelijk gespecificeerd te worden;
- hogere, algemeen erkende programmeertalen verdienen de voorkeur;
- programmeer modulair en gestructureerd waarbij de modulen een zo groot mogelijke zelfstandigheid moeten hebben en zo mogelijk apart te testen zijn;
- houdt rekening met de door randapparatuur opgelegde communicatievoorwaarden.
- realiseer testbaarheidsaspecten (foutdetectie-graad, foutlocalisatiegraad, testduur en juistheid van de testresultaten) zo goed mogelijk in het programma;
- voeg, om het programma ook voor andere gebruikers toegankelijk te maken, zoveel mogelijk verhelderend en zinnig commentaar toe aan het programma;
- zorg voor correcte en duidelijke documentatie;
- pas een ver doorgevoerde programmastructuur toe, tezamen met uitgebreide testmogelijkheden, zowel voor de modulen apart als in groepen.

Bijlage

B.1. Toegepaste Laplace-transformaties

$f(t) = \mathcal{L}^{-1}\{F(s)\}$	$F(s) = \mathcal{L}\{F(t)\}$	
1	$\frac{1}{s}$	$(s > 0)$
e^{-at}	$\frac{1}{s+a}$	
$\frac{t^n}{n!}e^{-at}$	$\frac{1}{(s+a)^{n+1}}$	
$\lim_{t\to\infty} f(t)$	$\lim_{s\downarrow 0} s\,F(s)$	(eindwaardestelling)
$\lim_{t\downarrow 0} f(t)$	$\lim_{s\to\infty} s\,F(s)$	(beginwaardestelling)

B.2. De centrale limietstelling

De centrale limietstelling uit de statistiek zegt dat de som van een groot aantal onafhankelijke stochastische variabelen die alle een willekeurige maar identieke verdeling bezitten nadert tot een normale verdeling. Ofwel:

$$y = \lim_{n\to\infty} \sum_{i=1}^{n} x_i$$

is normaal verdeeld.

B.3. Lijst van de meest gebruikte symbolen

symbool	naam	dimensie
A	beschikbaarheid	–
A_∞	steady state beschikbaarheid	–
F	faalkans	–
R	bedrijfszekerheid	–
f	faalkansdichtheid	s^{-1}
z	hazard rate (conditionele faalkansdichtheid)	s^{-1}
λ	failure rate	s^{-1}
μ	repair rate	s^{-1}
α	inzetbaarheid	–
θ	gemiddelde levensduur	s
θ_m	mediane levensduur	s
MTTF	mean time to failure	s
MTTFF	mean time to first failure	s
MTBF	mean time between failure	s
σ	spreiding	s
η	veiligheidsfactor of redundantiegraad	–
$P(x)$	kans op gebeurtenis x	–
S_i	toestand i	–
P_{S_i}	kans op de toestand i	–
N	aantal	–
n	aantal	–
t	tijd	s
s	variabele in het Laplace-domein	–

Literatuur

Inleidende literatuur

Becker, P.W., Jensen, F., Design of systems and circuits for maximum reliability and production yield, McGraw-Hill, New York, 1977.

Kapur, K.C., Reliability in engineering design, Wiley, New York, 1977.

Singh, C., e.a., System reliability modelling and evaluation, Hutchinson, London, 1977.

Tsokos, C.P., e.a., The theory and applications of reliability, Academic Press, New York, 1977.

Smith, C.O., Introduction to reliability in design, McGraw-Hill, 1976.

Mann, N.R., e.a., Methods for statistical analysis of reliability and life data, Wiley, New York, 1974.

Smith, D.J., Reliability engineering, Pitman, New York, 1973.

Smith, D.J., e.a., Maintainability engineering, Pitman, New York, 1973.

Brook, R.H.W., Reliability concepts in engineering manufacture, Butterworth, London, 1972.

Green, A.E., e.a., Reliability technology, Wiley Interscience, London, 1972.

Smith, D.J., Reliability engineering, Barnes and Noble Books, New York, 1972.

Kozlov, B.A., e.a., Reliability handbook, Holt Rinehart, New York, 1970.

Störmer, H., Mathematische Theorie der Zuverlässigkeit, Akademie-Verlag, Berlin, 1970.

Dummer, G.W. and Winston, R.C., An elementary guide to reliability, Pergamon, Elmsford, NY, 1968.

Hofman, W., Zuverlässigkeit von Mess-, Steuer-, Regel-, und Sicherheits-Systemen, Verlag Karl Thiemig, 1968.

Polovko, A.M., Fundamentals of reliability theory, Academic Press, New York, 1968.

Shooman, M.L., Probabilistic reliability, McGraw-Hill, New York, 1968.

Dummer, G.W.A., e.a., Electronics reliability, calculation and design, Pergamon Press, Oxford, 1966.

Roberts, N.H., Mathematical methods in reliability engineering, McGraw-Hill, New York, 1965.

Goldman, A.S., e.a., Maintainability, Wiley, New York, 1964.

Pieruschka, E., Principles of reliability, Prentice-Hall, Englewood Cliffs NJ, 1963.

Lloyd, D.K., e.a., Reliability, Prentice-Hall, Englewood Cliffs NJ, 1962.

Bazovsky, I., Reliability theory and practice, Prentice-Hall, Englewood Cliffs NJ, 1961.

Handboeken, standaarden

Kozlov, B.A., e.a., Reliability handbook, Holt Rinehart and Winston, New York, 1970.

Kozlov, B.A., e.a., Handbuch zur Berechnung der Zuverlässigkeit für Ingenieure, Hanser Verlag, München, 1979 (598 pagina's, aangevulde en herziene versie van het vorige boek).

Ireson, W.G., editor, Reliability handbook, McGraw-Hill, New York, 1966.

Juran, J.M., Quality control handbook, McGraw-Hill, New York, 1962.

British Standard BS4778: "Glossary of terms used in quality assurance", British Standards Institution, London.

British Standard BS5760: "Reliability of systems, equipments and components", British Standards Institution, London.

IEC publication 271: "List of basic terms, definitions, and related mathematics for reliability", IEC, Genève, 1974.

IEC publication 605-1: "Equipment reliability testing, part 1: General requirements", IEC, Genève, 1978.

IEC publication 605-2: "Equipment reliability testing, part 2: Guidance for the design of test cycles", 56(sec) 124, IEC, Genève, 1979.

IEEE: "Nuclear reliability data manual", IEEE Guide to the collection and presentation of electrical, electronic, and sensing components reliability data for nuclear-power generating stations, IEEE, New York, 1977.

INSPEC: "Electronic reliability data, a guide to selected components", The Institution of Electrical Engineers, London, 1981.

MIL-HDBK-217C: "Reliability prediction of electronic equipment", US Department of Defence, Washington, 1979.

MIL-STD-721: "Definitions of effectiveness terms for reliability, maintainability, human factors and safety", Issue B, US Department of Defence, Washington.

MIL-STD-781C: "Reliability design qualification and production acceptance tests: Exponential distribution", US Department of Defence, Washington, 1977.

NAVAIR-00-65-502/NAVORD OD-41146: "Reliability Engineering Handbook", June 1, 1964.

Tijdschriften

IEEE Transactions on reliability (IEEE, New York).

Journal of quality technology (American Society for Quality Control).

Microelectronics and Reliability (Pergamon Press, Oxford).

Symposia

Reliability Physics Symposium (jaarlijks, IEEE, geeft proceedings uit).

Reliability and Maintainability Symposium (jaarlijks, IEEE, geeft proceedings uit).

Reliability Symposium SRE (twee-jaarlijks, Canadian Society of Reliability Engineers, proceedings verschijnen in tijdschrift *Microelectronics and Reliability*).

Capita Selecta

Faalmodellen, distributies

Lawless, J.F., Statistical models and methods for lifetime data, Wiley, New York, 1982.

Elandt-Johnson, R.C. and Johnson, N.L., Survival models and data analysis, Wiley, New York, 1980.

Bury, K.V., Statistical models in applied science, Wiley, New York, 1975.

Gross, AJ. and Clark, V.A., Survival distributions: Reliability applications in the medical sciences, Wiley, New York, 1975.

Ross, S.M., Introduction to probability models, Academic Press, New York, 1972.

Johnson, N.L., Continuous univariate distributions, Houghton Mifflin Company, Boston, 1970.

Ross, S.M., Applied probability models with optimization applications, Holden-Day, San Francisco, 1970.

Dixon, W.J., e.a., Introduction to statistical analysis, McGraw-Hill, New York, 1969.

Gertsbakh, I.B., e.a., Models of failure, Springer Verlag, München, 1969.

Hahn, G.J. and Shapiro, S.S., Statistical models in engineering, Wiley, New York, 1967.

Cox, D.R. and Lewis, P.A., The statistical analysis of series of events, Wiley, New York, 1966.

Peck, D.S., The uses of semiconductor life distributions; In: Semiconductor Reliability, Vol. 2, W. Von Alren ed., Engineering Publishers, Elizabeth NJ, 1962.

Bowker, A.H. and Lieberman, G.J., Engineering statistics, Prentice-Hall, Englewood Cliffs NJ, 1959.

Gumbel, E.J., Statistics of extremes, Columbia University Press, New York, 1958.

Bedrijfszekerheidsberekeningen, theorie

Henley, E.J., Reliability engineering and risk assessment, Prentice-Hall, Englewood Cliffs NJ, 1981.

Miller, R., Survival analysis, Wiley, New York, 1981.

Bain, L.J., Statistical analysis of reliability, Dekker, New York, 1978.

Kapur, K.C., e.a., Reliability in engineering design, Wiley, New York, 1977.

Kaufmann, A., e.a., Mathematical models for the study of the reliability of systems, Academic Press, New York, 1977.

Bompas Smith, J.H., Mechanical survival, McGraw-Hill, London, 1973.

Jardine, A.K.S., Maintenance, replacement and reliability, Halsted Press-Wiley, New York, 1973.

Schneeweisz, W., Zuverlässigkeitstheorie, Springer Verlag, Berlin, 1973.

Amstadter, B.L., Reliability mathematics, McGraw-Hill, New York, 1971.

Bitter, P., e.a., Technische Zuverlässigkeit, Messerschmitt Bölkov, Springer Verlag, Berlin, 1971.

Feller, W., Probability theory and its applications, Vol. I and II, Wiley, New York, 1970.

Jardine, A.K.S., Operational research in maintenance, Halsted Press-Wiley, New York, 1970.
Rau, J.J., Optimization and probability in systems engineering, Van Nostrand-Reinhold, New York, 1970.
Gnedenko, B.V., e.a., Mathematical models of reliability theory, Academic Press, New York, 1969.
Grouchko, D., eds., Operations research and reliability, Gordon and Breach, New York, 1969.
Jorgenson, D.W., e.a., Optimal replacement policy, Rand McNally, Chicago, 1967.
Barlow, R.E., e.a., Mathematical theory of reliability, Wiley, New York, 1965.
Hummitzsch, P., Zuverlässigkeit von Systemen, Vieweg und Sohn, Braunschweig, 1965.
Roberts, N., Mathematical methods in reliability engineering, McGraw-Hill, New York, 1964.
Sandler, G.H., System reliability engineering, Prentice-Hall, Englewood Cliffs NJ, 1963.
Von Alven, W.H., editor, Reliability engineering, Prentice Hall, Englewood Cliffs NJ, 1963.
Zelen, M., eds., Statistical theory of reliability, University of Wisconsin Press, Madison WI, 1963.
Cox, D.R., Renewal theory, Methuen, London, 1962.
Khintchine, A., Mathematical methods in the theory of queueing, Griffin, London, 1960.
Morse, P.M., Queues, inventories and maintenance, Wiley, New York, 1958.

Toetsen op bedrijfszekerheid, meten, testen

Nelson, W., Applied life data analysis, Wiley, New York, 1982.
Sinha, S.K. and Kale, B.K., Life testing and reliability estimation, Wiley Eastern, New Delhi, 1980.
Lee, E., Statistical methods for survival data analysis, Lifetime Learning, Belmont CA, 1980.
Kalbfleisch, J.D. and Prentice, R.L., The statistical analysis of failure time data, Wiley, New York, 1980.
Barlow, R.E., e.a., Statistical theory of reliability and life testing, Holt Rinehart, New York, 1975.
Little, R.E. and Jebe, E.H., Statistical design of fatigue experiments, Halsted, New York, 1975.
Lipson, C. and Sheth, N.C., Statistical design and analysis of engineering experiments, McGraw-Hill, New York, 1973.
King, J.R., Probability plots for decision making, Industrial Press, New York, 1971.
Mann, N.R.R.E., e.a., Methods for statistical analysis of reliability and life data, Wiley, New York, 1974.
Johnson, L.G., The statistical treatment of fatigue experiments, American Elsevier Pub., New York, 1964.
Johnson, L.G., Theory and techniques of variation research, American Elsevier Pub., New York, 1964.
Mace, A.E., Sample-size determination, Reinhold Publishing Co., New York, 1964.
Myers, R.H., Reliability engineering for electronic systems, Wiley, New York, 1964.
Kulldorff, G., Estimation from grouped and partially grouped samples, Wiley, New York, 1961.
Weibull, W., Fatigue testing and the analysis of results, Pergamon, New York, 1961.

Onderhoud, organisatie, management en produktie

Welch, Ann, Accidents happen, John Murray Ltd., London, 1978.
Kletz, Trevor A., What went wrong? Case histories of process plant disasters, Gulf Publishing Company, Houston Texas, 1985.
Halpern, S., The assurance sciences: An introduction to quality control and reliability, Prentice-Hall, Englewood Cliffs NJ, 1978.
Enrick, N.L., Quality control and reliability, Industrial Press, New York, 1977.
Rowe, W.D., An anatomy of risk, Wiley, New York, 1977.
Lowrance, W.W., Of acceptable risk: Science and the determination of safety, William Kaufman, Los Altos CA, 1976.
Carrubba, E.R., e.a., Assuring product integrity, Lexington Books, Massachusetts, 1975.
Locks, M.O., Reliability, maintainability and availability assessment, Hayden, Rochelle Park NJ, 1973.
Smith, D.J., e.a., Maintainability engineering, Wiley, New York, 1973.
Nixon, F., Managing to achieve quality and reliability, McGraw-Hill, London, 1971.
Jardine, A.K.S., editor, Operational research in maintenance, Barnes and Nobles Books, New York, 1970.

Blanchard, B.S., e.a., Maintainability, McGraw-Hill, New York, 1969.
Jorgenson, D.W., e.a., Optimal replacement policy, Rand McNally, Chicago 1967.
Goldman, A.S., e.a., Maintainability, Wiley, New York, 1964.
Haviland, R.P., Engineering reliability and long life design, Van Nostrand, Princeton NJ, 1964.
Landers, R.R., Reliability and product assurance, Prentice-Hall, Englewood Cliffs NJ, 1963.
Calabro, S.R., Reliability principles and practices, McGraw-Hill, New York, 1962.
Lloyd, D.K., e.a., Reliability, management methods and mathematics, Prentice-Hall, Englewood Cliffs NJ, 1961.

Ontwerptechnieken, toepassingen

Klaassen, K.B., Reliability of analogue electronic systems, Elsevier, Amsterdam, 1984.
Jensen, F. and Petersen, N.E., Burn-in: An engineering approach to the design and analysis of burn-in procedures, Wiley, Chichester, 1982.
Dhillon, B.S., e.a., Engineering reliability, Wiley, New York, 1981.
O'Connor, P.D.T., Practical reliability engineering, Heyden and Son, London, 1981.
Longbottom, R., Computer system reliability, Wiley, New York, 1980.
Endrenyi, J., Reliability modelling in electric power systems, Wiley, New York, 1978.
Bennet, S.B., e.a., Failure prevention and reliability, Society of Mech. Eng., New York, 1977.
Anderson, R.T., Reliability design handbook, IIT Research Institute (RAC), RADC, Griffins Air Force Base, New York, 1976.
Myers, J., Software reliability principles and practice, Wiley Interscience, New York, 1976.
Smith, C.O., Introduction to reliability in design, McGraw-Hill, New York, 1976.
Myers, J., Reliable software through composite design, Petrocelli Books, New York, 1975.
Cluley, J.C., Electronic equipment reliability, Macmillan, London, 1974.
Jowett, C.E., Electronic and environments, Business Books, London, 1973.
Carter, A.D.S., Mechanical reliability, Wiley, London, 1972.
Cunningham, C.E. and Cox, W., Applied maintainability engineering, Wiley, New York, 1972.
Jowett, C.E., Reliable electronic assembly production, Tab Books, Blue Ridge Summit, 1971.
Kivenson, G., Durability and reliability in engineering design, Hayden, New York, 1971.
Billinton, R., Power system reliability evaluation, Gordon and Breach, New York, 1970.
Jelen, F.C., Cost and optimization engineering, McGraw-Hill, New York, 1970.
Jowett, C.E., Reliability of electronic components, London Iliffe Book, England, 1966.
Meyer, R.H., e.a., Reliability engineering for electronic systems, Wiley, New York, 1964.
Ankenbrandt, F.L, Maintainability design, Engineering Publishers Division of A.C. Book Co., Elisabeth NJ, 1963.
Landers, R.R., Reliability and product assurance, Prentice-Hall, Englewood Cliffs NJ, 1963.
Haugen, E.B., Probabilistic approaches to design, Wiley, New York, 1962.

Trefwoordenlijst

elektrotechniek en computerkunde

DIGITALE TECHNIEK *van probleemspecificatie tot realisatie,* door ir. A.P. Thijssen, ir. H.A. Vink en prof.ir. C.H. Eversdijk

In twee delen wordt een overzicht gegeven van de digitale techniek. De boeken worden gebruikt bij de colleges *Digitale Techniek I, II* en *III* voor studenten Elektrotechniek en Informatica.

Deel 1 behandelt de basiskennis van de componenten, waaronder schakelalgebra, Karnaughdiagrammen, SSI/MSI en LSI combinatorische schakelingen, flip-flops, schuifregisters en tellers. Fysische eigenschappen van componenten worden behandeld voor zover deze van belang zijn voor het logisch ontwerp van een component of deelsysteem. Een nieuw hoofdstuk (in de editie 1988) behandelt de basis van TTL, NMOS en CMOS logica. Daarnaast krijgt de timing van signalen, zowel bij data-overdracht als m.b.t. clock skew, ruime aandacht. Een en ander vormt de grondslag voor de betrouwbaarheid van een ontwerp.

Op diverse plaatsen wordt de relatie tussen de interne (logische) structuur van een component of deelsysteem en de uitwendige eigenschappen ervan toegelicht, zulks in het kader van top-down gericht ontwerpen.

Deel 2 begint met een behandeling van algoritmes voor optellen/aftrekken, vermenigvuldigen en delen en van code-omzetters. De implementatie ervan in hardware wordt uitvoerig toegelicht.

Vervolgens wordt het datapad-besturing ontwerpmodel geïntroduceerd en toegepast op enkele grotere voorbeelden. In de volgende editie van deel 2 zal ook de theorie van de sequentiële machines worden opgenomen. Deze theorie wordt o.a. toegepast bij reductie en het oplossen van passingsproblemen bij programmeerbare logica.

Vele opgaven en literatuurverwijzingen zijn toegevoegd. Antwoorden van opgaven zijn in beide delen opgenomen.

De systematische behandeling maakt de boeken ook uitstekend geschikt voor zelfstudie en voor gebruik op TH en HIO.

De stof is zo geordend dat een eerste, meer globale, oriëntatie op het vakgebied eruit gedoceerd kan worden, waarna desgewenst één of meer onderwerpen kunnen worden uitgewerkt (dit laatste vooral voor de richting Elektrotechniek).

Deel 1, 368 pag., ISBN 90-6562-068-0
(2e druk1987, 3e druk 1988)
Deel 2, 256 pag., ISBN 90-6562-069-9 (1987)

Overhead sheets

Voor docenten zijn lay-outs van *overhead sheets* (ca. 500 stuks) verkrijgbaar. Voor nadere inlichtingen wende men zich tot de uitgever.

DIGITEST

Opgaven behorend bij *Digitale Techniek*

De in deze bundel opgenomen vraagstukken hebben in de jaren 1982 t.e.m. 1985 deel uitgemaakt van de examens Digitale Techniek aan de TU-Delft. De vraagstukken zijn geordend naar onderwerp, overeenkomstig de hoofdstukindeling van het theorieboek. De vragen zijn gesteld in multiple choice vorm. De antwoorden zijn op de laatste bladzijde weergegeven.

112 pag., ISBN 90-6562-046-x (1987)

MICROPROCESSORS door ir. C.J. van Spronsen en ir. F. Bruggeman

In dit boek wordt de microprocessor geïntroduceerd uitgaande van een algemeen model, aan de hand waarvan de interne opbouw en de instructie-afhandeling worden toegelicht. De diverse methoden van adressering, zoals microprocessors die kennen, worden behandeld. Uitgebreide aandacht krijgt de in- en uitvoer, alsmede de speciaal daarvoor ontwikkelde circuits. Standaards voor zowel aansluiting met de 'buitenwereld' als voor de koppeling van modules tot een (multi-) processorsysteem komen aan de orde.

Ook de programmatuur wordt niet vergeten, zoals blijkt uit de hoofdstukken over de ontwikkeling van software en de daarvoor bestaande ondersteuning in apparatuur en programmatuur.

Bij de behandeling van de stof in dit boek wordt aangenomen dat de lezer een (beperkte) kennis heeft van digitale technieken. "Presentatie en inhoud van dit specialistische boek zijn zodanig dat op TH/TU-niveau het boek goed geschikt is voor zelfstudie", schreef het NBLC over het boek.

160 pag., ISBN 90-6562-034-6 (1984)

COMPUTERARCHITECTUUR door prof.dr.ir. A.J. van de Goor en ir. H.A. Spanjersberg

Dit boekwerk behandelt computerarchitectuur als raakvlak tussen de hardware en de software. Het poogt een achtergrond en verklaring te geven voor instructie-sets, adresseringsvormen, datatypen, interruptsystemen, etc. van traditionele computers. Daarnaast worden kwaliteitscriteria als orthogonaliteit, voorspelbaarheid, etc. waaraan een goede architectuur moet voldoen, behandeld; deze worden bij de behandelde voorbeelden als toets gebruikt. De gevolgde methodiek is toepasbaar op vele gebieden

buiten dat van de computerarchitectuur.
De behandelde stof is voorzien van voorbeelden uit diverse bestaande architecturen om bepaalde concepten te illustreren. Als voorkennis wordt enig inzicht in de PDP-11 of vergelijkbare architectuur en enige achtergrond in programmeertalen verondersteld. De geboden stof is ontstaan uit het college computerarchitectuur aan de TU te Delft en is geschikt voor TU-studenten in hun latere studiejaren en voor TH-studenten in hun laatste jaar.
Databus van februari 1987 beoordeelde Computerarchitectuur als 'een uitstekend boek; goed geschreven, functioneel en behoorlijk volledig.'

248 pag., ISBN 90-6562-025-7 (1985)

INFORMATIETHEORIE
door prof.dr.ir. D.E. Boekee en dr.ir. J.C.A. van der Lubbe

De informatie- en communicatietheorie vormt de grondslag voor de moderne technische ontwikkelingen in de informatica en de telecommunicatie.
In dit boek worden de theoretische grondslagen behandeld die de basis vormen zowel voor het meten van informatie, als ook voor het comprimeren, transporteren, opslaan en beveiligen ervan. Het betreft hierbij zowel digitale als analoge informatie die via symbolen dan wel signalen wordt vastgelegd.
Er wordt tevens ruim aandacht besteed aan een drietal aktuele technische toepassingen van de informatietheorie, namelijk datacompressie, foutverbeterende codes en cryptografie. De behandeling van deze drie toepassingen heeft een introducerend karakter.
Het boek kan worden gebruikt als ondersteuning bij colleges aan de Technische Universiteit, maar is ook zeer geschikt voor gebruik op de HTS en voor zelfstudie.

ca. 250 pag., ISBN 90-6562-082-6
(verschijnt zomer 1988)

ELEKTRONISCHE VERSTERKERS EN PHASELOCK LOOP
door prof.dr.ir. J. Davidse

Deze handleiding omvat een aantal onderwerpen die aan de orde komen in de colleges in de elektronica aan de TU-Delft.
De behandelde stof heeft betrekking op de moderne versterkertechniek en op de inrichting en toepassing van de zogenaamde phaselock loop.
Hoewel de moderne elektronica gebruik maakt van digitale technieken voor de bewerking van elektronische signalen, blijft analoge signaalverwerking onmisbaar bij de bron van de signalen. In het bijzonder op deze plaats in de signaalketen is ruis de grootste vijand van de correcte overdracht van het signaal. Om deze reden is aan dit aspect relatief veel aandacht besteed.
De phaselock loop is een schakeling die vooral van groot belang is in de moderne communicatietechniek.

232 pag., ISBN 90-6562-021-4 (1982)

ELEKTROTECHNISCH METEN
door dr.ir. K.B. Klaassen

De elektrotechniek en met name de elektronica, heeft ons vele hulpmiddelen voor het meten opgeleverd. Daarnaast vormt de elektrotechniek ook zelf een uitgebreid toepassingsgebied voor het meten.
Dit boek over elektrotechnisch meten stelt daarom beide categorieën aan de orde, dus zowel de elektrotechnische meetmiddelen als elektrotechnische metingen.
Het doel van het boek is een zodanige behandeling van de *grondslagen* van het meten, dat, naast het verstrekken van de benodigde *basiskennis*, het *inzicht* in het meten wordt bevorderd. Het einddoel daarbij is het zelfstandig kunnen *oplossen* van allerlei *meetproblemen*.
In dit boek is de aanpak van de vanouds sterk mechanisch en energie-technisch georiënteerde elektrotechnische meettechniek verlaten ten gunste van een meer systeemtechnisch georiënteerde aanpak.
Na een korte samenvatting van de fundamenten van het vak (*meettheorie*) blijkt het voor kwantitatief meten nodig te zijn eenheden af te spreken (*eenheden-stelsels*). Om dit optimaal te kunnen meten (dit is: met de geringst mogelijke inspanning het gestelde doel bereiken) wordt een aantal alternatieve *meetmethoden* besproken.
Een meting verschaft slechts een eindige zekerheid; er worden altijd fouten gemaakt. De *foutentheorie* bespreekt daarom de *soorten fouten, foutenvoortplanting* en *foutenoorzaken* .
Een meetsysteem heeft een bepaalde *structuur* waarin verschillende functies voorkomen (*transductie, signaalbewerking, indicatie* en *registratie*).
Deze meetfuncties worden in het hoofdstuk *elektronische meetmiddelen* besproken. Daarna komen de volledig *elektronische meetsystemen* aan de orde. Hierbij is een belangrijke plaats ingeruimd voor het automatisch *meten met de computer*, waarbij belangrijke zaken als *bemonstering, multiplexing* en *'aliasing'* aan de orde komen.

320 pag., ISBN 90-6562-033-8 (1986)

INSTRUMENTELE ELEKTRONICA
door dr.ir. P.P.L. Regtien

Dit leerboek bestrijkt het zeer brede terrein van de

elektronica voor instrumentele doeleinden. Van de lezer wordt slechts enige wiskundige voorkennis verwacht. Ieder hoofdstuk is verdeeld in tweeën, waarbij het eerste deel als basis geldt, terwijl het tweede deel, dat eventueel overgeslagen kan worden, wat dieper op de stof ingaat. Elk hoofdstuk wordt besloten met een samenvatting en opgaven, waarvan de antwoorden achterin het boek zijn opgenomen.
Enige onderwerpen die aan de orde komen zijn: systeem- en signaalbeschrijvingen, netwerken, filters, elektronische bewerkingssignalen en vensters, oscillatoren, modulatie en analoog-digitaal- en digitaal-analoog- omzetters. Voorts wordt een inleiding gegeven in de digitale techniek en in microprocessoren. Het boek wordt besloten met een hoofdstuk over (computer-)meetsystemen en fout-theorie, uitgewerkte antwoorden op de opgaven.

446 pag., ISBN 90-6562-093-1 (1987)

ELEKTRISCHE NETWERKEN
door ir. A. Henderson

Dit boek is in eerste instantie opgezet als dictaat van het college Elektrische Netwerken voor de eerstejaarsstudenten aan de afdeling Elektrotechniek van de TU-Delft. De aanpak bleek echter al ras ook docenten aan de TH's aan te spreken.
Na een bondige uiteenzetting van de basisbegrippen worden behandeld de netwerkstellingen, bestuurde bronnen, wisselstromen en wisselspanningen, complexe grootheden en enkele eigenschappen van netwerken. Daarna komen aan de orde gekoppelde spoelen en (ideale) transformatoren, driefasensystemen, complexe frequentie, Fourieranalyse en schakelverschijnselen.
Het boek wordt afgesloten met een hoofdstuk over computergerichte analyse.

340 pag., ISBN 90-6562-004-4 (1987)

VRAAGSTUKKEN ELEKTRISCHE NETWERKEN
door ir. A. Henderson

De stof in deze bundel is verdeeld in hoofdstukken, die parallel lopen met het boek Elektrische Netwerken.
De bundel is voorzien van antwoorden.

168 pag., ISBN 90-6562-005-2 (1986)

ELEKTRISCHE SCHAKELVERSCHIJNSELEN
door ir. A. Henderson

Het hoofdstuk schakelverschijnselen uit de theorie van de elektrische netwerken is een dankbaar onderdeel. Enerzijds heeft het de charme van een streng mathematisch betoog, anderzijds komt men voortdurend in aanraking met de fysische werkelijkheid. Soms blijken mathematische begrippen onverwacht een fysische betekenis te hebben. Vele uitgewerkte voorbeelden en vraagstukken zijn opgenomen.

128 pag., ISBN 90-6562-061-3 (1985)

DISCRETE SIGNALEN
door ir. A. Henderson

Digitale signaalbewerking komt steeds meer in de belangstelling. Niet alleen de digitale filters zijn in opmars, ook bij computergerichte netwerkanalyse komt men in aanraking met discrete signalen.
Bij de bestudering van deze stof wordt men getroffen door de analogie met de theorie van de continue signalen, zoals schakelverschijnselen, stationaire toestand, toestandsvergelijkingen, wiskundige transformaties, beginvoorwaarden, polen en nulpunten, enz. Kennis van de theorie van continue signalen is echter niet noodzakelijk voor de bestudering van deze stof. Wel wordt bekendheid verondersteld met gelijk- en wisselstroomtheorie, complexe grootheden, reeksen en (eenvoudige) matrixrekening.

72 pag., ISBN 90-6562-044-3 (1983)

ELEKTRISCHE EN MAGNETISCHE VELDEN
door ir. A. Henderson

In dit beknopte boek wordt de theorie van de elektrische en magnetische velden voor technici behandeld; daarbij wordt naast de noodzakelijke formules ook aandacht gegeven aan de ontwikkeling van het fysisch inzicht.
In een inleidend hoofdstuk wordt een beknopt overzicht gegeven van de vectoralgebra. Daarna volgen de elektrostatica, de elektrische stromen en magnetische velden, en vervolgens de wetten van Maxwell in integraalvorm.
Daarbij komen ook de voor de netwerktheorie noodzakelijke wetten van Kirchhoff naar voren.
Tenslotte volgen de wetten in differentiaalvorm, waarbij tevens wordt ingegaan op de beginselen van de vectoranalyse. Het boek wordt afgerond met 100 vraagstukken, voorzien van antwoorden.

106 pag., ISBN 90-6562-027-3 (1988)

wiskunde: analyse, lineaire algebra, stochastiek en statistiek

ANALYSE
door dr. J.H.J. Almering e.a. geheel herzien door dr.H. Bavinck en dr.ir. R.W. Goldbach

'Analyse' behandelt de analyse op moderne wijze. De hoofdstukken behandelen de grondbegrippen, complexe getallen, limieten en continuïteit, differentiaalrekening, integraalrekening, afbeeldingen, differentiaalvergelijkingen, meervoudige integralen, lijnintegralen, oppervlakteintegralen en reeksen.
Aan het eind van de meeste paragrafen is een aantal oefeningen opgenomen om de lezer vertrouwd te maken met de voorafgaande leerstof. Aan het eind van elk hoofdstuk is een paragraaf met vraagstukken toegevoegd, gerangschikt overeenkomstig de behandeling van de leerstof in het betreffende hoofdstuk.
Het boek doet o.a. dienst bij het analyseonderwijs bij nagenoeg alle afdelingen van de TU-Delft.

592 pag., ISBN 90-6562-078-8 (gebonden) (1987)

ANALYSE
209 tentamenopgaven met uitwerkingen, door dr. H. Bavinck

Aansluitend aan Analyse door dr. J.H.J. Almering e.a. redigeerde dr. H. Bavinck een boek met opgaven en uitwerkingen.
Het aan studenten ter beschikking stellen van vraagstukken met uitwerkingen, betekent didactisch gezien een risico; van de gebruikers moet dan ook, wil men het boekje met vrucht hanteren, een zekere zelfdiscipline worden verwacht.

96 pag., ISBN 90-6562-060-5 (1987)

DIFFERENTIAALVERGELIJKINGEN
220 voorbeelden en opgaven met oplossingen en beknopte theorie, door dr. A. Schuitman

Aan de hand van voorbeelden en vele opgaven wordt in dit boek een overzicht gegeven van de verschillende typen differentiaalvergelijkingen en op toepassingen op partiële differentiaalvergelijkingen.
Tenslotte worden Laplacetransformaties en randwaardeproblemen behandeld.
Het boek is vooral bedoeld als vraagstukkenverzameling naast een college of leerboek.

174 pag., ISBN 90-6562-026-5 (1988)

DICTAAT LINEAIRE ALGEBRA
door dr. G.W. Decnop, ir. H. van Iperen en dr. R. Martini

In een systematische opbouw behandelen de auteurs de lineaire algebra, zoals die wordt gegeven aan de TU-Delft. Daarbij zijn vele voorbeelden en vraagstukken opgenomen.
Vectorruimten, matrices en rekentechnieken in R^n, lineaire afbeeldingen en bilineaire vormen, inwendige productruimten, stelsels lineaire vergelijkingen, determinanten, lineaire operatoren van inwendige productruimten en kwadratische vormen zijn de onderwerpen van de hoofdstukken.

236 pag. (form. 19x26), ISBN 90-6562-036-2 (1987)

MATRIXREKENING
door ir. C.A. den Braber, ir. H. van Iperen, dr. A. Schuitman en dr.ir. M.A. Viergever

Dit boek onderscheidt zich van 'Dictaat Lineaire Algebra' door een directere aansluiting bij de programma-eisen van enkele studierichtingen aan de TU-Delft.
De lineaire algebra en matrixrekening zijn in dit boek vooral toepassingsgericht behandeld, bijvoorbeeld met het oog op vakken als technische mechanica, stelsels lineaire differentiaalvergelijkingen en statistiek.
De volgende hoofdstukken zijn in het boek opgenomen:

- Het oplossen van eenvoudige stelsels lineaire vergelijkingen
- Matrixen, bewerkingen met matrixen
- Analytische meetkunde in de ruimte en het platte vlak
- IR^n & C^n, rang van een matrix, methode der kleinste kwadraten
- Determinanten
- Eigenwaarden en eigenvectoren.

Het is een leerboek met veel oefenstof, waarbij de docent zonodig de weg kan wijzen.

328 pag. (form. 19 x 26), ISBN 90-6562-077-x (1986)

ANALYSE
door prof.dr. B. Meulenbeld en prof.dr. A.W. Grootendorst

In drie kloeke delen presenteren de auteurs een volledige cursus analyse.
Deel 1 beperkt zich in hoofdzaak tot *functies van één veranderlijke*. Beginselen van differentiaal- en integraalrekening, complexe getallen, extreme waarden en het schetsen van krommen, systematische berekening van de primitieven van enige klassen van functies, oneigenlijke integralen, rijen, reeksen, ver-

gelijkingen, numerieke integratie en differentiatie, en hyperbolische functies. Tenslotte wordt kort aandacht besteed aan functies van twee veranderlijken.
Deel 2 behandelt *functies met twee of meer variabelen*. De hoofdstukken gaan over impliciete functies, extreme waarden, vectoranalyse, vlakke krommen, ruimtekrommen, lijnintegralen, meervoudige integralen, integraalstellingen, massa, zwaartepunt en traagheidsmoment, en de gamma- en bêtafunctie.
De differentiaalvergelijkingen zijn het onderwerp van *deel 3*. Gewone differentiaalvergelijkingen, het oplossen van differentiaalvergelijkingen met behulp van machtreeksen, simultane differentiaalvergelijkingen, de Laplace-transformatie, numerieke methoden voor het oplossen van differentiaalvergelijkingen en partiële differentiaalvergelijkingen.
Over deel 1 schreef O. Bottema in het Nieuw Tijdschrift voor Wiskunde van februari 1982:
"Dit werk is voorwaar een leerboek. Bij het schrijven moet de toekomstige lezer voortdurend in de geest aanwezig zijn geweest. De hoge didactische kwaliteit berust op een streven naar evenwicht; de behandeling is exact maar een acribie die het wezenlijke kan verslulieren is vermeden. Evenwicht is er ook tussen de zakelijke tekst en een groot aantal goed gekozen voorbeelden. Ook de typografie werkt mee aan de uitnemende presentatie."

Deel 1, 433 pag., ISBN 90-6562-064-8 (1988)
Deel 2, 344 pag., ISBN 90-6562-065-6 (1986)
Deel 3, 256 pag., ISBN 90-6562-066-4 (1987)

ELEMENTAIRE STATISTIEK
door ir. J. van Soest

Het bekende boekje van ir. Van Soest richt zich vooral op de *toepassingen* van de statistiek. Achtereenvolgens worden behandeld de beschrijvende statistiek, de kansrekening, stochastische variabelen, populatie en steekproef, de binomiale verdeling, de Poissonverdeling, de normale verdeling, functies van continue stochastische variabelen, de centrale limietstelling, statistische toetsen voor ligging, toetsen voor verschil in ligging en toetsten voor varianties, regressie- en correlatierekening. Tal van vraagstukken zijn opgenomen.

176 pag., ISBN 90-6562-003-6 (1987)

aanvulling
ELEMENTAIRE STATISTIEK
door ir. J. van Soest, ir. A.J. Meelen en ir. J.M.G. Vermeulen

Ten behoeve van een meer mathematische benadering van de statistiek is een aanvulling beschikbaar, die een verdieping inhoudt van hetgeen in de hoofdstukken 3, 7, 8 en 13 van Elementaire Statistiek is weergegeven.
63 pag., ISBN 90-6562-006-0 (1987)

INLEIDING KANSREKENING EN STATISTIEK
door ir. S.J. de Lange

In dit boek is er van uitgegaan dat de kansrekening niet alleen maar ondersteuning is van de statistiek.
In de eerste hoofdstukken wordt een algemene inleiding in de kansrekening gepresenteerd: kansrekening, stochastische variabelen, een-dimensionale verdelingen, meer-dimensionale verdelingen en verdelingen van functies van stochastische variabelen.
Daarna worden statistische standaardtechnieken behandeld: populatie en steekproef, steekproefverdelingen, punt- en intervalschatters, toetsen van hypothesen en enige verdelingsvrije toetsen.
Het boek wordt afgesloten met een groot aantal vraagstukken met antwoorden en de voor het gebruik benodigde tabellen.
Enige kennis van meervoudig integreren is bij het bestuderen van deze stof nodig; het boek is dan ook bruikbaar in het tweede jaar van TU- en in het vierde jaar van sommige TH-opleidingen.

ca. 200 pag., ISBN 90-6562-095-8
(verschijnt zomer 1988)

GREPEN UIT DE GESCHIEDENIS VAN DE WISKUNDE
door prof dr. A.W Grootendorst

Dit werk bevat opstellen over zeer diverse onderwerpen uit de geschiedenis van de wiskunde.Voor een deel zijn het verhandelingen die de auteur reeds eerder in vaktijdschriften deed verschijnen; er zijn echter ook stukken opgenomen die speciaal voor dit boek zijn geschreven.
Na een algemeen oriënterend hoofdstuk volgen enkele opstellen over de wiskunde bij de Grieken. waarin wordt getoond hoe de Grieken met scherpzinnige en doorzichtige methoden fundamentele resultaten wisten te bereiken. Tot dit gedeelte behoort een artikel over het omgaan met getallen in de oudheid en een beschouwing over rekenkunde en de 'meetkundige algebra' en de oorsprong van de woorden parabool, hyperbool en ellips.
De bundel bevat ook de vertaling (met oorspronkelijke tekst en commentaar) van enkele in het Latijn geschreven brieven, nl. die van Johan Hudde (1628–1704), burgemeester van Amsterdam, over het bepalen van maxima en minima en een brief van Hendrik van Heuraet (1634–1660?), waarin voor het eerst de lengte van een kromme wordt berekend. Verder zijn er stukken gewijd aan Leonhard Euler (1707–1783), Daniel Bernoulli (1701–1782) en aan

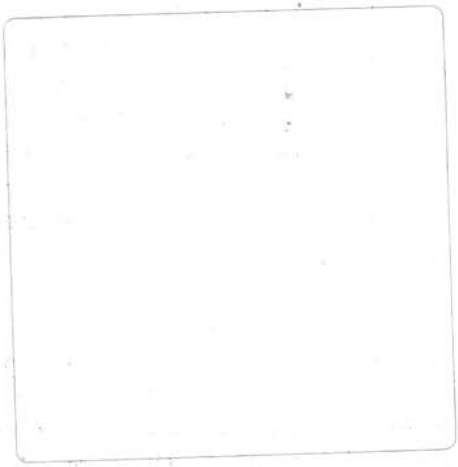
de nagenoeg onbekende Pierre Louis Wantzel (1814–1848) die als eerste bewees dat een willekeurige hoek niet in drie gelijke delen verdeeld kan worden met behulp van passer en liniaal alleen, een eeuwenoud probleem waarvan de oplosser in de vergetelheid is geraakt. Zijn naam komt zelfs niet voor in de Dictionary of Scientific Biography!

ca. 200 pag., ISBN 90-6562-94-x
(verschijnt april 1988)

Andere publicaties op het terrein van de wiskunde:

Vectoranalyse, door prof.dr. R. Timman en dr. J.W. Reijn; 164 pag.

Vraagstukken over Waarschijnlijkheidsrekening, door dr. P.J.A. Kanters; 178 pag.



Bedrijfszekerheid speelt, bij een toenemende complexiteit van systemen, een steeds belangrijkere rol. Voorbeelden van gebieden in de techniek waar de bedrijfszekerheid een zeer belangrijke grootheid is, zijn de vliegtuigindustrie en elektronische geïntegreerde schakelingen (zoals microprocessors) die uit een enorm groot aantal componenten bestaan.

Dit boek behandelt elementaire theorie waarmee men zich een basis kan eigen maken. Behalve *deterministische* bedrijfszekerheidstechniek (het bepalen van een faaloorzaak) en *statistische* bedrijfszekerheidstechniek (het statistisch bepalen van parameters als: de gemiddelde levensduur, de onderhoudbaarheid, de onderhoudstrategie en het al dan niet nuttig zijn van enige vorm van onderhoud) worden evaluatiemethoden (voornamelijk faalbomen) behandeld. Het boek besluit met ruim 40 bladzijden met uitwerkingen van de opgaven en een uitgebreide literatuurlijst.

ISBN 90-6562-073-7

DELFTSE UITGEVERS MAATSCHAPPIJ – 1988