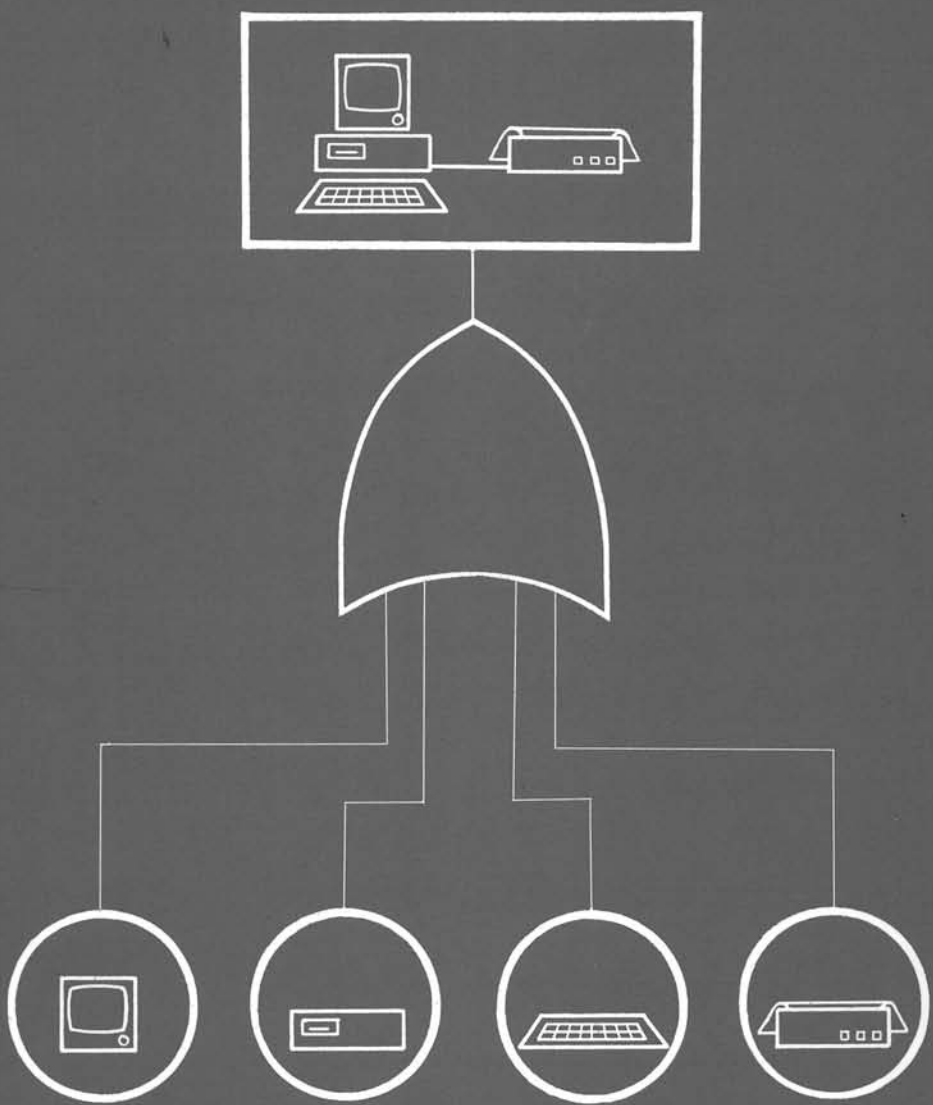
Bedrijfszekerheidstechniek

prof. dr. ir. J. van Dam
drs. F.J.M. Raaijmakers
ir. R.A. Bosman



Delftse Universitaire Pers

Bedrijfszekerheidstechniek

Bedrijfszekerheidstechniek

prof. dr. ir. J. van Dam
drs. F. J. M. Raaijmakers
ir. R. A. Bosman

Delftse Universitaire Pers / 1990

Uitgegeven en gedistribueerd door

Delftse Universitaire Pers
Stevinweg 1
2628 CN DELFT
Telefoon (015) 783254

CIP-GEGEVENS KONINKLIJKE BIBLIOTHEEK, DEN HAAG

DAM, J. van

Bedrijfszekerheidstechniek/J. van Dam. — Delft: Delftse Universitaire Pers. — Ill
Met lit. opg. — tweede herziene druk
ISBN 90-6275-579-8
SISO 640 UDC 62:658.58 — NUGI: 684
Trefw.: bedrijfszekerheid.

INHOUDSOPGAVE

Betrouwbaarheid wordt als een deugd ervaren indien het een persoon betreft, als een kwaliteit zo er sprake is van een technisch systeem.
Betrouwbaarheidstheorie, (reliability theory, in de internationale literatuur) is een deelgebied van de Operationele Analyse met als taak de mate, waarin een gestructureerd systeem aan zijn doelstellingen beantwoordt, te karakteriseren door één of meerdere kwaliteitsgetallen.

De theorie heeft in de laatste drie decennia een snelle ontwikkeling doorgemaakt, een uitgebreide literatuur is momenteel beschikbaar.
Als een "engineering discipline" heeft het zijn waarde bewezen en is het stadium bereikt, waarin de ideeën en principes van de betrouwbaarheidstheorie niet meer gemist kunnen worden in het hogere technische onderwijs.

Deze monograaf is de eerste die beschikbaar is voor het Nederlandse taalgebied en op grond hiervan al reeds aan te bevelen. Er is echter veel meer wat deze inleiding aantrekkelijk maakt. De stijl is helder en eenvoudig, de begripsvorming wordt ondersteund door vele voorbeelden, de modellen zijn goed gekozen, de nadruk ligt op inzicht en doorzicht; met een minimaal gebruik van wiskundige technieken slaagt de auteur er in het karakter van de vereiste berekeningen doeltreffend te presenteren.

Een voortreffelijke inleiding, die de lezer een goed inzicht verschaft in de mogelijkheden en doelstellingen van de betrouwbaarheidstheorie.

Prof.dr.ir. J.W. Cohen,
Hoogleraar
Operationele Analyse,
Rijksuniversiteit Utrecht.

IX

VOORWOORD BIJ DE EERSTE DRUK

In de wereld van de techniek gold (en geldt trouwens nog steeds) de aloude, klassieke vraag: "*Hoe* werkt een systeem?"
Het technische onderwijs van weleer sloot zich hierbij aan door in het lesprogramma de behandeling van allerlei fundamentele vakgebieden op te nemen, zoals natuurkunde, sterkteleer, wiskunde, elektronica, etcetera, met behulp waarvan de *werking* van een systeem kon worden verklaard.

Vanwege (a) allerlei droeve operationele situaties, (b) vaak extreem hoge onderhoudsoffers en (c) inmiddels (onder maatschappelijke druk) verrichte risico-analyses is van lieverlee een andere vraagstelling naar voren gekomen, namelijk: "*Waarom* werkt een systeem (niet)?"

Dit betekent, dat een verlegging van het lesprogrammatische zwaartepunt bij het technische onderwijs noodzakelijk is gebleken en de technische student — naast bovengenoemd analytisch onderwijs — expliciet in kennis wordt gebracht met:

a. De aspecten van *Bedrijfszekerheid*, dus met de parameters, die het proces van uitval en voortijdig verval van een systeem beheersen.
b. De aspecten van *Onderhoud*, dus met de instandhouding, ook als logistiek-economisch probleem.
c. De aspecten van *Veiligheid*, dus met de inventarisatie van kritieke delen en kansen op calamiteiten voor mens en omgeving als gevolg van een storing.

In het kader van deze doelstelling moet dit boek worden geplaatst. Het is onder meer bedoeld voor:

1. Diegene, die — al of niet door industriële ervaring gerijpt — met vele van de bovengenoemde aspecten op de hoogte zijn (of willen zijn) en het zinvol achten, (nog eens) in verzamelde vorm er kennis van te nemen.
2. Het moderne technische onderwijs, dat pretendeert vandaag op te leiden voor de wereld van morgen. Het is de bedoeling, dat — mede afhankelijk van de studierichting — de docent(e) de leerstof vanuit zijn (of haar) eigen discipline zal behandelen en met praktische voorbeelden zal larderen.

Bij het verzorgen van cursussen, lezingen, colleges (aan de TU te Delft en aan het Koninklijk Instituut voor de Marine) en contacten met de industrie is het de schrijvers gebleken, dat er een duidelijke behoefte bestaat aan een handzaam werkje op het gebied van de bedrijfszekerheidstechniek, waarvoor de belangstelling de laatste jaren zozeer is gestegen. Dit gegeven heeft stimulerend gewerkt op de verschijning van dit boek, waarin allerlei hierbij opgedane ervaringen en ideeën zijn verwerkt.

Tenslotte moge nog de volgende opmerkingen worden gemaakt:

i. Het boek is als inleiding bedoeld. Dat wil zeggen, dat vele zaken, die ter sprake worden gebracht, vaak tot verdere studie en nadere bezinning oproepen, waartoe een (beknopte) literatuurlijst is toegevoegd. Door de enorme uitgebreidheid van het onderwerp moesten zelfs verschillende delen onbesproken blijven (zoals het testen op bedrijfszekerheid, etc.).

ii. Bij de wiskundige behandeling van bedrijfszekerheidsmodellen is er van uitgegaan, dat de lezer(es)/student(e) enigszins op de hoogte is van de elementaire kanstheorie en verder enige kennis bezit omtrent de toepassing van Laplace-transformatie en eenvoudige Booleaanse algebra. In het licht van de huidige lesprogramma's bij het technische onderwijs is deze veronderstelling redelijk te noemen. Mocht dit desondanks niet het geval zijn, dan is in het derde hoofdstuk een eenvoudiger methode behandeld die (nog) minder mathematische voorkennis veronderstelt en waarmee men zonder Laplace in staat is elementaire configuraties door te rekenen.

iii. De schrijvers houden zich voor opmerkingen en suggesties vanuit de industrie en het onderwijs ten sterkste aanbevolen.

Den Helder, voorjaar 1986,
Prof.dr.ir. J. van Dam.

BIJ DE TWEEDE DRUK

Deze tweede druk, die door de grote vraag naar dit leermiddel en door de nog steeds groeiende belangstelling voor dit vakgebied noodzakelijk is gebleken, is op vele punten uitgebreid, verdiept en geactualiseerd.

Dank aan de beide collegae, die met hun vakkennis en kritische zin een grote bijdrage aan deze vernieuwing hebben geleverd; hun namen zijn deswege op de titelpagina vermeld.

Ook nu weer houden de schrijvers zich voor opmerkingen en suggesties vanuit de industrie en het onderwijs ten zeerste aanbevolen.

Den Helder, najaar 1989,
Prof.dr.ir. J. van Dam.

1 ENIGE DEFINITIES

1.1 Inleiding

Sinds onheugelijke tijden is de mensheid geconfronteerd met het falen van haar (technische) produkten. Helaas is dat heden ten dage nog niet veranderd. Een ieder onzer weet dat de apparatuur, waarmee wij ons in de gang van alle dag hebben omringd, vroeg of laat (en dan meestal vroeg) kapot gaat. Daarmee wil dan gezegd zijn, dat deze systemen niet helemaal, óf helemaal niet meer de functie kunnen vervullen, waartoe ze zijn geproduceerd.

De TV, die op de voetbalavond plotseling uitvalt; de auto, die des morgens niet starten wil; de laatste punaise die krom is en het alarmlampje dat niet brandt bij een dreigende calamiteit. Het zijn enige van de ontelbare storingsgevallen, die wij als zodanig in de praktijk herkennen.

Mede vanwege dit droeve gegeven — met alle nadelige gevolgen daarvan, zoals stagnaties, onveiligheid en oplopende onderhoudskosten — is men een jaar of twintig geleden intensief gaan speuren naar mogelijke faaloorzaken en is men zich bovendien gaan bezinnen, langs welke weg en op welke wijze de *uitval* en het *voortijdig verval* van onze technische verworvenheden zouden kunnen worden bestreden.

Deze activiteiten spelen zich af op een gebied, dat met *bedrijfszekerheidstechniek* (reliability engineering) wordt aangeduid. Dit (zich nog steeds uitbreidend) terrein is van lieverlee een aantal wiskundige en organisatorische technieken en methoden gaan omvatten, die de opvoering van:

de Bedrijfszekerheid de Onderhoudbaarheid en de Veiligheid

van technische systemen beogen. Welke parameters daarbij een rol spelen en hoe deze kunnen worden gekwantificeerd zal in onderstaande paragrafen ter sprake worden gebracht.

1.2 Aandachtsgebieden bedrijfszekerheidstechniek

De bedrijfszekerheidstechniek omvat een enorm studiegebied met vele aspecten, die nauw verband houden met het schatten, meten, rapporteren van en reageren op faalverschijnselen en uitvalskansen en met het voor berekening toegankelijk maken van operationele modellen.

We zullen hieronder enige aandachtsgebieden opsommen, waarbij we nog deze kanttekening willen maken, dat het niet doenlijk is al deze facetten in het kader van dit boekwerk te behandelen.

A. Het *theoretische* gedeelte, zoals het omschrijven van hanteerbare operationele grootheden (bedrijfszekerheid, beschikbaarheid, etc.), het definiëren van afgeleide wiskundige begrippen (failure rate, hazard rate, etc.) en het ontwikkelen van berekeningsmethodieken voor onder andere een optimale reservedelenvoorziening en de juiste onderhoudsstrategieën.

B. Het *analyseren* van de inmiddels bereikte bedrijfszekerheid door middel van het steekproefsgewijs meten en testen op overlevingskans van een beperkt aantal produkten. Ook het verzamelen van faalgegevens en het intelligent verwerken hiervan behoren hiertoe, evenals de terugkoppeling van de testresultaten naar de ontwerpfase van toekomstige produkten. Voor de manier, waarop de *inherente* bedrijfszekerheid van een systeem kan worden vergroot, wordt verwezen naar paragraaf 1.13.
Hoewel wij ons in het hierna volgende tot de overlevingskans van de hardware zullen beperken, moet worden opgemerkt, dat bij de bepaling van de bedrijfszekerheid van een modern systeem de *software-kwaliteit* een opkomende rol speelt (zie paragrafen 1.5 en 1.6).

C. Het formuleren van een *onderhoudsconcept*, dat wil zeggen van een samenstel van doordachte maatregelen tot *instandhouding* van apparatuur en tot bevordering van de veiligheid daarvan.

1.3 Definitie bedrijfszekerheid

In de hieronder volgende opmerkingen wordt onder *bedrijfszekerheid* verstaan:

> *de kans, dat een systeem een gespecificeerde functie (of functies) storingsvrij verricht gedurende een gedefinieerd interval van een levensduurvariabele, op voorwaarde dat aan gespecificeerde omgevingscondities is voldaan.*

In de Engelse literatuur wordt de *reliability* omschreven als: *the probability of performing without failure a specified function under given conditions for a specified period of time.*

Ter toelichting:

- Met de genoemde levensduurvariabele wordt in verreweg de meeste gevallen de *tijd* bedoeld. Met R (300 h) = .95 wordt dan aangegeven, dat de kans, dat een systeem gedurende 300 h naar behoren functioneert, 95% bedraagt. Er bestaan overigens nog andere relevante grootheden om de overlevingskans te beschrijven, zoals de kans, dat een relais goed werkt gedurende 100.000 *omschakelingen* of dat een autoband 40.000 *kilometer* zonder problemen zijn functie vervult.

- Een *systeem* is een samenhangende en doelgerichte verzameling van elementen (entiteiten), waartussen relaties bestaan, op elk niveau van complexiteit. We hebben hierbij te doen met een zogenaamd *open* systeem, dat in wisselwerking staat met zijn (omringende) omgeving, daarvan door de "systeemgrens" afgescheiden. Het systeem beïnvloedt de omgeving en wordt zelf ook door die omgeving beïnvloed.
  Bij het begrip systeem wordt meestal aan een technisch systeem gedacht, opgebouwd uit componenten, units, subsystemen, modules, etcetera. Maar het is inmiddels gebleken, dat met name de mens een duidelijke rol speelt in het hele operationele gebeuren en als zodanig bij voorkeur — zoals bij reparatiemodellen — binnen de systeemgrens geplaatst dient te worden. Door het (al of niet verkeerd) gebruik, door de wijze van bediening, fabricage en onderhoud heeft hij (of zij) een enorme invloed op de bedrijfszekerheid van een systeem gedurende een bepaalde periode.

* De bedrijfszekerheid van onze auto wordt — naast uiteraard de kwaliteit van het technisch ontwerp van de wagen — sterk bepaald door menselijke factoren, zoals rijstijl, de zorgvuldigheid van het garagegebeuren en de kwaliteitsbeheersing tijdens de fabricage.

□ In bovenstaande definitie van bedrijfszekerheid moet blijkbaar de te verrichten functie (of functies) gespecificeerd zijn. Dat wil zeggen, dat de systeemprestaties scherp omschreven dienen te zijn, teneinde tot de falende toestand te kunnen besluiten. Bij een plotseling optredende storing (zoals een lekke band) is het functieverlies wel duidelijk, maar bij een geleidelijke achteruitgang van de conditie is dat niet altijd het geval. Van een auto bijvoorbeeld wordt een vervoersfunctie verwacht. Is deze nog mogelijk bij een kapotte voorruit of bij een op drie cylinders lopende motor? Moet een fiets zonder zadel of zonder verlichting tijdens de nachtelijke uren als een falend systeem worden beschouwd? Hoe dan ook, het is duidelijk dat voor een zinvolle berekening van de overlevingskans van een systeem de grenzen van het nog juist functioneren eenduidig bepaald moeten zijn.

□ Hetzelfde geldt in wezen voor de *omgevingscondities*, die in de omschrijving van bedrijfszekerheid zijn genoemd. Als een systeem in een *verkeerde* (want niet afgesproken) omgeving functioneert, kan het versneld uitvallen of verouderen. Hierbij kan gedacht worden aan een te hete of te natte omgeving, een te hoge voedingsspanning, te grote ingangssignalen of een te grote belasting. Maar ook een verkeerd gebruik (*misuse*) en onjuist onderhoud vallen buiten het vastgestelde omgevingsgebied en zijn daarom in de bedrijfszekerheidsdefinitie uitgesloten.

Tenslotte moge nog worden opgemerkt dat — met name in het contractuele verkeer tussen fabrikant en afnemer — het van bijzonder groot belang is alle bovengenoemde zaken precies te omschrijven in verband met eventuele latere juridische en financiële consequenties (wettelijke aansprakelijkheid voor en garantie van produkten, etc.).

1.4 Enkele operationele grootheden

Alvorens tot de wiskundige formulering van enige fundamentele begrippen over te gaan, zullen we eerst nog enige aandacht aan enkele operationele grootheden schenken.

Van de *bedrijfszekerheid* (reliability) R(t) van een systeem is in de vorige paragraaf de definitie vermeld. Huiselijk omschreven als de kans, dat dit systeem "het" nog ten tijde t doet, mits niet verkeerd gebruikt.
Voor het wederom in bedrijf brengen van een falend systeem is (correctief) *onderhoud* nodig, trouwens voor het in bedrijf houden soms eveneens (preventief). Zie in dit verband paragraaf 5.1 en verder. Essentieel in ieder geval is hierbij het *menselijk ingrijpen* en we spreken in dit verband dan ook van een *bewaakt* systeem.

* Dat menselijke tussenkomst bij een *niet-bewaakt* systeem ontbreekt kan *onontkoombaar* zijn (zoals bij onbemande vaartuigen) of kan economisch verdedigbaar zijn, òf vanwege de lage kostprijs (zoals bij de flitslamp, de punaise en andere wegwerpartikelen) òf vanwege hoge reparatiekosten (bijvoorbeeld à *f* 50,= per uur bij een radio van ruim *f* 100,=).

De *onderhoudbaarheid* (maintainability) M(t) van een systeem is gedefinieerd als *de kans, dat dit systeem na een storing in een bepaalde periode wederom in de werkende toestand kan worden teruggebracht.* In het Engels: the maintainability is the probability that a failed system will be restored to operable condition within a specified time interval.

* Het is evident, dat de onderhoudbaarheid, die — evenals de bedrijfszekerheid — als een *systeemeigenschap* dient te worden herkend, reeds in de *ontwerpfase* in hoge mate wordt beïnvloed.
  De bereikbaarheid van de onderdelen, de verkrijgbaarheid hiervan gedurende de *bedrijfsperiode* en de mogelijkheid tot een snelle verwisseling van falende subsystemen dankzij een modulaire opbouw zijn evenzovele aspecten, die een snel herstel bevorderen.

Het *risico* (risk) heeft te maken met de *gevolgen* van een optredende storing voor mens en omgeving en voor het milieu. We zullen dan ook onder risico *de kans verstaan, dat het systeem zodanig faalt, dat mens, milieu en andere systemen daarvan gevaarlijke of schadelijke gevolgen ondervinden.*

Nauw verbonden met risico is het begrip veiligheid. Risico is een objectief begrip: deze kansgrootheid kan aan de hand van historische faalgegevens

worden berekend (hoe groot is bijvoorbeeld de kans dat een olietanker op een bepaald traject dusdanig beschadigd wordt dat dit in een milieuramp resulteert).
Veiligheid (safety) S(t) *is de mate waarin het risico aanvaardbaar wordt geacht.* Dit begrip is dus subjectief, zuiver een waarde-oordeel over de gevaren die het functioneren van onze woongemeenschap dan wel ons systeem bedreigen. Er zijn gebeurtenissen met een betrekkelijk groot risico die toch als veilig worden ervaren: het vergeten van een tentharing op vakantie of het droogkoken van een ketel theewater.
Zo zijn er ook gebeurtenissen met een heel klein risico die toch niet veilig worden geacht, bijvoorbeeld het plakken van een verkeerd etiket op een flesje medicijnen of chemicaliën. Of erg veilige gebeurtenissen met een klein risico: het noodlottig falen van de televisie op de avond van het favoriete programma.
Het blijkt hieruit dat een *risico-analyse* onvoldoende informatie biedt omtrent de te nemen maatregelen ter beveiliging van een systeem: daartoe moet onderzocht worden hoe *kritiek* ieder risico is (criticality analysis) waaruit volgt hoe veilig het systeem is. In een later stadium zullen we hierop terugkomen (paragraaf 8.4).

Als laatste operationele grootheid noemen we de *beschikbaarheid* (instantaneous availability) A(t) van een systeem. Hieronder verstaan we *de kans dat het systeem in bedrijf (ofwel bedrijfsgereed) is op een willekeurig tijdstip, waarop een beroep op dit systeem wordt gedaan.* In het Engels: the probability that at time t the system will be available for mission. Zie in dit verband paragraaf 7.2.
Het is hierbij goed te wijzen op het verschil tussen het zojuist genoemde begrip A(t) en de grootheid bedrijfszekerheid R(t). Met R(t) drukken we de kans uit op een storingsvrij opereren *gedurende* het interval (0,t), terwijl A(t) slechts de kans op storingsvrij zijn *òp* het tijdstip t aangeeft.

* Zo zal de trotse bezitter van een gloednieuwe personal computer er van overtuigd zijn dat dit apparaat over drie jaar zeer waarschijnlijk voor werk beschikbaar zal zijn; een gedegen marktonderzoek en het niet willen besparen bij de aankoop heeft de eigenaar deze overtuiging gegeven. A (drie jaar) $\simeq$ 95%, zo luidt de uitspraak van de eigenaar in onze termen uitgedrukt.
  Tijdens de voorbereiding van de aankoop heeft hij echter ook met diverse leden van de computer hobbyclub gesproken en daarvan heeft hij geleerd dat (kleine) storingen bij deze apparatuur vrij gebruikelijk zijn. De kans

om binnen de drie jaar tenminste één storing mee te maken schat hij (helaas) vrij groot in, dus op dit punt luidt zijn formulering R (drie jaar) $\simeq$ 25%.

Voor apparatuur waarbij herstel na defect raken om welke reden dan ook niet mogelijk is geldt dat R(t) en A(t) steeds dezelfde waarde aannemen. Zo zullen de bedrijfszekerheid en de beschikbaarheid van serviesgoed in het algemeen gelijk aan elkaar zijn.
In dit boekje zal onder de *uptime* van een systeem de periode worden verstaan, waarin een systeem functioneert dan wel *kan* functioneren. Zoals een auto, die daadwerkelijk in gebruik is of anders ten gebruike (in de garage) gereed staat.

De *downtime* daarentegen betreft het tijdsverloop, waarin een bewaakt systeem gedurende stilstand wordt onderhouden. Met name bij grote systemen is het daarbij van belang de totale onderhoudstijd te onderscheiden in een *actief* deel (dat is de tijd, die nodig is voor het foutzoeken en het feitelijk herstel) èn in een *logistiek* deel (dat is de tijd, nodig voor de voorbereiding van de reparatie, zoals de toevoer van het benodigde personeel en de vereiste onderdelen).

* Er zij nog op gewezen, dat de reparatietijd alleen met de downtime samenvalt, als er geen reserve voorhanden is. We hebben dan te doen met het geval, dat òf het systeem òf de reparateur werkt. Bij aanwezigheid van reservedelen is het uiteraard mogelijk, dat er herstelwerkzaamheden plaatsvinden, terwijl het systeem door het gebruik van *spare parts* toch in bedrijf is.

1.5 Software reliability

Door de steeds toenemende aantallen toepassingen van de computer is de software (en de kwaliteit daarvan) in de techniek en in het maatschappelijk bestaan een steeds grotere rol gaan spelen. En dat niet alleen op financieel gebied, waar blijkt dat de hoge kosten van de ontwikkeling en het onderhoud van software-produkten die van de hardware vaak vele malen te boven gaan. Maar ook op operationeel gebied is inmiddels gebleken, dat een fout of een virus in de programmatuur minstens evenveel ellende of schade teweeg kan brengen als een storing in de hardware ten gevolge van een componentuitval, van een foutieve bediening of van onvolkomen onderhoud. Het zal dan ook niet verbazen, dat de laatste jaren een discipline zich is gaan

ontwikkelen, die met software reliability engineering wordt aangeduid en die onder meer ten doel heeft zich bezig te houden met storingen in de programmatuur, de kansen daarop en de vermijding, opsporing en bestrijding daarvan.

Men kan zich afvragen of de benaming software reliability wel juist is. Reliability is namelijk in paragraaf 1.3 omschreven als de kans, dat (in een bepaalde periode en bij normale behandeling) geen storing in de hardware optreedt. Bij software treffen we een binaire situatie aan: òf er zit een fout in de programmatuur vanaf den beginne, òf er zit géén fout in.
De kansneming — zoals door het begrip reliability verwoord — zit 'm dan ook niet in een storing, die kàn optreden, waarbij (zoals bij hardware) het systeem een toestandsverandering ondergaat, maar in de mogelijkheid, dat *een reeds aanwezige fout bij het doorlopen van het programma wordt ontmoet.* Kenmerkend daarbij is dat de toestand van de software vóór en na de ontdekking van een fout dezelfde is; een toestandsverandering vindt plaats, indien de fout wordt hersteld. De *omschrijving* van software reliability is dan ook als volgt: the probability of a given software operating for a specified time period, without a software error, when used within the design limits on the appropriate machine.

1.6 Hardware- en software-storingen

De ontwikkeling van de bedrijfszekerheidstechniek voor de hardware is (uiteraard) aanzienlijk ouder dan die voor de programmatuur. Het ligt dan ook voor de hand dat vele pogingen zijn ondernomen (en nog steeds worden ondernomen op dit nog vrij braak liggend terrein) om de inmiddels verkregen kennis, vaardigheid en methodieken van de hardware reliability engineering op het gebied van de software over te brengen en toe te passen. Het blijkt echter dat deze vertaling moeizaam verloopt en trouwens maar beperkt mogelijk is, vanwege de significante verschillen tussen de beide gebieden. We zullen hieronder enkele noemen.

Hardware	Software
1. Fouten kunnen worden veroorzaakt door tekortkomingen in *ontwerp*, *produktie*, *gebruik en onderhoud*.	1. Fouten komen alléén voor door vergissingen in het ontwerpstadium. Produktie (dit is het copiëren), gebruik en onderhoud hebben (praktisch) geen invloed.
2. *Slijtageverschijnselen* (of andere energie-gebonden verschijnselen) kunnen optreden. Soms is het mogelijk te alarmeren voor een er aankomende storing (waarschuwingsinterventie).	2. Slijtage is hier onbekend. Softwarestoringen dienen zich zonder waarschuwing aan.
3. *Reparatie* brengt een systeem in een conditie, die niet optimaal behoeft te zijn. Een uitval daarna blijft weer mogelijk.	3. Reparatie werkt hier weer binair: als de reparatie slaagt, is de software optimaal, als er geen andere fouten meer in zitten. Een uitval is dan niet meer mogelijk. Trouwens, het is de vraag of reparatie hier wel het juiste woord is. Het is een herprogrammering, met de stille hoop, dat daardoor de fout geëlimineerd is en er geen andere fouten zijn geïntroduceerd.
4. De bedrijfszekerheid wordt mee bepaald door *omgevingsfactoren*.	4. Externe factoren hebben géén invloed op de software reliability (behalve uitzonderlijke toestanden, zoals verwoesting door brand, etc.).
5. Hardware reliability kan vaak krachtig door toepassing van *redundantie* worden verbeterd.	5. Het gebruik van twee volkomen identieke programma's op een redundantiewijze heeft geen enkele zin, omdat beide storingen volkomen gekoppeld zijn in hun optreden. Iets anders is, als het gaat om een parallel

(Vervolg)

Hardware	Software
	programma, dat door andere ontwerpteams volledig onafhankelijk is ontwikkeld.
6. Technieken, die bijvoorbeeld resulteren in een lijst van *kritieke delen*, zijn bijzonder nuttig bij het evalueren van de overlevingskans bij hardware.	6. Deze methodieken zijn bij software niet van toepassing. Zwakke delen bestaan niet. Elke statement kan in principe goed zijn (en blijven). En anders is deze niet zwak of kritisch, maar gewoon fout.
7. De bedrijfszekerheid van hardware kan *van tevoren* redelijk met behulp van ontwerp en gebruiksgegevens worden benaderd.	7. De bedrijfszekerheid van software kan nauwelijk worden voorspeld, omdat deze slechts afhangt van *menselijke* factoren in het ontwerpstadium (bijvoorbeeld de vakbekwaamheid van de ontwikkelaars). Ook is het mogelijk dat de software wordt toegepast op gevallen, die bij het ontwerp niet werden voorzien.

Vele mathematische modellen zijn de laatste jaren ontwikkeld om de storingskansen van de software te evalueren. Hoewel de behandeling hiervan buiten het bestek van dit boekwerk valt, kunnen in dit verband worden genoemd: (a) het Shooman-model, (b) het Markov-model, (c) het Jelinski-Moranda model en (d) het Schick-Wolverton model.

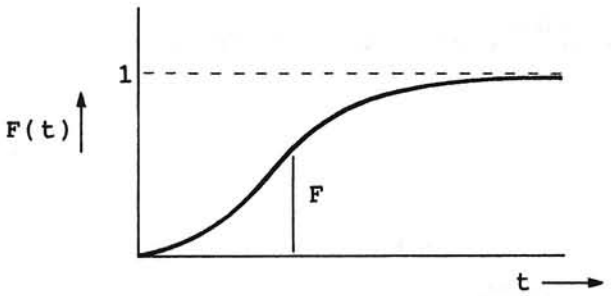
1.7 Enkele afgeleide grootheden

Stel de levensduur van een eenheid (en dat kan zijn een systeem, een subsysteem, een component, etc.) is $\underline{X}$, een niet-negatieve, stochastische variabele. We veronderstellen dat deze veranderlijke een continue verdeling bezit in het gebied $(0,\infty)$. Ook nemen we aan dat er geen onderhoud, in welke vorm dan ook, aan deze eenheid wordt gedaan.

A. Onder de (*cumulatieve*) *verdelingsfunctie* F(t) verstaan we de uitvalskans voor de periode vanaf de in-bedrijfstelling tot aan het tijdstip t, in formulevorm

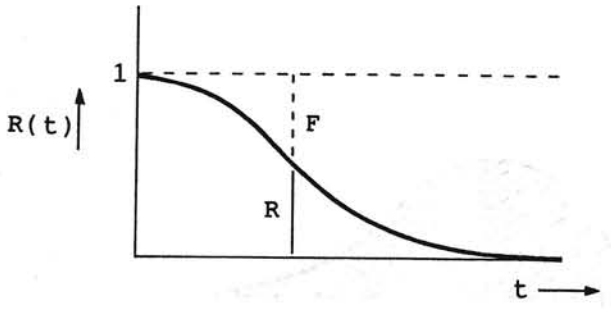
$$F(t) = P(\underline{X} \leq t).$$

Dit begrip wordt ook wel aangeduid met de *bedrijfsonzekerheid* (in de Nederlandse literatuur soms sneuvelkans).



De functie F(t) zal een monotoon niet-dalende functie zijn met F(0) = 0 en $\lim_{t\to\infty} F(t) = 1$.

B. De complementaire kans 1 - F(t) = P($\underline{X}$ > t) geeft de situatie weer waarbij de eenheid gedurende het interval (0,t) niet is uitgevallen en dus naar behoren heeft gefunctioneerd; we zien dus dat R(t) = 1 - F(t) de *bedrijfszekerheid* of de *overlevingskans* van de eenheid beschrijft.



C. Vaak zal de functie F(t) bepaald kunnen worden met behulp van een andere functie f(t), de *kansdichtheidsfunctie* genaamd (Engels: probability density function = pdf).
Het verband wordt als volgt gegeven

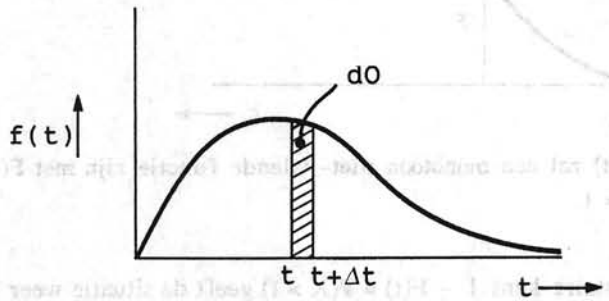
$$F(t) = \int_0^t f(u)\,du.$$

Eenvoudig is in te zien dat $f(t) = F'(t) \geq 0$ en $\int_0^\infty f(u)\,du = 1$; overigens geldt ook $f(t) = -R'(t)$.
Bovendien geldt (mits Δt klein)

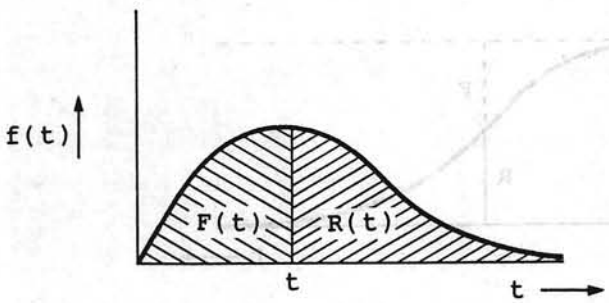
$$f(t) = F'(t) \approx \frac{F(t + \Delta t) - F(t)}{\Delta t} = \frac{P(\underline{X} \leq t + \Delta t) - P(\underline{X} \leq t)}{\Delta t};$$

$$f(t) \approx \frac{P(t \leq \underline{X} \leq t + \Delta t)}{\Delta t} \Rightarrow P(t \leq \underline{X} \leq t + \Delta t) \approx f(t)\,\Delta t.$$

Grafisch:



Het gearceerde oppervlakje stelt dan de kans voor dat de levensduur $\underline{X}$ een waarde aanneemt uit het interval $(t, t + \Delta t)$.



Hierboven is het verband tussen de drie tot nu toe behandelde begrippen aangegeven.

D. Voorts blijkt de *hazard rate* (conditionele faaldichtheid)

$$z(t) = \lim_{\Delta t \to 0} \frac{P(t < \underline{X} \leq t + \Delta t \mid \underline{X} > t)}{\Delta t}$$

een zeer belangrijke rol te spelen bij de bedrijfszekerheidstechniek. Deze grootheid (beter bekend als de *storingsgraad*) geeft opnieuw de kans aan, dat de eenheid in de periode $(t, t + \Delta t)$ faalt, maar nu onder de *voorwaarde*, dat de unit ten tijde t nog goed functioneerde.
Uit de laatste expressie volgt het verband tussen z(t) en R(t)

$$z(t) = \lim_{\Delta t \to 0} \frac{P(t < \underline{X} \leq t + \Delta t)}{P(\underline{X} > t)\,\Delta t} = \lim_{\Delta t \to 0} \frac{f(t)\,\Delta t}{R(t)\,\Delta t} = \frac{f(t)}{R(t)}$$

of

$$z(t) = -\frac{R'(t)}{R(t)} = -\frac{d}{dt}\,[\ln R(t)],$$

waaruit

$$\ln R(t) = -\int_0^t z(u)\,du, \qquad \text{mits } R(0) = 1$$

of

$$R(t) = \exp\left(-\int_0^t z(u)\,du\right).$$

Door ieder van de vier hiervoor behandelde begrippen is de levensduur van een eenheid volledig gekarakteriseerd. Het gemeenschappelijke nadeel van de vier begrippen is echter dat ze de kwaliteit van de eenheid vastleggen door middel van een functie die tijdsafhankelijk is. De praktijkman werkt liever met één getal als maat voor de kwaliteit. De gemiddelde levensduur is daarbij een vaak gehanteerde grootheid, waarbij de aantekening gemaakt dient te worden dat deze grootheid bepaald niet een volledige karakterisering van de kwaliteit geeft maar vooral een eerste indicatie wil geven. De definitie luidt als volgt:

E. De *gemiddelde waarde* θ van de levensduur $\underline{X}$ (ook wel de *gemiddelde levensduur* van $\underline{X}$ genoemd) wordt gevonden door het eerste moment

$$\theta = E(\underline{X}) = \int_0^{\infty} t\, f(t)\, dt$$

en omdat aan te tonen is dat $\lim_{t\to\infty} t\, R(t) = 0$, kan worden afgeleid dat

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

> *Inzicht in en het kunnen hanteren van de boven omschreven grootheden A, B, C, D en E zijn noodzakelijk voor het volgen van de theorie en van berekeningen aan bedrijfszekerheids-modellen.*

Berekeningsvoorbeeld:

Bij de zogenaamde negatief-exponentiële verdeling is de hazard rate z(t) constant in de tijd en wordt als de failure rate λ aangegeven. De overlevingskans is dan $R(t) = \exp\left(-\int_0^t \lambda du\right) = \exp(-\lambda t)$, de bedrijfsonzekerheid $F(t) = 1 - R(t) = 1 - \exp(-\lambda t)$.
De kansdichtheidsfunctie $f(t) = -dR(t)/dt = \lambda \exp(-\lambda t)$, terwijl de gemiddelde levensduur $\theta = \int_0^{\infty} \exp(-\lambda t)\, dt = 1/\lambda$.

Resumerend kan de negatief-exponentiële distributie als volgt worden gekarakteriseerd:

A. $f(t) = \lambda \exp(-\lambda t)$
B. $F(t) = 1 - \exp(-\lambda t)$
C. $R(t) = \exp(-\lambda t)$
D. $z(t) = \lambda$
E. $\theta = 1/\lambda$.

1.8 Onderling verband afgeleide grootheden

De in de vorige paragraaf onder A tot en met D genoemde grootheden kunnen in elkaar worden herleid en bevatten dus, ieder voor zich, alle informatie omtrent het faalproces van de beschouwde systemen.

In onderstaande tabel zijn de onderlinge relaties gegeven.

Probability density function	$f(t)$	$F'(t)$	$-R'(t)$	$z(t) \exp\left(-\int_0^t z(u)\,du\right)$
Unreliability	$F(t)$	$\int_0^t f(u)\,du$	$1 - R(t)$	$1 - \exp\left(-\int_0^t z(u)\,du\right)$
Reliability	$R(t)$	$\int_t^\infty f(u)du$	$1 - F(t)$	$\exp\left(-\int_0^t z(u)\,du\right)$
Hazard rate	$z(t)$	$\dfrac{f(t)}{\int_t^\infty f(u)\,du}$	$\dfrac{F'(t)}{1 - F(t)}$	$\dfrac{-R'(t)}{R(t)}$

Voorbeeld:

De levensduur van een eenheid heeft de volgende kansdichtheidsfunctie

$f(t) = k(1 - t^2)$ voor $0 \le t \le 1$, t in jaren
$= 0$ voor $t > 1$.

□ Hoe groot is k? Voor elke pdf geldt $\int_0^\infty f(t)\,dt = 1$, dus $\int_0^1 k(1 - t^2)\,dt = 1$, zodat $k = 3/2$. Let op de integratiegrenzen.

□ Hoe groot is R (1/6) = R (2 maand)? $R(t) = \int_t^\infty f(t)\,dt =$
$= \int_t^1 k(1 - t^2)\,dt = 1 - 3/2\,t + 1/2\,t^3 \rightarrow R(1/6) = .75.$

□ Hoe groot is de gemiddelde levensduur θ? $\theta = \int_0^\infty R(t)\,dt =$

$= \int_0^\infty (1 - 3/2\ t + 1/2\ t^3)\,dt = 3/8$ jaar $= 4.5$ maand.

Opgave 1.1:

De hazard rate van een eenheid is $z(t) = a\ t^{a-1}/\theta^a$.
Toon aan dat de overlevingskans van die eenheid berekend kan worden met $R(t) = \exp(-(t/\theta)^a)$.

Opgave 1.2:

De reliability van een systeem is gedefinieerd door
$R(t) = \exp(-(\exp(ct^b) - 1))$.
Laat zien dat in dat geval geldt voor de hazard rate van het systeem $z(t) = cbt^{b-1} \exp(ct^b)$.

Opgave 1.3:

De levensduurverdeling van een systeem wordt gekenmerkt door een storingsgraad (= hazard rate), die lineair met de tijd toeneemt volgens $z(t) = .02\ t$, $t \geq 0$, t in maand.

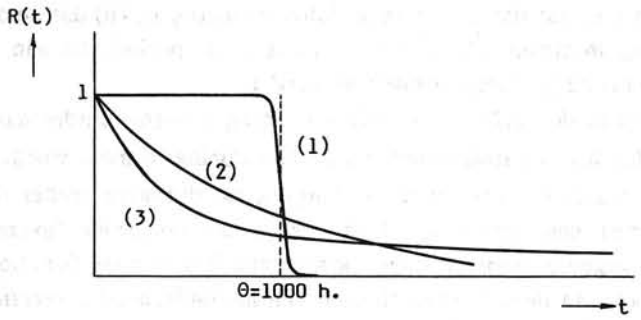
Toon aan dat: (a) R (1 maand) $\simeq .99$
(b) $\theta_{syst} \simeq 8.9$ maand.

(hint: $\int_0^\infty \exp(-a^2x^2)\,dx = \frac{1}{2a}\sqrt{\pi}$).

1.9 Overlevingskans R(t)

Zoals reeds gesteld, wordt met de R(t) van een eenheid de kans bedoeld dat die unit ten tijde t "het nog doet", dat wil zeggen dat op dat tijdstip nog de functie wordt verricht, die ervan wordt verwacht. Voorts nemen we praktisch altijd aan dat de unit ten tijde $t = 0$ werkt, met andere woorden dat $R(0) = 1$. In dat geval hebben we in R(t) met een monotoon dalende functie te maken, beginnend bij de waarde 1 en voor $t \to \infty$ naderend tot nul. Met dit laatste verloop wordt tot uitdrukking gebracht, dat vroeg of laat elk technisch voortbrengsel het laat afweten en dat in dit ondermaanse niets tot in het oneindige blijft doorfunctioneren.

Enige mogelijke overlevingskanscurven zijn hieronder grafisch weergegeven.



De oppervlakken onder de curven worden aan elkaar gelijk verondersteld, met andere woorden we nemen aan dat de desbetreffende eenheden dezelfde $\theta = \int_0^\infty R(t)\,dt$ bezitten.

Curve (1) heeft betrekking op het zogenaamde (nagenoeg) constante levensduurgeval, dat we bijvoorbeeld bij een gloeilamp van 1000 branduren tegenkomen. De vorm van deze kromme suggereert, dat de uitvalskans van een dergelijke lichtbron tussen (zeg) 950-1050 h gelijk aan 1 is. Een andere benadering is deze: bij een proefveld met een groot aantal van deze lampen zal blijken, dat de waarden van de levensduur hiervan (praktisch) alle tussen 950-1050 h liggen, dus met een kleine *spreiding* om de 1000 h heen.

Bij curve (2) hebben we te doen met eenheden, die in hun levensduur de (reeds eerder genoemde) negatief-exponentiële verdeling volgen, met andere woorden $R(t) = \exp(-\lambda t) = \exp(-t/1000)$. De spreiding hier is aanzienlijk toegenomen: enerzijds een grote uitvalskans nog lang voor de gemiddelde levensduur θ en anderzijds nog een overlevingskans van $R(\theta) = \exp(-1) \simeq 37\%$ voor $t = 1000$ h. Dit verschijnsel is — gezien het verloop — nog sterker bij curve (3) aanwezig.

Overigens is het in dit verband interessant om op te merken dat voor twee reliability curves $R_1(t)$ en $R_2(t)$ die beide dezelfde θ opleveren moet gelden dat er tijdstippen t_0 zijn waarvoor geldt $R_1(t_0) > R_2(t_0)$, maar evengoed tijdstippen t_1 met $R_1(t_1) < R_2(t_1)$.

Het ligt voor de hand dat het karakter van eventueel te nemen *onderhoudsmaatregelen* sterk door de waarde van de spreiding van de levensduur-

verdeling zal worden bepaald. Bij onderhoud denken we in dit verband aan menselijk ingrijpen, dat tot *vervanging* of *reparatie* van de falende eenheid leidt (zie hoofdstuk 5). Zo kan bij de verlichting van een flatgebouw een *groepsvervanging* van alle lampen na 900 branduren worden overwogen.
Voordeel hierbij is, (a) dat er continue lichtverzorging is, (b) dat de onderhoudsinspanning minimaal zal zijn en (c) dat in de periode tot aan 900 h geen bedrijfscontrole gepleegd behoeft te worden.
Het effect van een dergelijke *preventieve* maatregel wordt minder naarmate de spreiding der levensduren groter wordt. Het storingsmoment wordt steeds minder voorspelbaar, een eventuele vervanging zal derhalve eerder moeten plaatsvinden, met een groter wordend verlies aan potentiële levensduur, omdat het vervangen exemplaar mogelijk nog lang had kunnen functioneren. Er komt dan ook van lieverlee een situatie, dat het onderhoud *correctief* van aard zal moeten zijn, dat wil zeggen dat pas gereageerd wordt, *nadat* de storing is opgetreden. Dit punt zal in de volgende paragraaf nog nader ter sprake komen.

Samenvattend kunnen we stellen dat het gegeven van *gemiddelde levensduur* een nuttige, maar — indien alleen bekend — een te beperkte informatie kan zijn ten aanzien van het toekomstige storingsgedrag van een systeem en het bijbehorend onderhoudsconcept. Bij de pogingen om het verloop van de bedrijfszekerheidscurve van een systeem — bestaand of in ontwerp — uit bijvoorbeeld operationele faalgegevens te weten te komen, zal tevens bijzondere aandacht moeten worden besteed aan *de spreiding* van de storingsmomenten.

1.10 Negatief-exponentiële verdeling

De negatief-exponentiële verdeling is verreweg de meest gebruikte faal- en reparatiedistributie uit de bedrijfszekerheidstechniek. Deze voorkeur is vooral toe te schrijven aan de mogelijkheid om in dit geval vrij eenvoudig berekeningen van operationele grootheden bij bedrijfszekerheidsmodellen uit te voeren, zoals later uit dit boekwerk zal blijken. Bij (de vele) andere verdelingen is het vaak erg moeilijk deze modellen voor dit soort berekeningen toegankelijk te maken.

Kenmerkend voor de negatief-exponentiële verdeling is — zoals eerder opgemerkt — de (in de tijd) constante waarde van de hazard rate of storingsgraad, die hier met failure rate λ wordt aangeduid. We spreken dan ook zo treffend van dè failure rate van een component of systeem, bijvoorbeeld: de λ van een IC $\simeq 10^{-8}$ f/h (= failure/hour). Dit wil zeggen, dat er gemiddeld 1 fout optreedt in de 10^{+8} h of, bij 10^{+8} componenten, gemiddeld 1 uitval per uur.
De praktische betekenis van een constante failure rate is, dat het optreden van de storingen volkomen willekeurig (*at random*) geschiedt, een geheugenloos gebeuren dus, waarvan het verkrijgen van een lekke band een typisch voorbeeld is (mits de banden nog profiel vertonen, anders is het slijtage).
Omdat de uitvalskans op een tijdstip t niet afhangt van het arbeidsverleden van het desbetreffende systeem, wordt dit — mits nog werkend — te allen tijde als "as good as new" bekeken. Dus: de kans op een lekke band gedurende 1000 km, vanaf een "leeftijd" van 6000 km van een autoband wordt even groot verondersteld als de eerste 1000 km (dus vanaf nieuw). Het heeft derhalve geen enkele zin om na 6000 km gebruik van tevoren een nieuwe band te monteren met het doel de kans op uitval te verkleinen.

> *Maar dit betekent dat men zich door middel van preventief onderhoud niet kan indekken tegen dit soort random failures (zie paragraaf 5.2).*

Indien men ten aanzien van het faalgedrag van een systeem van de negatief-exponentiële verdeling uitgaat, dient de waarde van de gemiddelde levensduur $\theta = 1/\lambda$ *in operationeel opzicht* voorzichtig te worden geïnterpreteerd. Indien bijvoorbeeld een fabrikant van een apparaat een $\theta = 240$ h garandeert, dan houdt dat in, dat — na in bedrijfstelling — de eerste storing *gemiddeld* na 10 etmalen optreedt. Bij een (toch alleszins redelijke) eis van een maximale uitvalskans van 1% na een periode T volgt echter uit $R(T) = \exp(-T/240) = .99$ een $T \simeq 2.4$ h, met andere woorden na ruim twee uur moet het desbetreffende systeem reeds op goed functioneren worden gecontroleerd.

De vraag in hoeverre vanuit de praktijk blijkt, dat de aanname van een constante storingsgraad gewettigd is, is niet gemakkelijk te beantwoorden. Het is reeds lang een punt van voortdurende zorg en aanhoudend onderzoek in welke mate faalgegevens van mechanische en elektronische systemen —

uit bedrijf of van testing afkomstig, zie paragraaf 5.3 — zich bij een negatief-exponentiële verdeling aansluiten (*curve fitting*).
In het algemeen kan wel worden gesteld:

- Dat halfgeleiderschakelingen een faalpatroon laten zien, dat vrij goed met een negatief-exponentiële distributie te beschrijven is, mits gevrijwaard van vocht, trilling en overspanning (zie paragraaf 5.5*).
- Dat complexe systemen met een grote variëteit aan componenten en subsystemen, een ieder met zijn eigen failure rate, leeftijd en vervangingsritme (waardoor een middelingseffect ontstaat) een constant faaltempo blijken te bezitten, mits het complexe systeem niet redundant is.
- Dat de negatief-expontiële distributie moet worden aangenomen, als er te weinig storingsgegevens voorhanden zijn of indien de berekeningen anders te ingewikkeld worden. Men moet deze aanname dan maar opvatten als een eerste orde benadering van een tijdsafhankelijke storingsgraad. Bovendien kan een bedrijfszekerheidsmodel, dat op zich een (te) grove benadering van de werkelijkheid vormt, zeer nuttig zijn bij een zogenaamde *gevoeligheidsanalyse*, waarbij wordt nagegaan, in hoeverre het resultaat afhankelijk is van variatie in de waarden van de invoerparameters.

1.11 Aspecten van de gemiddelde levensduur

Bij de inventarisatie van afgeleide grootheden in paragraaf 1.7 is de gemiddelde levensduur θ omschreven als de verwachtingswaarde van de levensduur $\underline{X}$

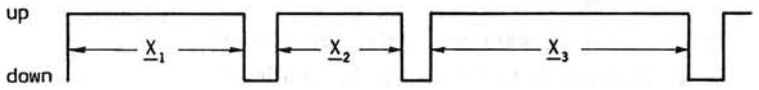
$$\theta = E(\underline{X}) = \int_0^\infty R(t)\,dt.$$

Het betreft hier een eenheid, die niet-repareerbaar is of die om allerlei redenen toch maar niet meer gerepareerd wordt (zie paragraaf 1.4*). Na het optreden van een storing wordt de unit veelal weggegooid (throw-away-item of consumable; zie paragraaf 6.3), zoals een kapotte gloeilamp òf mogelijk gekannibaliseerd, zoals een goedkoop transistorradiootje.

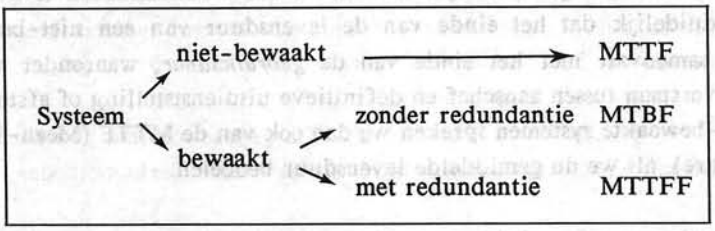
We zullen in het vervolg dergelijke eenheden als *niet-bewaakte* systemen omschrijven, omdat bewaking onderhoud (= menselijk ingrijpen) impliceert,

met het doel een uitgevallen systeem weer aan het functioneren te krijgen. Het is duidelijk dat het einde van de levensduur van een niet-bewaakt systeem samenvalt met het einde van de *gebruiksduur*, waaronder we de periode verstaan tussen aanschaf en definitieve uitdienststelling of afstorting. Bij niet-bewaakte systemen spreken we dan ook van de MTTF (Mean-Time-To-Failure), als we de gemiddelde levensduur bedoelen.

Bij *bewaakte* systemen hebben we daarentegen met een andere situatie te maken. Na een storing zal het systeem (al of niet vertraagd) worden hersteld en wederom in bedrijf worden gebracht. Het functioneren zal opnieuw worden beëindigd door het optreden van een tweede storing, ook weer gevolgd door een herstelperiode (zie paragraaf 7.2).



Het bedrijfsleven van een bewaakt systeem bestaat derhalve uit een aaneenschakeling van up- en downtoestanden, waarbij de levensduur $\underline{X}$ de periode voorstelt tussen de indienststelling en de daarop volgende storing. De gemiddelde waarde daarvan wordt aangeduid als MTBF (Mean-Time-Between-Failures).
Er is nog een derde tijdgemiddelde. Bij aanwezigheid van (snel uitwisselbare) reserve-eenheden kan in een verwaarloosbare tijd een falend onderdeel worden vervangen, zodat de systeemfunctie (praktisch) ononderbroken doorgaat.
Intussen zal de reparatie van de kapotte component ter hand worden genomen en — indien hersteld — aan de voorraad spares worden toegevoegd. Treedt er een systeemstoring op, terwijl het herstel nog niet is afgerond en er geen goede reserve meer aanwezig is, dan is de downtime van het systeem aangebroken. Kenmerkend voor een dergelijke configuratie is, dat onderhoud en functioneren tegelijkertijd plaatsvinden. In hoofdstuk 7 zullen enige berekeningen plaatsvinden, waaruit blijkt dat we in de *combinatie* van onderhoud en redundantie een zeer machtig middel hebben de systeemoverlevingskans te vergroten. Analoog aan het bewaakte systeem zónder reserve wordt de gemiddelde levensduur aangegeven als MTTFF (Mean-Time-To-*First*-Failure). Derhalve geldt voor de gemiddelde levensduur θ:



Opgave 1.4:

Gegeven een kaars met 3 branduren.

Hoe groot is θ_{kaars}?

Twee suggesties:

(a) $\theta_{kaars} = 3$ h, want na 3 uur is de kaars opgebrand.

(b) $\theta_{kaars} \rightarrow \infty$, want een storing "onderweg" (bijvoorbeeld door een onderbroken lont) is praktisch uitgesloten.

Opmerking: Het uitwaaien van de kaars is geen storing, maar misuse: een kaars hoort niet op de tocht te staan. U kunt er de fabrikant dan ook niet op aanspreken.

1.12 Andere verdelingen

We hebben in paragraaf 1.9 reeds gesteld, dat elke overlevingskromme als functie van de tijd start bij de waarde 1, om daarna op de één of andere manier monotoon voor $t \rightarrow \infty$ naar de waarde 0 te dalen. Omdat een dergelijk verloop op vele wijzen tot stand kan komen (zie de schets in paragraaf 1.9) zal het niet verbazen, dat in de bedrijfszekerheidstheorie vele levensduurverdelingen zijn geformuleerd, een ieder met zijn karakteristieke eigenschappen, zoals de ligging van het gemiddelde, de grootte van de spreiding, etcetera.

Enige voorbeelden zijn:

- De *normale* verdeling, die met name van toepassing is op onderdelen die falen ten gevolge van slijtageprocessen, bijvoorbeeld doorbranden van gloeidraadlampen, doorslijten van touw en het verbruikt raken van het smerend vermogen van kogellagervet.

- De *lognormale* verdeling kan gebruikt worden voor de beschrijving van reparatieduurverdelingen en het falen ten gevolge van materiaalvermoeidheidsbreuken.

- De *uniforme* verdeling die vooral wordt toegepast voor het genereren van stochastische verdelingen met behulp van de Monte Carlo methode.

- De *Weibull*-verdeling die vanwege haar flexibiliteit zeer geschikt is voor curve-fitting (zie paragraaf 1.10), met name indien men een "badkuipkromme" (zie hieronder) wil beschrijven. Bij experimentele verdelingen zoals deze optreden bij de inloop-, gebruiks- en slijtageperiode van bijvoorbeeld kogellagers en elektrische apparaten wordt de Weibulldistributie zeer veel toegepast.
  De negatief-exponentiële verdeling is een bijzondere vorm van de Weibull-distributie.

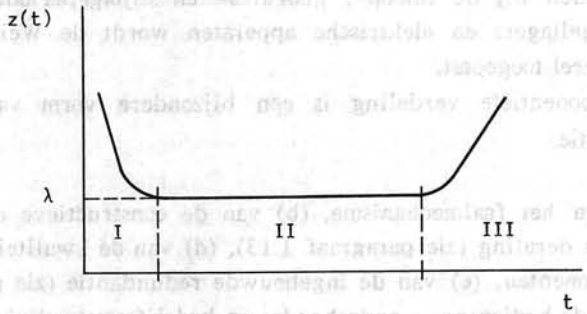
Afhankelijk (a) van het faalmechanisme, (b) van de constructieve opzet, (c) van de mate van derating (zie paragraaf 1.13), (d) van de kwaliteit van de toegepaste componenten, (e) van de ingebouwde redundantie (zie paragraaf 2.1), (f) van de bedienings-, onderhouds- en bedrijfsomstandigheden, etcetera, zal een systeem tijdens testing of bedrijf een faalpatroon laten zien, waaruit dan — middels intelligente verwerking van de faalgegevens — de levensduurverdeling van dit systeem door één van bovengenoemde distributies kan worden benaderd. Voorts kan dan het (globale) verloop van de storingsgraad (zie paragraaf 1.7D) worden afgeleid, dat een belangrijke rol speelt bij de vaststelling van het onderhoudsconcept (zie paragraaf 5.2).

Doel van al deze activiteiten is uiteindelijk enig inzicht en gefundeerd vermoeden te verkrijgen omtrent het storingsgedrag van het desbetreffende systeem in de nabije bedrijfstoekomst en op grond daarvan slagvaardige maatregelen ter zake van onderhoud en reservedelenvoorziening te kunnen nemen.

Een onzekere factor echter hierbij is de mogelijkheid, dat *tijdens (langdurig) bedrijf het storingsgedrag zich (sterk) wijzigt*, waardoor deze voorspellende werkwijze minder effectief wordt, of zelfs onbruikbaar voor de instandhouding van het systeem.

Een vaak in de praktijk voorkomend faalpatroon (van met name complexe systemen) is namelijk dat, waarbij in het begin de uitvalskans relatief groot

is, veroorzaakt door het vroegtijdig falen van componenten. Dan volgt een tijdinterval met relatief weinig fouten, waarin de storingen vrij willekeurig (at random; zie paragraaf 1.10) optreden. Tenslotte volgt dan nog een periode, die zich vanwege slijtage (wear-out) kenmerkt door een steeds groter wordende sneuvelkans.
Grafisch wordt één en ander weergegeven door de zogenaamde *badkuip-kromme* (bath-tub curve), waarin de storingsgraad (hazard rate) z(t) tegen de tijd is uitgezet. Aldus:



I = inbrandperiode
II = bedrijfsperiode
III = slijtageperiode

Door toepassing van het aloude middel "inbranden" kunnen de zwakke exemplaren met "early failures" (kinderziekten) — overigens slechts ten dele — uit een produktieserie worden verwijderd.
In de bedrijfsperiode wordt de storingsgraad (nagenoeg) constant geacht en aangeduid als de failure rate λ (zie paragraaf 1.7; negatief-exponentiële verdeling). Tenslotte zal een snel stijgende hazard rate in de "wear-out" periode voor een spoedige uitval zorgen. De gemiddelde levensduur, die bij een badkuipvormig-verloop van de storingsgraad behoort, is dan ook veel kleiner dan de $\theta = 1/\lambda$ (zie paragraaf 1.7E).

Opgave 1.5:

We beschouwen een gloeilamp waarvan gegeven is dat het gemiddeld aantal branduren 1000 bedraagt. Anderzijds schatten we dat in de periode tot 900 h de uitvalskans per uur heel klein is, zeg 10^{-5}.

(a) Ga na dat beide genoemde gegevens reëel kunnen zijn.
(b) Toon aan dat de exponentiële verdeling niet past op deze gegevens.
(c) Wat kunt U zeggen over de storingsgraad in de periode na 900 h?

1.13 Vergroting van de bedrijfszekerheid

We zullen tenslotte nog enige maatregelen memoreren, die ten doel hebben de *inherente bedrijfszekerheid* van een systeem èn de beschikbaarheid daarvan te vergroten. Daarbij wordt vooropgesteld, dat het bijzonder doelmatig èn doeltreffend blijkt te zijn, dat zowel door de fabrikant als door de afnemer in een zo vroeg mogelijke fase van de systeemconceptie deze bedrijfszekerheid als één van de *ontwerpdoelstellingen* wordt herkend en als zodanig geïntroduceerd. De eisen ten aanzien van de bedrijfszekerheid, onderhoudbaarheid, bedienbaarheid en veiligheid dienen daartoe (bij voorkeur contractueel) in de systeemspecificatie te zijn vastgelegd. Worden deze aspecten pas achteraf ter sprake gebracht, dan blijft soms alleen de mogelijkheid over een extra systeem als reserve aan te schaffen (redundantie op systeemniveau) om aan de operationele eisen te voldoen. Het behoeft geen betoog dat deze (te) late correctie veel kosten met zich meebrengt en gewoon niet nodig is.

> Voorts mag in dit verband niet onvermeld worden gelaten, dat de "reliability-mindedness" en het opleidingsniveau in de bedrijfszekerheidstechniek van de ontwerper van zeer grote invloed zijn bij het streven om uiteindelijk tot een bedrijfszeker en veilig produkt te komen.

Enige van de bovenbedoelde maatregelen zijn:

- Het toepassen van onderbelasting. Hierbij wordt het belastingniveau van de componenten verlaagd of worden "zwaardere" onderdelen toegepast. De levensduur hiervan wordt door deze zogenaamde *derating* met factoren verbeterd. De keuze van een 1 W weerstand bij een dissipatie van 1/2 W is een zeer eenvoudig voorbeeld.

- Toepassing van ingebouwde redundantie, mits afhankelijke fouten vermeden kunnen worden; zie paragraaf 4.6. Met name op elektronisch gebied

is het door de microminiaturisatie volumineus mogelijk geworden allerlei subsystemen (minstens) te dupliceren.

- Bedacht zijn op de toegankelijkheid (accessibility) tot de verschillende onderdelen van een complex systeem. Het is duidelijk, dat een goede bereikbaarheid de uitwisselbaarheid van componenten of subsystemen bevordert, hetgeen — door de kortere reparatietijden — de systeembeschikbaarheid uiteraard ten goede komt. De noodzaak om een apparaat half te ontmantelen teneinde een falend deeltje ter vervanging te bereiken is in de technische wereld geen onbekende ervaring.
- Het (ook tijdens de ontwikkeling) testen van produkten op bedrijfszekerheid. De gemeten waarde van de gemiddelde levensduur is dan — indien deze nog niet aan de specificatie voldoet — bepalend, hoe lang nog aan het desbetreffende ontwerp verder moet worden ontwikkeld.
- Het introduceren van een inbrandperiode ten einde de kinderziekten (*early failures*) op te sporen.
- Het opstellen van een goed bruikbaar onderhoudsconcept en van een reservedelenlijst voor de totale gebruiksduur in verband met de *beperkte* periode, waarin — bij dreigende tekorten — door de fabrikant nog *nalevering* van spares kan worden gegarandeerd.

2 BEDRIJFSZEKERHEIDSMODELLEN

2.1 Bedrijfszekerheidsmodellen

Teneinde enig inzicht te krijgen in de overlevingskans van een complex systeem (een vliegtuig, een computer, een radarapparaat, een centrale verwarming, etc.) wordt gebruik gemaakt van *bedrijfszekerheidsmodellen.* Een aantal hiervan zullen in hoofdstuk 8 worden besproken (faalboom, FMECA, etc.); deze modellen worden voor kwalitatieve en kwantitatieve systeemanalyses gebruikt. In dit hoofdstuk beschouwen we het *catastrofaal faalmodel*, dat in de bedrijfszekerheidstechniek het meest wordt toegepast.

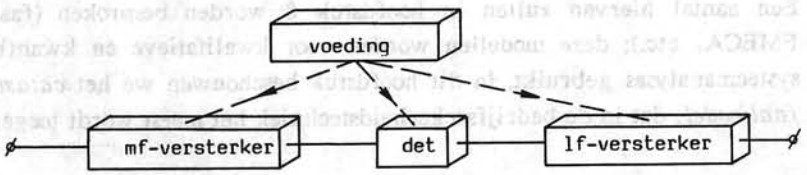
Het catastrofaal faalmodel betreft een blokschematische opsplitsing van het desbetreffende systeem in eenheden (modulen, subsystemen, componenten, onderdelen, etc.). Deze blokken zijn op een aantal manieren onderling en met een tweetal punten verbonden via paden. Het systeem werkt nu wanneer er een pad bestaat via functionerende blokken tussen de twee genoemde punten. De meest eenvoudige structuren met dit model zijn de *serie-* en *parallel-*structuur (de zogenaamde *grondmodellen*).

Bij de seriestructuur (meestal seriesysteem genaamd) is er sprake van een kettingconfiguratie, dat wil zeggen van een *achter elkaar* geschakeld zijn van de samengestelde eenheden.
Schematisch aldus voorgesteld:

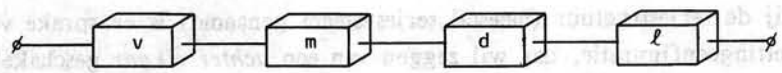
Deze opstelling houdt in dat *alle* units goed moeten werken om het totale systeem te doen functioneren. Kenmerkend voor een serieschakeling is derhalve, dat uitval van één schakel nodig én voldoende is voor het falen van de gehele keten.

* Overigens moeten we zo'n serieschakeling ruimer opvatten dan (om maar eens een voorbeeld te noemen) een aantal galvanisch verbonden weerstandjes of een serie lampjes in de kerstspar.

Zo zijn de vier (actieve) banden van een (overigens goed sporende) personenauto als een serieschakeling te beschouwen, omdat er in het geval van slechts één lekke band toch gestopt moet worden. Ditzelfde is trouwens ook het geval bij een loszittend stuurwiel. Op deze wijze blijkt onze auto één grote serieschakeling te zijn van samenstellende delen, wier falen ieder voor zich belemmerend is voor het functioneren van het voertuig.
Nog een voorbeeld. Een mf-versterker (m), een detector (d) en een lf-versterker (ℓ) zijn aangesloten op éénzelfde voeding (v).

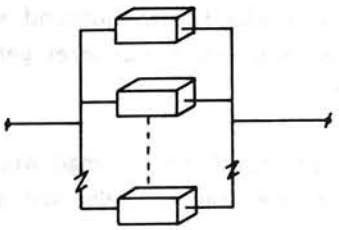


Omdat voor het leveren van output óók de voeding goed moet werken is het bijbehorende bedrijfszekerheidsmodel weer te geven als de volgende serieschakeling:



Overigens omvat in de praktijk de serieschakeling vaak meer dan het technische systeem (de hardware) alleen. Ook de software, de procedures, de omstandigheden, de bediening en de mate, waarin de vereiste vakkennis en ervaring aanwezig is, spelen een operationeel noodzakelijke rol. Een goed uitgevoerde landing van een vliegtuig hangt niet alleen af van de juiste toestand van het landingsgestel maar tevens van de weersomstandigheden, van de landingsprocedures, van de fysieke en psychische toestand van de piloot, van de motivatie en ervaring van het personeel op de verkeerstoren, van de verbindingsapparatuur, etcetera. Hoewel het bijzonder moeilijk is al deze factoren te kwantificeren, mogen deze bij een eventuele *criticality-analyse* (zie paragraaf 8.3) niet buiten beschouwing worden gelaten.

Bij een parallelstructuur (of parallelsysteem) functioneren minstens twee eenheden *naast elkaar* en tegelijkertijd.
Schematisch aldus voorgesteld:



De toegepaste eenheden zijn als zodanig elkaars reserve en — tenzij anderszins vermeld — dit systeem faalt dan en slechts dan als alle eenheden falen. Een parallelschakeling blijkt bij het ontwerp een steeds meer toegepast, krachtig hulpmiddel te zijn om de bedrijfszekerheid van een complex systeem op te voeren bij de toepassing van componenten, die ieder voor zich te onbetrouwbaar zijn om de systeemeis te halen. We hebben hier te doen met een bepaalde vorm van *redundantie*, dit is de invoering van een zekere *overmaat* of *overtalligheid* aan (ingebouwde) onderdelen, waarbij het mogelijk blijkt, dat een complex systeem ongestoord doorwerkt, ook nadat er componenten stuk zijn gegaan.

* Vanwege de gelijktijdige werking van alle eenheden spreken we in dit geval van *actieve* redundantie. Het beschikbaar zijn van reservedelen, die pas worden ingezet, indien dat nodig is (denk aan de reserveband van onze auto) wordt als *passieve* redundantie omschreven.

2.2 Voorwaarden voor berekeningen

In de volgende paragrafen zullen we de overlevingskansen van de (in paragraaf 2.1 genoemde) grondmodellen in het kort bespreken.
Vooraf echter poneren we enige voorwaarden (of vooronderstellingen) die nodig zijn, omdat anders de gehanteerde begrippen, zoals R(t), f(t) en z(t) niet eenduidig vastliggen of de modellen niet of zeer moeizaam voor berekening toegankelijk zijn.
Deze premissen zijn:

(a) Een eenheid (subsysteem, onderdeel, etc.) is goed of fout, dat wil zeggen de unit is wel of niet bedrijfsgereed (*catastrofaal faalmodel*). Er wordt geen rekening gehouden met een eventueel teruggelopen conditie, zoals het *verminderen* van het zendvermogen bij een radioverbinding (zie paragraaf 1.3). Er moet in dat geval een bedrijfsnorm afgesproken worden, die bepalend is voor de al of niet falende toestand van de zender. Schemerachtige tussentoestanden in het operationeel gebeuren worden derhalve niet mogelijk geacht.

(b) Eens gefaald, blijft gefaald, totdat er onderhoud gepleegd wordt. Er zijn geen *intermitterende storingen*, die "vanzelf", dat wil zeggen zonder menselijk ingrijpen, verdwijnen.

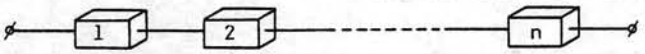
(c) De levensduurvariable is de tijd (zie paragraaf 1.3).

(d) De uitvalskansen door eenheden zijn onderling *onafhankelijk*. Dit betekent dat het falen van één component de faalkans van de andere componenten niet beïnvloedt. Voor gemeenschappelijke faaloorzaken wordt verwezen naar paragraaf 4.6.

(e) Een eenheid kan slechts op één manier kapot zijn (*single mode failure*). De werkelijkheid kent overigens wel de *multi-mode failure*. Zo kan een falende diode zich in (a) open dan wel in (b) kortgesloten toestand bevinden (zie paragraaf 4.4).

2.3 Het seriesysteem

Gegeven een serieschakeling van n eenheden:



Indien we met E_i, $i = 1,2,...,n$ de gebeurtenis bedoelen aan te geven, dat de i-de eenheid werkt en met $\bar{E}_i$ dat deze niet meer normaal functioneert, dan geldt

$$R_{syst} = P\{E_1 \cap E_2 \cap ... \cap E_n\},$$

waarmee tot uitdrukking wordt gebracht, dat alle n eenheden moeten functioneren voor de werking van het totale systeem.
Bij stochastisch onafhankelijke uitval (premisse d) kunnen we hiervoor schrijven:

$$R_{syst} = P\{E_1\} * P\{E_2\} * \ldots * P\{E_n\}.$$

Indien tenslotte $P\{E_i\} = R_i(t)$, $i = 1,2,\ldots,n$, zijnde de overlevingskans van eenheid i ten tijde t, dan is $R_{syst}(t) = R_1(t) * R_2(t) * \ldots * R_n(t)$ of

$$\boxed{R_{syst}(t) = \prod_{i=1}^{n} R_i(t)} .$$

Dit is de produktregel voor een seriesysteem:

> De bedrijfszekerheid van een seriesysteem wordt verkregen door de afzonderlijke bedrijfszekerheden van de samenstellende delen met elkaar te vermenigvuldigen.

Bovenstaande formule is door een meer praktische uitdrukking te benaderen. In de praktijk zijn veelal slechts waarden van $R_{syst}(t) \geq .90$ operationeel interessant. En bijgevolg geldt dan $F_{syst}(t) = 1 - R_{syst}(t) < .10$. Dit levert door de kleine waarden van F_i, $i = 1,2,\ldots,n$ de volgende benadering

$$R_{syst}(t) = (1 - F_1(t))\,(1 - F_2(t)) \ldots (1 - F_n(t))$$

of

$$R_{syst}(t) \simeq 1 - \sum_{i=1}^{n} F_i(t)$$

waarin $F_i(t)$ de bedrijfs*on*zekerheid van de i-de eenheid ten tijde t voorstelt. Voor n identieke eenheden geldt dan tenslotte

$$R_{syst}(t) \simeq 1 - n\,F(t)$$

waarin F(t) de bedrijfs*on*zekerheid van een enkele unit ten tijde t betekent.

Voorbeeld:

Indien bij het voorbeeld in paragraaf 2.1 $R_d = .99$, $R_\ell = .98$, $R_m = .97$ en $R_v = .96$ voor een bepaalde bedrijfsperiode, dan geldt volgens de produktregel: $R_{syst} = .9035$, terwijl via de benadering gevonden wordt: $R_{syst} \simeq 1 - (.01 + .02 + .03 + .04) \simeq .90$ voor diezelfde periode.

2.4 Hazard rate van een seriesysteem

Indien bij het seriesysteem tevens wordt verondersteld, dat de eenheden in hun levensduur de negatief-exponentiële verdeling volgen (random failures), dan resulteert dat in

$$\begin{aligned} R_{syst}(t) &= \exp(-\lambda_1 t) * \exp(-\lambda_2 t) * \ldots * \exp(-\lambda_n t) \\ &= \exp(-(\lambda_1 + \lambda_2 + \ldots + \lambda_n)\,t), \end{aligned}$$

zodat

$$\boxed{R_{syst}(t) = \exp\left(-\sum_i \lambda_i t\right)}.$$

De faaldistributie van een seriestructuur van eenheden met een negatief-exponentiële uitval is dus zelf ook weer negatief-exponentieel. De failure rate λ_{syst} van het seriesysteem is dan gelijk aan $\sum_i \lambda_i$ en de gemiddelde levensduur van het systeem is derhalve

$$\boxed{\theta_{syst} = \frac{1}{\sum_i \lambda_i}}.$$

Hieruit volgt dat de zwakste component in relatieve zin de grootste verkorting van de levensduur geeft en daarom ook als eerste bij een eventuele ontwerpherziening voor verbetering in aanmerking komt.

Op bovenstaande beschouwingen berust een (ruwe) benadering van de bedrijfszekerheid van (met name) subsystemen. Bij deze methodiek — ook wel de *hazard rate analysis* genoemd — worden bijvoorbeeld bij een print of elektronische schakeling van alle componenten de toegepaste aantallen en de failure rate bepaald, waarna de λ_{syst} door optelling kan worden verkregen.

Voorbeeld:

Een schakeling heeft de volgende componenten, waarvan de failure rates aan de literatuur kunnen worden ontleend.

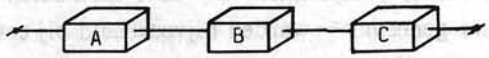
Aantal	Component	Failure rate	
20	weerstand	4×10^{-9} f/h	80×10^{-9} f/h
8	transistor	8×10^{-9} f/h	64×10^{-9} f/h
120	soldeerverbinding	0.2×10^{-9} f/h	24×10^{-9} f/h
4	elektrol. condens.	120×10^{-9} f/h	480×10^{-9} f/h
4	tantaal condensator	8×10^{-9} f/h	32×10^{-9} f/h
		λ_{syst} =	680×10^{-9} f/h

De gemiddelde levensduur van een dergelijke schakeling is dan blijkbaar $\theta_{syst} = 1/\lambda_{syst} \simeq 170$ jaar. Hoewel het hier om een (voor operationele begrippen) zeer lange periode gaat, is het nuttig tevens te beseffen dat van een dergelijk onderdeel vaak een overlevingskans van .9999 wordt geëist, om zodoende bij het totale systeem (van zeg 100 schakelingen in serie) een bedrijfszekerheid van .99 te mogen verwachten. Maar een dergelijke eis (dus R(t) = .9999) houdt in $t \simeq 6$ dagen (ga dat na). Dat wil zeggen, dat reeds na 6 dagen de systeemeis R = .99 is bereikt!

* Uit bovenstaande tabel volgt dat de elektrolytische condensatoren verantwoordelijk zijn voor het grootste deel van de λ_{syst}. Het ware — zoals reeds boven opgemerkt — bij een "redesign" te overwegen een andere oplossing te kiezen. In het algemeen kan worden gesteld, dat een bijkomend voordeel van de hazard rate methode de mogelijkheid is tot analyseren en

opsporen van zwakke delen van een serieschakeling, die aanleiding tot een *herontwerp* geven.

Opgave 2.1:



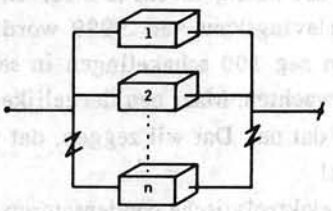
De gemiddelde levensduren zijn respectievelijk θ_A, θ_B en θ_C.
Toon aan dat $\theta_{syst} = 1/(1/\theta_A + 1/\theta_B + 1/\theta_C)$.

Opgave 2.2:

Een seriesysteem bestaat uit 500 identieke units ($\lambda_u = 10^{-6}$ f/h).
Bepaal de gemiddelde levensduur θ_u van een unit in jaren.
Antwoord: Ongeveer 115 jaar.
Hoe groot is de overlevingskans van dit seriesysteem na 100 h?
Antwoord: Ongeveer 95%.

2.5 Het parallelsysteem

Gegeven een parallelschakeling van n eenheden:



Het totale systeem is down, indien alle n eenheden falen. Indien we wederom met E_i, i = 1,2,...,n de gebeurtenis aangeven, dat de i-de eenheid functio-

neert en met $\bar{E}_i$ de complementaire gebeurtenis, dan geldt voor de bedrijfs-*on*zekerheid F_{syst} van de schakeling

$$F_{syst} = P\{\bar{E}_1 \cap \bar{E}_2 \cap \ldots \cap \bar{E}_n\}.$$

Bij onafhankelijke uitvalskansen gaat deze formule over in

$$F_{syst} = P\{\bar{E}_1\} * P\{\bar{E}_2\} * \ldots * P\{\bar{E}_n\}.$$

Indien tenslotte $P\{\bar{E}_i\} = F_i(t)$, i = 1,2,...,n, zijnde de bedrijfs*on*zekerheid van de eenheid ten tijde t, dan is

$$F_{syst}(t) = F_1(t) * F_2(t) * \ldots * F_n(t)$$

of

$$\boxed{F_{syst}(t) = \prod_{i=1}^{n} F_i(t)} \; .$$

Dit nu is de produktregel voor een parallelsysteem:

> De bedrijfs*on*zekerheid van een parallelsysteem wordt verkregen door de afzonderlijke bedrijfs*on*zekerheden van de samenstellende delen met elkaar te vermenigvuldigen.

De bedrijfszekerheid van het systeem kan dan uiteraard gevonden worden met

$$R_{syst}(t) = 1 - F_{syst}(t).$$

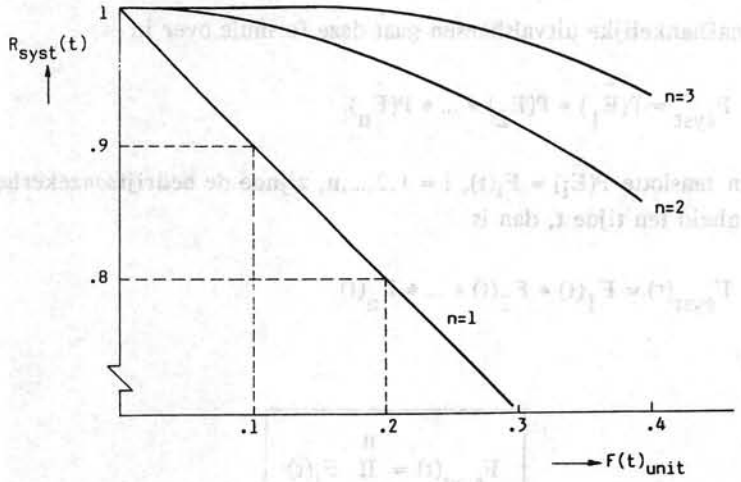
Voor n identieke parallel-geschakelde eenheden geldt dan tenslotte

$$F_{syst}(t) = F(t)^n$$

en

$$R_{syst}(t) = 1 - F(t)^n \; ,$$

waarin F(t) de bedrijfs*on*zekerheid van een enkele unit ten tijde t voorstelt. Hieronder is de $R_{syst}(t)$ uitgezet tegen de bedrijfs*on*zekerheid van een eenheid voor de waarden n = 1, 2 en 3. Hieruit is de invloed van de actieve redundantie duidelijk waarneembaar.



2.6 Toepassing van redundantie

Indien bij de produktformule $F_{syst}(t) = \prod_{i=1}^{n} F_i(t)$ tevens de levensduurverdeling van de toegepaste eenheden negatief-exponentieel wordt geacht, dan worden de formules voor een parallelschakeling van n identieke units

$$F_{syst}(t) = (1 - \exp(-\lambda t))^n$$

en

$$R_{syst}(t) = 1 - (1 - \exp(-\lambda t))^n.$$

Het is, na enig rekenwerk, aan te tonen dat in dit geval geldt:

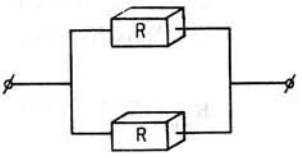
$$\theta_{syst} = \frac{1}{\lambda} \sum_{i=1}^{n} \frac{1}{i},$$

waarin $1/\lambda = \theta_{unit}$.

Uit het voorgaande kunnen we concluderen, dat als de levensduur van de afzonderlijke eenheden negatief-exponentieel verdeeld is, dit dan *niet* het geval is bij het parallelsysteem (dit in tegenstelling tot een seriesysteem).

Voorbeeld:

$$R_{syst}(t) = 1 - F_{syst}(t) =$$
$$= 1 - (1 - \exp(-\lambda t))^2 =$$
$$= 2\exp(-\lambda t) - \exp(-2\lambda t),$$

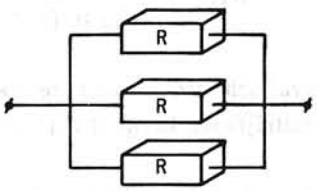


hetgeen dus géén exponentieel verloop weergeeft.
Voorts volgt uit de formule voor θ_{syst} dat toevoeging van extra, redundante eenheden *het meeste effect* heeft, wanneer er nog weinig redundantie is (dus kleine n).

* Uit deze formule ziet men tevens dat als men een eenheid (met gemiddelde levensduur $\theta_u = 1/\lambda$) van een identiek redundant exemplaar voorziet, dat $\theta_{syst} = 3/2\ \lambda = 1.5\ \theta_u$, terwijl de (aanschaf-) kosten zonder meer verdubbelen. Het zou kunnen zijn dat men voor dit bedrag een betere eenheid kan aanschaffen, met een gemiddelde levensduur, die groter is dan $1.5\ \theta_u$ ("*high-rel. component*"). Toepassing van redundante structuren moet in de ontwerpfase derhalve zorgvuldig worden overwogen.

Voorbeeld:

Gegeven is dat bij een 3-parallel-systeem elke unit voor een periode van 500 h een overlevingskans R heeft.
Gevraagd: Hoe groot is $R_{syst}(500\ h)$?



Toepassing van de produktregel levert:

$$F_{syst}(500\ h) = \prod_{i=1}^{3} F(500\ h) = (1 - R)^3,$$

zodat $R_{syst}(500\ h) = 1 - (1 - R)^3 = 3R - 3R^2 + R^3$.

* Dit resultaat kan overigens ook als volgt worden verkregen:
  - De kans, dat na 500 h dit systeem nog werkt met drie goede units = R^3.
  - De kans, dat na 500 h dit systeem nog werkt met één falende unit = $\binom{3}{1} R^2(1 - R)$; ga dat na.
  - De kans, dat na 500 h dit systeem nog werkt met twee falende units = $\binom{3}{2} R(1 - R)^2$.

Daar het hier om drie elkaar uitsluitende bedrijfstoestanden van de parallelschakeling gaat, geldt:

$$R_{syst}(500\ h) = R^3 + 3R^2(1 - R) + 3R(1 - R)^2 = 3R - 3R^2 + R^3.$$

2.7 Hazard rate van een parallelsysteem

De hazard rate z(t) — ook wel *storingsgraad* genoemd, zie paragraaf 1.7D — die bij een n-parallelsysteem behoort, is

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

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

Ga dit na. Voor n = 2 geldt dan blijkbaar

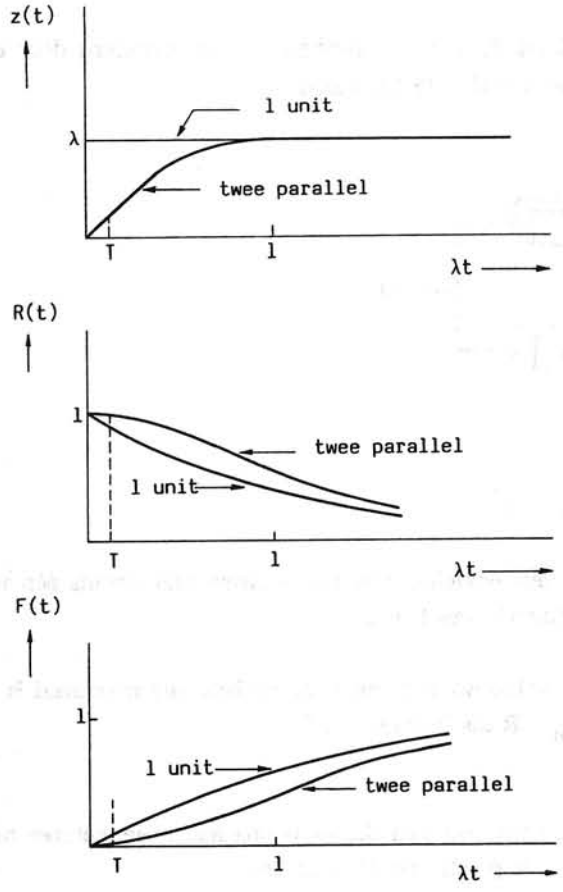
$$z(t) = 2\lambda \frac{\exp(-\lambda t) - \exp(-2\lambda t)}{2\exp(-\lambda t) - \exp(-2\lambda t)},$$

grafisch aldus weer te geven, evenals de bedrijfszekerheid R(t) en de bedrijfs*on*zekerheid F(t) (zie nevenstaande figuur).

Voor $t \to 0$ wordt $z(t) \to 0$ en voor $t \to \infty$ wordt $z(t) \to \lambda$.

> In het algemeen kan worden gesteld dat de storingsgraad van een parallelsysteem bij nul begint en daarna asymptotisch naar λ (dat wil zeggen de hazard rate van een enkele unit) nadert.

Nu zullen in het algemeen bij modelberekeningen bedrijfstijden T worden bekeken, waarvoor geldt dat $\lambda T << 1$ of $T << \theta_u$, daar anders $R_{syst}(t) = 2\exp(-\lambda T) - \exp(-2\lambda T)$ te klein en derhalve operationeel oninteressant wordt. Bij dit praktische gegeven blijkt inderdaad uit de schets van z(t) door de toepassing van redundantie de storingsgraad duidelijk te verminderen.

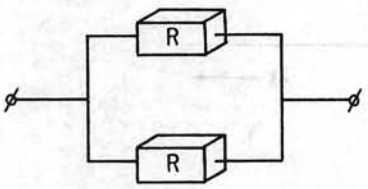


Maar toch bestaat er bij actieve redundantie een sluimerend gevaar. Voor $\lambda T << 1$ kan $R_{syst}(T)$ namelijk benaderd worden door $R_{syst}(T) \simeq 1 - \lambda^2T^2$ met $\exp(-\lambda T) \simeq 1 - \frac{\lambda T}{1!} + \frac{(\lambda T)^2}{2!}$, zodat $F_{syst}(T) \simeq \lambda^2T^2$. Een dramatisch gegeven is dus, dat bij een 2-parallelsysteem voor kleine bedrijfstijden de bedrijfsonzekerheid kwadratisch met T toeneemt!

Op welk tijdstip T onderhoudsmatig van tevoren ingegrepen zal moeten worden, dient per geval te worden bekeken, maar door de stijgende storingsgraad zal correctief onderhoud (dit is onderhoud, *nadat* er storing is opgetreden) als niet wenselijk moeten worden beoordeeld (zie paragraaf 5.9).

Opgave 2.3:

De overlevingskans R van een eenheid wordt verbeterd door er een identieke unit aan parallel te schakelen.



Toon aan dat:

(a) $R_{syst} = 2R - R^2$.

De verbetering ten opzichte van een systeem met slechts één unit is $R_{syst} - R$, een functie van R dus.

(b) Ga na voor welke waarde van R de verbetering maximaal is.
(c) Teken $R_{syst} - R$ als functie van R.

Opgave 2.4:

Een viermotorig vliegtuig kan desnoods nog met twee motoren blijven vliegen, ongeacht de plaats van de motoren.
Toon aan dat:

(a) De kans dat het vliegtuig behouden aankomt, gelijk is aan .996 indien de bedrijfszekerheid van elke motor gedurende een vlucht 90% bedraagt.
(b) Deze kans gelijk is aan .980, als bovendien nog vereist is, dat in het geval nog twee motoren werken, deze zich aan weerszijde van de romp dienen te bevinden, dus aan iedere vleugel één.

Opgave 2.5:

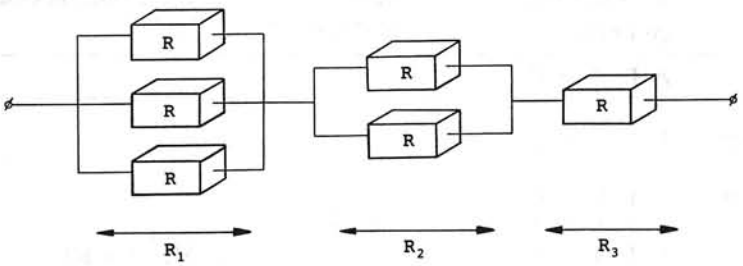
Voor een bepaalde bedrijfstijd heeft een unit een overlevingskans van R = .70.
Toon aan dat minstens drie eenheden hieraan moeten worden parallel geschakeld, opdat $R_{syst} \geq .99$.

2.8 Complexe systemen

Tot dusver hebben wij te maken gehad met twee basisconfiguraties: het *seriesysteem* en het *parallelsysteem.* In deze en de volgende paragraaf zullen een drietal methoden worden besproken om de R_{syst} te berekenen uit de R van de afzonderlijke units voor het geval van complexere systemen. Als eerste methode noemen we de mogelijkheid om in een complex systeem de samenstellende delen zodanig te groeperen en samen te nemen, dat het *bedrijfszekerheidsblokschema* tot een combinatie van de twee grondvormen kan worden teruggebracht.

Voorbeeld:

Zij de overlevingskans van ieder der units R.



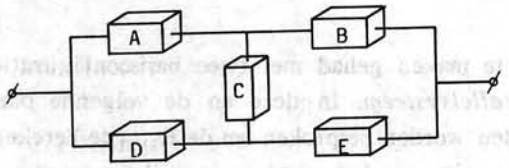
Ga na dat in dit geval geldt $R_{syst} = R_1R_2R_3$ met
$R_1 = (3R - 3R^2 + R^3)$, $R_2 = (2R - R^2)$ en $R_3 = R$, mits de uitvalskansen onafhankelijk zijn.

Veelal echter resulteert een bedrijfszekerheidsanalyse in een blokschema, dat een dergelijke vereenvoudiging niet toestaat, zoals bij een brugconstructie bijvoorbeeld. We noemen nog een tweetal methodieken om — ondanks deze belemmering — toch de overlevingskans in zo'n geval te berekenen.

Bij de volgende methode worden *alle* actieve toestanden geïnventariseerd, waarin het totale systeem kan verkeren, waarbij dan tevens de kansen hierop worden berekend. De sommatie van al deze kansen levert de systeemoverlevingskans R_{syst} vanwege het disjuncte karakter van al deze up-toestanden.

Voorbeeld:

Bepaal R_{syst} van onderstaande brugconfiguratie van vijf identieke eenheden, ieder met een overlevingskans R.



Indien we uitgaan van het catastrofale faalmodel, dat wil zeggen als we aannemen dat een unit (en ook het systeem) slechts goed kan functioneren (toestand 1) òf gefaald heeft (toestand 0), dan ziet de bovenbedoelde toestandsinventarisatie er als volgt uit:

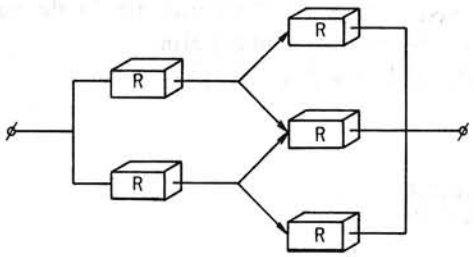
	Toestand van de units	Idem systeem	Kans systeemtoestand "up"
	A B C D E		
0 fout	1 1 1 1 1	1	R^5
1 fout	1 1 1 1 0	1	
	1 1 1 0 1	1	
	1 1 0 1 1	1	$\rightarrow 5R^4(1 - R)$
	1 0 1 1 1	1	
	0 1 1 1 1	1	
2 fout	1 1 1 0 0	1	
	1 1 0 1 0	1	
	1 0 1 1 0	0	
	0 1 1 1 0	1	
	0 0 1 1 1	1	$\rightarrow 8R^3(1 - R)^2$
	0 1 0 1 1	1	
	0 1 1 0 1	0	
	1 0 1 0 1	1	
	1 1 0 0 1	1	
	1 0 0 1 1	1	
3 fout	0 0 0 1 1	1	
	0 0 1 0 1	0	
	0 1 0 0 1	0	
	1 0 0 0 1	0	
	0 1 1 0 0	0	$\rightarrow 2R^2(1 - R)^3$
	1 1 0 0 0	1	
	1 0 1 0 0	0	
	1 0 0 1 0	0	
	0 1 0 1 0	0	
	0 0 1 1 0	0	

Omdat bij vier en vijf falende units geen actieve systeemtoestanden meer voorkomen, geldt

$$R_{syst} = R^5 + 5R^4(1 - R) + 8R^3(1 - R)^2 + 2R^2(1 - R)^3$$
$$= 2R^2 + 2R^3 - 5R^4 + 2R^5.$$

Een eenvoudige, doch helaas — zoals uit het voorbeeld blijkt — een bewerkelijke methode.

Opgave 2.6:



De overlevingskans van iedere unit is R. De paden kunnen slechts in de pijlrichting doorlopen worden. Ga voor uzelf na dat deze structuur niet in een serie-parallelstructuur kan worden omgezet.
Laat zien dat $R_{syst} = 4R^2 - 3R^3 - R^4 + R^5$.

2.9 Conditioneel theorema

Een snellere methode om de bedrijfszekerheid van een *gemengd systeem* te berekenen is de toepassing van het *conditioneel theorema.* Hierbij zonderen we één eenheid af, die een centrale positie in de structuur van het bedrijfszekerheidsmodel inneemt.
Er geldt dan

$$P\{S\} = P\{S \mid U\}\, P\{U\} + P\{S \mid \bar{U}\}\, P\{\bar{U}\},$$

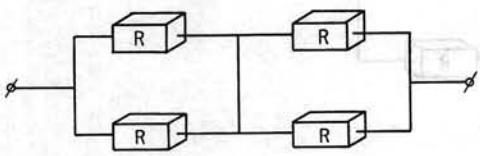
waarin U de gebeurtenis voorstelt, dat de centrale unit functioneert, S de gebeurtenis dat het totale systeem werkt, terwijl met $\bar{U}$ de complementaire gebeurtenis bedoeld wordt.

De juistheid van deze uitdrukking kan als volgt worden ingezien.
Daar $P\{A \cap B\} = P\{B \mid A\}\, P\{A\}$ volgt:
$P\{S \mid U\}\, P\{U\} = P\{U \cap S\}$ en $P\{S \mid \bar{U}\}\, P\{\bar{U}\} = P\{\bar{U} \cap S\}$, zodat de overlevingskans $R_{syst} = P\{S\}$ gevonden kan worden door
$P\{S \mid U\}\, P\{U\} + P\{S \mid \bar{U}\}\, P\{\bar{U}\} = P\{U \cap S\} + P\{\bar{U} \cap S\} = P\{S\}$.

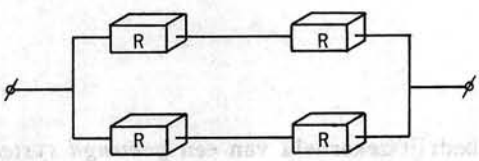
* Indien nodig, moet deze *decompositiemethode* enige malen worden herhaald om de totale configuratie tot een combinatie van serie- en parallelsystemen te reduceren.

Voorbeeld:

We zullen opnieuw de R_{syst} van de brugconfiguratie in de vorige paragraaf berekenen. Laat C de centrale eenheid zijn.
Stel C faalt niet, dan geldt $P\{S \mid U\} = (2R - R^2)^2$.



Stel C faalt wel, dan geldt $P\{S \mid \bar{U}\} = 2R^2 - R^4$.



Dan is $R_{syst} = P\{S \mid U\}\, P\{U\} + P\{S \mid \bar{U}\}\, P\{\bar{U}\}$

$$= (2R - R^2)^2\, R + (2R^2 - R^4)\,(1 - R)$$

$$= 2R^2 + 2R^3 - 5R^4 + 2R^5,$$

hetzelfde resultaat dus als in de vorige paragraaf.

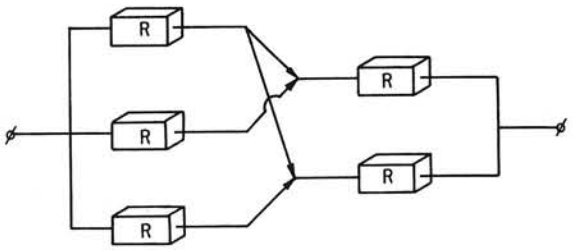
Opgave 2.7 :

Bereken R_{syst} voor een twee-unit parallelsysteem met behulp van het conditioneel theorema, en controleer het resultaat met de produktregel.

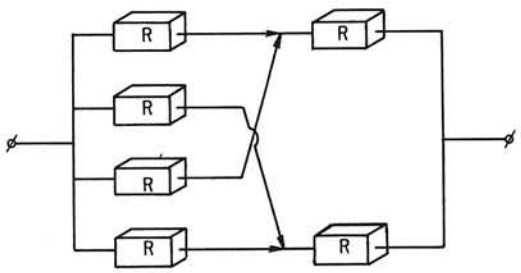
Opgave 2.8 :

Toon aan dat de systeemoverlevingskans R_{syst} van onderstaande configuratie van vijf identieke systemen (ieder met een overlevingskans R) gelijk is aan

$$R_{syst} = 4R^2 - 3R^3 - R^4 + R^5.$$



Opgave 2.9 :

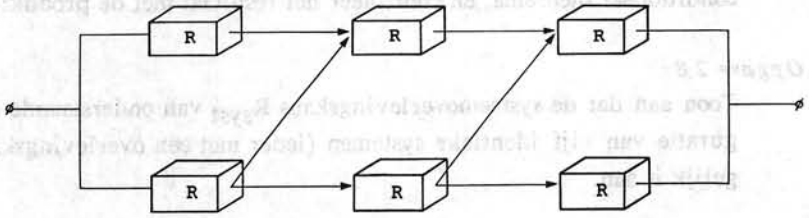


Toon aan dat:

$$R_{syst} = 4R^2 - 2R^3 - 4R^4 + 4R^5 - R^6.$$

Doe dit volgens twee methoden.

Opgave 2.10 :



Toon aan dat: $R_{syst} = 4R^3 - 3R^4$.

3 BEREKENING VAN OPERATIONELE GROOTHEDEN

In dit hoofdstuk zullen we een tweetal berekeningsmethodieken laten zien die gebruikt kunnen worden om voor allerlei systemen vanuit het catastrofaal faalmodel verschillende operationele grootheden te berekenen zoals de beschikbaarheid, de MTTF en de overlevingskans van het systeem. Beide methodieken kunnen naast elkaar gebruikt worden waarbij de eerste methodiek de minste voorkennis op wiskundig gebied vooronderstelt en de tweede methodiek, gebaseerd op de Laplace-transformatie, in vele modellen voor een korte en elegante oplossing zorgt.

3.1 Splitsing van de levensduur

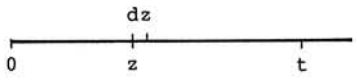
De eerste methodiek gaat ervan uit dat we de levensduur X van een systeem op kunnen splitsen in twee perioden. In de eerste periode geven we de levensduur aan met U, in de tweede periode met V. Het moment van overgang van de eerste naar de tweede periode moeten we daarbij zo kiezen dat de verdelingen van de stochasten U en V bekend zijn, bijvoorbeeld door hun respectievelijke betrouwbaarheden R_U en R_V. We nemen verder aan dat de stochasten U en V onafhankelijk zijn. Het is duidelijk dat voor de totale levensduur X van het systeem zal gelden

$$X = U + V.$$

Verder is dan

$$R_{syst}(t) = P\{X > t\} = P\{U > t\} + P\{U < t \cap U + V > t\}. \qquad (3.1)$$

De laatste stelt de kans voor dat de eerste periode voor het tijdstip t eindigt waarna echter de tweede periode voldoende lang duurt om het totale systeem tenminste tot tijdstip t te laten functioneren.
Om $P\{U < t \cap U + V > t\}$ te bepalen berekenen we eerst de kans dat de levensduur U eindigt tussen tijdstip z en z + dz (zie onderstaande figuur), waarna de tweede periode tenminste nog t - z duurt.



Eenvoudig is in te zien dat de kans op deze deelgebeurtenis gegeven wordt door

$$P\{z < U < z + dz \cap U + V > t\} = f_U(z)\, dz \cdot R_V(t - z).$$

Sommatie van alle intervallen $(z, z + dz)$ tussen 0 en t en tevens $dz \to 0$ levert dan de uitdrukking

$$P\{U < t \cap U + V > t\} = \int_0^t f_U(z)\, R_V(t - z)\, dz.$$

Dit invullen in (3.1) geeft dan

$$R_{syst}(t) = R_U(t) - \int_0^t R_U'(z)\, R_V(t - z)\, dz. \qquad (3.2)$$

Aan de hand van enkele voorbeelden zullen we laten zien hoe met formule (3.2) gewerkt kan worden en vooral hoe de splitsing in twee perioden gekozen moet worden.

3.2 Gemiddelde levensduur van een parallelsysteem

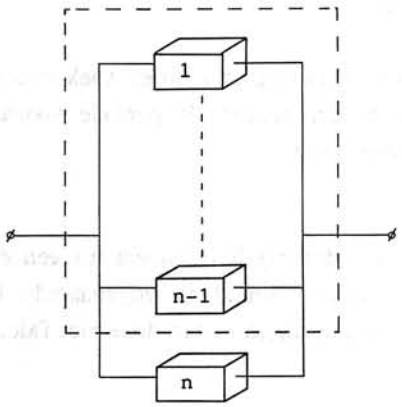
We bestuderen een parallelsysteem met n identieke componenten. Met θ_n geven we de verwachte levensduur van zo'n systeem aan. We weten dan dat

$$\theta_n = \int_0^\infty R_n(t)\, dt,$$

waarin $R_n(t)$ de betrouwbaarheid van het systeem aangeeft. We weten dat in geval van exponentieel verdeelde levensduur van de aparte units geldt

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

Helaas levert rechtstreekse integratie nu complex rekenwerk, vandaar dat we de methode uit paragraaf 3.1 kiezen.
We splitsen het parallelsysteem in twee delen, namelijk de "bovenste" n-1 componenten en de laatste component.



Met de eerste periode duiden we nu aan de periode waarin de "bovenste" n-1 componenten als deel-parallelsysteem functioneren en de tweede periode is de periode waarin, na het falen van het n-1 deelsysteem de laatste component eventueel nog functioneert.
Nu geldt $R_U(t) = R_{n-1}(t)$ en $R_V(t - z) = e^{-\lambda z} \cdot e^{-\lambda(t-z)}$ waarbij de laatste term opgebouwd is uit twee kansen, de eerste kans dat de n-de unit nog functioneert op tijdstip z en de tweede kans dat de n-de unit daarna nog t - z functioneert. Invullen in formule (3.2) geeft

$$R_n(t) = R_{n-1}(t) - \int_0^t R_U'(z)\, e^{-\lambda z}\, e^{-\lambda(t-z)}\, dz,$$

waaruit volgt

$$R_n(t) = R_{n-1}(t) + e^{-\lambda t} - e^{-\lambda t} R_{n-1}(t).$$

Integratie over het interval $(0,\infty)$ geeft nu

$$\theta_n = \theta_{n-1} + \frac{1}{\lambda} - \int_0^\infty e^{-\lambda t}(1 - (1 - e^{-\lambda t})^{n-1})\, dt,$$

dus

$$\theta_n = \theta_{n-1} + \frac{1}{n\lambda}.$$

Omdat eenvoudig geldt $\theta_1 = 1/\lambda$ levert deze recurrente betrekking

$$\theta_n = \left(\sum_{i=1}^{n} \frac{1}{i}\right) \cdot \frac{1}{\lambda}.$$

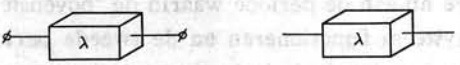
Deze formule was reeds in paragraaf 2.6 aangekondigd.

3.3 Systemen met een reserve-eenheid

Systemen waarbij een reserve-eenheid aanwezig is kunnen vaak doorgerekend worden door als perioden te onderscheiden de periode voordat de reserve-eenheid ingezet is en de periode daarna.

Voorbeeld:

In het eenvoudigste geval bestaat daarbij het systeem uit een enkele component en een identieke reserve-eenheid in zogenaamde koude standby (zolang de reserve niet ingeschakeld is kan deze niet falen).



Voor de periode U geldt dan $R_U(t) = e^{-\lambda t}$, en voor de periode V geldt analoog $R_V(t) = e^{-\lambda t}$, mits natuurlijk weer de exponentiële verdeling wordt aangenomen.
Met formule (3.2) volgt dan

$$R_{syst} = e^{-\lambda t} - \int_0^t - \lambda e^{-\lambda z} e^{-\lambda(t-z)} dz$$

$$= (1 + \lambda t) e^{-\lambda t}.$$

Voorbeeld:

Een systeem bestaat uit twee parallel geschakelde identieke eenheden met één eenheid als reserve; deze reserve-eenheid wordt ingezet als beide units uit het oorspronkelijke systeem gefaald hebben.
Er geldt:

$$R_U(t) = (1 - (1 - e^{-\lambda t})^2) = 2e^{-\lambda t} - e^{-2\lambda t};$$

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

Met formule (3.2) volgt

$$R_{syst}(t) = 2e^{-\lambda t} - e^{-2\lambda t} - \int_0^t (-2\lambda e^{-\lambda z} + 2\lambda e^{-2\lambda z}) \cdot e^{-\lambda(t-z)} dz,$$

en vereenvoudigd geeft dit

$$R_{syst}(t) = e^{-2\lambda t} + 2\lambda t\, e^{-\lambda t}.$$

Hieruit kan eenvoudig θ_{syst} berekend worden:

$$\theta_{syst} = \frac{1}{2\lambda} + \frac{2}{\lambda} = \frac{5}{2}\,\theta_{unit}.$$

Voorbeeld:

Voor het brugsysteem uit 2.8 hebben we gevonden dat in geval van exponentieel verdeelde units geldt

$$R(t) = 2e^{-2\lambda t} + 2e^{-3\lambda t} - 5e^{-4\lambda t} + 2e^{-5\lambda t};$$

$$\theta = \frac{49}{60}\,\theta_{unit}.$$

We voegen aan dit systeem een reserve-unit toe die we direct inzetten als de eerste unit faalt. Dit falen leidt niet tot een system failure, maar ons vervangingsvoorschrift schrijft directe vervanging voor. Verder dienen we ons goed te realiseren dat op het moment van falen de overige units nog functioneren, en op grond van de exponentiële verdeling dus als nieuw te beschouwen zijn.
Vandaar dat

$$R_U(t) = e^{-5\lambda t};$$

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

Nu geldt

$$R_{syst}(t) = e^{-5\lambda t} + \int_0^t 5\lambda e^{-5\lambda z}\, R(t - z)\, dz,$$

waaruit volgt

$$R_{syst}(t) = \frac{10}{3}\, e^{-2\lambda t} + 5e^{-3\lambda t} - 25e^{-4\lambda t} + (\frac{53}{3} + 10\lambda t)\, e^{-5\lambda t};$$

$$\theta_{syst} = \frac{61}{60}\,\theta_{unit}.$$

Opgave 3.1:

Een seriesysteem bestaat uit twee identieke componenten, ieder met een failure rate λ, en een identieke reserve.
Toon aan dat $R_{syst}(t) = (1 + 2\lambda t)\, e^{-2\lambda t}$.

Opgave 3.2:

Een seriesysteem bestaat uit twee componenten, met failure rates λ respectievelijk μ. Bij falen is er een reserve-unit die op beide plaatsen ingezet kan worden, waarbij de levensduur van de reserve-unit zich gaat gedragen als de levensduur van de unit die vervangen is (dit kan bijvoorbeeld als de slijtage van de unit sterk afhankelijk is van de plaats waar deze wordt ingezet).
Toon aan dat

$$R_{syst}(t) = (1 + (\lambda + \mu)\, t)\, e^{-(\lambda+\mu)t};$$

$$\theta_{syst} = \frac{2}{\lambda + \mu}.$$

3.4 Berekeningsmethodiek met behulp van Laplace

Deze methodiek is gebaseerd op een Markov-proces, waarbij van een *overgangsmatrix* gebruik wordt gemaakt. Daarbij nemen we aan, dat er een verzameling discrete, elkaar wederzijds uitsluitende toestanden bestaat, waarin het desbetreffende systeem door het optreden van storingen en eventueel door het verrichten van herstelwerkzaamheden kan terechtkomen. De bepaling van die volledige verzameling zullen we voortaan als de *toestandsinventarisatie* aanduiden. De (*conditionele*) *overgangskansen* (transition probabilities) tussen al deze toestanden (states) zijn dan in bovenbedoelde matrix ondergebracht.

De toestand van het systeem ten tijde t kan door een vector P(t) in een (n+1)-dimensionale ruimte aldus worden beschreven

$$P(t) = (P_0(t)\ P_1(t) \ldots P_j(t) \ldots P_n(t)),$$

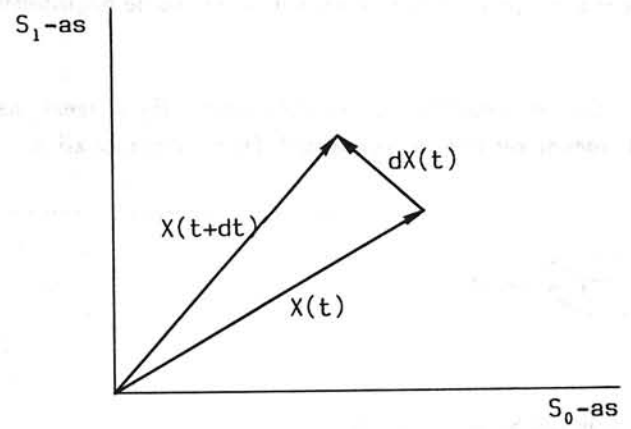
waarin $P_j(t)$ de kans voorstelt, dat het systeem zich op het tijdstip t in toestand S_j, $j = 0,1,\ldots,n$ bevindt.
Indien we veronderstellen dat de overgangskansen λ_{jk}, $j = 0,1,\ldots,n$; $k = 0,1,\ldots,n$; $j \neq k$ om van toestand S_j naar S_k over te gaan, constant zijn

(homogeen Markov-proces) en dus onafhankelijk van de voorgeschiedenis, dan is de overgangsmatrix als volgt weer te geven:

$$U = \begin{pmatrix} 1 - \lambda_{00}dt & \lambda_{01}dt & \cdots & \lambda_{0n}dt \\ \lambda_{10}dt & 1 - \lambda_{11}dt & \cdots & \lambda_{1n}dt \\ \vdots & & & \vdots \\ \lambda_{n0}dt & \cdots & & 1 - \lambda_{nn}dt \end{pmatrix}.$$

Hierin stelt verder $1 - \lambda_{00}dt$ de kans voor dat het systeem, gegeven dat het zich ten tijde t in toestand S_0 bevindt, zich ten tijde $t + dt$ daar alsnog bevindt, waaruit volgt dat

$$\lambda_{00} = \sum_{j=1}^{n} \lambda_{0j} \text{ , etcetera.}$$



Treedt in het interval (t, t + dt) een toestandsverandering op, dan geldt hiervoor de volgende matrixvergelijking:

$$P(t + dt) = P(t)\, U.$$

Invulling hiervan in $dP(t) = P(t + dt) - P(t)$ (zie bijgaande figuur) geeft:

$$dP(t) = P(t)\,(U - I),$$

waarin I een eenheidsmatrix voorstelt. Omdat in $M = U - I$ alle termen 1 wegvallen, worden alle componenten van de orde dt.
Vandaar

$$dP(t) = P(t)\, M\, dt$$

of uitgeschreven

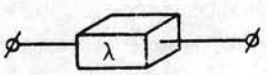
$$\left(\frac{dP_0(t)}{dt} \ \ldots \ \frac{dP_n(t)}{dt}\right) = (P_0(t) \ldots P_n(t)) \begin{pmatrix} -\lambda_{00} & \lambda_{01} & & \lambda_{0n} \\ \lambda_{10} & -\lambda_{11} & \cdots\cdots & \lambda_{in} \\ \lambda_{n0} & \lambda_{ni} & \cdots\cdots & -\lambda_{nn} \end{pmatrix}.$$

Uitwerking hiervan levert n+1 differentiaalvergelijkingen van de volgende vorm:

$$\frac{dP_k(t)}{dt} = \sum_{j=0}^{n} P_j(t)\, \lambda_{jk}, \qquad k = 0,1,\ldots,n,$$

waaruit $P_j(t)$, $j = 0,1,\ldots,n$ kunnen worden berekend, als de begintoestand P_0 bekend is.

We zullen deze theorie toepassen op een zéér eenvoudig systeem, namelijk een enkele unit, zonder reparatiemogelijkheid. De failure rate zij λ.



Toestandsinventarisatie: $S_0 \equiv$ unit goed.
$S_1 \equiv$ unit gefaald.
Toestandsvector $P(t) = (P_0(t)\ P_1(t))$.
Overgangsmatrix

$$U = \begin{array}{c} \\ S_0 \\ S_1 \end{array} \begin{array}{c} \begin{array}{cc} S_0 & S_1 \end{array} \\ \begin{pmatrix} 1 - \lambda dt & \lambda dt \\ 0 & 1 \end{pmatrix} \end{array}.$$

* De waarde 1 in de matrix duidt op een *absorberende* toestand: éénmaal in toestand S_1 beland, blijft het systeem aldaar, daar er géén herstel mogelijk is.

De matrixvergelijking wordt hier

$$\left(\frac{dP_0(t)}{dt} \quad \frac{dP_1(t)}{dt}\right) = (P_0(t)\ P_1(t)) \begin{pmatrix} -\lambda & \lambda \\ 0 & 0 \end{pmatrix},$$

zodat $\frac{dP_0(t)}{dt} = -\lambda P_0(t)$ en $\frac{dP_1(t)}{dt} = \lambda P_0(t)$ met als beginvector $P(0) = (1 \quad 0)$.

Laplace-transformatie van de differentiaalvergelijking geeft $sP_0(s) - 1 = -\lambda P_0(s)$ en $sP_1(s) = \lambda P_0(s)$, waaruit

$$P_0(s) = 1/(s + \lambda) \rightarrow P_0(t) = \exp(-\lambda t).$$
$$P_1(s) = \lambda/s(s + \lambda) \rightarrow P_1(t) = 1 - \exp(-\lambda t).$$

Zie bijlage voor een verklaring van dit resultaat.

3.5 Gemiddelde levensduur met behulp van Laplace

We hebben in paragraaf 1.11 de gemiddelde levensduur θ van een *niet-bewaakt* systeem ter sprake gebracht. Daarmee is dan bedoeld de MTTF (Mean-Time-To-Failure), dus de verwachtingswaarde van de periode, die verloopt vanaf de in bedrijfstelling tot aan de eerstvolgende storing.
Indien de overlevingskansfunctie R(t) bekend is, is de θ te berekenen met behulp van $\theta = \int_0^\infty R(t)\,dt$. Maar er is nog een andere weg om deze grootheid te vinden. Een weg, die met name voordelen biedt indien de integratie moeilijk, bewerkelijk of onmogelijk is.

Per definitie is de Laplace-getransformeerde R(s) van de bedrijfszekerheid R(t)

$$R(s) \stackrel{\text{def}}{=} \int_0^\infty e^{-st} R(t)\,dt,$$

waaruit direct volgt

$$\theta = \lim_{s \to 0} R(s) = \int_0^\infty R(t)\,dt.$$

* In het voorbeeld van paragraaf 3.2 is $R(s) = P_0(s) = 1/(s + \lambda)$, waaruit $\theta = \lim_{s \to 0} R(s) = 1/\lambda$, hetgeen eveneens door $\int_0^\infty \exp(-\lambda t)\, dt$ kan worden verkregen.

3.6 Samenvatting Laplace berekeningsprocedure

Samenvattend kan de procedure ter berekening van bedrijfszekerheids- en onderhoudsmodellen stapsgewijs als volgt worden weergegeven:

Stap 1: Inventariseer alle mogelijke systeemtoestanden $S_0 \; S_1 \ldots S_n$.

↓

Stap 2: Stel de overgangsmatrix U op:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \\ \vdots \\ S_n \end{array} \begin{array}{c} \begin{array}{ccccc} S_0 & & S_1 & & S_n \end{array} \\ \begin{pmatrix} 1 - \lambda_{00}dt & \lambda_{01}dt & \cdots & \lambda_{0n}dt \\ \lambda_{10}dt & 1 - \lambda_{11}dt & \cdots & \vdots \\ \lambda_{20}dt & \lambda_{21}dt & \cdots & \vdots \\ \vdots & & & \\ \lambda_{n0}dt & \cdots & & 1 - \lambda_{nn}dt \end{pmatrix} \end{array}.$$

↓

Stap 3: Het opstellen van de differentiaalvergelijkingen door de matrix *kolomsgewijs* af te tasten.
Dus

$$\frac{dP_0(t)}{dt} = -\lambda_{00}P_0(t) + \lambda_{10}P_1(t) + \lambda_{20}P_2(t) + \ldots$$

↓
etc.

↓

Stap 4:

Oplossen van de differentiaalvergelijking met behulp van Laplace-transformatie

$$sP_0(s) - P_0(t=0) = -\lambda_{00}P_0(s) + \lambda_{10}P_1(s) + \lambda_{20}P_2(s) + \ldots$$

$\downarrow$

etc.

waaruit uitdrukkingen gevonden kunnen worden voor $P_0(s),\ldots,P_n(s)$.

Stap 5:

Uit de Laplace-getransformeerde van de overlevingskans R(t):

$$R(s) = \sum_j P_j(s),$$ j = werkende toestand van het systeem,

kan de MTTF worden berekend volgens

$$\theta = \lim_{s\to 0} R(s).$$

Stap 6:

Indien praktisch mogelijk, kan uit $P_i(s)$, i = 0,1,...,n door terugtransformatie $P_i(t)$ worden gevonden (zie bijlage), waaruit de systeemoverlevingskans volgt

$$R(t) = \sum_j P_j(t),$$ j = werkende toestand van het systeem.

We zullen aan de hand van een voorbeeld bovenstaande procedure stapsgewijs volgen. Gegeven een parallelschakeling van twee identieke eenheden.

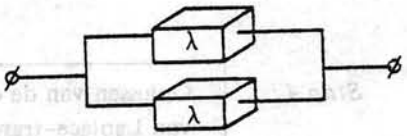
Bereken met behulp van een overgangsmatrix de bedrijfszekerheid $R_{syst}(t)$ van deze schakeling.

Stap 1: Toestandsinventarisatie:

$S_0 \equiv$ twee eenheden goed.

$S_1 \equiv$ één eenheid goed; één eenheid fout.

$S_2 \equiv$ twee eenheden fout.



Stap 2: Stel de overgangsmatrix op:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{pmatrix} 1 - 2\lambda dt & 2\lambda dt & 0 \\ 0 & 1 - \lambda dt & \lambda dt \\ 0 & 0 & 1 \end{pmatrix} \end{array},$$

daar de kans, dat in het tijdperk (t, t + dt) één van de twee actieve units faalt, gelijk is aan $2\lambda dt$.
Ga dat na.

Stap 3: Stel de differentiaalvergelijkingen op, door kolomsgewijze aftasting van U

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t)$$

$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - \lambda P_1(t)$$

$$\frac{dP_2(t)}{dt} = \lambda P_1(t).$$

Stap 4: Laplace-transformatie van de differentiaalvergelijking met als beginvoorwaarden $P_0(0) = 1$, $P_1(0) = 0$ en $P_2(0) = 0$ levert

$$sP_0(s) - 1 = -2\lambda P_0(s)$$

$$sP_1(s) = 2\lambda P_0(s) - \lambda P_1(s)$$

$$sP_2(s) = \lambda P_1(s),$$

waaruit

$$P_0(s) = \frac{1}{s + 2\lambda}$$

$$P_1(s) = \frac{2\lambda}{(s + \lambda)(s + 2\lambda)}$$

$$P_2(s) = \frac{2\lambda^2}{s(s + 2\lambda)(s + \lambda)} .$$

Stap 5: De twee werkende toestanden van het systeem zijn S_0 en S_1, dus

$$R_{syst}(s) = P_0(s) + P_1(s),$$

zodat

$$\theta = \lim_{s \to 0} R_{syst}(s) = \frac{1}{2\lambda} + \frac{1}{\lambda} = \frac{3}{2\lambda} .$$

Stap 6: Uit $P_0(s) = \frac{1}{s + 2\lambda}$ volgt $P_0(t) = \exp(-2\lambda t)$.

Uit $P_1(s) = \frac{2\lambda}{(s + \lambda)(s + 2\lambda)} = \frac{2}{s + \lambda} - \frac{2}{s + 2\lambda}$ (breuksplitsen)

volgt $P_1(t) = 2 \exp(-\lambda t) - 2 \exp(-2\lambda t)$, zodat

$$R_{syst}(t) = P_0(t) + P_1(t) = 2 \exp(-\lambda t) - \exp(-2\lambda t).$$

Opgave 3.3:

Gegeven een systeem bestaande uit drie identieke units, met ieder een failure rate λ. Dit systeem functioneert zolang twee van de drie units goed zijn (zo'n systeem wordt wel een twee-uit-drie-systeem genoemd). Bepaal $R_{syst}(t)$.

4 ONBEWAAKTE SYSTEMEN

4.1 Onbewaakte systemen

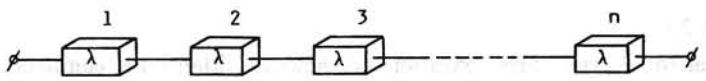
In dit hoofdstuk zullen we de in hoofdstuk 3 behandelde Laplace berekeningsmethodiek toepassen op systemen, die niet zijn *bewaakt*, dat wil zeggen waaraan in de bedrijfsfase geen aandacht wordt besteed en waaraan — nadat er een storing is opgetreden — géén reparatie wordt verricht. De faaltoestand is derhalve als een *absorberende toestand* op te vatten, die in de overgangsmatrix met een 1 wordt aangegeven, omdat het hier een blijvende situatie betreft.

* In hoofdstukken 5 en 7 zijn daarentegen de *bewaakte* systemen in beschouwing genomen, waarbij door menselijk ingrijpen het falende systeem wordt hersteld en opnieuw in bedrijf wordt gebracht. In dat geval wordt eveneens de *beschikbaarheidsgraad* als operationele grootheid berekend.

Aan de hand van enige voorbeelden wordt hieronder nagegaan, hoe de berekening van (a) de overlevingskans R(t) en (b) de gemiddelde levensduur θ van enige modellen wordt uitgevoerd. Na bestudering hiervan is het zeer aan te bevelen de afleidingen nog eens zelfstandig uit te werken.

4.2 Enige berekeningsvoorbeelden

Voorbeeld 1:



Bereken R(t) en θ van dit seriesysteem.
Toestandsinventarisatie: S_0 ≡ n eenheden goed.
S_1 ≡ 1 eenheid fout; (n-1) eenheden goed (system down).

Overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \end{array} \begin{array}{c} \begin{array}{cc} S_0 & S_1 \end{array} \\ \begin{pmatrix} 1 - n\lambda dt & n\lambda dt \\ 0 & 1 \end{pmatrix} \end{array},$$

want de kans dat van de n eenheden er één faalt in de periode $(t, t + dt)$ is $n\lambda dt$.
Ga na dat hieruit volgt

$$\frac{dP_0(t)}{dt} = -n\lambda P_0(t) \quad \text{en} \quad \frac{dP_1(t)}{dt} = n\lambda P_0(t) .$$

Laplace getransformeerd levert dit, aannemende dat in de begintoestand alle eenheden goed functioneren:

$$sP_0(s) - 1 = -n\lambda P_0(s) \quad \text{en} \quad sP_1(s) = n\lambda P_0(t).$$

We zien hieruit dat $P_0(s) = 1/(s + n\lambda)$ en $P_1(s) = n\lambda/(s(s + n\lambda))$, waaruit volgt

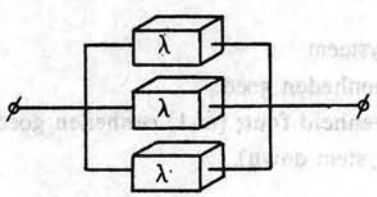
$$R(t) = P_0(t) = \exp(-n\lambda t)$$

en

$$\theta = \lim_{s \to 0} P_0(s) = \frac{1}{n\lambda} = \frac{1}{n}\,\theta_{\text{unit}} .$$

Voorbeeld 2:

Bereken θ van drie parallel geschakelde identieke eenheden. Het systeem is down als alle eenheden falen.



Toestandsinventarisatie: $S_0 \equiv$ 3 eenheden goed.
$S_1 \equiv$ 2 eenheden goed.
$S_2 \equiv$ 1 eenheid goed.
$S_3 \equiv$ systeem faalt.

Overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{cccc} S_0 & S_1 & S_2 & S_3 \end{array} \\ \begin{pmatrix} 1 - 3\lambda dt & 3\lambda dt & 0 & 0 \\ 0 & 1 - 2\lambda dt & 2\lambda dt & 0 \\ 0 & 0 & 1 - \lambda dt & \lambda dt \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Hieruit volgen de differentiaalvergelijkingen

$$\frac{dP_0(t)}{dt} = -3\lambda P_0(t)$$

$$\frac{dP_1(t)}{dt} = 3\lambda P_0(t) - 2\lambda P_1(t)$$

$$\frac{dP_2(t)}{dt} = 2\lambda P_1(t) - \lambda P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda P_2(t) .$$

Laplace-transformatie hiervan geeft ($P_0(0) = 1$)

$$P_0(s) = \frac{1}{s + 3\lambda}$$

$$P_1(s) = \frac{3\lambda}{s + 2\lambda} \cdot \frac{1}{s + 3\lambda}$$

$$P_2(s) = \frac{2\lambda}{s + \lambda} \cdot \frac{3\lambda}{s + 2\lambda} \cdot \frac{1}{s + 3\lambda}$$

zodat uiteindelijk

$$\theta_{syst} = \lim_{s \to 0} (P_0(s) + P_1(s) + P_2(s)) = 11/6\lambda = 11/6\ \theta_{unit},$$

omdat zowel S_0 als S_1 en S_2 tot de up-toestanden van de schakeling behoren. Ga dat na.

* Dit resultaat zou uiteraard ook zijn verkregen met

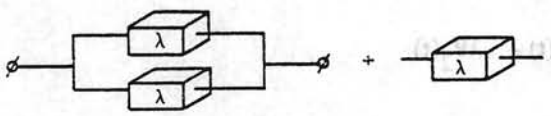
$$\theta_{syst} = \int_0^\infty R(t)\,dt \text{ en } R(t) = 1 - (1 - \exp(-\lambda t))^3, \text{ zie paragraaf 2.5.}$$

Waren overigens voor een goede werking van het systeem minstens twee goede units vereist, dan zou

$$\theta_{syst} = \lim_{s \to 0} (P_0(s) + P_1(s)) = 1/3\lambda + 1/2\lambda = 5/6\lambda.$$

Voorbeeld 3:

Een systeem bestaat uit twee parallel geschakelde identieke eenheden, met één eenheid als reserve. Deze reserve-eenheid wordt direct ingezet als één van de twee parallel geschakelde units faalt. Het systeem is down als alle eenheden falen. Wat is de gemiddelde levensduur van het systeem?



Toestandsinventarisatie: $S_0 \equiv$ 2 eenheden goed; 1 reserve.
$S_1 \equiv$ 2 eenheden goed; geen reserve.
$S_2 \equiv$ 1 eenheid goed; geen reserve.
$S_3 \equiv$ systeem down.

Overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \\ S_3 \end{array} \begin{array}{c} \begin{array}{cccc} S_0 & S_1 & S_2 & S_3 \end{array} \\ \begin{bmatrix} 1 - 2\lambda dt & 2\lambda dt & 0 & 0 \\ 0 & 1 - 2\lambda dt & 2\lambda dt & 0 \\ 0 & 0 & 1 - \lambda dt & \lambda dt \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}.$$

Hieruit lezen we af, dat:

$$\frac{dP_0(t)}{dt} = -2\lambda P_0(t)$$

$$\frac{dP_1(t)}{dt} = 2\lambda P_0(t) - 2\lambda P_1(t)$$

$$\frac{dP_2(t)}{dt} = 2\lambda P_1(t) - \lambda P_2(t)$$

$$\frac{dP_3(t)}{dt} = \lambda P_2(t),$$

waaruit ($P_0(0) = 1$)

$$sP_0(s) - 1 = -2\lambda P_0(s)$$

$$sP_1(s) = 2\lambda P_0(s) - 2\lambda P_1(s)$$

$$sP_2(s) = 2\lambda P_1(s) - \lambda P_2(s)$$

$$sP_3(s) = \lambda P_2(s),$$

zodat $P_0(s) = 1/(s + 2\lambda)$; $P_1(s) = 2\lambda/(s + 2\lambda)^2$;
$P_2(s) = 4\lambda^2/(s + 2\lambda)^2 (s + \lambda)$ en

$$\theta_{syst} = \lim_{s\to 0} (P_0(s) + P_1(s) + P_2(s)) = 2/\lambda = 2\,\theta_{unit}.$$

Opgave 4.1:

Een parallelschakeling bestaat uit vijf identieke units. Elk daarvan heeft een overlevingskans van .90 voor een periode van 500 h.
Toon aan dat de kans, dat er na 500 h precies één eenheid stuk is, gelijk is aan .328.

Opgave 4.2:

Een systeem bestaat uit een eenheid on-line en een reserve-eenheid off-line. De failure rate van de actieve unit is λ_1 en van de niet actieve unit λ_2. Er is geen reparatiemogelijkheid.
Laat zien dat

$$R_{syst}(t) = \frac{\lambda_1 + \lambda_2}{\lambda_2} \exp(-\lambda_1 t) - \frac{\lambda_1}{\lambda_2} \exp(-(\lambda_1 + \lambda_2)\, t).$$

Opgave 4.3:

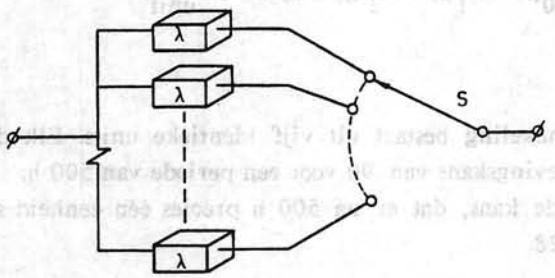
Een systeem bestaat uit twee identieke units A en B (failure rate λ) met daaraan toegevoegd een *feilbaar* omschakelmechanisme S (failure rate λ_s). De niet in bedrijf zijnde eenheid kan niet kapot gaan. Er is geen reparatiemogelijkheid. Van S wordt verondersteld, dat deze — mits nog werkend — direct naar B wordt omgeschakeld, indien A uitvalt. Een foutieve schakelaar kan niet meer omschakelen, maar laat het signaal wel door.

Toon aan dat $\theta_{syst} = \frac{1}{\lambda} + \frac{1}{\lambda + \lambda_s}$.

4.3 De standby-configuratie

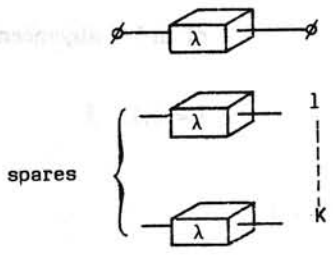
In paragraaf 2.5 zijn we in de parallelschakeling reeds een geval van redundantie tegengekomen en wel de *actieve* vorm ervan. Kenmerkend hiervoor is, dat de aanwezige (en ingebouwde) reserve bij het begin al in bedrijf wordt gezet, met bijbehorende kans op uitval vanaf t = 0.

We zullen nu in het kort enige aandacht besteden aan de *passieve* vorm van redundantie en doen dat aan de hand van onderstaande figuur:



De eerste eenheid is in bedrijf, terwijl een schakelaar (of switch) S de mogelijkheid biedt om, indien deze unit uitvalt, (praktisch) zonder vertraging op een volgende eenheid om te schakelen. Indien k (identieke) eenheden in koude of passieve reserve staan, kan dit omschakelproces k maal plaatsvinden, totdat ook de (k+1)-de unit faalt en het totale systeem als down wordt beschouwd.

Onder aanname, dat de schakelaar ideaal (dat wil zeggen onfeilbaar) is en een niet-in-bedrijf-zijnde eenheid niet kan falen, zullen we de overlevingskans $R_{syst}(t)$ en de gemiddelde levensduur θ_{syst} daarvan met de in paragraaf 3.4 aangegeven procedure berekenen.



Een eenheid met k eenheden in standby kent (k+2) elkaar uitsluitende toestanden S_i, i = 0,1,...,k+1. Voor i = 0,1,...,k stelt S_i de toestand voor, dat inmiddels i units zijn uitgevallen en (k-i+1) eenheden nog in orde zijn, waarvan één in bedrijf. Met S_{k+1} wordt de down-toestand van het totale systeem aangegeven, waarbij alle (k+1) eenheden falen.
De overgangsmatrix is in dat geval

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \\ \vdots \\ S_{k+1} \end{array} \begin{array}{c} \begin{array}{ccccc} S_0 & S_1 & S_2 & \cdots\cdots & S_{k+1} \end{array} \\ \begin{pmatrix} 1-\lambda dt & \lambda dt & & & \\ & 1-\lambda dt & \lambda dt & & \\ & & 1-\lambda dt & & \\ & & & 1-\lambda dt & \lambda dt \\ & & & & 1 \end{pmatrix} \end{array}.$$

Hieruit volgen de differentiaalvergelijkingen

$$\begin{aligned} \frac{dP_0(t)}{dt} &= -\lambda P_0(t) \\ \frac{dP_1(t)}{dt} &= \lambda P_0(t) - \lambda P_1(t) \\ &\vdots \\ \frac{dP_{k+1}(t)}{dt} &= \lambda P_k(t), \end{aligned}$$

met $P_i(t)$ = kans dat het systeem zich ten tijde t in toestand S_i, i = 0,1,...,k+1 bevindt.

Bij de begincondities $P_0(0) = 1$ en $P_j(0) = 0$, j = 1,2,...,k+1 vinden we voor de Laplace-transformatie

$$P_0(s) = \frac{1}{s + \lambda}, \qquad P_1(s) = \frac{\lambda}{(s + \lambda)^2} \qquad \text{of in het algemeen}$$

$$P_i(t) = \frac{\lambda^i}{(s + \lambda)^{i+1}}, \qquad i = 0,1,...,k .$$

Terugtransformatie van deze uitdrukking levert

$$P_i(t) = \frac{(\lambda t)^i}{i!} \exp(-\lambda t),$$

waaruit door sommering van alle actieve toestanden van het systeem de overlevingskans hiervan ten tijde t kan worden gevonden

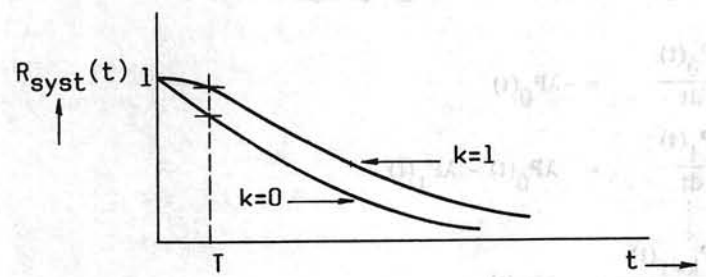
$$R_{syst}(t) = \exp(-\lambda t) \sum_{i=0}^{k} \frac{(\lambda t)^i}{i!},$$

terwijl de gemiddelde levensduur θ_{syst} eenvoudig volgt uit

$$\theta_{syst} = \lim_{s \to 0} R_{syst}(s) = \frac{k + 1}{\lambda} = (k + 1)\, \theta_{unit},$$

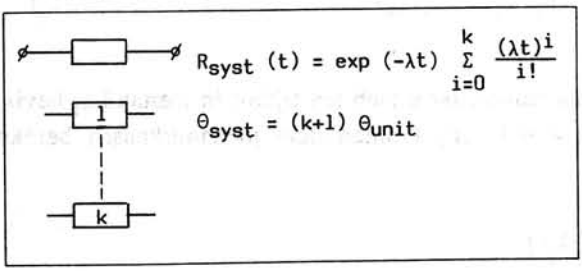
een in de praktijk goed hanteerbare formule: de gemiddelde systeemlevensduur kan worden verkregen door de gemiddelde levensduur van de actieve eenheid en die van de spares op te tellen.

* Het blijkt overigens dat het toevoegen van één enkele spare aan een in bedrijf zijnde eenheid een krachtige bijdrage levert aan de overlevingskans ervan. Voor k = 1 geldt $R_{syst}(t) = (1 + \lambda t) \exp(-\lambda t)$, een uitdrukking die grafisch ongeveer het volgende verloop heeft:



Voor operationeel interessante waarden ($R \geq .95$) is de horizontale start van de $k = 1$ curve van opvallende betekenis, hetgeen voor een bedrijfstijd T grafisch is aangegeven.
Voor $\lambda T = T/\theta_u = .05$ geldt voor $k = 0$: $R_{syst} \simeq .950$ en voor $k = 1$:
$R_{syst} \simeq 1 - \lambda^2 T^2 = .997$, een duidelijke verbetering.

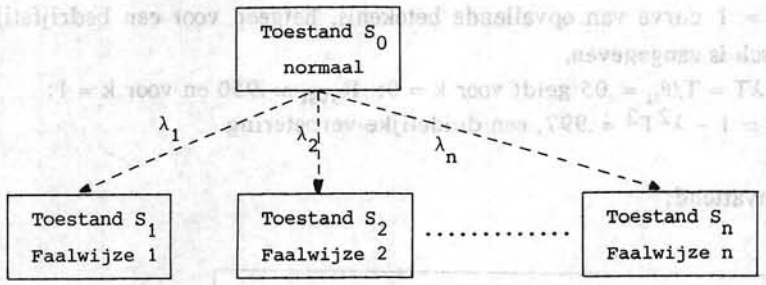
Samenvattend:



4.4 Meer dan één faalwijze

We hebben reeds gememoreerd dat een (sub)systeem kan falen, dat wil zeggen dat dit niet meer de functie verricht, die we hiervan redelijkerwijs mogen verwachten. De manier waarop dit falen plaatsvindt, kan verschillend zijn. In dit verband spreken we van de zogenaamde *faalwijzen* (Engels: *failure modes*), dat zijn dus onderling verschillende storingsvormen van het desbetreffende (sub)systeem. Zo kan een fiets niet alleen door een gebroken ketting uitvallen, maar tevens door een lekke band, een vastgelopen achterwiel of een doorgeroeste zadelveer. Een kapotte diode kan zich zowel in een open als in een kortgesloten toestand bevinden.

Het beschreven uitvalsproces kan schematisch door middel van een overgangsdiagram worden aangegeven, waarbij aangenomen wordt dat bij een storing slechts één faalwijze kan optreden. De (bij elke storingsvorm behorende) storingsgraden λ_i, $i = 1,2,...,n$ dienen in dit schema te worden aangegeven.



Indien we de kans, dat het (sub)systeem zich ten tijde t in toestand S_i bevindt, aangeven met $P_i(t)$, i = 0,1,...,n, kunnen deze toestandskansen berekend worden met

$$P_0(t) = \exp\left(-\sum_i \lambda_i t\right)$$

$$P_i(t) = \frac{\lambda_i}{\sum_i \lambda_i}\left(1 - \exp\left(-\sum_i \lambda_i t\right)\right).$$

Ga dat na.

Voorbeeld:

Bij een klep in een vloeistofleiding worden de volgende storingsvormen vastgesteld: (1) klep sluit niet; te beschrijven met een storingsgraad $\lambda_1 = .001$ f/dag = 24 h; (2) klep opent niet: $\lambda_2 = .002$ f/dag; (3) lekkage: $\lambda_3 = .005$ f/dag.

De kans dat in een periode van twee dagen de klep vanwege lekkage (*en niet door een andere storingsvorm*) uitvalt is dan

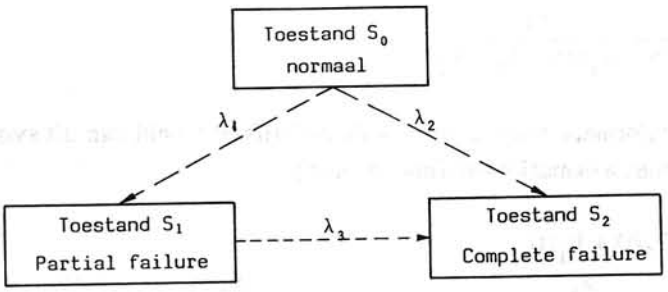
$$P_3\ (2 \text{ dagen}) = \frac{.005}{.001 + .002 + .005}\ (1 - \exp(-.016)) = 0.0099,$$

dus een kans op lekkage van ongeveer 1%.

4.5 Partial failure

Door conditieverloop kan een (sub)systeem in een toestand verkeren dat het "helemaal niet meer" (complete failure) of "niet helemaal meer" (partial failure) naar behoren functioneert. Hoewel men zich in de bedrijfszekerheid in het algemeen beperkt tot een model met twee toestanden, is het goed om te

weten hoe zo'n *multistate* model wordt doorgerekend. Voor zo'n model ziet het overgangsdiagram er als volgt uit



Uit de overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{pmatrix} 1 - (\lambda_1 + \lambda_2)\,dt & \lambda_1 dt & \lambda_2 dt \\ 0 & 1 - \lambda_3 dt & \lambda_3 dt \\ 0 & 0 & 1 \end{pmatrix} \end{array},$$

volgen de differentiaalvergelijkingen

$$\frac{dP_0(t)}{dt} = -(\lambda_1 + \lambda_2)\,P_0(t)$$

$$\frac{dP_1(t)}{dt} = \lambda_1 P_0(t) - \lambda_3 P_1(t)$$

$$\frac{dP_2(t)}{dt} = \lambda_2 P_0(t) - \lambda_3 P_1(t)\,,$$

zodat door Laplace-transformatie (met $P_0(0) = 1$)

$$sP_0(s) - 1 = -(\lambda_1 + \lambda_2)\,P_0(s)$$

$$sP_1(s) = \lambda_1 P_0(s) - \lambda_3 P_1(s)$$

$$sP_2(s) = \lambda_2 P_0(s) + \lambda_3 P_1(s)\,,$$

waaruit

$$P_0(s) = \frac{1}{s + \lambda_1 + \lambda_2}$$

$$P_1(s) = \frac{\lambda_1}{(s + \lambda_3)(s + \lambda_1 + \lambda_2)}.$$

Door terugtransformatie vinden we voor de bedrijfszekerheid van dit systeem (inclusief het niet helemaal meer functioneren)

$$R_{syst} = P_0(t) + P_1(t)$$

$$= \frac{\lambda_1}{\lambda_1 + \lambda_2 - \lambda_3} \exp(-\lambda_3 t) + \frac{\lambda_2 - \lambda_3}{\lambda_1 + \lambda_2 - \lambda_3} \exp(-(\lambda_1 + \lambda_2)\, t).$$

Voorbeeld:

Een kogellager kent drie toestanden: goed (g), speling (s) en fout (f). De failure rates tussen deze toestanden zijn:

$g \rightarrow s$: $\lambda_1 = 10^{-4}$ f/h

$g \rightarrow f$: $\lambda_2 = 10^{-5}$ f/h

$s \rightarrow f$: $\lambda_3 = 6 \times 10^{-5}$ f/h.

De overlevingskans van de lager voor een periode van 1000 h is dan volgens bovenstaande formule

$$R\ (1000\ h) = \frac{10^{-4}}{10^{-4} + 10^{-5} - 6 \times 10^{-5}} \exp(-6 \times 10^{-5} \times 10^{3}) +$$

$$+ \frac{10^{-5} - 6 \times 10^{-5}}{10^{-4} + 10^{-5} - 6 \times 10^{-5}} \exp(-(10^{-4} + 10^{-5})\, 10^{3}) =$$

$$= 0.987.$$

4.6 Afhankelijke fouten

De aanname, dat fouten in een systeem onderling onafhankelijk optreden, is niet altijd geoorloofd. In dat geval spreken we van *afhankelijke fouten*, waarop de eenvoudige produktregels voor serie- en parallelschakelingen (zie paragrafen 2.3 en 2.5) niet van toepassing zijn.
In dit verband kan de *secundaire* fout worden genoemd, die het gevolg is van een eerder opgetreden storing. Indien bijvoorbeeld in een compact gebouwd systeem een kortsluiting ontstaat (*primaire* fout), zullen andere componenten door de daardoor ontstane hitte een grotere uitvalskans vertonen (secundaire fout).

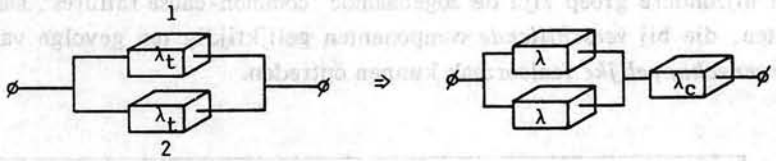
Een bijzondere groep zijn de zogenaamde "common-cause failures". Dat zijn fouten, die bij *verschillende* componenten gelijktijdig ten gevolge van een *gemeenschappelijke* faaloorzaak kunnen optreden.

Deze zogenaamde CC-fouten kunnen onder meer veroorzaakt worden door:
- Suboptimaal ontwerp, doordat in de ontwikkelingsfase van een systeem onvolkomenheden zijn blijven zitten.
- Bedrijfs- en bedieningsfouten, ten gevolge van onjuiste installatie, onzorgvuldig onderhoud, zorgeloze bediening etc.
- Externe omstandigheden, zoals extreme vochtigheid, temperatuur en trilling.
- Externe rampen, met name brand, explosie en aardbeving.
- Gemeenschappelijke fabrikant, die bijvoorbeeld voor al zijn produkten dezelfde verkeerde materiaalkeuze doet of slechte aansluitcontacten verzorgt.
- Enkel uitgevoerde voeding bij een redundant systeem.

Dat door CC-fouten het effect van een parallelstructuur weer grotendeels teniet kan worden gedaan, is vrij eenvoudig in te zien. Indien bijvoorbeeld een regelunit dubbel is uitgevoerd om de bedrijfszekerheid op te voeren, dan zullen in een chemisch agressieve sfeer beide eenheden op gelijke wijze worden aangetast en zal het voordeel van redundantie op die wijze praktisch verloren gaan.
Als voorbeeld, hoe de onderlinge afhankelijkheid in het faalmechanisme voor *berekening* toegankelijk kan worden gemaakt, is hieronder een parallel-

schakeling van twee identieke units gekozen. Daarbij wordt een grootheid β ingevoerd, die dat gedeelte van de fouten bedoelt aan te geven, die een gemeenschappelijke oorzaak hebben (beta factor methode).
We nemen namelijk aan dat zowel stochastisch onafhankelijke fouten (failure rate λ) als CC-fouten (failure rate λ_c) kunnen optreden, met als totale storingsgraad $\lambda_t = \lambda + \lambda_c$. De bovengenoemde grootheid β kan dan worden voorgesteld door $\beta = \lambda_c/(\lambda + \lambda_c) = \lambda_c/\lambda_t$.

Bij een parallelschakeling wordt nu een gemodificeerd netwerk voorgesteld, waarbij nog een derde (denkbeeldige) eenheid in serie is opgenomen.
Aldus:

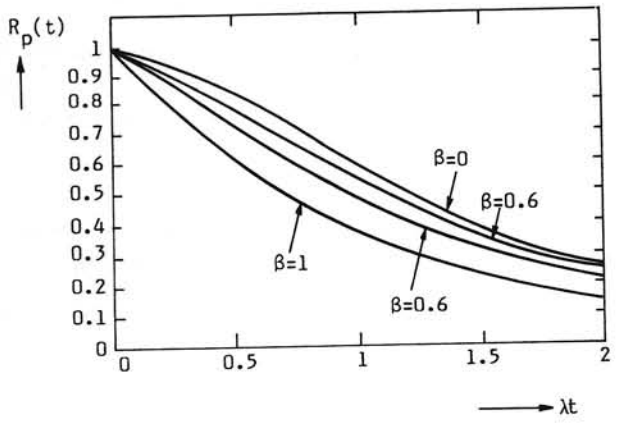


In deze extra serie-eenheid is dan gesymboliseerd de gevoeligheid voor common-cause failures, die inderdaad beide eenheden 1 en 2 tegelijkertijd doen sneuvelen en het parallelsysteem in één keer down doen gaan.
De overlevingskans $R_p(t)$ van een 2-parallelsysteem met de mogelijkheid van CC-fouten is dan:

$$R_p(t) = (1 - (1 - \exp(-\lambda t))^2) \exp(-\lambda_c t),$$

waarbij we blijkbaar veronderstellen, dat de common-cause failures en de andere fouten stochastisch onafhankelijk zijn.
Door invulling van $\lambda_c = \beta\lambda_t$ en $\lambda = (1 - \beta)\lambda_t$ kan door variatie van β de $R_p(t)$ als functie van de tijd worden uitgezet, zoals hieronder is weergegeven. Daarbij kan de waarde van β lopen van de waarde 0 (dat wil zeggen onafhankelijke uitvalskansen) tot de waarde 1 (dat wil zeggen totale afhankelijkheid).

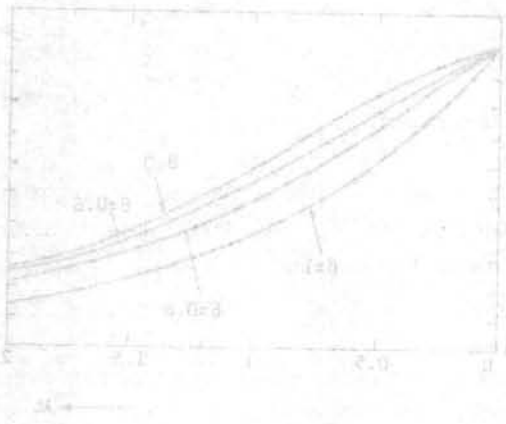
Het behoeft geen betoog dat in het laatste geval het parallelsysteem als een enkele eenheid functioneert.



Opgave 4.4:

Leid bovenstaande formule af en bepaal de gemiddelde levensduur θ van het systeem.

Antwoord: $\theta = \dfrac{2}{\lambda + \lambda_c} - \dfrac{1}{2\lambda + \lambda_c}$.



5 ONDERHOUD

5.1 Definitie onderhoud

Eénmaal geïnstalleerde (of althans aangekochte) apparatuur dient veelal in stand te worden gehouden. Voor een dergelijke *instandhouding* grijpt (op de één of andere manier) de mens in.

> Al deze (menselijke) activiteiten worden samengevat en aangeduid met onderhoud.

Hetgeen we uiteindelijk (en dat mede door middel van dit onderhoud) trachten te bereiken is: een systeem te laten opereren volgens de gespecificeerde eisen gedurende de gewenste gebruiksduur.

* Er zijn overigens vele technische voortbrengselen — met name verbruiksartikelen — waarop geen of nauwelijks onderhoud wordt gepleegd. Een flitslamp, een punaise, een cassettebandje en zelfs een goedkope radio-ontvanger (zie paragraaf 1.4*) zijn daarvan zo maar een paar huiselijke voorbeelden.

De definitie door de Commissie Nomenclatuur van de NVDO (= Nederlandse Vereniging voor Doelmatig Onderzoek) opgesteld, luidt aldus:

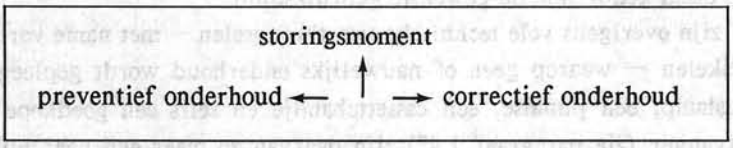
> Onderhoud omvat alle activiteiten, die ten doel hebben de duurzame produktiemiddelen, waarover wordt beschikt, in de toestand te houden of weer in die toestand te brengen, die voor de vervulling van hun functie nodig wordt geacht.

Deze omschrijving betreft blijkbaar onderhoud in de *engere* zin des woords. Ze heeft namelijk slechts betrekking op handelingen, die verricht (moeten) worden aan een technisch systeem, dat zich in de *bedrijfsfase* bevindt. Maar ook in deze levensfase van het systeem is de doelstelling van onderhoudspleging, zoals in de NVDO-omschrijving bedoeld, ruimer dan mogelijk

vermoed. Want het is niet altijd de *functievervulling*, waaraan bij toepassing van onderhoud wordt gedacht, maar ook kan daarmee de opvoering van de *levensduur* en de *veiligheid* tijdens bedrijf van het desbetreffende systeem worden beoogd. Zoals de ons allen bekende onderhoudsbeurt van een automobiel niet alleen de *storingskans* bedoelt te verkleinen, maar tevens de levensduur van het vehikel èn de veiligheid van de inzittende(n) en andere weggebruikers in positieve zin dient te beïnvloeden.

Dè grote snede in het onderhoudsgebied sluit aan bij de bovenvermelde NVDO-definitie: het in de juiste toestand *houden* (preventief onderhoud) vs. het wederom in de juiste toestand *brengen* (correctief onderhoud) van apparatuur.
Als onderscheidingscriterium wordt blijkbaar het *storingsmoment* gehanteerd, dat is het moment, waarna het systeem niet meer binnen de daartoe gestelde normen functioneert.

Schematisch aldus weergegeven:



Preventief (= strekkend tot verhindering van iets, dan ongewenst is) *onderhoud* is dus het (menselijk) ingrijpen vóór de functie-uitval, *correctief onderhoud* ernà.

* De omschrijving correctief onderhoud kent in de literatuur ook andere benamingen: repressief onderhoud, storingsonderhoud, brandweeronderhoud, contingent maintenance, breakdown maintenance en de minder gelukkige term curatief onderhoud. In dit boek zullen wij ons beperken tot de term storingsafhankelijk onderhoud.

Bij een dergelijke tweedeling zal het duidelijk zijn, dat de scharniervraag van het onderhoudsgebeuren is: aan welke onderhoudsvorm zal door de fabrikant, de gebruiker of de maintenance engineer de voorkeur moeten worden gegeven en waarom? Hoe de keuze ook moge uitvallen: een dominant voordeel van preventief onderhoud is in ieder geval gelegen in de *planbaarheid* van de zo broodnodige activiteiten. En dat is uiteraard een administratief en economisch bij uitstek goede zaak als het om de beheersbaarheid

van de onderhoudscapaciteit gaat: aanvoer van reservedelen, doordachte werkplanning, etcetera, het kan allemaal (min of meer) van tevoren bekeken worden. De aanduiding *scheduled* en *non-scheduled* (in het Nederlands: planbaar en niet-planbaar) hebben we hieraan overgehouden.

* Anderzijds kan toepassing van preventief onderhoud het gevaar van "*overmaintenance*" inhouden. De "ziezo, dat is weer eens goed nagekeken" strategie geeft soms de gebruiker en/of onderhouder een gevoel van apparatieve bedrijfszekerheid voor de nabije toekomst, dat — rationeel gezien — nergens op steunt, maar dat toch emotioneel behaaglijk aandoet. Trouwens het ligt voor de hand te veronderstellen, dat een fabrikant — niet bekend zijnde met het toekomstige storingsgedrag van zijn nieuwe produkt — een onderhoudsritme zal adviseren (althans voor zover hij dat doet), waarvan achteraf de frequentie te hoog blijkt te zijn.

5.2 Verloop van de storingsgraad

De motieven om tot een preventieve onderhoudsvorm te besluiten, kunnen verschillend zijn. Mogelijk vanwege hoge eisen op het gebied van veiligheid (medische apparatuur; luchtvaart) of in het geval van wettelijke voorschriften. Maar er is één parameter, die in deze materie een voorname rol speelt en waarbij kennisname van het verloop in de tijd hiervan belangrijk is bij de keuze van de te volgen onderhoudsmethodiek. Het is de *storingsgraad*, een grootheid, die reeds in paragraaf 1.7 ter sprake kwam en die de (conditionele) kans op een storing aangeeft, mits het systeem tot dan storingsvrij heeft gefunctioneerd.

In voorgaande paragrafen werd deze storingsgraad constant in de tijd geacht, daarbij veronderstellende, dat de storingen volkomen willekeurig optreden. Een geheugenloos gebeuren dus, hetgeen inhoudt, dat men zich middels preventief onderhoud (vervanging) niet kan indekken tegen dit soort *random failures*. Zoals het geen zin heeft, vandaag zijn (nog goede) banden van zijn auto voor splinternieuwe te verwisselen, met het oogmerk morgen er zeker van te zijn, geen lekke band te krijgen.

Dit geldt uiteraard in nog sterkere mate voor een dalende storingsgraad (zie het linkerdeel van de badkuipkromme, paragraaf 1.12) zodat we kunnen concluderen, dat onderhoudsacties met een preventief karakter pas zinvol zijn, indien de storingsgraad van een systeem (significant) met de tijd toeneemt. *In het andere geval kan beter het moment van falen worden afgewacht.*

Een relevante vraag in dit verband is uiteraard: hoe kan het verloop van de storingsgraad worden bepaald, als dat dan zo'n belangrijke parameter blijkt te zijn?
Een mogelijkheid hiertoe is het *verzamelen* en *zinvol verwerken* van faalgegevens, afkomstig van het operationele gebruik. Hoewel het collecteren hiervan een eenvoudige en voor de hand liggende bezigheid schijnt te zijn, moet toch worden opgemerkt, dat deze methodiek in de barre praktijk tegenvalt. Een foutenrapportage-systeem, nodig ter verkrijging van de bedoelde storingsgegevens, is (a) zeer arbeidsintensief, (b) vrij kostbaar en (c) dan vaak nog niet eens waterdicht. Daar komt dan nog bij dat bij gebruikers (en onderhouders) de meldingsbereidheid van faaldata vrij sterk aan erosie onderhevig is vanwege de eventuele omstandigheid, dat deze niets meer van hun trouw opgezonden storingsmeldingen vernemen en slechts omtrent het resultaat van hun activiteiten kunnen gissen. Bovendien blijft het een klemmende vraag, welke de zo begeerde gegevens zijn en wat daarvan geregistreerd moet worden. Als minimum informatie aan onderhoudsgegevens kan in dit verband worden genoemd:

Storingsgegevens:
- storingsvorm
- correctieve actie
- verbruikte onderdelen
- mogelijke oorzaak
- storingstijdstip
- bedrijfsurenstand
- storingsgevolgen.

Preventieve onderhoudsgegevens:
- defecten door inspectie
- logistieke moeilijkheden.

5.3 Storingsgegevens

Als voorbeeld, hoe uit enige bedrijfsgegevens een onderhoudsindicatie kan worden verkregen, volgen hieronder een tweetal uitwerkingen. Stel dat de volgende storingsvrije intervallen (in uren) van een apparaat A bekend zijn:

28	231	88	180
131	105	324	81
56	38	406	267
95	78	63	42
194	440	30	168

Na indeling naar klasse, worden achtereenvolgens de kansdichtheidsfunctie f(t), de bedrijfsonzekerheid F(t), de bedrijfszekerheid R(t) en de storingsgraad z(t) bepaald met als resultaat:

klasse	aantal storingen	t	F(t)	R(t)	f(t)	z(t)
		0	0.00	1.00	$5{,}0 \cdot 10^{-3}$	$5{,}0 \cdot 10^{-3}$
0-100 h	10	100	0.50	0.50	$2{,}5 \cdot 10^{-3}$	$5{,}0 \cdot 10^{-3}$
101-200 h	5	200	0.75	0.25	$1{,}0 \cdot 10^{-3}$	$4{,}0 \cdot 10^{-3}$
201-300 h	2	300	0.85	0.15	$0{,}5 \cdot 10^{-3}$	$3{,}3 \cdot 10^{-3}$
301-400 h	1	400	0.90	0.10	$1{,}0 \cdot 10^{-3}$	$10{,}0 \cdot 10^{-3}$
401-500 h	2	500	1.00	0.00	-	-

De hierbij gebruikte formules zijn:

$$F(t) = P(X \leq t);$$

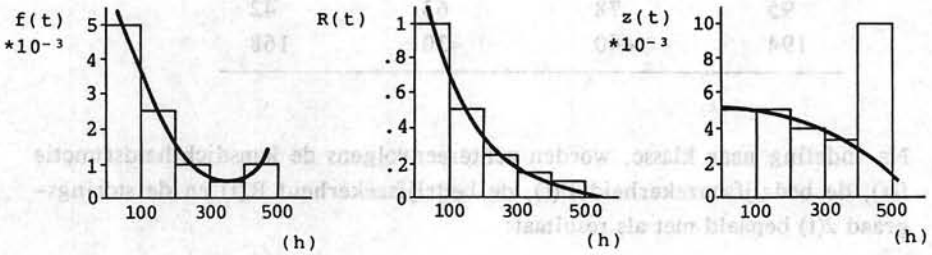
$$R(t) = 1 - F(t);$$

$$f(t) = F'(t) \approx \frac{F(t + \Delta t) - F(t)}{\Delta t};$$

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

Voor het bestuderen van het verloop van de storingsgraad zijn de eerste vier getallen uit de laatste kolom slechts informatief: het laatste getal is op zo weinig materiaal gebaseerd dat daar geen waarde meer aan gehecht mag worden.

Grafisch weergegeven:



Uit het niet-stijgende verloop van de storingsgraad moeten we (althans voorlopig) afzien van preventief onderhoud.

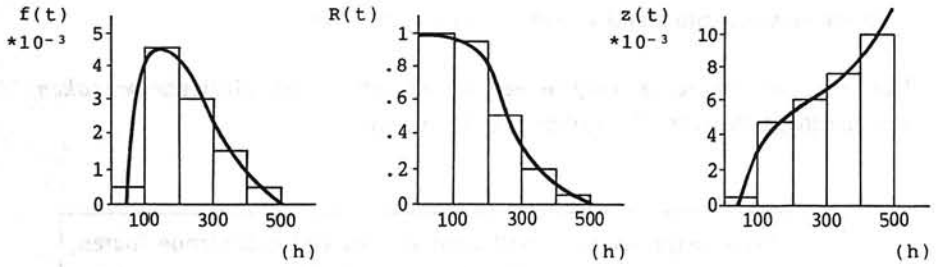
Voorts zijn van een apparaat B de volgende storingsvrije intervallen (in uren) binnengekomen, die op dezelfde wijze worden verwerkt.

209	333	365	121
269	88	195	220
132	108	146	310
166	241	158	183
411	290	273	190

Het tabellarisch overzicht wordt dan:

klasse	aantal storingen	t	F(t)	R(t)	f(t)	z(t)
		0	0.00	1.00	$0{,}5 \cdot 10^{-3}$	$0{,}5 \cdot 10^{-3}$
0-100 h	1	100	0.05	0.95	$4{,}5 \cdot 10^{-3}$	$4{,}7 \cdot 10^{-3}$
101-200 h	9	200	0.50	0.50	$3{,}0 \cdot 10^{-3}$	$6{,}0 \cdot 10^{-3}$
201-300 h	6	300	0.80	0.20	$1{,}5 \cdot 10^{-3}$	$7{,}5 \cdot 10^{-3}$
301-400 h	3	400	0.95	0.05	$0{,}5 \cdot 10^{-3}$	$10{,}0 \cdot 10^{-3}$
401-500 h	1	500	1.00	0.00	-	-

Grafisch:



Door de sterke stijging van de storingsgraad z(t) in de loop van de tijd zal in dit geval wèl preventief onderhoud in overweging moeten worden genomen.

5.4 Storing en defect

Het goed functioneren van een systeem eindigt met het optreden van een storing. Een *storing* zullen we dan ook omschrijven als een overgang naar de toestand, waarin een systeem niet meer in staat is de vereiste functie te vervullen. In dit verband wordt ook wel gebruikt de terminologie: *bedrijfsgerede* en *niet-bedrijfsgerede* toestand van een systeem.
De bedoeling is in ieder geval aan te geven, dat een dergelijke fout (failure) zowel kan optreden tijdens bedrijf als tijdens een stilstand van een systeem, waarin dit beschikbaar werd geacht.

* Als op een vochtige morgen de auto niet starten wil, is er blijkbaar in de loop van de nacht tijdens de stilstandperiode in het voertuig een storing opgetreden. Achteraf is het storings*moment* in zo'n geval veelal niet meer vast te stellen.

Een *defect* is eveneens een afwijking van de normale systeemtoestand, maar behoeft niet onmiddellijk te worden verholpen, omdat het functioneren niet is aangetast.

* Zo zal de uitval van de kofferbakverlichting ons niet direct tot onderbreking van een nachtelijke autotrip en alarmering van de wegenwacht nopen. Opheffing van dit defect kan bij de eerstvolgende doorsmeerbeurt worden meegenomen. Een defect treedt met name op als het een *redundant*

onderdeel betreft, dat wil zeggen indien daarvoor reserve aanwezig is. Schoolvoorbeeld hiervan is de auto met een *lekke reserveband*. De vervoersfunctie is door een dergelijk defect weliswaar niet verdwenen, maar de systeemtoestand is wel kritieker geworden.

Het *ontstaan* van een storing of een defect kan aan verschillende *oorzaken* worden toegeschreven. We zullen er enige noemen:

- *willekeurige fouten:*	willekeurig in de tijd optredende fouten, die soms niet verklaard kunnen worden.
- *constructiefouten* :	zoals marginale onderdelen, foutief ontwerp en onvoldoende bescherming tegen de omgeving.
- *onderhoudsfouten* :	zoals onjuiste storingslokalisering, foutieve reparatie- en montageprocedures en onjuist opleidingsniveau.
- *bedieningsfouten* :	zoals onvoldoende documentatie, onjuiste bedieningsprocedures en dismotivatie van het personeel.

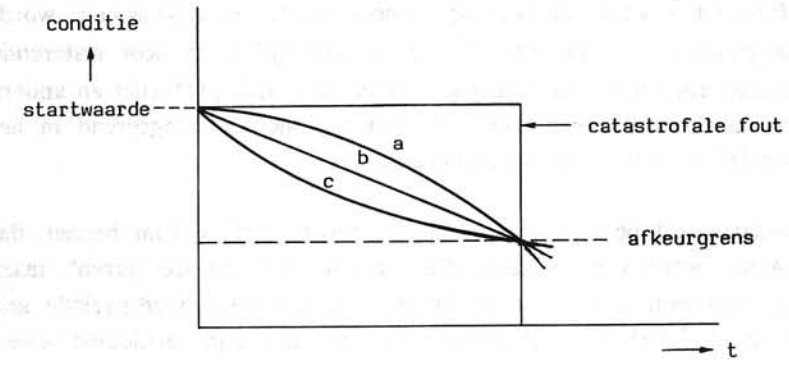
5.5 Degradatieverschijnselen

Overigens moet worden opgemerkt, dat het vaak niet eenvoudig is te bepalen, of er inderdaad een fout is opgetreden. Bij een *catastrofale* fout is dit uiteraard niet zo moeilijk, omdat in dat geval een systeem plotseling een totaal functieverlies heeft. Bijvoorbeeld als tijdens een uitzending ineens het TV-beeld wegvalt.
Maar er zijn ook *degradatieverschijnselen*, die de conditie geleidelijk doen achteruit gaan. Onder de *conditie* van een systeem verstaan we in dit verband de toestand, waarin een bepaalde mate van functievervulling mogelijk is.

* De conditie — zowel *mechanisch* als *elektronisch* — zal in de praktijk door allerlei verdrietige oorzaken afnemen, zoals slijtage, corrosie, erosie, vocht, vervuiling, veroudering, oververhitting, vibratie, overspanning, wangebruik, etcetera.

Bij een geleidelijke conditievermindering moet dan een *afkeurgrens* worden afgesproken, waaronder een systeem als falend of niet-bedrijfsgereed wordt

beschouwd. Het teruglopen van het zendvermogen van 10 W (als specificatiewaarde) tot 4 W (als nog net acceptabel) zou hiervan een voorbeeld kunnen zijn. Schematisch kan een dergelijk conditieverloop aldus worden weergegeven:



Overigens zal de *ligging* van de afkeurgrens sterk afhankelijk zijn van het oordeel van de gebruiker en van de bedrijfsomstandigheden. Of een fiets zonder zadel nog berijdbaar is hangt onder meer van de atletische vermogens van de berijder af. Het laat zich verder denken, dat in een tijdelijke geïsoleerde positie (bijvoorbeeld op zee) met een lagere systeemprestatie "genoegen wordt genomen", dan op een plek met meer onderhoudsfaciliteiten om de conditie wederom snel op te voeren. Het is nu de *onderhoudstechnologie*, die zich bezighoudt met het vinden van de juiste onderhoudsmethodieken en -strategieën op grond van het *conditieverloop*, dat bekend is of dat vermoed wordt, waarbij het onderscheid tussen progressief (a), lineair (b) en degressief (c) verlopende curven (zie schets) een essentiële rol kan spelen.

5.6 Preventief onderhoud

Er zijn in de praktijk enkele belangrijke verschijningsvormen van preventief onderhoud te onderscheiden:

- In zijn lichte vorm bestaat dit soort onderhoud uit enige routinematige controle en enkele bij- en afstelhandelingen. Dit *verzorgend* onderhoud (*servicing*), zoals brandstofbijvulling, schoonmaken van onderdelen, doorsmeren, globale controle van functies, stelt geen hoge eisen aan de kennis en opleidingsniveau van het personeel.

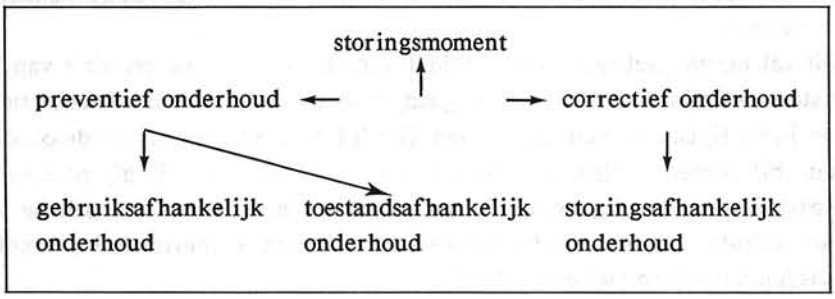
- Indien de algehele conditie van een systeem daartoe aanleiding geeft, is dit aan *revisie* toe. Het betreft hier een grondige onderhoudsbeurt, waarbij niet geschroomd wordt het gehele systeem te demonteren, alle componenten te inspecteren en de daarvoor in aanmerking komende onderdelen te vervangen, waarna (a) montage, (b) in bedrijfstelling en (c) uittesting volgen.
  * Hoewel het aldus gereviseerde systeem dan als "as good as new" wordt aangenomen te zijn, valt dit in de praktijk tegen door resterende montagefouten ("maandagmorgen-effecten"), inloopeffecten en andere inschakelverschijnselen. Een aanvankelijk hoge storingsgraad in het bedrijf is daarvan het dramatische gevolg.

Een fundamenteel bezwaar van revisie is voorts, dat de kans bestaat, dat componenten worden verwisseld, die "er nog niet aan toe waren", maar waarvan uitwisseling niet op de daarna volgende onderhoudsperiode kon wachten en die derhalve veiligheidshalve toch maar zijn vernieuwd (*over-maintenance*).

- Ook kan worden overgegaan op de methodiek van *verwisseling* van onderdelen. Hierbij moet aan een tweetal voorwaarden zijn voldaan, namelijk (a) *modulaire opbouw* van het systeem en (b) goede *toegankelijkheid* (accessibility) van de uit te wisselen modulen. Hieruit volgt al het belang om reeds in de *ontwerp*fase van een systeem rekening te houden met de te volgen onderhoudspolitieken in de *bedrijfs*fase (zie paragraaf 1.4*).
  Het gaat bij deze strategie om het creëren van *korte stilstandstijden* met daarin een snelle vervanging van de daarvoor in aanmerking komende subsystemen (modulen), waarna de verwijderde examplaren kunnen worden gecontroleerd en (indien nodig) hersteld òf worden weggeworpen (throw-away-items; zie paragraaf 6.3). Een punt is wel, dat elk onderdeel zijn eigen vervangingsfrequentie kan hebben, zodat een intensieve *registratie* van alle mutaties een noodzakelijk gevolg is. Maar hoe dan ook: hoewel bij deze vorm van preventief onderhoud het systeem vaker (maar ook korter) uit bedrijf wordt genomen dan bij revisie, wordt er toch ruimschoots tegemoet gekomen aan het bezwaar van revisie, waarbij (door de grondigheid van de aanpak) een zeer lange aaneengesloten down-periode noodzakelijk is.

Preventief onderhoud kan ook worden uitgesplitst in gebruiksafhankelijk onderhoud en toestandsafhankelijk onderhoud. De eerste duidt erop dat het

systeem op kalenderbasis of na een bepaald aantal draaiuren wordt onderhouden.
Voor het tweede type onderhoud wordt met regelmaat gekeken wat de toestand van het apparaat is. Pas wanneer deze hier aanleiding toe geeft, wordt de onderhoudsbeurt verricht. Een andere veelgebruikte naam hiervoor is "condition monitoring"; het grote voordeel is dat het systeem door kan functioneren tot er daadwerkelijk iets aan de hand is.
Het schematisch overzicht van paragraaf 5.1 kan thans als volgt worden aangevuld:



5.7 Gebruiksafhankelijk onderhoud

Bij gebruiksafhankelijk onderhoud — het woord geeft het reeds aan — zal een menselijk ingrijpen plaatsvinden na een bepaalde "hoeveelheid" gebruik, bijvoorbeeld uitgedrukt in een aantal gebruiksuren, in afgelegde kilometers, in gemaakte omwentelingen of in een aantal omschakelingen.
Zo werd in vroeger dagen het luchtfilter bij een automotor na 10.000 km — zonder nadere controle van de conditie van dit onderdeel — zonder meer verwisseld. Een dergelijke strategie vereist uiteraard een goed inzicht in, of althans een sterk vermoeden van het verloop van de conditie van het te onderhouden (sub)systeem als functie van de desbetreffende levensduurvariabele (zie paragraaf 1.3).

Ook is de gebruiksafhankelijke onderhoudsvorm te verkiezen in het geval de levensduur (min of meer) bekend èn de spreiding hiervan klein is. De voortijdige verwisseling van een unit op een moment vlak voor de te verwachten levensduur levert slechts een gering verlies aan potentiële levensduur, zoals in paragraaf 1.9 getracht is duidelijk te maken in het voorbeeld van een gloeilamp (met een kleine spreiding in de levensduur om de 1000 branduren)

die ten tijde t = 900 h wordt vervangen. De voordelen van een dergelijke onderhoudspolitiek zijn eveneens in de genoemde paragraaf vermeld.

5.8 Toestandsafhankelijk onderhoud

Indien (a) het conditieverloop van het te bewaken object niet bekend is, dan wel (b) de spreiding van de levensduur onvoldoende klein is of zelfs (c) in het geval er helemaal niets bekend is omtrent het storingsgedrag, dan zal het onderhoudsgebeuren moeten plaatsvinden wanneer de toestand van dit object dit noodzakelijk maakt. In dat geval spreken we van toestandsafhankelijk onderhoud.

Dit zal moeten gebeuren door middel van inspectie om de conditie van het systeem in zijn onderdelen na te gaan, teneinde de juiste onderhoudsactie op het juiste tijdstip te kunnen bepalen. Het (globaal) vaststellen van de conditie kan bijvoorbeeld visueel gebeuren, zoals dat het geval is bij *borescopie*, waarbij het inwendige van moeilijk toegankelijke ruimten via optische weg met behulp van glasvezeltechnieken kan worden gecontroleerd (vergelijk maagonderzoek op medisch gebied).

Langs *spectrometrische* weg wordt smeerolie op de aanwezigheid van metaaldelen (Al, Fe, Ta, etc.) onderzocht, waaruit — indien de verontreiniging te hoog blijkt te zijn — mechanische onregelmatigheden kunnen worden geconstateerd, zodat vervanging of nadere inspectie nodig is. Tenslotte kan in het kader van de conditiebewaking nog het *trillingsonderzoek* genoemd worden, waarmee een beeld wordt gevormd ten aanzien van inwendig optredende slijtage bij roterende werktuigen (wat bijvoorbeeld gepaard gaat met speling in een kogellager).

Van belang bij *inspectief onderhoud* kan nog zijn of het desbetreffende systeem daartoe al dan niet buiten werking gesteld moet worden.

In de praktijk is hier vaak een speciale inspection manager voor, die iedere dag de machines afloopt om te kijken of hij een verloop in het geluid of de prestaties, die duiden op slijtage of onbalans, kan ontdekken.

5.9 Correctief onderhoud

Zoals boven reeds opgemerkt, zijn onderhoudsacties met een preventief karakter pas zinvol *als de storingsgraad van een (sub)systeem met de tijd toeneemt.* Dat houdt dus in dat voortijdige vervanging of revisie achterwege

gelaten dient te worden bij die onderdelen, die in hun uitvalsgedrag volkomen willekeurig (at random) zijn en waarbij de storingsgraad constant wordt geacht.
In dat geval kan dan beter op het moment van falen worden gewacht, met andere woorden dient correctief onderhoud te worden toegepast.

Bij voorkeur moet correctief onderhoud worden overwogen:
- Indien de storingsgraad aantoonbaar niet met de tijd toeneemt (zie boven).
- Bij storingen met een zeer kleine kans van optreden.
- Indien de gevolgen van een storing zéér beperkt zijn.
- Indien reservedelen aanwezig zijn of systeemdelen meervoudig zijn uitgevoerd.

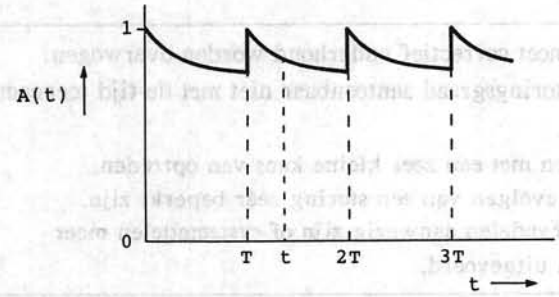
Ga eens na welke voorbeelden, zowel in de professionele als in de huiselijke sfeer, U hiervan kunt vinden.

5.10 Gemiddelde levensduur bij periodiek onderhoud

Periodiek onderhoud kan op iedere vorm van onderhoud worden toegepast. Denk maar aan storingsafhankelijk onderhoud: periodiek controleren welke functies niet meer werken, en deze repareren. Wanneer het systeem redundantie heeft kan het misschien zelfs gewoon doorfunctioneren.
Zo ook periodiek gebruiksafhankelijk onderhoud: periodieke verwisseling of revisie/servicing. Of periodiek toestandsafhankelijk onderhoud: het periodiek opnemen van de conditie, of periodieke inspectie. De begrippen spreken voor zich.
Een groot voordeel van het periodiek onderhouden is het regelmatige karakter die de tijddiagrammen krijgen, waardoor analyses eenvoudiger zijn uit te voeren. Laten we eens kijken hoe periodiek onderhoud de gemiddelde levensduur beïnvloedt:

Een systeem wordt met een interval T gecontroleerd en — indien nog werkend — in conditie zodanig bijgesteld dat het systeem na de behandeling wederom als "as good as new" mag worden bekeken. Het systeem is down indien het bij een (periodieke) controle kapot wordt aangetroffen.
In de grafiek is de beschikbaarheid A(t) van het systeem uitgezet tegen de

tijd. Op t = 0 is de beschikbaarheid gelijk aan de R(t). De kans dat het systeem blijft werken neemt af naarmate de tijd toeneemt. Op t = T wordt het systeem weer helemaal opgeknapt, en keert terug naar een beschikbaarheid van 1. Dit proces herhaalt zich voor iedere nieuwe bedrijfsperiode.



De vraag is nu: hoe groot is de gemiddelde levensduur θ (de Mean-Time-To-First-Failure, zie paragraaf 1.11), dus de gemiddelde waarde van de eerste storingsvrije periode? De overlevingskans van het totale systeem (dus technisch systeem + onderhouder) zij $R_{syst}(t)$.

De kans dat het systeem ten tijde t in het eerste interval $0 \leq t \leq T$ sneuvelt bedraagt R(t), gegeven dat de beginconditie voortreffelijk is: R(0) = 1. Treedt in het tweede interval $T \leq t \leq 2T$ een storing op, dan zal niet alleen in het eerste interval, maar ook in de periode van T tot t geen storing mogen optreden. Als we aannemen dat het systeem na ieder onderhoud weer in de oorspronkelijke toestand terugkeert, dan is de systeem-beschikbaarheidsfunctie voor de tijdstippen $T \leq t \leq 2T$ precies gelijk aan R(t - T). Voor de betrouwbaarheid van het systeem geldt dan $R_{syst}(t) = R(T)\, R(t - T)$. Zo doorgaand vinden we

$$R_{syst}(t) = R^k(T)\, R(t - kT) \qquad \text{voor } kT \leq t \leq (k+1)\,T, \quad k = 0,1,2,\ldots .$$

Nu is

$$\theta_{syst} = \int_0^\infty R_{syst}(t)\, dt = \sum_{k=0}^{\infty} \left\{ \int_{kT}^{(k+1)T} R_{syst}(t)\, dt \right\} =$$

$$= \sum_{k=0}^{\infty} \int_{kT}^{(k+1)T} R^k(T)\, R(t - kT)\, dt =$$

$$= \sum_{k=0}^{\infty} R^k(T) \int_0^T R(u)\,du = \frac{1}{1 - R(T)} \int_0^T R(u)\,du .$$

* Toepassing van dit resultaat op de negatief-exponentiële verdeling $R(t) = \exp(-\lambda t)$ levert $\theta_{syst} = 1/\lambda$. Dit wil zeggen dat de onderhoudsinspanning geen enkele verbetering van de θ oplevert vergeleken met het geval dat er geen onderhoud wordt gepleegd. Het periodieke onderhoud blijkt derhalve voor deze specifieke verdeling zinloos te zijn (voor wat de MTTFF betreft), hetgeen we reeds in paragraaf 1.10 hebben geconstateerd. Bij andere verdelingen kan het uiteraard wel succes opleveren.

Opgave 5.1:

De bedrijfszekerheid van een systeem wordt gegeven door

$$R(t) = \frac{24}{t + 24}, \qquad t \text{ in h.}$$

Er wordt periodiek onderhoud op het systeem toegepast, met een periodetijd T.
Ga na dat:

(a) $\theta_{syst} \simeq 33$ h voor T = 24 h (iedere dag);
(b) $\theta_{syst} \simeq 40$ h voor T = 48 h (iedere 2 dagen).
(c) Hoe is het te verklaren dat het resultaat beter is bij minder onderhoud?

Oplossing:

$$\theta_{syst} = \frac{1}{1 - R(T)} \int_0^T R_{syst}(t)\,dt = \frac{T + 24}{T}\ 24 \ln\left(\frac{T + 24}{24}\right).$$

Invullen van T = 24 en 48 h geeft de antwoorden (a) en (b).
De hazard rate $z(t) = 1/(t + 24)$, een dalende functie.
Het systeem is blijkbaar niet geschikt voor periodiek onderhoud.

5.11 Onderhoud in ruimere zin

Dat de definitie van onderhoud, zoals in paragraaf 5.1 te vinden, in een ruimer kader kan (en moet) worden geplaatst, wordt duidelijk als we beseffen, dat het *bedrijfszeker* en *veilig functioneren* van een systeem te maken heeft met aspecten op het gebied van:

- de software reliability;
- de logistiek van reservedelen;
- de kwaliteit van de bediening;
- de onderhoudsvriendelijkheid van het ontwerp;
- de geoefendheid in noodprocedures;
- de budgettaire beperking;
- het motivatiepeil van het personeel;
- het technisch opleidingsniveau van de onderhoudsman of -vrouw;
- de onderhoudsarmheid van het ontwerp;
- etc.

Al deze gebieden spelen een beduidende rol in het onderhoudsgebeuren, niet alleen in de bedrijfsfase van het systeem, maar ook in het ontwerpstadium ervan. We spreken dan ook zo treffend van *terotechnologie*. Dit woord is afgeleid van het Griekse: $\tau\eta\rho\epsilon\omega$, hetgeen — vertaald — zoiets betekent als: "behoeden, waken, handhaven", met andere woorden de volledige broedzorg tot een optimaal functioneren van het systeem, "van de wieg tot het graf".

Door — om zomaar eens wat te noemen — reeds in de ontwerpfase hoge prioriteit te verlenen aan:

- snelle storingsalarmering (zie paragraaf 8.4*),
- opvoering van de inherente bedrijfszekerheid (zie paragraaf 1.13),
- toepassing van standaardisatie (zie paragraaf 6.4),
- modulaire opbouw (zie paragraaf 6.2),
- slim ontworpen toegankelijkheid tot de onderdelen (zie paragraaf 5.6),

kan de bedrijfszekerheid, de veiligheid, de onderhoudsbeheersing en daardoor de apparatieve beschikbaarheid sterk worden opgevoerd.

En hoewel het in het algemeen geen eenvoudige zaak is na te gaan of de gebrachte onderhoud*soffers* in redelijke verhouding staan tot het bereikte onderhoud*sresultaat*, zal toch op basis van allerlei kosten-, veiligheids-, en personeelsoverwegingen (bij voorkeur met of door de fabrikant) een *onderhoudsconcept* opgesteld dienen te worden, dat dan — indien nodig — in de bedrijfsfase van het systeem kan worden bijgesteld.

5.12 Beslissingsdiagram voor het onderhoud

Bovenstaande beschouwingen zijn verwerkt in een *beslissingsdiagram*, met behulp waarvan een gebruiker/onderhouder op grond van zijn particuliere gegevens zich die onderhoudsvorm kan laten adviseren, die in eerste instantie als het meest doelmatig voor hem kan worden opgevat.
Het behoeft overigens geen betoog, dat allerlei omstandigheden, redenen of overwegingen het zouden kunnen wettigen, van dit advies af te wijken en tot een andere onderhoudsstrategie te besluiten. De visie op het onderhoud zal in de wereld van bijvoorbeeld het luchtverkeer sterk verschillen van die van een terrein- en gebouwendienst.

In het beslissingsdiagram zijn een viertal *criteria* ingevoerd, die bepalend zijn voor de gang door het diagram, namelijk:

- de storingsfrequentie,
- de storingsgevolgen,
- de storingsgraad,
- de conditiebewaking.

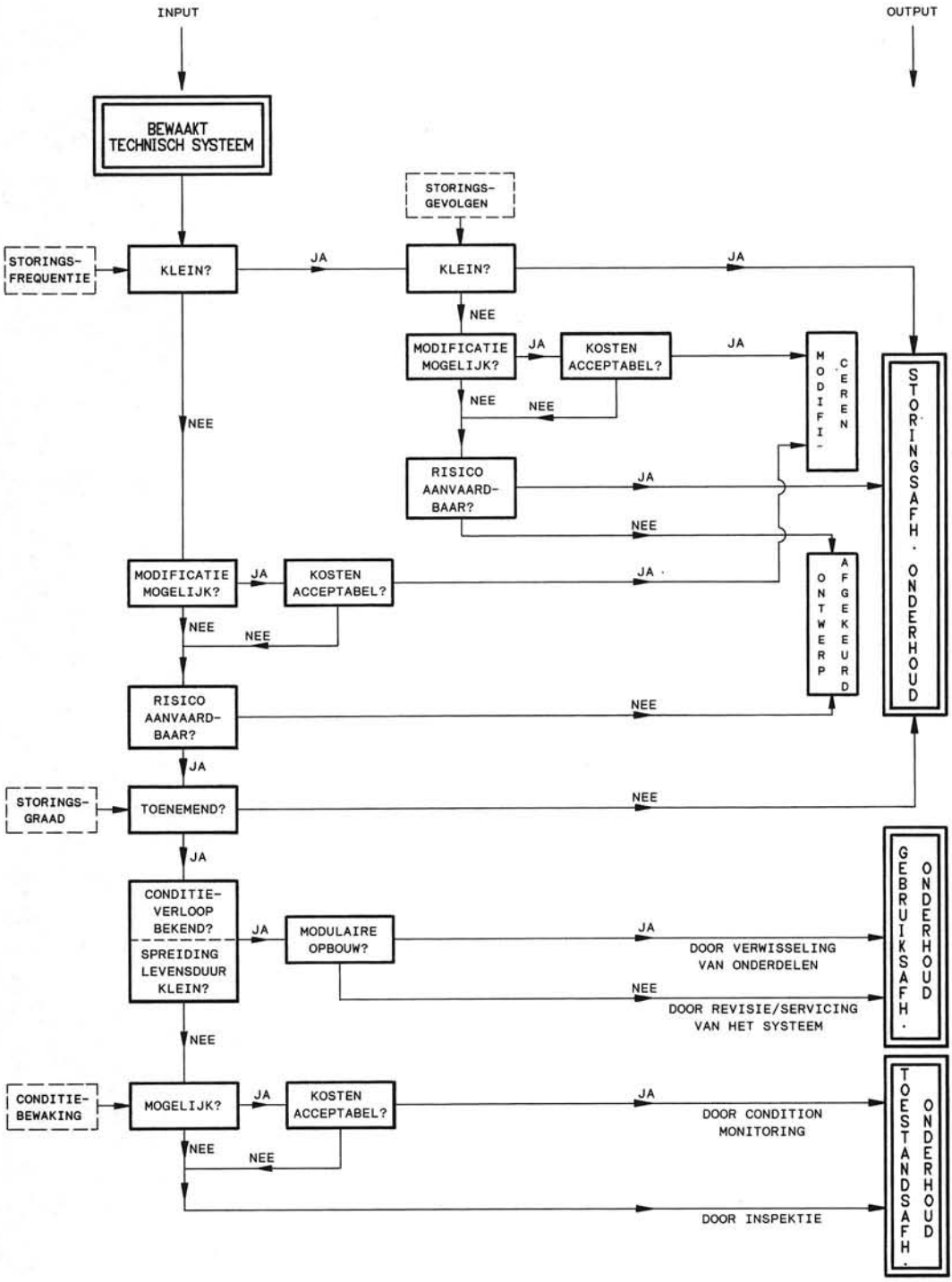
In paragraaf 5.9 is reeds benadrukt, dat bij een lage *storingsfrequentie* correctief onderhoud moet worden overwogen (de zogenaamde run-to-break strategie). Vooral als dan ook nog de *gevolgen* van het falen klein tot verwaarloosbaar zijn, kan de storing beter worden afgewacht alvorens in het operationele bedrijf in te grijpen. Maar zelfs bij calamiteuze gevolgen kan voortijdig optreden soms achterwege blijven. Zo bleek in de praktijk dat het afbreken van een vliegtuigvleugel zo zelden voorkomt dat deze storingsmogelijkheid geen reden is om tot preventief onderhoud over te gaan.

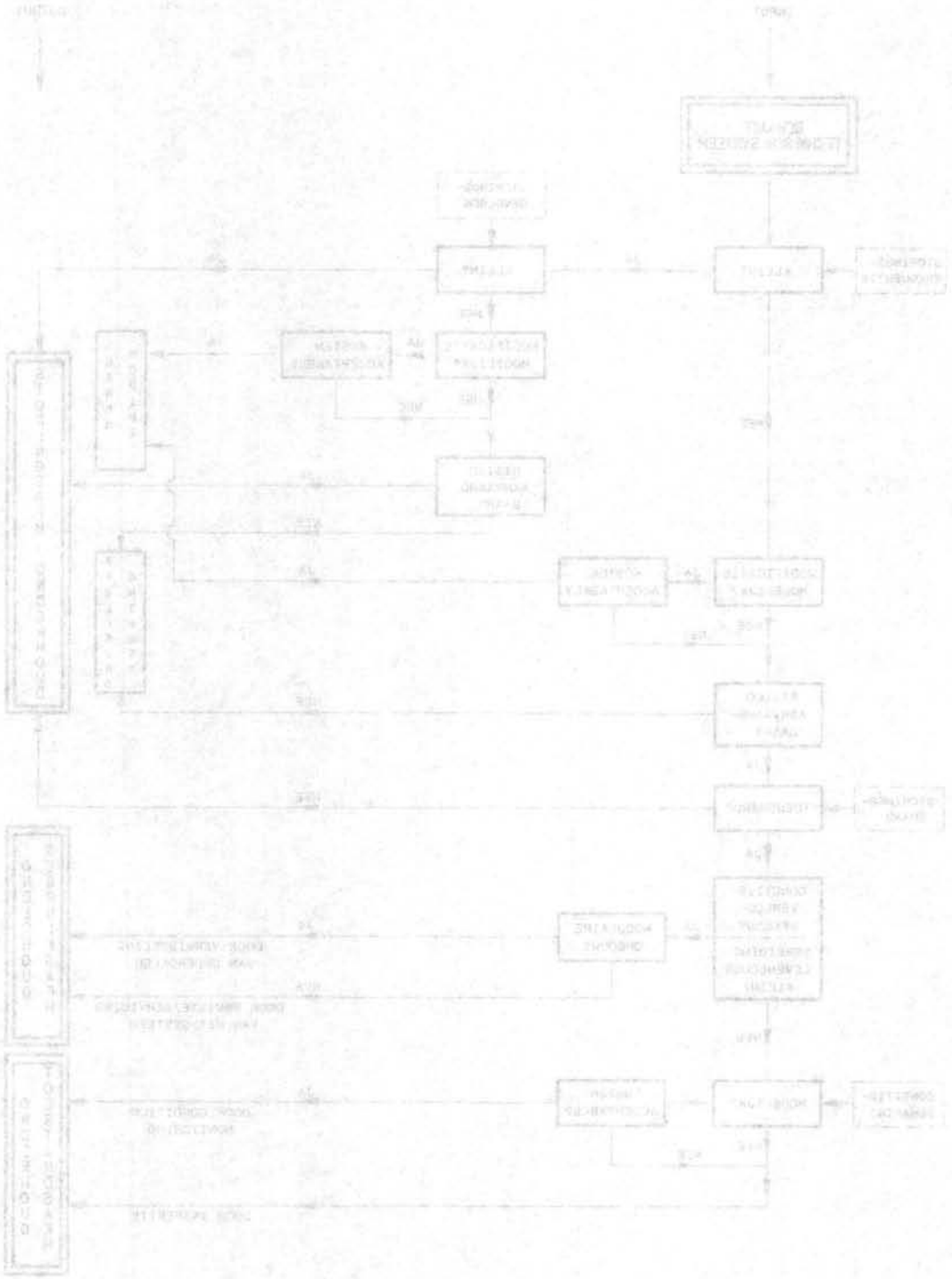
Overigens zal reeds in het ontwerpstadium een *risico-aftasting* moeten plaatsvinden van de ongewenste faalgevolgen, waarbij de hoogte van de acceptatiedrempel terzake van de onveiligheid afhangt van allerlei overwegingen en omstandigheden. Bij het ontstaan van een gaslek mag dan de falende afsluiter — dankzij voldoende reservering en doordachte organisatie — zeer snel zijn vervangen, de opgelopen schade aan mens en milieu kan inmiddels onvoorstelbaar zijn.
Met name is de vraag naar een toelaatbare risiconeming lastig te beantwoorden, indien het om eventuele bedieningsfouten gaat. Moet bijvoorbeeld een medisch apparaat intern worden beveiligd, als een zuurstof- en een stikstofaansluitnippel door onzorgvuldigheid van het ziekenhuispersoneel kan

worden verwisseld?
Indien het als een noodzakelijkheid wordt beoordeeld, zal (binnen de gestelde financiële grenzen) tot *modificatie* moeten worden overgegaan, zoals de inbouw van alarmering of het kiezen van hoogwaardige onderdelen.
Zijn de wijzigingen van een fundamenteel en ingrijpend karakter, dan zal een *herontwerp* van het systeem de enige oplossing zijn.

Indien de gang door het beslissingsdiagram naar beneden wordt gevolgd, zal het verloop van de *storingsgraad* in de tijd een belangrijke beslissingsfactor zijn. Wij verwijzen in dit verband naar paragraaf 1.10, waar reeds preventief onderhoud werd afgeraden bij de negatief-exponentiële distributie, dat wil zeggen bij een constante failure rate.
Bij een toenemende hazard rate (zoals bij veroudering of bij toepassing van redundantie, zie paragraaf 2.7) zal bekeken moeten worden in hoeverre het conditieverloop of de grootte van de levensduurspreiding bekend is, zoals dat in paragraaf 5.8 uiteengezet is.

Hier valt blijkbaar de keuze tussen gebruiks- en toestandsafhankelijk onderhoud, waarbij de uitvoering van de eerstgenoemde onderhoudsvorm afhangt van het al of niet modulair opgebouwd zijn van het systeem in kwestie.
Bij het ontbreken van nadere conditie- en bedrijfszekerheidsgegevens of een te grote levensduurspreiding, zal tenslotte via monitoring of inspectie aan de hand van de systeemtoestand moeten worden bepaald, waar en op welke wijze moet worden gehandeld teneinde de conditie weer op te voeren en het moment van de eerstvolgende storing in positieve zin te verleggen.


INPUT
OUTPUT
BEWAAKT TECHNISCH SYSTEEM
STORINGS-GEVOLGEN
STORINGS-FREQUENTIE
KLEIN?
JA
KLEIN?
JA
NEE
MODIFICATIE MOGELIJK?
JA
KOSTEN ACCEPTABEL?
JA
MODIFI-CEREN
NEE
NEE
NEE
RISICO AANVAARD-BAAR?
JA
NEE
STORINGSAFH.-ONDERHOUD
MODIFICATIE MOGELIJK?
JA
KOSTEN ACCEPTABEL?
JA
ONTWERP AFGEKEURD
NEE
NEE
RISICO AANVAARD-BAAR?
NEE
JA
STORINGS-GRAAD
TOENEMEND?
NEE
JA
CONDITIE-VERLOOP BEKEND?
SPREIDING LEVENSDUUR KLEIN?
JA
MODULAIRE OPBOUW?
JA
DOOR VERWISSELING VAN ONDERDELEN
NEE
DOOR REVISIE/SERVICING VAN HET SYSTEEM
GEBRUIKSAFH.-ONDERHOUD
NEE
CONDITIE-BEWAKING
MOGELIJK?
JA
KOSTEN ACCEPTABEL?
JA
DOOR CONDITION MONITORING
NEE
NEE
DOOR INSPEKTIE
TOESTANDSAFH.-ONDERHOUD



6 RESERVE-EENHEDEN

6.1 De reserve-eenheid in vroeger dagen

Het is een ervaringsfeit, dat elk technisch produkt de eigenschap bezit, dat het kan falen. Daarmee wordt bedoeld, dat een toestand is bereikt, waarin het produkt niet helemaal ("partial failure") of helemaal niet ("complete failure") meer de functie kan verrichten, waartoe het is geproduceerd.
Nu bestaat er een krachtig middel om (a) de ongemakken, (b) de irritatie en/of (c) de economische verliezen tegen te gaan, die onlosmakelijk aan een dergelijke uitval verbonden zijn.
Dit middel — overigens reeds van oudsher bekend — is de toepassing van de *reserve-eenheid* en het in voorraad houden dan wel het meevoeren ervan. Het is uiteraard de bedoeling dat deze eenheden (ook wel *spare parts* genoemd) de plaats innemen van de uitgevallen exemplaren. Of deze *substitutie* manuaal (bijvoorbeeld het verwisselen van een autoband) òf door middel van omschakeling plaatsvindt, is daarbij niet essentieel.

De vraag, *hoeveel* dan wel als reserve van een bepaald onderdeel in voorraad moest worden gehouden of onderweg moest worden meegenomen, was in vroeger dagen geen probleem. Of het werd nauwelijks als een probleem herkend. Een getalsmatige benadering van de *bevoorradingspolitiek* (*spare part provisioning*) van magazijnen en schepen was (en is vaak nog steeds) een kwestie van allerlei vuistregeltjes, zoals het als reserve meenemen van 20% van alle in een installatie toegepaste onderdelen of de aankoop van reservedelen ten bedrage van 10% van de systeemprijs. Een dergelijke *heuristische* benadering werd daarbij krachtig in de hand gewerkt door de *lage echelon*, waarop de vervanging van het falende onderdeel tot stand kwam, namelijk op het niveau van het enkelvoudige componentje. Op elektronisch gebied bijvoorbeeld betekende dit de substitutie van één doorgebrand weerstandje, waarna de radio-ontvanger na enig knutselen en montagewerk wederom kon functioneren.
Trouwens de *kostprijs* van een dergelijk reservedeel was meestal dermate laag — mede vanwege het ongecompliceerde karakter ervan — dat het economisch toelaatbaar werd geacht zich tot in de verzadiging met reserve te voorzien, zodat men te allen tijde aan geen onderdeel gebrek had.
Bovendien vormde het *overschot* aan reserve op het moment, dat de

desbetreffende apparatuur werd afgeschaft, geen enkel bezwaar: de resterende onderdeeltjes waren zonder meer wederom in een daarop volgende type toepasbaar. Kortom, er bestond geen enkele behoefte aan een nauwkeurige kwantificering bij de voorraadbeheersing, analoog aan het jampotje met spijkers, dat zich op menige zolder bevindt.

6.2 De reserve-eenheid thans

Evenwel. Het karakter van de reserve-eenheid is — met name op elektronisch gebied — in de loop van de laatste jaren grondig gewijzigd. De eenvoudige apparatuur van weleer heeft plaats gemaakt voor een zeer gecompliceerd systeem (a) dat in staat wordt geacht veel meer functies te vervullen, (b) waarin veel meer geld is geïnvesteerd en (c) waaraan veel hogere eisen ten aanzien van de beschikbaarheid, de onderhoudbaarheid, de bedienbaarheid en de veiligheid worden gesteld dan vroeger het geval was. De operationele gevolgen — door één enkele fout veroorzaakt — kunnen thans bijzonder ingrijpend van karakter zijn voor het totale systeem. Het haperen van één onderdeel in een computer kan de normale werkzaamheden bij een bankinstelling urenlang vertragen.
De gevolgen van deze ontwikkelingen zijn zeer ingrijpend gebleken en dat niet alleen op technisch gebied, maar zeker ook ten aanzien van de logistieke organisatie. Zo is — om eens iets te noemen — de zogenaamde *modulaire opbouw* van apparatuur opgekomen, die alleen al uit een oogpunt van onderhoudbaarheid noodzakelijk is gebleken. Daarbij worden allerlei onderdelen in grotere of kleinere functionele groepen (en dat zijn dan de "modulen") samengevoegd tot één enkel subsysteem, dat in het totale systeem eenvoudig *bereikbaar* èn *uitwisselbaar* is aangebracht, zodat — vaak door middel van een enkele handeling — een snelle vervanging mogelijk is (repair by replacement).

* Bijzonder stimulerend voor de modulaire opbouw is het steeds kleiner worden van de componenten geweest. Door deze zogenaamde *microminiaturisatie* is het mogelijk gebleken een steeds groeiend aantal functies te laten verzorgen door een steeds groter aantal bouwstenen binnen een aanvaardbaar volume (in de vorm van IC's) onder te brengen.

Voorts moet in dit verband de *snelle veroudering* van de in gebruik zijnde apparatuur worden genoemd. Bij het op de markt brengen van systemen loopt deze — voor wat betreft de technologie — vaak al weer bij de laatste stand van de techniek achter en binnen de geprojecteerde *gebruiksduur* (dit

is de periode tussen aanschaf en uitdienststelling) van een apparaat worden soms twee of drie opvolgers ontwikkeld, gefabriceerd èn op de markt gebracht, een ieder met zijn eigen specifieke reserve-eenheden-assortiment. Het naast elkaar in gebruik zijn van apparatuur, behorende tot verscheidene technische generaties, is in de huidige praktijk geen onbekend verschijnsel.
In deze stroom van onderlinge niet-uitwisselbare modulen is bovendien de fabrikant soms genoodzaakt een steeds korter wordende naleveringsgarantie te hanteren, hetgeen de afnemer van complexe systemen opnieuw dwingt zich op een scherpere kwantificering van zijn aan te schaffen reserve-eenheden-pakket te bezinnen.

Samenvattend kan worden gesteld dat de reserve-eenheid in de loop van een beperkt aantal jaren een enorme gedaanteverwisseling heeft ondergaan. De vroegere elementaire component is thans uitgegroeid tot een kostbaar en compact subsysteem, een modulaire eenheid met vele functies, met (a) een gefocusseerd toepassingsgebied en (b) samengesteld uit onderdelen, waaraan — veel meer dan vroeger — bijzonder hoge eisen ten aanzien van het bedrijfszekerheidsgedrag moet worden gesteld.

6.3 Indeling reserve-eenheden

In de vorige paragraaf werd de modularisatie van de huidige apparatuur ter sprake gebracht, dat wil zeggen het samenbouwen van verschillende onderdelen (en functies) tot een fysieke eenheid.
Enige voordelen van een dergelijke apparatieve opbouw zijn:

- Het storingzoeken wordt sterk vereenvoudigd, met name bij toepassing van bedrijfszekere alarmeringsapparatuur of ingebouwde testapparatuur (bite = built-in-test-equipment). Ook door de eenvoud van de reparatiebehandeling — namelijk een snelle uitwisseling van de kapotte module — kan veelal met een *lager opleidingsniveau* van het onderhoudspersoneel worden volstaan.
  - Het betreft hier een *fysieke* uitwisselbaarheid van modulen. Dit in tegenstelling tot een *functionele* uitwisselbaarheid, waarbij een niet-identiek systeem de uitgevallen functie(s) overneemt. Bij uitval van de

centrale verwarming bijvoorbeeld kan overgegaan worden op de elektrische kachel of open haard (*functionele redundantie*).

- Verder valt vrij eenvoudig in te zien dat door de samenvoeging van onderdelen het aantal *soorten* te voeren reserve-eenheden verminderd wordt, overigens wel afhankelijk van het niveau van modularisatie. Wordt deze namelijk steeds hoger gekozen (dat wil zeggen steeds meer onderdelen samengebracht in één module) dan zal uiteraard het assortiment reservedelen beperkter worden, hetgeen allerlei administratieve en logistieke voordelen biedt.
  Nadeel is natuurlijk wel, dat een modulaire eenheid, die in onklare toestand een installatie verlaat en ter herstel verder wordt behandeld, steeds meer goede onderdelen bevat, die — onlosmakelijk aan elkaar gekoppeld — eveneens het reparatiekanaal dienen te doorlopen, waardoor de investering in het *turn around circuit* (dit is de omloop van alle opgezonden + op reparatie wachtende + in reparatie zijnde + wederom voor gebruik ter beschikking zijnde modulen) toe zal nemen.

Nu komt — zo leert ons de praktijk — niet elk reservedeel op economische en/of technische gronden voor reparatie in het turn around circuit in aanmerking. Bijvoorbeeld omdat de noodzakelijke herstelwerkzaamheden te duur zijn. Of omdat deze als zéér moeilijk — zo niet onmogelijk — worden beoordeeld. Of omdat de aanschafprijs te laag is om er nog enige reparatiehandelingen aan te laten verrichten (zie paragraaf 1.4*).

De indeling van reserve-eenheden in *repareerbare* en *niet-repareerbare* exemplaren ligt dan ook voor de hand, hoewel hierbij de kanttekening moet worden geplaatst, dat de ligging van de scheiding tussen beide groepen afhankelijk is van de aanwezige of bereikbare reparatiefaciliteiten. De herstelwerkzaamheden kunnen zich namelijk afspelen op verschillende niveaus: (a) van de gebruiker, (b) van de werkplaats, niet ver van het systeem verwijderd, (c) van het meer centraal gelegen depot en uiteindelijk (d) van de fabrikant, die — al of niet contractueel — in laatste instantie aanspreekbaar dient te zijn voor een fundamentele storingsbehandeling. Met een stijgend onderhoudsniveau mag tevens een groter *vakmanschap* van het personeel worden verwacht, waaronder eventueel specialisten voor bepaalde modulen, voorzien van betere testapparatuur en benodigde uitrusting. Het gevolg van een dergelijke trapsgewijze intensivering van het onderhoud is, dat de *repareerbaarheid* van een falend onderdeel afhankelijk is van de echelon van behandeling.

Het *onderhoudsconcept* van een complex systeem dient dan ook te vermelden, welke reparatiestrategieën voor welke modulen moeten worden gevolgd (dus repairable of throw-away-item) en — indien tot herstel wordt besloten — welke onderhoudstaken op welk niveau zullen worden uitgevoerd ter minimalisering van de exploitatiekosten.
Een aparte groep wordt gevormd door reservedelen met een lage tot zeer lage vraag, de zogenaamde *slow movers*. Dit zijn units, waaraan zeer sporadisch behoefte is (zeg éénmaal per jaar). De moeizaamheid van een slagvaardige bevoorrading hiervan laat zich vermoeden, indien we met reservedelen te maken hebben, die enerzijds kostbaar zijn, maar anderzijds — indien niet voorradig — een lange levertijd vergen en daardoor een langdurige stilstand van het desbetreffende systeem veroorzaken. De schroef van een schip is hiervan een pakkend voorbeeld. Een noodzakelijke nabestelling van dit noodzakelijke onderdeel onderweg kan het vaartuig tot een langdurige stilligperiode dwingen, terwijl anderzijds een schroef als reserve in standby een kostbare investering betekent, indien daar jarenlang geen vraag naar is.

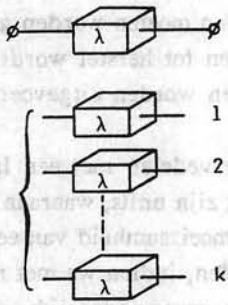
Samenvattend kunnen we de reserve-eenheden als volgt indelen:

- *verbruiksdelen*	:	voor éénmalig gebruik; throw-away-item.
- *mutatie- of wisseldelen*	:	reparatie na falen; repairable.
- *risicodelen*	:	eenheden, die naar verwacht mag worden, normaal niet (of nauwelijks) nodig zijn; slow movers.

6.4 Standaardisatie

In paragraaf 4.3 is de overlevingskans afgeleid voor een eenheid, met k (identieke) reserve-eenheden in koude reserve (= standby) daaraan toegevoegd. Er is géén reparatie, de eenheden worden als consumables (throw-away-items) beschouwd.

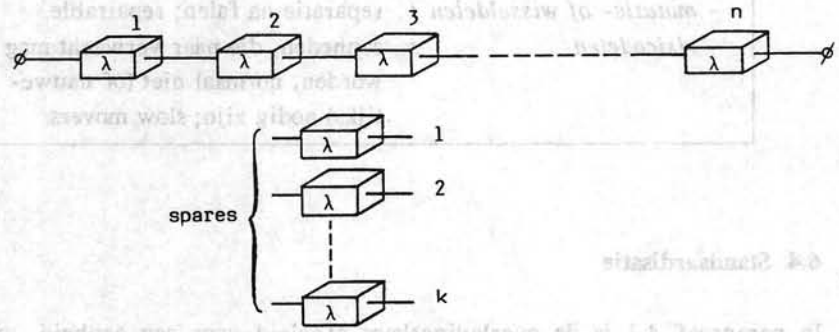
* Ter herinnering:



$$R(t) = \exp(-\lambda t) \sum_{i=0}^{k} \frac{(\lambda t)^i}{i!} .$$

Nu komt het bij de technische opbouw van (computer)systemen steeds vaker voor dat een aantal (zeg n) identieke modulen (bijvoorbeeld geheugeneenheden) in serie worden geplaatst. De uitval van één dezer units betekent dan tevens een systeemstoring, zo kenmerkend voor een serieschakeling. Het aantal spares, dat aan een dergelijk seriesysteem moet worden toegevoegd om de bedrijfszekerheid hiervan op de gewenste waarde te brengen, wordt groter, naarmate de waarde van n stijgt.

* De bedrijfszekerheid van een n-seriesysteem, met k (identieke) spares daaraan toegevoegd



kan berekend worden met behulp van:

$$R(t) = \exp(-n\lambda t) \sum_{i=0}^{k} \frac{(n\lambda t)^i}{i!} .$$

Ga dat na.

Door de onderlinge identiciteit der units is elk van de spares uiteraard inzetbaar op een ieder van de n posities in de installatie. En het is juist vanwege deze onderlinge uitwisselbaarheid, dat de toename van het benodigde aantal spares k geen gelijke tred houdt met de stijging van n.

* Een getallenvoorbeeld ter illustratie. Voor een serieschakeling van n identieke eenheden (gemiddelde levensduur θ) is als operationele eis gesteld, dat de overlevingskans van het systeem $\geq .950$ moet zijn voor een bedrijfstijd $T = .05\ \theta$. Voor de waarden n = 1, 5, 20 en 100 worden dan de benodigde spares:

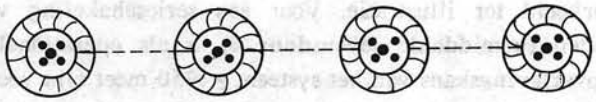
n units in serie	aantal spares k	$R_{syst}(T)$
1	0	.951
5	1	.974
20	3	.981
100	9	.968

Dat wil dus zeggen dat bij een serieschakeling van 100 units (θ = 100 h) 9 eenheden in voorraad moeten zijn om voor een bedrijfstijd van 5 h een overlevingskans van $\geq .95$ te verkrijgen.

In de (sterke) a-lineariteit tussen n en k is het zeer voordelig *standaardisatie* op de componenten toe te passen, met name indien de aanschaf zich over verscheidene typen apparatuur uitstrekt.
Technisch worden momenteel allerlei mogelijkheden geboden om tot een grote mate van uniformiteit te komen. De operationele versterker is hiervan een voorbeeld, waarbij één type voor verschillende bewerkingen kan worden aangepast.
Dat een duidelijke beperking van het aantal toegepaste onderdelen een administratief toe te juichen zaak is, behoeft geen betoog. Maar een voordeel is bovendien dat door de toename van de onderlinge uitwisselbaarheid van gestandaardiseerde eenheden de omvang van de benodigde reserve kan verminderen, waarbij tenslotte de ruimere informatie kan worden genoemd omtrent uitvalsgegevens, omdat bij typebeperking meer eenheden van éénzelfde uitvoering in bedrijf zijn en daardoor statistisch nauwkeuriger de uitvalskans en dus het aantal benodigde spares kan worden bepaald.

Opgave 6.1:

De bandenbezetting van een personenauto is:



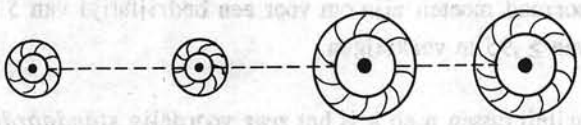
dat wil zeggen vier identieke banden in serie.
Toon aan dat voor $\lambda t << 1$ voor dit seriesysteem geldt:

(a) Met één reserveband $R_{syst}(t) \simeq 1 - 8\lambda^2 t^2$.

(b) Met twee reservebanden $R_{syst}(t) \simeq 1 - \frac{32}{3} \lambda^3 t^3$.

Opgave 6.2:

De bandenbezetting van een tractor is:



Alle banden hebben dezelfde failure rate λ.
Toon aan dat voor $\lambda t << 1$ voor dit seriesysteem geldt:

met één kleine en één grote reserveband $R_{syst}(t) = 1 - 4\lambda^2 t^2$.

7 BEWAAKTE SYSTEMEN

7.1 Bewaakte systemen

We gaan nu over tot de behandeling van bewaakte systemen (*maintained systems*). Tot dusver zijn hoofdzakelijk bedrijfszekerheidsberekeningen gemaakt, waarbij geen *onderhoud* te pas kwam. Dat wil zeggen, dat praktisch alle tot nu toe behandelde modellen gemeen hebben, dat tijdens bedrijf géén bewaking aanwezig is en géén menselijk ingrijpen — op welke wijze dan ook — mogelijk wordt verondersteld om het systeem in bedrijf te houden dan wel wederom in bedrijf te krijgen.
In de hierna volgende opmerkingen zal onder een *bewaakt* systeem worden verstaan (zie paragraaf 1.11):

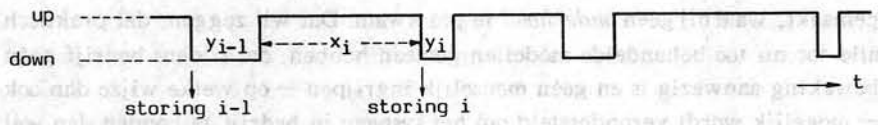
- Òf een systeem zonder reserve, dat na uitval tijdens de down-periode wordt gerepareerd.

- Òf een systeem dat tijdens bedrijf wederom in de normale toestand kan worden gebracht, doordat redundantie aanwezig is (*repair by replacement*), waarna het falende onderdeel (terwijl dus het systeem alweer functioneert) in reparatie wordt genomen. Hierbij wordt de tijd, nodig voor alarmering en lokalisering van de storing en substitutie van het falende onderdeel, verwaarloosbaar klein geacht. We duiden dit aan als ideale vervanging.

Een dergelijke reparatie door vervanging kan op verschillende *systeemniveaus* plaatsvinden. Bijvoorbeeld op modulair niveau, zoals bij het verwisselen van een (lekke) band, een manuale actie, waardoor het voertuig wederom kan functioneren. Vindt daarentegen een reparatie in de garage plaats, dan kan vervanging op een hoger level plaatsvinden door middel van een leenwagen, die op dat moment als redundant in orde èn beschikbaar is. Er zij nog op gewezen dat in het laatste geval de *grenzen* van het totale systeem eveneens het garagegebeuren omvatten.

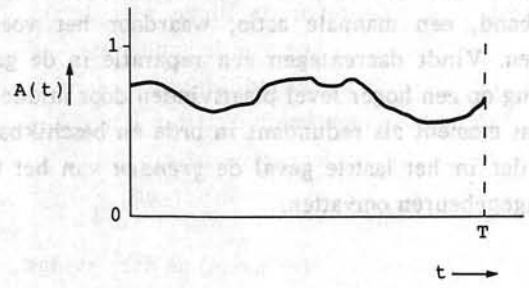
7.2 Beschikbaarheid

Is op het faalmoment geen redundantie (meer) aanwezig of inzetbaar, dan is blijkbaar de down-periode van het systeem aangebroken, waarin de herstelwerkzaamheden beginnen of worden doorgezet, totdat het systeem weer in bedrijfsgerede toestand is gebracht.
Schematisch is het bedrijfsleven van een systeem dan als volgt weer te geven:



Het is een registratie van achtereenvolgende up- en down-toestanden, waarbij x_i de i-de ononderbroken bedrijfsperiode voorstelt en y_i de i-de daaropvolgende noodzakelijke down-periode met herstelactiviteiten. Het is zinvol in verband hiermee een belangrijke operationele grootheid te memoreren, namelijk de *beschikbaarheid* of (point-wise) *availability* A(t), die reeds in paragraaf 1.4 ter sprake kwam als de kans, dat het desbetreffende systeem ten tijde t in de werkende of anders in de bedrijfsgerede toestand wordt aangetroffen.

Naast deze vorm van momentane beschikbaarheid zijn een paar hiervan afgeleide grootheden in praktische zin zeker net zo belangrijk.
Beschouw een operationeel interessante bedrijfsperiode (0,T). Door het schetsen van de grafiek van A(t), $t \in (0,T)$ kunnen we een indruk krijgen van de beschikbaarheid op ieder tijdstip.



Willen we deze indruk vervangen door een getal, dan leent zich daartoe het wiskundig gemiddelde over het interval (0,T), gegeven door de uitdrukking

$\frac{1}{T}\int_0^T A(t)\,dt$. We noemen deze grootheid de *mission availability* of ook wel de interval availability, genoteerd als MA(T).

Indien $\lim_{T\to\infty} MA(T)$ bestaat (we praten hier dus over de mission availability van een zéér lange periode), dan noemen we deze grootheid de *long-term* of *steady-state availability*, notatie A_∞. Een Nederlandse term voor A_∞ is beschikbaarheidsgraad, een treffend gekozen woordgebruik voor een bewaakt systeem.

* Een klok — bijvoorbeeld — die gedurende twee kalenderjaren getrouw de tijd heeft aangewezen, met uitzondering van (in totaal) twee weken aan reparatieperioden, blijkt achteraf een beschikbaarheidsgraad van 102/104 = 98% te hebben gehad. Met deze kwantificering wordt overigens geen enkele uitspraak gedaan over het aantal en de duur van de afzonderlijke herstelperioden; het enige beschikbare gegeven is, dat de som hiervan twee weken bedraagt.

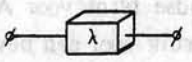
Herstel vindt plaats door (minstens) één reparatiekanaal, dat wil zeggen door een onderhoudspersoon met de benodigde vakkennis, gereedschappen en reservedelen. Een man of vrouw, die op ieder moment bereid en in staat is om — waar nodig — technisch in te grijpen.

De *reparatieduur* van een (sub)systeem of van een module is in het algemeen niet constant. Deze hersteltijd is een niet-negatieve stochastische variabele, verdeeld volgens de *repairability*, dit is de kans, dat het herstel binnen de tijd t tot een goed einde wordt gebracht. We nemen bij de nu volgende berekeningen en vraagstukken aan (tenzij anders vermeld) dat de reparatieduur de *negatief-exponentiële verdeling* volgt, met als gemiddelde waarde $1/\mu$, waarin de repair rate μ onafhankelijk van de tijd is. In dat geval stelt μdt de conditionele kans voor, dat de reparatie in de periode (t, t + dt) wordt afgerond, mits het herstel ten tijde t nog aan de gang was.
Het betekent verder dat $1 - \exp(-\mu t)$ de kans aanduidt, dat de herstelperiode kleiner is dan t. De keuze van de bovengenoemde distributie houdt praktisch in dat voor een groot deel de reparatietijden vrij kort zijn, terwijl anderzijds enkele herstelactiviteiten een vrij lange periode vergen.

In de hierna volgende paragrafen gaan we na hoe (a) de overlevingskans en (b) de beschikbaarheidsgraad van bewaakte systemen — mèt en zonder reservedelen — kunnen worden berekend.

7.3 Beschikbaarheid zonder redundantie

We geven eerst een voorbeeld van de berekeningen bij een systeem *zonder redundantie*, namelijk een enkele eenheid plus een reparatiekanaal (repair rate μ).



Toestandsinventarisatie: S_0 ≡ eenheid goed; géén reparatie.
S_1 ≡ eenheid gefaald en in reparatie.

Overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \end{array} \begin{array}{c} \begin{array}{cc} S_0 & S_1 \end{array} \\ \begin{pmatrix} 1 - \lambda dt & \lambda dt \\ \mu dt & 1 - \mu dt \end{pmatrix} \end{array},$$

waaruit

$$\frac{dP_0(t)}{dt} = -\lambda P_0(t) + \mu P_1(t)$$

$$\frac{dP_1(t)}{dt} = \lambda P_0(t) - \mu P_1(t) ,$$

waarin $P_i(t)$, $i = 0,1$ de kans voorstelt dat het systeem zich ten tijde t in toestand S_i, $i = 0,1$ bevindt. Met $P_0(0) = 1$ en $P_1(0) = 0$ als beginvoorwaarden volgt hieruit voor de beschikbaarheid:

$$A(t) = P_0(t) = \mu/(\lambda + \mu) + \lambda/(\lambda + \mu) \exp(-(\lambda + \mu)\, t) .$$

De mission availability is dan

$$MA(T) = \frac{1}{T} \int_0^T A(t)\, dt$$

$$= \mu/(\lambda + \mu) + \lambda(\lambda + \mu)^2\, T - \lambda/(\lambda + \mu)^2 \exp(-(\lambda + \mu)\, T) ,$$

waaruit voor een zéér lange bedrijfstijd geldt

$$A_\infty = \lim_{T\to\infty} MA(T) = \mu/(\lambda + \mu)$$

$$= \frac{\text{gemiddelde levensduur eenheid}}{\text{gemiddelde reparatieduur + gemiddelde levensduur eenheid}},$$

een in de eenvoudige bedrijfszekerheidsliteratuur bekende formule.

7.4 Beschikbaarheidsgraad in het geval van steady-state

In het voorbeeld van de vorige paragraaf zijn we in staat geweest de drie beschikbaarheids-maten op een directe manier uit te rekenen. In complexe situaties brengt deze methode echter veel rekenwerk met zich mee, waardoor expliciete oplossingen lang niet altijd mogelijk zijn. Het probleem zit vaak in het oplossen van de differentiaalvergelijkingen. Nu treedt in onze modellen vaak een bijzondere situatie op die we ook in het onderhavige voorbeeld zien: het blijkt dat $\lim_{t\to\infty} P_0(t)$ bestaat, evenals $\lim_{t\to\infty} P_1(t)$. Als deze limieten voor alle toestanden bestaan dan spreken we van de zogenaamde *steady-state toestand.* Vaak zal bovendien in deze steady-state toestand gelden $\lim_{t\to\infty} P_i'(t) = 0,\ i = 0,1,...,n.$
Dit geeft ons een middel om zonder de differentiaalvergelijkingen op te lossen, uit diezelfde vergelijkingen de *steady-state kansen* π_i op te lossen. Bovendien kunnen we bewijzen dat in zo'n geval geldt:

$$A_\infty = \sum_w \pi_i,$$

waarin $\sum_w$ de sommatie van alle werkende toestanden voorstelt.
Toepassen van deze methode op ons voorbeeld levert eerst het volgende stelsel voor de steady-state kansen:

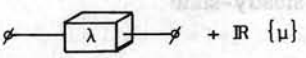
$$\begin{aligned} -\lambda\pi_0 + \mu\pi_1 &= 0 \\ \lambda\pi_0 - \mu\pi_1 &= 0\ , \end{aligned}$$

een afhankelijk stelsel dat zich éénduidig op laat lossen door toevoeging van de vergelijking

$$\pi_0 + \pi_1 = 1 ,$$

waarmee de geruststeldende gedachte tot uitdrukking wordt gebracht dat het systeem zich te allen tijde in één van de toestanden S_0 of S_1 moet bevinden. We vinden dan dat $A_\infty = \pi_0 = \mu/(\lambda + \mu)$, uiteraard geen nieuw resultaat maar wel sneller gevonden.

Samenvattend kunnen we stellen dat de beschikbaarheid van een enkele unit met één reparatiekanaal



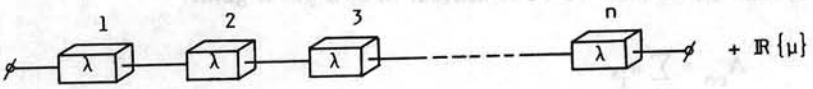
berekend kan worden met

$$A_\infty \approx 1 - \rho ,$$

wanneer $\rho = \lambda/\mu << 1$.

Opgave 7.1:

Toon aan dat voor n identieke eenheden in serie zonder reserve en met één reparatiekanaal geldt



$$A_\infty \approx 1 - n\rho, \qquad \text{als } n\rho = n\lambda/\mu << 1.$$

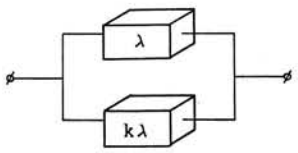
Opgave 7.2:

Verifieer dat de beschikbaarheidsgraad $A_\infty \approx 0.96$ van een park met tien terminals (θ van één terminal = 5000 h), waaraan één reparatiekanaal is toegevoegd (gemiddelde reparatieduur vier etmalen).

Voor een goede werking van het park zijn tien terminals noodzakelijk. Er is één extra terminal als (koude) reserve aanwezig.

7.5 Beschikbaarheid met redundantie

we zullen nu aan de hand van een voorbeeld onderzoeken wat de invloed is van redundantie in een bewaakt systeem. Deze redundantie kan in diverse vormen optreden, waarbij de uitersten gevormd worden door de situaties van reserve-onderdelen (passieve redundantie) en parallelschakeling (actieve redundantie, soms met identieke failure rates). Ook tussenvormen zijn denkbaar waarbij onderdelen wel in het systeem zijn opgenomen, maar daar onderbelast meefunctioneren (hetgeen zal leiden tot een lagere failure rate). Het voorbeeld houden we eenvoudig:



$+ R\{\mu\}$ $\qquad 0 < k \leq 1.$

We beschouwen een systeem van twee eenheden, een eenheid volledig belast met failure rate λ, de tweede eenheid gedeeltelijk belast met failure rate $k\lambda$ $(0 < k \leq 1)$. Faalt de volledig belaste eenheid, dan neemt de andere eenheid deze rol over (indien deze eenheid tenminste nog functioneert) en krijgt dan een failure rate λ.
We onderscheiden drie toestanden:

S_0: één volledig belaste eenheid, één partieel belaste eenheid;
S_1: één volledig belaste eenheid, één eenheid in reparatie;
S_2: één eenheid in reparatie, één eenheid defect.

Via deze drie mogelijke systeemtoestanden komen we dan uit op de volgende overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{bmatrix} 1 - (k+1)\,\lambda dt & (k+1)\,\lambda dt & 0 \\ \mu dt & 1 - (\lambda+\mu)\,dt & \lambda dt \\ 0 & \mu dt & 1 - \mu dt \end{bmatrix} \end{array} .$$

Hieruit volgen de differentiaalvergelijkingen:

$$\frac{dP_0}{dt} = -(k+1)\,\lambda P_0 + \mu P_1 \;;$$

$$\frac{dP_1}{dt} = (k+1)\,\lambda P_0 - (\lambda+\mu)\,P_1 + \mu P_2 \;;$$

$$\frac{dP_2}{dt} = \lambda P_1 - \mu P_2 \;.$$

Veronderstellende dat er een steady-state is vinden we hieruit:

$$\begin{aligned} -(k+1)\,\lambda\pi_0 + \mu\pi_1 &= 0 \;; \\ \lambda\pi_1 - \mu\pi_2 &= 0 \;; \\ \pi_0 + \pi_1 + \pi_2 &= 1 \;. \end{aligned}$$

Hieruit volgt voor de beschikbaarheidsgraad

$$A_\infty = \pi_0 + \pi_1 = \frac{\mu^2 + (k+1)\,\lambda\mu}{\mu^2 + (k+1)\,\lambda\mu + (k+1)\,\lambda^2} = \frac{1 + (k+1)\,\rho}{1 + (k+1)\,\rho + (k+1)\,\rho^2}$$

waarin $\rho = \lambda/\mu$. In het geval van passieve redundantie geldt $k = 0$, met andere woorden het reserve-onderdeel kan niet sneuvelen. Hiervoor volgt dan dat

$$A_\infty = \frac{1+\rho}{1+\rho+\rho^2} \approx 1 - \rho^2 \qquad (\text{als } \rho \ll 1) \;.$$

* De eisen, die de FAA (= Federal Aviation Administration) stelt aan het airtraffic-system DARC (= Direct Access Radar Channel), waarbij de functie — bij uitval — automatisch door een back-up systeem wordt overgenomen, zijn $\theta \geq 1250$ h en de gemiddelde reparatieduur $\theta_R \leq 0.5$ h. De *niet-beschikbaarheidsgraad* $U_\infty = 1 - A_\infty \simeq \rho^2$ bedraagt dan $\rho^2 = (0.5/1250)^2 = 16 \times 10^{-8}$, hetgeen neerkomt op een gemiddelde down-time van enige seconden per jaar.

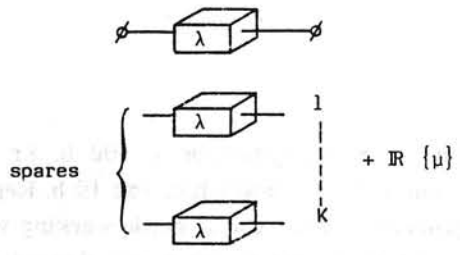
Voor het geval van de volledig actieve redundantie, parallelschakeling dus, volgt door $k = 1$ te nemen dat

$$A_\infty = \frac{1+2\rho}{1+2\rho+2\rho^2} \approx 1 - 4\rho^2 \qquad \text{met } \rho \ll 1.$$

Ten opzichte van de situatie van passieve redundantie neemt de niet-beschikbaarheidsgraad toe met een factor 4!

Opgave 7.3 :

Aan een actieve eenheid met k eenheden in standby is één reparatiekanaal toegevoegd.



Toon aan dat de beschikbaarheidsgraad gelijk is aan

$$A_\infty = 1 - 1 \Big/ \sum_{j=0}^{k+1} \rho^{-j}, \quad \text{met } \rho = \lambda/\mu .$$

Opgave 7.4 :

Een systeem bestaat uit twee identieke units A en B en een reparatiekanaal. De volgende reparatiepolitiek wordt gevolgd:

Ten tijde t = 0 wordt A in bedrijf gesteld en staat B standby. Op het moment dat A faalt, wordt B on-line gebracht, maar vindt nog géén reparatie van A plaats. Bij uitval van B faalt het systeem en beginnen de herstelwerkzaamheden achtereenvolgens aan A en daarna aan B. Pas nadat beide eenheden weer zijn hersteld, wordt A wederom ingeschakeld.

De failure rate van een actieve unit is λ_1, die van een unit in standby λ_2 ($< \lambda_1$).

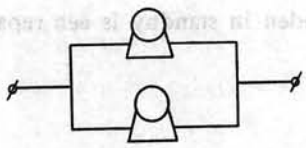
Toon aan dat de beschikbaarheidsgraad

$$A_\infty = \frac{(2 + \lambda_2/\lambda_1)\,\mu}{(2 + \lambda_2/\lambda_1)\,\mu + 2(\lambda_1 + \lambda_2)} .$$

Controleer dit resultaat voor $\lambda_2 \to 0$ en $\lambda_2 = \lambda_1$.

Opgave 7.5:

Twee generatoren staan parallel geschakeld



$+\mathbb{R}\{\mu\}$

De gemiddelde levensduur van een generator is 500 h. Er is één reparatiekanaal met een gemiddelde reparatieduur van 10 h. Reparatie vindt plaats zodra een generator faalt. Voor de goede werking van het systeem is minstens één goed functionerende generator voldoende.
Laat zien dat de beschikbaarheidsgraad $A_\infty = .9992$.

7.6 MTTFF

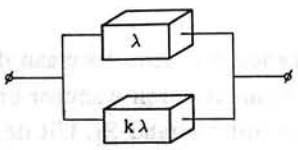
Zoals we al in hoofdstuk 1 lazen speelt naast de beschikbaarheid een andere grootheid een belangrijke rol bij het bestuderen van dit soort systemen. Het gaat hierbij om de verwachte levensduur. Nu zal de verwachte levensduur van een technisch systeem in het geval van (geslaagd) onderhoud in principe oneindig groot worden, deze grootheid interesseert ons dus niet echt. Wat wel interessant is, is de verwachte duur van een periode van functioneren, dat wil zeggen: hoelang gaat het systeem gemiddeld mee van de tewerkstelling tot aan de eerstvolgende storing? We maken hierbij ook weer onderscheid tussen de aanvangssituatie en de stabiele toestand-situatie. In de aanvangssituatie spreken we van MTTFF (*Mean Time To First Failure*), de verwachte tijd totdat het systeem voor het eerst down gaat. In de steady-state situatie spreken we van MTBF (*Mean Time Between Failures*), de verwachte (gemiddelde) tijd tot het systeem weer down gaat nadat het juist is gerepareerd.
In het laatste geval nemen we aan dat na een periode van down zijn het systeem weer start in een vaste situatie die niet noodzakelijk de beginsituatie hoeft te zijn; ware dit wel het geval dan vallen de begrippen MTTFF en MTBF samen! Zijn er meerdere startsituaties na een periode van down zijn, dan zijn er evenzovele MTBF's! (Door wat voor oorzaken zou de nieuwe startsituatie van de beginsituatie kunnen afwijken?)

Welke grootheid we ook willen berekenen, steeds doen we dit met de formule

$$\theta = \int_0^\infty R_{syst}(t)\,dt = \sum_w P_i(s = 0)\,,$$

waarin we voor $R_{syst}(t)$ wel de goede reliability functie moeten kiezen en $\sum_w$ weer de sommatie over alle werkende toestanden is.

We illustreren dit aan de hand van het in paragraaf 7.5 behandelde voorbeeld



+ R{μ}

Als we de MTTFF van dit systeem willen bepalen dienen we eerst $R_{syst}(t)$ te bepalen. Dit kan weer met dezelfde techniek met de overgangsmatrix als in paragraaf 7.5, waarbij de falende toestanden echter als absorberend beschouwd dienen te worden!
De overgangsmatrix wordt dan:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{pmatrix} 1 - (k+1)\,\lambda dt & (k+1)\,\lambda dt & 0 \\ \mu dt & 1 - (\lambda+\mu)\,dt & \lambda dt \\ 0 & 0 & 1 \end{pmatrix} \end{array}.$$

Nemen we aan dat we in toestand S_0 starten dan geldt

$$\begin{aligned} -1 &= -(k+1)\,\lambda P_0(s=0) + \mu P_1(s=0)\,; \\ 0 &= (k+1)\,\lambda P_0(s=0) - (\lambda+\mu)\,P_1(s=0)\,, \end{aligned}$$

waaruit volgt

$$\text{MTTFF} = P_0(s = 0) + P_1(s = 0) = \frac{(k + 2)\,\lambda + \mu}{(k + 1)\,\lambda^2} .$$

Voor de situatie van passieve redundantie (koude standby, reserve) geldt $(k \to 0)$

$$\text{MTTFF} = \frac{2\lambda + \mu}{\lambda^2} .$$

Voor actieve redundantie (parallelschakeling) geldt $(k = 1)$

$$\text{MTTFF} = \frac{3\lambda + \mu}{2\lambda^2} .$$

Gaan we uit van de wens de MTBF te berekenen dan nemen we aan dat het systeem na een down-periode direct begint te functioneren wanneer er weer een eenheid beschikbaar is; we starten dus vanuit toestand S_1. Uit de overgangsmatrix lezen we dan de volgende vergelijkingen af:

$$0 = -(k + 1)\,\lambda P_0(s = 0) + \mu P_1(s = 0) ;$$
$$-1 = (k + 1)\,\lambda P_0(s = 0) - (\lambda + \mu)\,P_1(s = 0) ,$$

waaruit volgt

$$\text{MTBF} = \frac{(k + 1)\,\lambda + \mu}{(k + 1)\,\lambda^2} .$$

Voor passieve redundantie geeft dit

$$\text{MTBF} = \frac{1}{\lambda} + \frac{\mu}{\lambda^2} ,$$

en voor actieve redundantie

$$\text{MTBF} = \frac{1}{\lambda} + \frac{\mu}{2\lambda^2} .$$

Dit betekent dat het rendement van de reparateur ten opzichte van de MTBF in geval van actieve redundantie slechts de helft bedraagt van het geval van passieve redundantie.

Opgave 7.6:

Een systeem bestaat uit twee parallel geschakelde identieke eenheden A en B, die beide een goede werking van het systeem noodzakelijk zijn.

Aan het systeem is, behalve een (identieke) eenheid als reserve, nog een reparatiekanaal toegevoegd. De reparateur stopt zodra het systeem faalt.

Toon aan dat $\theta_{syst} = (\mu + 2\lambda)/4\lambda^2$ voor het geval dat ten tijde t = 0 de reserve-eenheid onklaar is en terstond in reparatie gaat.

Opgave 7.7:

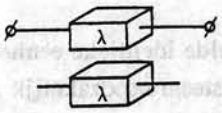
Idem als opgave 7.6, met dit verschil: voor een goede werking van het systeem is slechts één van de eenheden noodzakelijk.
Antwoord: $(\mu^2 + 3\mu\lambda + 6\lambda^2)/4\lambda^3$.

7.7 Meer dan één reparatiekanaal

De beschikbaarheidsgraad A_∞ wordt — zoals uit voorgaande voorbeelden en opgaven blijkt — onder meer bepaald door de snelheid, waarmee een falende eenheid wordt hersteld. Indien — bijvoorbeeld vanwege operationele redenen — de availability moet worden opgevoerd, kan worden overwogen een beroep te doen op een *tweede* reparateur, die met zijn werkzaamheden start op een moment dat een eenheid faalt, terwijl er reeds een reparatie aan een andere unit aan de gang is.
Aan de hand van een voorbeeld zal hieronder de invloed van een extra reparatiekanaal op de A_∞ worden nagegaan.

Voorbeeld:

Systeem *met* redundantie: een enkele eenheid in bedrijf, een identieke eenheid in koude reserve (standby) plus *twee* reparatiekanalen.



Toestandsinventarisatie:

$S_0 \equiv$ twee eenheden goed; géén reparatie.
$S_1 \equiv$ één eenheid goed; één eenheid in reparatie.
$S_2 \equiv$ twee eenheden gefaald en in reparatie.

Overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{pmatrix} 1 - \lambda dt & \lambda dt & 0 \\ \mu dt & 1 - (\lambda+\mu)\,dt & \lambda dt \\ 0 & 2\mu dt & 1 - 2\mu dt \end{pmatrix} \end{array} .$$

De kans namelijk dat in toestand S_2 *één* der units in de periode $(t_1, t + dt)$ wordt hersteld — mits beide reparaties ten tijde t nog aan de gang waren — is gelijk aan $2\mu dt$.

Ga na dat met behulp van de matrix U het volgende resultaat gevonden kan worden:

$$A_\infty = P_0 + P_1 = \frac{2\mu^2 + 2\lambda\mu}{2\lambda^2 + 2\lambda\mu + \lambda^2} = \frac{2 + 2\rho}{2 + 2\rho + \rho^2} \simeq 1 - \frac{\rho^2}{2},$$

met $\rho = \lambda/\mu << 1$.

De niet-beschikbaarheidsgraad $U_\infty = 1 - A_\infty$ is ten opzichte van het voorbeeld in paragraaf 7.5 (met één reparateur) met een factor twee verkleind.

Een andere mogelijkheid om de effectiviteit van de aanwezige reparatie-faciliteit te verhogen is het adviseren van een *tweede* man (of vrouw) bij de reparatie van de *eerste* kapotte eenheid. In tegenstelling tot het voorbeeld in

de voorgaande paragraaf, waar het ging om een *onafhankelijke* dienstverlening, is hier sprake van een "joint service", met het doel de gemiddelde reparatieduur te bekorten.

Nu is het voorstelbaar dat in dat geval met het toenemen van het aantal reparateurs de persoonlijke bijdrage in het herstelproces van een enkele eenheid afneemt. Door dit "elkaar enigszins voor de voeten lopen" wordt door het optreden van een tweede onderhoudsman de herstelduur wel bekort, maar niet gehalveerd, hetgeen tot uitdrukking wordt gebracht door invoering van een repair rate $k\mu$, met $1 \leq k \leq 2$. In het geval beide units falen is er wederom sprake van een onafhankelijke service.

De overgangsmatrix in het vorige voorbeeld wordt dan

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{pmatrix} 1 - \lambda dt & \lambda dt & 0 \\ k\mu dt & 1 - (\lambda + k\mu)\, dt & \lambda dt \\ 0 & 2\mu dt & 1 - 2\mu dt \end{pmatrix} \end{array} .$$

Hieruit volgt dan

$$A_\infty = \pi_0 + \pi_1 = \frac{2k + 2\rho}{2k + 2\rho + \rho^2} = 1 - \frac{\rho^2}{2k} ,$$

met $\rho = \lambda/\mu << 1$ en $1 \leq k \leq 2$.

De niet-beschikbaarheid is blijkbaar nog met een factor k te verkleinen. Door het nemen van slagvaardige maatregelen en het scheppen van geëigende omstandigheden, zoals een doordachte organisatie, voldoende ruimte en gereedschapsvoorziening, een positieve intermenselijke verhouding en goede bereikbaarheid van onderdelen, is de k in de richting van de waarde 2 te verschuiven.

Opgave 7.8:

Twee identieke eenheden (θ = 8 h) staan parallel geschakeld. Bij uitval van één der eenheden treedt onmiddellijk een reparatiekanaal $\mathbb{R}_1$ in werking met een gemiddelde reparatieduur van 1 h. Het systeem is down als beide eenheden falen. Voor het geval deze situatie zich voordoet, is nog een tweede reparatiekanaal $\mathbb{R}_2$ aanwezig met een gemid-

gemiddelde reparatieduur van 2 h. Indien $\mathbb{R}_1$ als eerste het herstel beëindigt, neemt deze de reparatiewerkzaamheden over van het (langzame) kanaal $\mathbb{R}_2$.

Toon aan dat de steady-state availability $A_\infty = 60/61$.

Opgave 7.9:

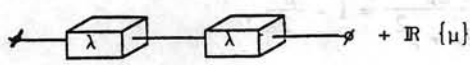
Toon aan dat met k (koude) reserve-eenheden en (k + 1) reparateurs geldt

$$A_\infty = 1 - 1 \Big/ \left(\sum_{j=0}^{k+1} \frac{(k+1)!}{j!} \frac{1}{\rho^{k-j+1}} \right).$$

Bij bewaakte systemen *zonder* redundantie blijkt de invoering van een extra, onafhankelijk werkende reparateur nauwelijks van invloed te zijn.

Voorbeeld:

Gegeven een serieschakeling van twee identieke units plus één reparatiekanaal. Bij uitval van één der units blijft de goede eenheid tijdens de reparatie van de ander in bedrijf. In deze toestand werkt het systeem dus niet, maar kan de goede unit wel uitvallen.



Toon aan dat $A_\infty = 1/(1 + 2\rho + 2\rho^2)$, met $\rho = \lambda/\mu$. Toon dan verder aan in het geval van een *tweede* onafhankelijke reparateur $A_\infty = 1/(1 + 2\rho + \rho^2)$. Voor $\rho << 1$ blijken beide uitkomsten onderling nauwelijks te verschillen, hetgeen voor de hand ligt, als we bedenken, dat bij een snelle reparatie van een falende unit nauwelijks een beroep op de tweede onderhoudsman zal behoeven te worden gedaan.

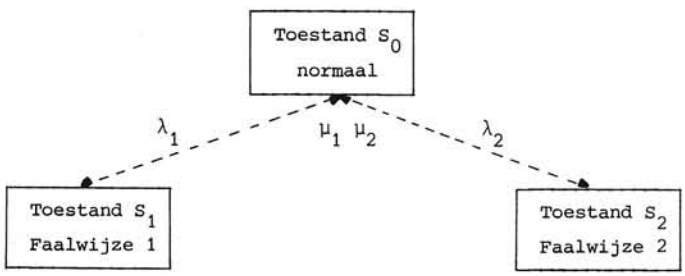
Tevens kan nog worden opgemerkt, dat in het geval de goede eenheid tijdens reparatie wèl wordt afgeschakeld en er dus maar één reparateur nodig is, dat dan geldt $A_\infty = 1/(1 + 2\rho)$, praktisch gelijk aan bovenstaand resultaat zonder afschakeling.
Daar komt nog bij dat het "aanzetten" van een apparaat vaak een "wrede" aangelegenheid is. Daarmee wil dan gezegd zijn, dat het onder spanning of

belasting brengen van nog onbelaste componenten of systemen een grotere storingskans met zich meebrengt dan in een continue bedrijfssituatie.

Samenvattend kunnen we formuleren dat:
- Een gezond onderhoudsbeheer vereist, dat $\rho = \lambda/\mu << 1$.
- Bij afwezigheid van redundantie het inzetten van extra onafhankelijke (dat wil zeggen onderling niet samenwerkende) reparateur(s) niet veel effect sorteert.
- Het afschakelen van goede eenheden tijdens herstelwerkzaamheden aan een gefaalde eenheid niet aan te bevelen is.
- Bij "joint-service" bij goede omstandigheden de beschikbaarheidsgraad van een systeem kan worden verhoogd.

7.8 Meer dan één faalwijze

Door herstelwerkzaamheden is een systeem terug te brengen van de gefaalde naar de actieve toestand. Bij meer dan één faalwijze zal de gemiddelde reparatieduur van de desbetreffende storingsvorm afhangen. Het verwisselen van een fietsketting zal veelal meer tijd vergen dan het verwisselen van een zadel.
Bij de berekening van de beschikbaarheidsgraad A_∞ beperken we ons tot twee faalwijzen.



Uit de overgangsmatrix:

$$U = \begin{array}{c} \\ S_0 \\ S_1 \\ S_2 \end{array} \begin{array}{c} \begin{array}{ccc} S_0 & S_1 & S_2 \end{array} \\ \begin{pmatrix} 1 - (\lambda_1 + \lambda_2)\,dt & \lambda_1 dt & \lambda_2 dt \\ \mu_1 dt & 1 - \mu_1 dt & 0 \\ \mu_2 dt & 0 & 1 - \mu_2 dt \end{pmatrix} \end{array}$$

volgt uiteindelijk

$$A_\infty = \pi_0 = 1/(1 + \rho_1 + \rho_2)\,,$$

met $\rho_1 = \lambda_1/\mu_1$ en $\rho_2 = \lambda_2/\mu_2$.

Opgave 7.10:

Een component kan op twee manieren stukgaan:

Faalwijze 1: de storingsgraad λ_1 is daarvoor 10^{-3} f/h en de gemiddelde reparatieduur is in dat geval $1/\mu_1 = 1$ uur.

Faalwijze 2: hiervoor geldt $\lambda_2 = 4 \times 10^{-4}$ f/h en $1/\mu_2 = 10$ uur.

Toon aan dat de beschikbaarheidsgraad van deze component $A_\infty \simeq .995$.

8 EVALUATIETECHNIEKEN

8.1 Evaluatietechnieken

In de loop van de laatste jaren is men veel waarde gaan hechten aan de afschatting van de *bedrijfszekerheid* van een complex technisch systeem. Maar ook de *onderhoudbaarheid* (vanwege de vaak enorme kosten) en de *veiligheid* (mede door maatschappelijke druk) komen steeds meer in het brandpunt van de belangstelling, met name van gebruikerszijde.
Het laat zich daarom denken, dat getracht is analytische procedures te vinden, die enig inzicht verschaffen in de drie genoemde *systeemeigenschappen*. Dit pogen heeft geresulteerd in een aantal *evaluatiemethodieken*, met behulp waarvan men in staat is zwakke en kritieke delen van (of in) een installatie op te sporen. Toepassing hiervan in het ontwerpstadium heeft uiteraard grote voordelen: de identificatie van (mogelijke catastrofale) ontwerpfouten kan het beste in een vroegtijdig stadium plaatsvinden, zodat bijvoorbeeld auto's niet meer door de fabrikant behoeven te worden teruggeroepen om alsnog het remsysteem te verbeteren.
Bovengenoemde evaluatiemethodieken zijn in wezen niets anders dan procedures met een tweeledig doel: enerzijds inzicht te verkrijgen in de *oorzaken*, die leiden tot een storing in een complex technisch systeem èn de daarmee verbonden *effecten*, anderzijds een maat te vinden voor de grootte van de kans dat die effecten optreden. In dit verband moge er nog op gewezen worden, dat het inderdaad om niet meer dan (zinvolle) *pogingen* gaat, omdat het nog steeds niet mogelijk is gebleken, de ons omringende wereld in een sluitend model vast te leggen.
Op grond van een fundamenteel verschillende benaderingswijze kunnen deze methodieken in *twee groepen* worden gesplitst, die hieronder achtereenvolgens zullen worden behandeld.

De eerste groep methodieken is *inductief* van karakter. Hierbij wordt uitgegaan van een bepaalde storing in een (sub)systeem of component, waarna getracht wordt de daarmee verbonden effecten op de omgeving en op het desbetreffende systeem vast te stellen. Dus bijvoorbeeld: "wat kan er allemaal gebeuren, doordat de koelwaterpomp het niet meer doet?" Vanwege het doorlopen van de relaties tussen de gebeurtenissen in causale richting (dus van oorzaak tot gevolg), worden deze methodieken ook wel "forward" of

"bottom-up" procedures genoemd, waarvan in paragraaf 8.2 een voorbeeld zal worden behandeld.

De tweede groep is *deductief* van karakter, waarbij de gang van zaken als volgt is. We stellen allereerst, dat het desbetreffende systeem (bijvoorbeeld een auto) op een bepaalde manier heeft gefaald en noemen dit droeve voorval de *topgebeurtenis* T, die dan moet worden opgevat als een éénduidig omschreven ongewenste toestand van het systeem, die zelfs catastrofaal kan zijn (bijvoorbeeld "de motor start niet" of "de remmen weigeren"). Daarna volgt een systematische speurtocht teneinde erachter te komen, welke faalwijzen van welke componenten een bijdrage tot het optreden van deze ongewenste topgebeurtenis konden leveren.
Omdat de genoemde faalwijzen eveneens gebeurtenissen zijn, bestaat het opsporingswerk uit de opstelling van een logische gebeurtenissenreeks, dat wil zeggen een keten van storingen, foutieve handelingen, etcetera, die in hun logische relatie laten zien, hoe het systeemfalen heeft kunnen ontstaan.
Van deze "backward" of "top-down" procedure zal in paragraaf 8.5 en verder een voorbeeld worden gegeven.

* Ook buiten de technische sfeer is deze werkwijze bekend. Het "nakaarten" bij het bridgen na een verloren spel is hiervan een huiselijk voorbeeld.

8.2 De FMEA-methode

De *Failure Mode and Effect Analysis* (FMEA) vindt met name plaats in de *ontwerpfase* van een systeem als onderdeel van een bedrijfszekerheidsprogramma. Het betreft hier een inductieve methode ("*wat* zijn de gevolgen van een storing?") met het doel mogelijke storingsvormen of faalwijzen (*failure modes*; zie paragraaf 4.4) van een (sub)systeem te catalogiseren en de effecten daarvan op de systeemfunctie na te gaan. Op deze manier kunnen dan de *kritieke* (*onder*)*delen* worden opgespoord en — indien nodig — worden (a) verbeterd, (b) bewaakt of (c) geredundanceerd. Het is ook een *kwalitatieve* methode (in tegenstelling tot "kwantitief"), wat betekent dat de methode meer ingaat op oorzaak-gevolg relaties dan op de kansen van optreden.

Behalve in de ontwerpfase blijkt deze methodiek tevens goed bruikbaar in de *gebruiksfase* van een systeem te zijn als hulpmiddel ter vaststelling van de *onderhoudsbehoefte* daarvan.

Bij de FMEA-methode worden achtereenvolgens de volgende stappen doorlopen:

Stap 1: Ontleed het beschouwde (sub)systeem in een functioneel blokschema en geef een beschrijving van de bedoeling en de werking van ieder blok.

↓

Stap 2: Maak per blok een lijst van alle onderdelen en de bijbehorende storingsvormen daarvan.
Voor een voedingslijn in een computer kan dit bijvoorbeeld zijn:
(a) kortsluiting naar aarde;
(b) kortsluiting naar + spanning;
(c) kortsluiting naar andere spanning;
(d) voedingslijn niet aangesloten.

↓

Stap 3: Beschrijf de relatie van ieder falend onderdeel ten opzichte van het desbetreffende blok èn hiervan ten opzichte van het totale systeem. Hierdoor kan worden nagegaan of de rol van deze component in de vervulling van de systeemfunctie kritisch van karakter is of dat mogelijk functionele redundantie (zie paragraaf 6.3) aanwezig is.

↓

Stap 4: Tevens moet bij elke faalwijze worden bepaald, welke gevaren of rampen voor mens, milieu, andere technische systemen of voor het systeem zelf deze storing met zich meebrengt.
De potentiële effecten van zo'n storing dienen bijvoorbeeld te worden gecategoriseerd in:
(a) er zijn mensenlevens mee gemoeid;
(b) de missie is (tijdelijk) mislukt;
(c) het functioneren van het systeem is verstoord;
(d) geen noemenswaardig effect.

↓

Uit deze analyse volgt rechtstreeks een lijst met welke gevolgen *kunnen* optreden, wanneer één van de beschreven storingsvormen optreedt (cause-consequence analysis).

8.3 Criticality analysis

De analyse uit de vorige paragraaf geeft een goed beeld hoe storingen hun doorwerking hebben in het systeem. In de praktijk wordt veelal aansluitend onderzocht welke risico's iedere storing met zich meebrengt, en of men deze risico's aanvaardbaar acht (of ze "veilig" zijn, zie paragraaf 1.4). Combinatie van deze *criticality analysis* (CA) met FMEA noemt men vaak *failure mode effects and criticality analysis* (FMECA).
Het doel van de criticality analysis is om inzicht te verkrijgen in de te nemen constructieve en procedurele maatregelen, die nodig zijn de mens min of meer te beschermen voor het geval de catastrofale storingsvorm is opgetreden of dreigt op te treden.

De te ondernemen stappen (aansluitend op de FMEA) gaan als volgt:

Stap 5: Bepaal de kans dat iedere storingsvorm optreedt.

Stap 6: Maak een puntenwaardering voor de mogelijke gevolgen, bijvoorbeeld:

- er zijn mensenlevens mee gemoeid 20
- de missie is mislukt 10
- het systeem is verstoord 4
- geen noemenswaardig effect 0.

Bereken voor alle storingsvormen hoe kritiek ze zijn, door het produkt van dit puntenaantal met de kans van optreden te nemen.

Stap 7: Maak op basis van deze gegevens een lijst met *kritieke delen.*

Stap 8:

Naar behoefte kan voor ieder kritiek deel aangegeven worden:

(a) hoe de aldus geselecteerde storingsvormen tijdig kunnen worden ontdekt;

(b) welke correctieve acties ondernomen moeten worden, indien de storing zich onverhoopt voordoet;

(c) welke noodprocedures er dan in werking treden;

(d) of één of meer onderhoudspolitieken (inspectie, verwisseling, alarmering, etc.) per storingsvorm wordt aanbevolen;

(e) of ontwerpverbeteringen worden voorgesteld (andere materiaalkeuze, grotere wanddikte, redundantie, etc.).

De laatste twee punten hebben hun grootste kracht in de mogelijkheid om bepaalde storingsvormen te kunnen voorkomen of het effect te beperken.

Overigens moet worden toegegeven, dat het bijzonder moeilijk is, de vraag te beantwoorden, *hoe veilig een bepaalde veiligheid wel is*. Het is vaak niet mogelijk elk risico volledig te elimineren, hoogstens te reduceren, waarbij de grens tussen veilig en niet-veilig niet altijd duidelijk is. Huiselijk geformuleerd wordt meestal iets als "veilig" aangemerkt als het (vermoede) risico zodanig klein is, dat het niet meer realistisch is om er rekening mee te houden. Wat is — als voorbeeld — de veiligheid van een verkeersportaal, dat boven een rijksweg is aangebracht? De kans, dat een dergelijke constructie ongecontroleerd en voortijdig bezwijkt en een passerende auto treft, moge dan klein zijn, maar is niet gelijk aan nul, terwijl (spaarzamelijke) faalgegevens — indien al aanwezig — niet tot een scherpe kwantificering van het risico leiden. Desondanks wordt de veiligheid ten aanzien van het verkeer blijkbaar voldoende geacht om de portalen in grote aantallen toe te passen.

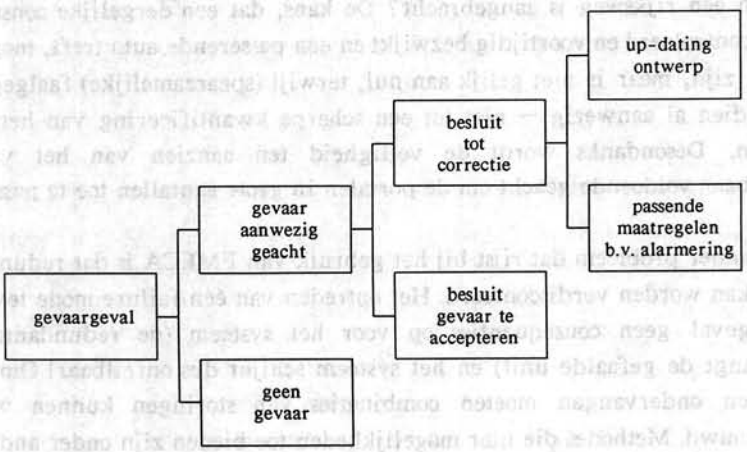
Een ander probleem dat rijst bij het gebruik van FMECA is dat redundantie niet kan worden verdisconteerd. Het optreden van één failure mode levert in dat geval geen consequenties op voor het systeem (de redundante unit vervangt de gefaalde unit) en het systeem schijnt dus onfeilbaar! Om dit te kunnen ondervangen moeten combinaties van storingen kunnen worden beschouwd. Methodes die hier mogelijkheden toe bieden zijn onder andere de faalboom-analyse (8.5) en de event tree analyse (8.4).

8.4 Veiligheid

Voornaamste drijfveer van criticality analyses is het oogmerk om tot een *veilig* functionerend systeem te komen. Het betreft hier gevarenanalyses, dat wil zeggen een identificatie van risico-dragende componenten, onderdelen en constructies, die als mogelijke bron voor ernstige storingen kunnen worden aangemerkt. Daarna wordt een onderzoek gedaan naar mogelijke gevaren en incidenten, die hieruit kunnen ontstaan, met een inschatting van de ernst van de gevolgen voor het systeem èn de omgeving (dat wil zeggen personele en materiële schade).
De geïnventariseerde risico's zijn op grond van dit onderzoek te classificeren naar de te verwachten effecten:

Klasse	Risico
1	verwaarloosbare effecten
2	marginale effecten
3	kritieke effecten
4	catastrofale effecten

De noodzaak tot het nemen van preventieve maatregelen kan worden ontleend aan een beslissingsboom, die per gevaargeval wordt opgesteld en waarbij tevens een beeld kan worden gevormd ten aanzien van de ernst van het te verwachten incident.

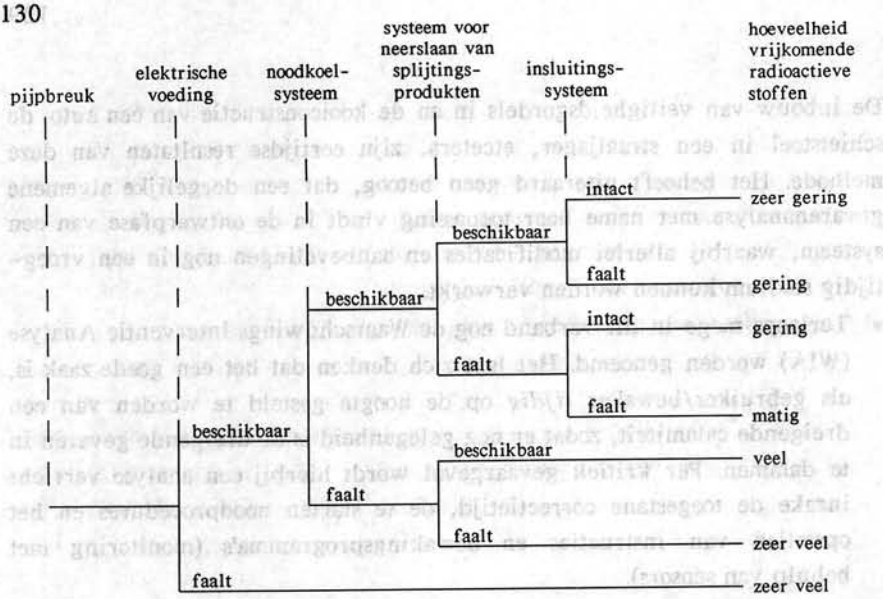


De inbouw van veiligheidsgordels in en de kooiconstructie van een auto, de schietstoel in een straaljager, etcetera, zijn eertijdse resultaten van deze methode. Het behoeft uiteraard geen betoog, dat een dergelijke algemene gevarenanalyse met name haar toepassing vindt in de ontwerpfase van een systeem, waarbij allerlei modificaties en aanbevelingen nog in een vroegtijdig stadium kunnen worden verwerkt.

* Terloops moge in dit verband nog de Waarschuwings Interventie Analyse (WIA) worden genoemd. Het laat zich denken dat het een goede zaak is, als gebruiker/bewaker *tijdig* op de hoogte gesteld te worden van een dreigende calamiteit, zodat er nog gelegenheid is de dreigende gevaren in te dammen. Per kritiek gevaargeval wordt hierbij een analyse verricht inzake de toegestane correctietijd, de te starten noodprocedures en het opstellen van instructies en bewakingsprogramma's (monitoring met behulp van sensors).

Tenslotte zij nog de Event Tree Analysis (ETA) vermeld. De *gebeurtenissenboom*, toegepast door Prof. Norman C. Rasmussen (en zijn team) bij zijn onderzoek naar storingskansen bij kerncentrales, bestaat uit een aantal reeksen gebeurtenissen in en om een (complex) systeem, die alle door het falen van een enkel subsysteem worden gestart. Deze vertakkingsgewijs verlopende series vermelden het zich al of niet voordoen van andere subsysteem-storingen, die van invloed zijn op het risico dat de oorspronkelijke storing met zich meebrengt. Aan het einde van de "takken" wordt de ernst van de gevolgen gemeld, afhankelijk van het verloop van de bovenbedoelde "accident sequences".

Als voorbeeld is hieronder een event tree weergegeven, afkomstig van de reactorveiligheidsstudie van Prof. Rasmussen, "WASH 1400" geheten. Beginnend bij een pijpbreuk van het koelsysteem als initiërende storing blijkt dat bij het intact blijven van de andere componenten de hoeveelheid vrijgekomen radioactieve stoffen zeer gering is, terwijl bij het wegvallen van de elektrische voeding na de pijpbreuk zeer veel stoffen ontsnappen en de omgevingstoestand als calamiteus moet worden beoordeeld (zie figuur).
Door storingskansen aan de vermelde gebeurtenissen toe te kennen, kunnen de mogelijke risico's worden gekwantificeerd.



De hier genoemde (kwalitatieve) methodes hebben hun nut in het verleden reeds meermalen kunnen bewijzen. Zij werken als een soort simulatiemiddel waarmee het systeem op papier reeds beproefd kan worden op zijn sterkte in het opvangen van component failures.

Het nadeel van kwantitatieve methodes zit in de nauwkeurigheid van de ingevoerde faalkansen. Omdat hiervan slechts zeer weinig bekend is zullen vaak geraamde waardes moeten worden gebruikt. Als deze waardes onvoldoende binding met de werkelijkheid hebben zullen de uitkomsten van het model ook niet bruikbaar zijn.

Dit euvel hebben de kwalitatieve methodes niet; de effecten van een component failure worden geëvalueerd, onafhankelijk of deze vaak of juist slechts zelden zullen falen. Men kan zich indenken dat dit voor vervoersmiddelen als de space-shuttle de juiste aanpak is.

8.5 Faalboom-analyse

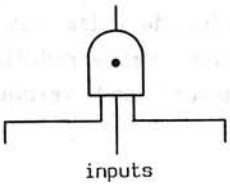
De "Fault Tree Analysis" (FTA: faalboom-analyse) is de bekendste uit de groep evaluatiemethodieken, die zich door een deductieve aanpak kenmerken. Het betreft hier een techniek, die in 1962 door H.A. Watson van de Bell Telephone Laboratories is ontwikkeld en sindsdien niet alleen in de lucht- en ruimtevaartindustrie maar ook (en vooral) bij veiligheidsanalyses van kernreactoren wordt aangepast.

De benaming "boom" is ontleend aan de vorm van de grafische weergave van de verzameling gebeurtenissen, die onderling door logische symbolen met elkaar verbonden zijn en die tezamen systematisch aangeven hoe deze hebben kunnen bijdragen tot het bereiken van de veronderstelde faalwijze van het systeem, die we in paragraaf 8.1 als topgebeurtenis hebben omschreven. Startend vanuit deze top wordt via (met name) EN- en OF- poorten (die het meest worden toegepast) het "gevolg-en-oorzaak-proces" langs het subsysteem- en componentenniveau gevolgd tot aan een serie *basisgebeurtenissen*, waar verdere expansie van de boom wordt gestaakt.
Alvorens tot behandeling van een voorbeeld over te gaan zal eerst een overzicht worden gegeven van een beperkt aantal symbolen, waarmee faalbomen kunnen worden opgebouwd en die ieder voor zich één of ander verband aangeven tussen opéénvolgende gebeurtenissen.

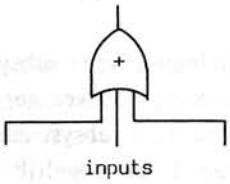
8.6 Faalboom-constructie

Hieronder staan een aantal symbolen waarmee de faalbomen worden opgebouwd.

A. Poortsymbolen



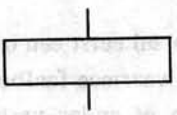
AND- of EN-poort; de output (uitgangsgebeurtenis) doet zich dan en alleen dan voor als alle inputs (ingangsgebeurtenissen) zich voordoen.



OR- of OF-poort; de output doet zich dan en alleen dan voor als één of meer van de inputs zich voordoen.

B. Gebeurtenissymbolen

Basisgebeurtenis; hierin wordt een basisstoring (falen van een component, menselijke fout) beschreven, die niet verder wordt nagegaan. Dit teken symboliseert een eindpunt in de ontwikkeling van de boom.



Resulterende gebeurtenis; geeft de uitgangsgebeurtenis van een poort weer.

C. Transfersymbolen

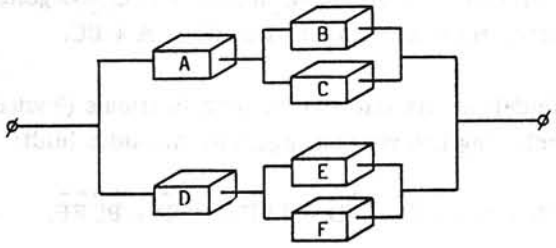
Transfer in.

Transfer out; beide symbolen kunnen worden gebruikt om verschillende delen van een boomdiagram dat zich over verschillende pagina's uitspreidt, met elkaar te verbinden.

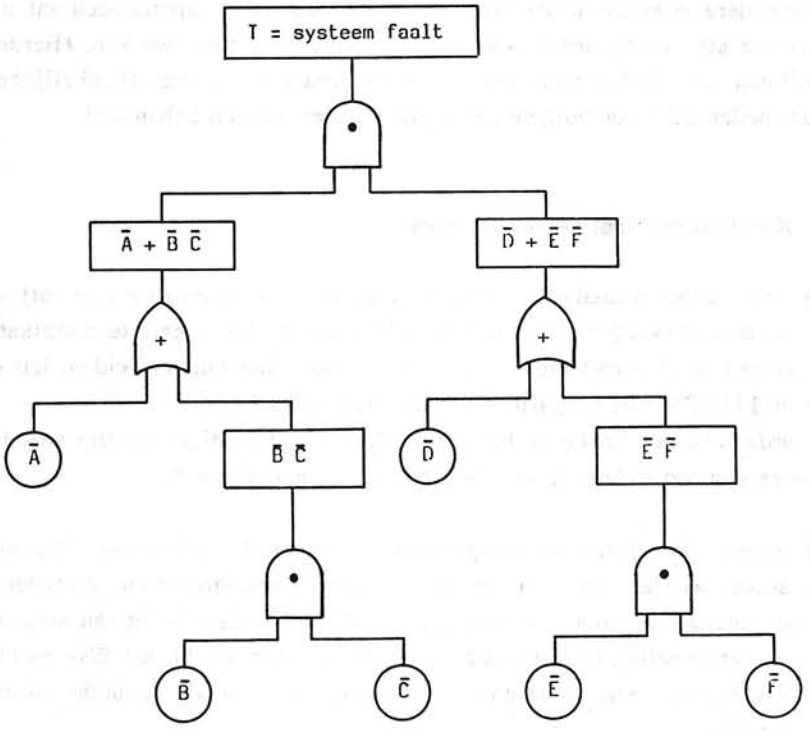
Essentieel bij het opstellen van een faalboom is dat de topgebeurtenis de system failure voorstelt, net zoals de basisgebeurtenissen component of unit failures zijn.

Ga hierbij als volgt te werk: bekijk welke (combinaties van) subsysteem failures het totale systeem doen falen en hoe dit met een poort weergegeven kan worden. Doe vervolgens hetzelfde voor ieder van deze subsystemen en daal zo af in deze faalboom tot deze zover als wenselijk of mogelijk is, is uitgesplitst. Voorbeeld: een vliegtuig faalt wanneer de voortstuwing, òf het casco faalt (OF-poort). De voortstuwing faalt wanneer beide vliegtuigmotoren falen (EN-poort), etcetera.

Construeer nu de faalboom, behorende bij onderstaande configuratie.



Deze ziet er als volgt uit:



De basisgebeurtenissen worden weergegeven door $\bar{A}$, $\bar{B}$, etcetera, hetgeen hier betekent dat de eenheden A, B, etcetera, uitgevallen zijn. Indien we

deze letters tevens opvatten als Booleaanse variabelen, dan kunnen eveneens de resulterende gebeurtenissen (rechthoeken) als Booleaanse expressies worden voorgesteld. Een EN-poort vereist beide inputs $B \cap C$ voorgesteld door BC; een OF-poort daarentegen resulteert in $A \cup BC$ of $A + BC$.

Op deze wijze zal het duidelijk zijn dat van de topgebeurtenis ("systeem faalt") een Booleaanse vergelijking kan worden opgesteld, die aldus luidt:

$$T = \overline{\text{systeem}} = (A + BC)(D + EF) = AD + AEF + BCD + BCEF.$$

De vier gevonden termen worden *sneden* genoemd, dat zijn verzamelingen van gebeurtenis(sen) die nodig en voldoende zijn voor het doen plaatsvinden van de topgebeurtenis. Operationeel gezien is de bepaling van deze sneden een belangrijke bezigheid, met name bij een risico-analyse.
Tijdens de opstelling van een faalboom kan blijken dat één basisgebeurtenis op meerdere plaatsen in de boom voorkomt: door een kapotte accu zal niet alleen de startmotor, maar ook de verlichting niet meer werken. Hierdoor wordt een *afhankelijkheid* in de boom geïntroduceerd. Deze afhankelijkheid in de sneden zal in de volgende paragraaf nader worden behandeld.

8.7 Kwalitatieve analyse met faalbomen

Met een faalboom-analyse kan de gehele *sneden verzameling* (cut set) van een systeem verkregen worden. Hierdoor kunnen alle mogelijke combinaties van fouten worden onderzocht die tot een systeemfout kunnen leiden, iets dat met de FMECA niet mogelijk was (zie paragraaf 8.3).
De *orde* van een snede is het aantal failures, benodigd om die snede te veroorzaken. Zo is de orde van de snede $BCEF$ gelijk aan 4.

Bij herhaald voorkomende basisgebeurtenissen kan de faalboom-analyse vaak met succes worden gebruikt om de snedenset te minimaliseren. Wanneer de snedenverzameling niet verder gereduceerd kan worden, is dit een *minimum sneden verzameling* (minimum cut set). Als de boom slechts uit EN- en OF-poorten bestaat (een "coherente" faalboom) kan voor de reductie volstaan worden met:

$$AA = A;$$
$$AB + A = A;$$

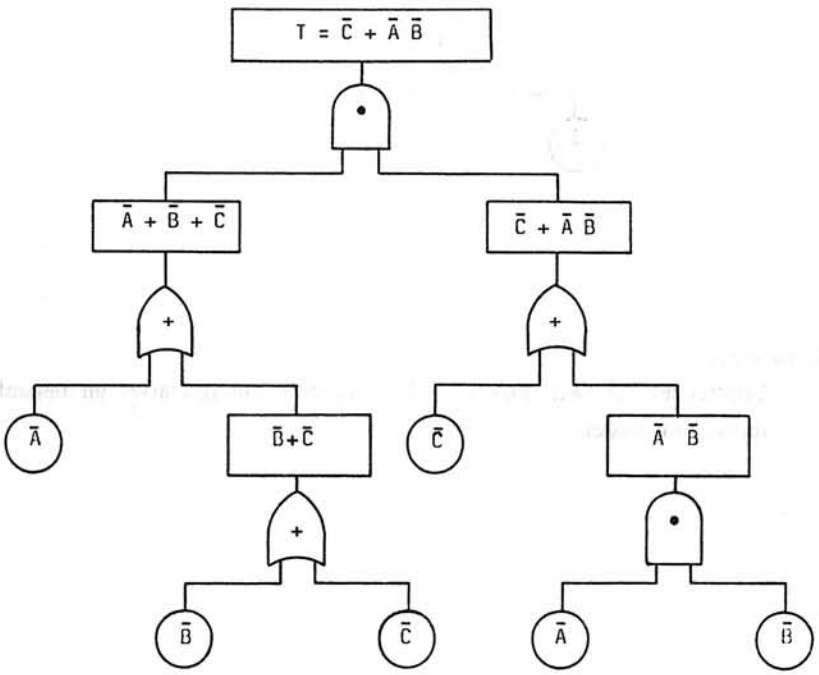
maar dus ook:

$$\bar{A}\bar{C} + \bar{A}BCDE = \bar{A}\bar{C}.$$

Men rangschikt de minimum sneden vaak in oplopende orde: de sneden van de eerste en tweede orde verdienen — vanwege hun kritisch karakter — de grootste aandacht. De kans op een derde orde snede is gelijk aan het produkt van de faalkansen van de afzonderlijke eenheden. Naarmate de orde toeneemt, zal de kans op die snede dan ook vaak drastisch afnemen. Vaak zullen de sneden boven de vierde orde van ondergeschikt belang zijn.
Om het systeem veiliger te maken, moet de eerste aandacht geschonken worden aan de minimum sneden van de laagste orden, men kan proberen om het gecombineerd falen van de units in deze sneden te voorkomen. Hierbij dient echter ook gelet te worden op gebeurtenissen die zeer frequent in sneden van hogere orden voorkomen, zoals $\bar{A}$ in $T = \bar{A}\bar{B}\bar{C} + \bar{A}\bar{C}D + \bar{A}\bar{B}D$. We spreken in dat geval van *geassocieerde sneden.*

Voorbeeld:

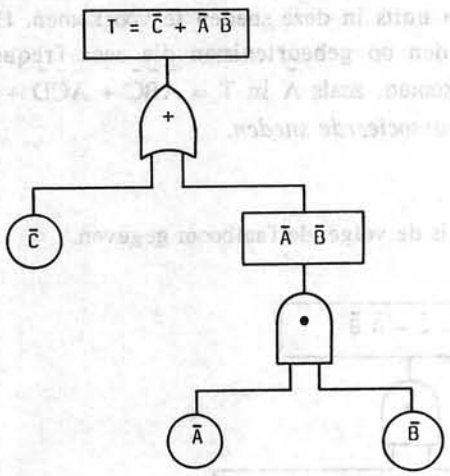
Stel van een configuratie is de volgende faalboom gegeven.



Voor de topgebeurtenis geldt blijkbaar:

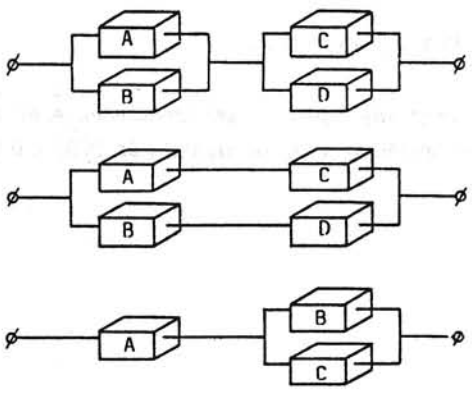
$$T = (\bar{A} + \bar{B} + \bar{C})(\bar{C} + \bar{A}\bar{B})$$
$$= \bar{A}\bar{C} + \bar{A}\bar{A}\bar{B} + \bar{B}\bar{C} + \bar{B}\bar{A}\bar{B} + \bar{C}\bar{C} + \bar{C}\bar{A}\bar{B}$$
$$= \bar{C} + \bar{A}\bar{B}\,.$$

Aan de hand van de laatste expressie (de minimum sneden) kan onderstaande *gereduceerde* faalboom worden geconstrueerd, die niet alleen noodzakelijk identiek is met de oorspronkelijke boom, maar die zich tevens meer voor een *kwantitatieve* benadering leent (waarom?).



Opgave 8.1:

Construeer de faalboom van de volgende configuraties en bepaal de minimum sneden.



Doe dit nogmaals, maar nu met C = A.

8.8 Kwantitatieve analyse met faalbomen

Zowel het reduceren van een faalboom als de bepaling van de minimum sneden behoren tot de *kwalitatieve* analyse van deze evaluatiemethodiek.
Tot de *kwantitatieve* analyse kan worden gerekend:

- De berekening van de *kans* op het optreden van de topgebeurtenis, gebaseerd op de kansen van de basisgebeurtenissen (zie hieronder).

- De berekening van de *hazard rate* (storingsgraad) van de topgebeurtenis uit de afzonderlijke failure rates van de basisgebeurtenissen (zie paragraaf 8.9).

Voor de berekening van de kans op de topgebeurtenis T van een OF-poort dienen we de volgende relaties te memoreren:

$$P(\bar{A} \cup \bar{B}) = P(\bar{A}) + P(\bar{B}) - P(\bar{A} \cap \bar{B})$$

of

$$P(\bar{A} + \bar{B}) = P(\bar{A}) + P(\bar{B}) - P(\bar{A}\bar{B}).$$

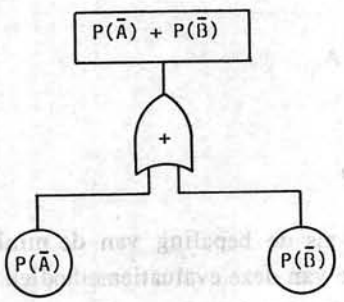
Voor méér dan twee ingangen kan deze relatie verder ontwikkeld worden, bijvoorbeeld:

$$P(\bar{A} + \bar{B} + \bar{C}) = P(\bar{A}) + P(\bar{B}) + P(\bar{C}) - P(\bar{A}\bar{B}) - P(\bar{A}\bar{C}) +$$
$$- P(\bar{B}\bar{C}) + P(\bar{A}\bar{B}\bar{C}) \text{ (ga dit na).}$$

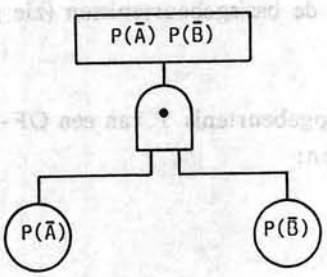
Wanneer (voor het geval van twee ingangen) de gebeurtenissen $\bar{A}$ en $\bar{B}$ disjunct (kunnen niet gelijktijdig optreden) zijn, of als $P(\bar{A})$ èn $P(\bar{B}) \leq 0.1$, dan geldt bij benadering:

$$P(\bar{A} + \bar{B}) \simeq P(\bar{A}) + P(\bar{B}) ,$$

zodat



Verder is $P(\bar{A}\bar{B}) = P(\bar{A})\,P(\bar{B})$ bij onafhankelijke gebeurtenissen, zodat:



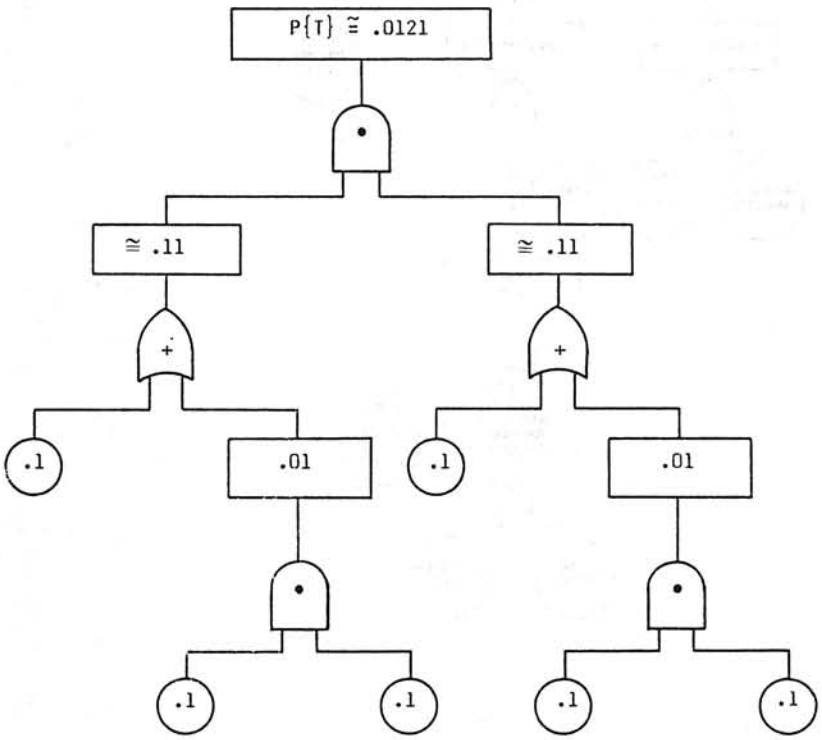
Deze schematische voorstellingen zijn eenvoudig uitbreidbaar, indien we niet met twee, maar met n input-gebeurtenissen te doen hebben.

$$P(A_1 A_2 \ldots\ldots A_n) = P(A_1)\,P(A_2) \ldots\ldots P(A_n)$$

$$P(A_1 + A_2 + \ldots + A_n) \simeq P(A_1) + P(A_2) + \ldots + P(A_n)\,.$$

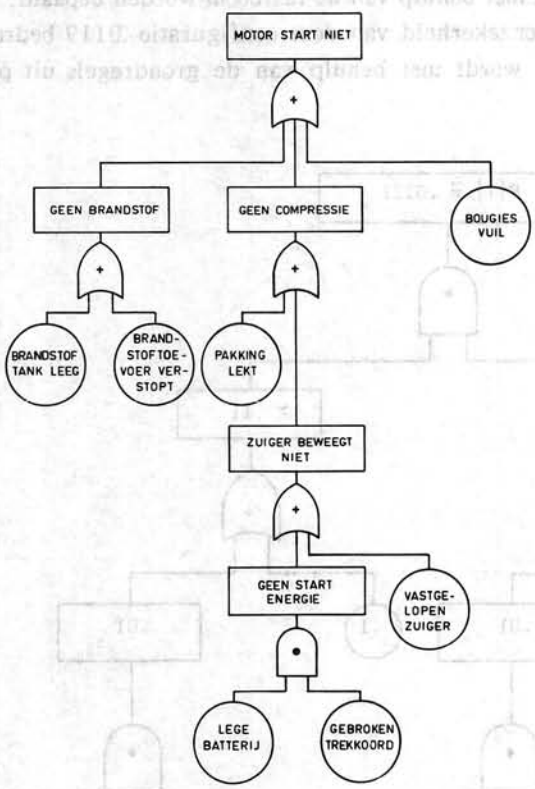
We verwijzen naar de configuratie in paragraaf 8.6 waarbij we dan veronderstellen, dat alle zes eenheden voor een bepaalde periode een bedrijfsonzekerheid van 0.1 hebben. In dat geval kan de kans op de topgebeurtenis P{T} als volgt met behulp van de faalboom worden bepaald:

* Ga na dat de bedrijfsonzekerheid van deze configuratie .0119 bedraagt, indien deze berekend wordt met behulp van de grondregels uit paragrafen 2.3 en 2.5.



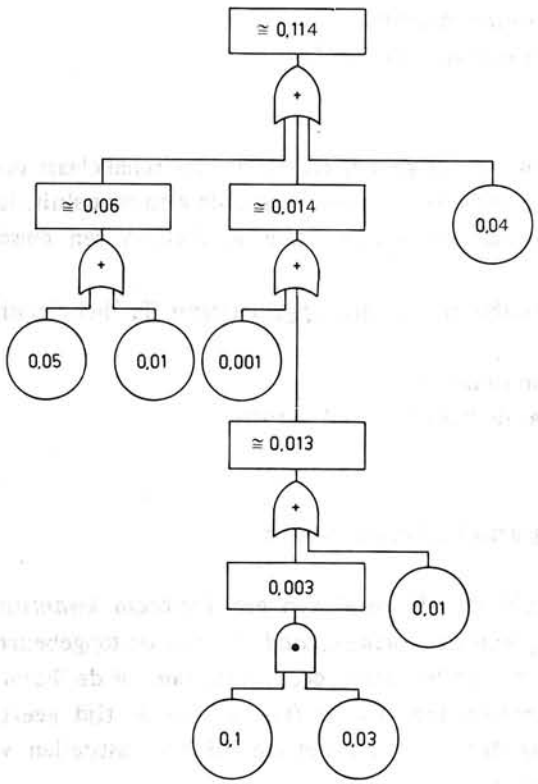
Tenslotte wordt nog — ter illustratie — een eenvoudige faalboom weergegeven, waarin enige mogelijke storingsbronnen van een (grasmaaimachine-) motor door middel van logische poorten met elkaar zijn verbonden.
Bedieningsfouten (zoals bijvoorbeeld het vullen van de brandstoftank met

een onjuiste vloeistof) zijn niet vermeld, of het moest het falen van het trekkoord zijn dat niet alleen door slijtage maar ook door een ruwe behandeling kan breken.
Als topgebeurtenis is gekozen: *motor start niet*, waarna via de deductieve weg mogelijke oorzaken worden opgespoord. Een weg, die eveneens door een reparateur bij een systematische "trouble shooting" zal worden gevolgd.



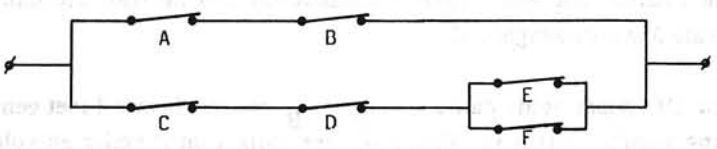
Hieronder is tevens met behulp van de basiskansen, die in nevenstaande faalboom zijn vermeld, de kans berekend op het optreden van de topgebeurtenis. Deze kans (dus dat de motor niet wil starten) blijkt dus ruim 11% te zijn.

Uit een dergelijke eenvoudige analyse blijkt, dat, hoewel de afzonderlijke storingskansen vrij regelmatig over de componenten verdeeld zijn, het onderhoud zich met name op de carburateur en de bougies moet richten.



Opgave 8.2:

Een circuit bestaat uit zes identieke schakelaars volgens onderstaand schema. De schakelaars staan in gesloten toestand.



De kans, dat een gesloten schakelaar na een commando niet open gaat, is 10^{-3}.

Op een bepaald moment krijgen alle schakelaars een omschakelcommando.

(a) Teken de faalboom, met als topgebeurtenis T: "het circuit blijft gesloten".

(b) Bepaal de minimum sneden.

(c) Toon aan dat de kans $P\{T\} \simeq 10^{-6}$.

Opgave 8.3:

In het circuit van de vorige opgave staan alle schakelaars open. De kans, dat een open schakelaar na een commando zich niet sluit, is 10^{-3}. Op een bepaald moment krijgen alle schakelaars een omschakelcommando.

(a) Teken de faalboom, met als topgebeurtenis T: "het circuit blijft open".

(b) Bepaal de minimum sneden.

(c) Toon aan dat de kans $P\{T\} \simeq 4 \times 10^{-6}$.

8.9 Berekening storingsgraad bij een faalboom

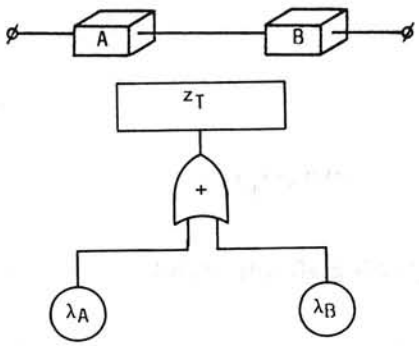
Een andere mogelijkheid om de opzet van een faalboom *kwantitatief* te benutten is de bepaling van de *storingsgraad* z(t) van de topgebeurtenis T. Een grootheid, die ook wel de "instanteneous failure rate" of de "hazard rate" wordt genoemd. Het verloop hiervan als functie van de tijd geeft nader inzicht in het storingsgedrag van het systeem bij het vaststellen van het vereiste onderhoudsconcept.

In paragraaf 1.7D is reeds afgeleid dat:

$$z(t) = -\frac{1}{R(t)}\frac{dR(t)}{dt} \quad \text{of} \quad R(t) = \exp\left(-\int_0^t z(u)\,du\right).$$

Zoals inmiddels bekend heeft z(t) bij de negatief-exponentiële verdeling een constante waarde, dat wil zeggen onafhankelijk van de tijd, die dan als de failure rate λ wordt aangeduid.

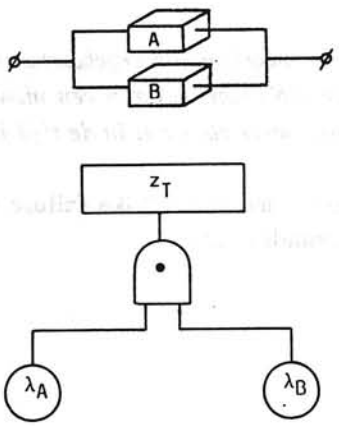
Voor een OF-poort geldt dan $z_T = \lambda_A + \lambda_B$, overeenkomend met een serieschakeling waarbij uitval van slechts één der units A en B nodig en voldoende is om het gebeuren T (= systeem down) te laten plaatsvinden.



* Bij een OF-poort met n invoergebeurtenissen $\bar{A}_i$, i = 1,2,...,n geldt dan voor de hazard rate van de topgebeurtenis:

$$z_T = \sum_{i=1}^{n} \lambda_{A_i} .$$

Een EN-poort daarentegen komt met een parallelschakeling (paragraaf 2.5) overeen, omdat de uitval van de beide units A en B nodig en voldoende zijn voor het optreden van T.



Er geldt

$$R_{syst} = 1 - F_{syst}$$
$$F_{syst} = F_A \cdot F_B$$
$$F_A = 1 - \exp(-\lambda_A t) \; ; \quad F_B = 1 - \exp(-\lambda_B t) .$$

Toepassing van $z_T(t) = -1/R_T(t)\, dR_T(t)/dt$ geeft uiteindelijk:

$$z_T(t) = \frac{\lambda_A(\alpha_A - 1) + \lambda_B(\alpha_B - 1)}{\alpha_A \alpha_B - 1} ,$$

met $\alpha_A = (1 - \exp(-\lambda_A t))^{-1}$ en $\alpha_B = (1 - \exp(-\lambda_B t))^{-1}$.

* Bij een EN-poort met n invoergegevens $\bar{A}_i$, i = 1,2,...,n blijkt voor de hazard rate van de topgebeurtenis te gelden:

$$z_T(t) = \frac{\sum_{i=1}^{n} \lambda_i(\alpha_i - 1)}{\left(\prod_{i=1}^{n} \alpha_i\right) - 1} ,$$

met $\alpha_i = (1 - \exp(-\lambda_i t))^{-1}$. Met andere woorden *invoergebeurtenissen met een constante storingsgraad bij een EN-poort leveren een uitvoergebeurtenis met een storingsgraad, die niet meer constant in de tijd is.*

In het geval van n parallel geschakelde eenheden met gelijke failure rate ($\lambda_1 = \lambda_2 = ... = \lambda_n = \lambda$) gaat bovenstaande formule over in

$$z_T(t) = \frac{n\lambda}{\alpha^{n-1} + \alpha^{n-2} + ... + \alpha + 1} ,$$

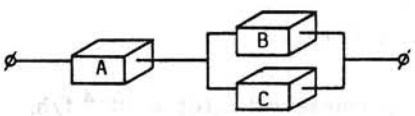
met $\alpha = (1 - \exp(-\lambda t))^{-1}$.
Voor $t \to 0$ wordt $\alpha \to \infty$ en $z_T(0) \to 0$.
Voor $t \to \infty$ wordt $\alpha \to 1$ en $z_T(\infty) \to \lambda$.

Conclusie:
We zien dus, dat de storingskans $z_T(t)$ hier vanaf de waarde nul met de tijd asymptotisch toeneemt tot de waarde λ, alsof het één unit betreft in plaats van n eenheden. De toename van de hazard rate, meestal met "veroudering" aangeduid (denk aan de badkuipkromme), behoeft dus niet altijd met slijtage samen te hangen. Bij parallelschakeling van units hebben we een voorbeeld, waarin de eenheden op zich geen veroudering vertonen, terwijl de schakeling als geheel zich wel als zodanig gedraagt.

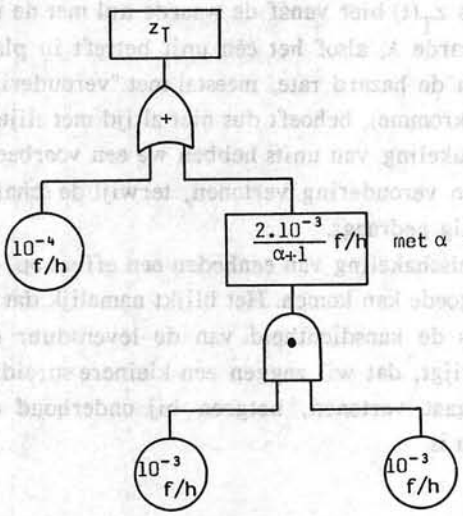
* Er treedt overigens bij parallelschakeling van eenheden een effect op, dat de beschikbaarheid zeer ten goede kan komen. Het blijkt namelijk dat bij toename van het aantal units de kansdichtheid van de levensduur een steeds meer gepiekte vorm krijgt, dat wil zeggen een kleinere spreiding in de levensduurverdeling gaat vertonen, hetgeen bij onderhoud een buitengewoon gunstig gegeven is.

Voorbeeld:

Drie eenheden hebben de volgende configuratie



met als failure rates $\lambda_A = 10^{-4}$ f/h; $\lambda_B = \lambda_C = 10^{-3}$ f/h.
De faalboom heeft dan de volgende gedaante:



Ga dat na met de formule uit de voorgaande opmerking.
Het resultaat is

$$z_T(t) = \left(10^{-4} + \frac{2 \times 10^{-3}}{\alpha + 1}\right) \text{ f/h.}$$

Voor $t \to 0$ wordt $\alpha \to \infty$ en de storingsgraad $z_T(0) = 10^{-4}$ f/h.
Voor $t \to \infty$ wordt $\alpha \to 1$ en de storingsgraad $z_T(\infty) = 11 \times 10^{-4}$ f/h.

Een *praktische* benadering voor bedrijfstijden $t << 1000$ h $(= \theta_B = \theta_C)$ is $z_T(t) \simeq (10^{-4} + 2 \times 10^{-6}\ t)$ f/h, waarmee een onderhoudsstrategie kan worden bepaald.

8.10 Beoordeling faalboom-analyse

Zoals elke andere procedure, brengt ook de faalboom-techniek zowel voor- als nadelen met zich mee. We noemen er tenslotte enkele van.

Nadelen:

- Het bouwen van bomen is een kostbare en tijdrovende bezigheid.
- Systeemcomponenten worden geacht òf te functioneren òf te falen; degradatiefouten en "partial failures" van de componenten zijn moeilijk te introduceren.

- Het niet benoemen van alle faalbronnen (en dat kan niet vanwege de boomomvang) betekent dat de verkregen resultaten met de nodige reserve moeten worden behandeld.
- Onderlinge afhankelijkheid van componenten (bijvoorbeeld de hazard rate van één unit neemt toe door overbelasting, wanneer een andere is gefaald) is moeilijk te modelleren.

Voordelen:

- Het bouwen van een faalboom levert — gedwongen — een goede analyse van het systeembedrag.
- Het is (ondanks het benaderend karakter) toch maar een mogelijkheid om een complex systeem op zijn bedrijfszekerheid en storingsgedrag enigszins te beoordelen.
- Bij een goed opgestelde boom kunnen de hieruit resulterende conclusies en suggesties — met name in de ontwerpfase — zeer waardevol zijn.
- Als grafisch hulpmiddel levert de foutenboom een nuttige gespreksbasis voor ontwerpers, produktiemensen, organisatie- en onderhoudsdeskundigen en gebruikers ten behoeve van ontwerpverbeteringen en "trade-off" studies.

APPENDIX A: LAPLACE-TRANSFORMATIE

Voor de transformatie van tijd- naar Laplace-domein en vice versa wordt doorgaans gebruik gemaakt van een tabel. De meest toegepaste Laplace-getransformeerden staan in de tabel hieronder.

$f(t) = \mathcal{L}^{-1}\{F(s)\}$	$F(s) = \mathcal{L}\{f(t)\}$
1	$\frac{1}{s}$
$e^{-\lambda t}$	$\frac{1}{s+\lambda}$
$\frac{t^n}{n!} e^{-\lambda t}$	$\frac{1}{(s+\lambda)^{n-1}}$
$\frac{d}{dt} f(t)$	$sF(s) - f(0)$
$\int_0^t f(t)\, dt$	$\frac{1}{s} F(s)$
$\lim_{t\to\infty} f(t)$	$\lim_{s\downarrow 0} sF(s)$
$\lim_{t\downarrow 0} f(t)$	$\lim_{s\to\infty} sF(s)$

In de tekst van dit boekje wordt geen onderscheid gemaakt tussen de functieletter in het tijds- of Laplace-domein. Het onderscheid tussen beide zit dus slechts in het gebruik van verschillende letters voor het argument. In wiskundige notatie dus:

$\mathcal{L}\{P(t)\} = P(s)$.

Indien we specifieke waarden invullen noteren we dit in het s-domein als

$P(s = a)$,

en in het tijddomein simpel als P(a), in plaats van P(t = a).

BEKNOPTE LITERATUURLIJST

Ascher, H. e.a., *Repairable systems reliability*, Marcal Dekker Inc., 1984.

Bǎjenescu, T.I., *Zuverlässigkeit elektronischer Komponenten*, VDE-Verlag GmbH, Berlin, 1985.

Barlow, R.E. e.a., *Statistical theory of reliability and life testing*, Holt, Rinehart & Winston, New York, 1975.

Becker, P.W., Jensen, F., *Design of systems and circuits for maximum reliability and production yield*, McGraw-Hill, New York, 1977.

Belli, F. e.a., *Software-Fehlertoleranz und - Zuverlässigkeit*, Springer-Verlag, Berlin, 1982.

Billington, R., *Power system reliability evaluation*, Gordon & Breach, New York, 1970.

Billington, R. e.a., *Power system reliability calculations*, the MIT Press, London, 1973.

Bitter, P. e.a., *Technische Zuverlässigkeit*, Messerschmitt Bölkov, Springer-Verlag, Berlin, 1971.

Carter, A.D.S., *Mechanical reliability*, John Wiley & Sons, London, 1972.

Cox, D.R. e.a., *Analysis of survival data*, Chapman & Hall, 1984.

Dhillon, B.S. e.a., *Engineering reliability*, John Wiley & Sons, New York, 1981.

Dhillon, B.S., *Systems reliability, maintainability and management*, PBI Books, New York, 1983.

Dummer, G.W.A. e.a., *Electronics reliability, calculation and design*, Pergamon Press, Oxford, 1970.

Green, A.E. e.a., *Reliability technology*, John Wiley & Sons, 1972.

Henley, E.J. e.a., *Generic techniques in systems reliability*, Noordhoff, Leiden, 1976.

Henley, E.J. e.a., *Reliability engineering and risk assessment*, Prentice-Hall, Englewood Cliffs, 1981.

Jensen, F. e.a., *Burn-in*, John Wiley & Sons, New York, 1982.

Kalbfleisch, John D. e.a., *The statistical analysis of failure time data*, John Wiley & Sons, New York, 1980.

Kapur, K.C., *Reliability in engineering design*, John Wiley & Sons, New York, 1977.

Käs, G., *Qualität und Zuverlässigkeit*, Oldenbourg-Verlag, München, 1983.

Kaufmann, A. e.a., *Mathematical models for the study of the reliability of systems*, Academic Press, New York, 1977.

Klaassen, Klaas B., *Reliability of analogue electronic systems*, Elsevier, Amsterdam, 1984.

Kochs, Hans-Dieter, *Zuverlässigkeit elektrotechnischer Anlagen*, Springer-Verlag, Berlin, 1984.

Kozlov, B.A. e.a., *Reliability Handbook*, Holt, Rinehart & Winston, New York, 1970.

Mann, N.R. e.a., *Methods for statistical analysis of reliability and life data*, John Wiley & Sons, New York, 1974.

Martz, H.F. e.a., *Bayesian reliability analysis*, John Wiley & Sons, 1982.

Moan, T. e.a., *Structural safety and reliability*, Elsevier, Amsterdam, 1981.

O'Connor, Patrick D.T., *Practical reliability engineering*, Heyden, London, 1981.

Preuss, H., *Zuverlässigkeit elektronischer Einrichtungen*, VEB-Verlag Technik, Berlin, 1978.

Ross, S.M., *Introduction to probability models*, Academic Press, New York, 1972.

Schneeweisz, W., *Zuverlässigkeitstheorie*, Springer-Verlag, Berlin, 1973.

Serra, A. e.a., *Theory of reliability*, Proc. of the Int. School of Physics "Enrico Fermi", North-Holland, 1986.

Shooman, M.L., *Probabilistic reliability*, McGraw-Hill, New York, 1968.

Singh, C. e.a., *Systems reliability modelling and evaluation*, Hutchinson, London, 1977.

Smit, K., *Onderhoud van intuïtie naar rationaliteit*, Kluwer, Deventer, 1981.

Smith, D.J., *Reliability engineering*, Pitman, New York, 1973.

Smith, D.J. e.a., *Maintainability engineering*, Pitman, New York, 1973.

Smith, D.J., *Reliability and maintainability in perspective*, MacMillan Publ. Ltd., 1985.

'Spectrum', IEEE, Vol. 18, No. 10, Oct. 1981.

Störmer, H., *Mathematische Theorie der Zuverlässigkeit*, Akademie-Verlag, Berlin, 1970.

Tsokos, C.P. e.a., *The theory and applications of reliability*, Academic Press, New York, 1977.

Walker, M.G., *Managing software reliability*, North-Holland, New York, 1981.

TREFWOORDENLIJST

In deze tijd, waarin geavanceerde technieken steeds meer hun weg vinden, wordt het kapot gaan van apparatuur als bijzonder hinderlijk ervaren. En soms zelfs als onaanvaardbaar.
Het falen van systemen – zowel thuis als in de professionele sector – past nauwelijks meer in onze apparatief ingesneeuwde samenleving. Het is dan ook niet zo verwonderlijk, dat in de wetenschap van lieverlee een studiegebied van de grond is gekomen, dat met Bedrijfszekerheidstechniek (Reliability Engineering) wordt aangeduid en waarin onder meer wordt getracht methoden te vinden om tot een bedrijfszeker, onderhoudbaar en veilig produkt te komen.

Dit boek is bedoeld als inleiding tot dit gebied. Naast een inventarisatie van enige operationeel belangrijke grootheden wordt een aantal bedrijfszekerheidsmodellen (met en zonder reparatie) voor berekening toegankelijk gemaakt, met vraagstukken ter oefening. Voorts worden – naast onderhoudsaspecten – evaluatietechnieken ter sprake gebracht, zoals de faalboomanalyse en de FMECA, die in de ontwerpfase steeds meer worden toegepast. Kortom een handzaam boek voor allen die in de industrie met deze aspecten te maken hebben.

Maar ook het technisch onderwijs van vandaag, dat mensen opleidt voor de wereld van morgen, zal in dit boek een doeltreffend leermiddel vinden de komende generatie vroegtijdig vertrouwd te maken met de parameters die het proces van uitval en voortijdig verval van een systeem beheersen en waarmee zij naderhand ongetwijfeld te maken zal krijgen.