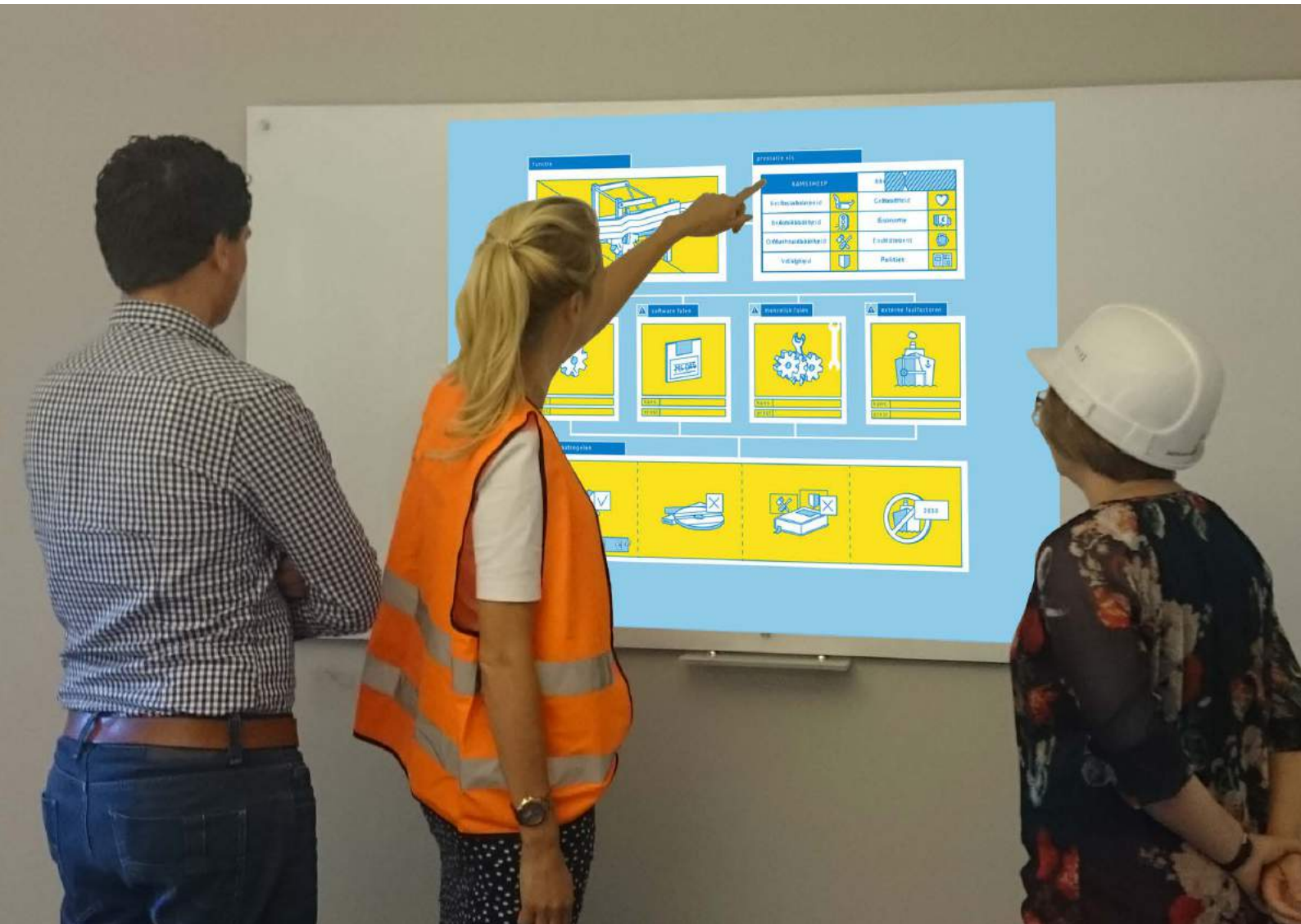
Rijkswaterstaat
Ministerie van Infrastructuur en Waterstaat

Handreiking prestatiegestuurde risicoanalyses (PRA)

Sturen op prestaties van systemen

Water. Wegen. Werken. Rijkswaterstaat.



Handreiking prestatiegestuurde risicoanalyses (PRA)

Sturen op prestaties van systemen

Colofon

Uitgave	Steunpunt ProBO
Informatie	Arjen van Maaren
E-mail	probo@rws.nl
Tekstredactie, vormgeving en productie	Infram, BCP
Datum	8 maart 2018
Status	Definitief
Versienummer	1.0.1
Nummer	5333
Netwerk	HWN, HVWN, HWS
Kennisveld	Assetmanagement

Inhoud

Managementsamenvatting

Rijkswaterstaat geeft invulling aan beleidsdoelen, wet- en regelgeving en bestuursafspraken door de afgesproken prestaties van de hoofdnetwerken te leveren. Rijkswaterstaat stuurt daarom op de prestaties van de netwerken. Prestatiegestuurde risicoanalyses zijn daarbij een belangrijk instrument. Het Bestuur van Rijkswaterstaat heeft in 2013 besloten dat prestatiesturing de basis wordt voor aanleg en onderhoud [1]. Prestatiegestuurde risicoanalyses moeten worden toegepast bij de aanleg en/of het onderhoud van viaducten, bruggen, vaarwegen, wegen, dijken, dammen en duinen. De handreiking prestatiegestuurde risicoanalyses (PRA) legt de werking van de 'prestatiegestuurde risicoanalyse' uit en maakt het instrument praktisch toepasbaar.

De handreiking PRA beschrijft hoe een reeks criteria, bekend onder de term RAMSSHE€P-aspecten, de prestaties van de systemen bepaalt. Aan elk van deze aspecten (*reliability, availability, maintainability, safety, security, health, environment, economics en politics*) kunnen 'aspecteisen' worden gesteld. De handreiking gaat in op het begrip aspecteis en op de manier waarop bepaalde aspecten, zoals beschikbaarheid en betrouwbaarheid, de prestaties van de hoofdnetwerken bepalen.

Niet voldoen aan de aspecteisen betekent risico's voor onze netwerken. De handreiking schetst het proces dat Rijkswaterstaat doorloopt om de (vaak samenhangende) risico's in beeld te brengen aan de hand van een kwalitatieve risicoanalyse en/of een kwantitatieve risicoanalyse. Rijkswaterstaat onderscheidt drie varianten van de risicoanalyse, die input zijn voor drie varianten van het instandhoudingsplan.

Aan de basis van een (kwalitatief) instandhoudingsplan (IHP) staat een kwalitatieve risicoanalyse ofwel *failure mode, effect and criticality analysis* (FMECA). Deze risicoanalyse geeft zicht op het risico van falen van het systeem door het inschatten van kans- en gevolgklassen op de RAMSSHE€P-aspecten. Die inschatting gebeurt op basis van expert judgement. Voor het overgrote, niet-kritische deel van de infrastructuur van Rijkswaterstaat (meer dan 6000 objecten) is deze analyse voldoende. Het resultaat van de kwalitatieve risicoanalyse is een set van maatregelen waarmee de risico's zover gereduceerd worden, dat de kans van falen van het systeem acceptabel klein is. Deze worden opgenomen in het instandhoudingsplan voor het betreffende netwerkdeel.

Het fundament van een prestatiegestuurd instandhoudingsplan (p-IHP) is een kwantitatieve risicoanalyse. Deze analyse is een wiskundige berekening of modellering van de kans van falen van een systeem. Deze variant richt zich dus alleen op 'betrouwbaarheid' en 'beschikbaarheid' en niet op de overige RAMSSHE€P-aspecten. De keuze voor een kwantitatieve risicoanalyse wordt ingegeven door de eisen aan het desbetreffende object. Dat is het geval bij kwantitatieve eisen, bijvoorbeeld eisen aan de waterkeringen, die volgen uit de *Waterwet*.

Ook als aan de betrouwbaarheid of beschikbaarheid van een object geen (wettelijke) kwantitatieve eisen zijn gesteld, kan een kwantitatieve risicoanalyse wenselijk zijn. Dit is het geval bij alle objecten die kritisch bijdragen aan de functionaliteit van de netwerken.

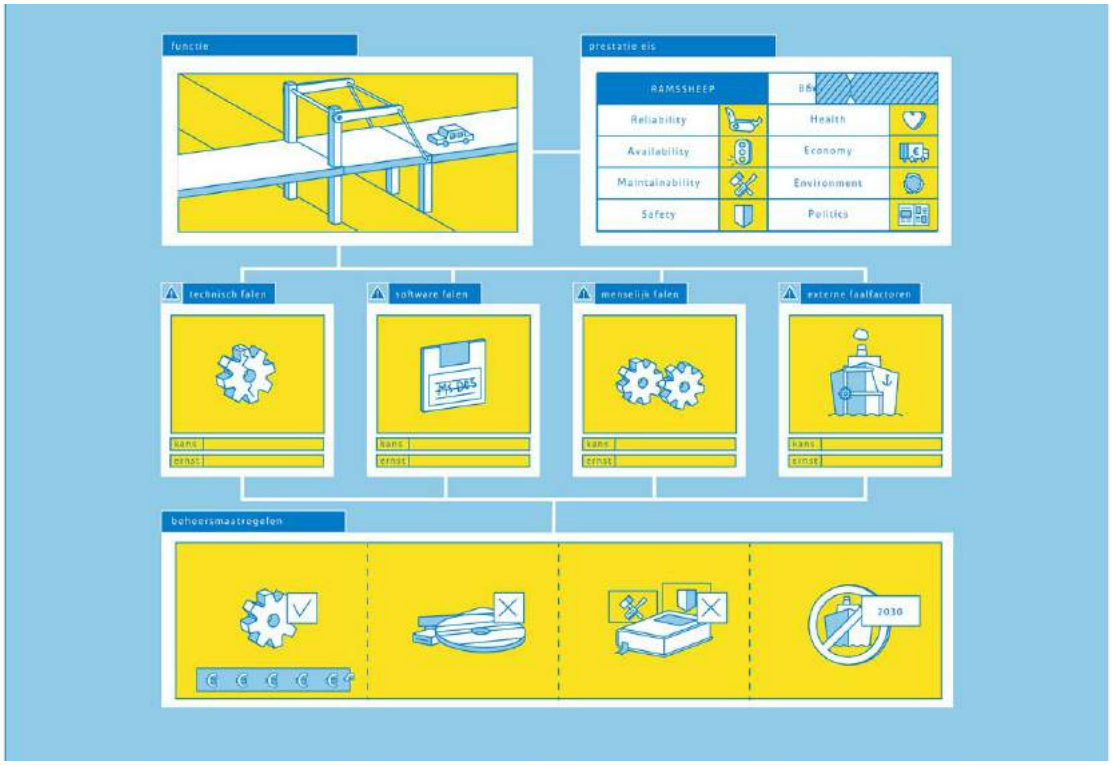
Ook de kwantitatieve variant van de risicoanalyse geeft als resultaat een set maatregelen, maar nu één waarmee aantoonbaar aan de gestelde prestatie-eisen

wordt voldaan. Bij de aanleg van een object geeft de kwantitatieve risicoanalyse dus het vertrouwen in voldoende betrouwbaarheid en beschikbaarheid. Tijdens de gebruiksfase legt deze variant een relatie tussen de onderhoudskosten en de daarmee samenhangende te verwachten prestatie. Naast het aantonen van de levering van de vereiste prestatie biedt de kwantitatieve risicoanalyse volgens de RCM-methode ook de mogelijkheid de onderhoudskosten te optimaliseren. In 2016 heeft het bestuur van Rijkswaterstaat 119 complexen vastgesteld waarvoor een p-IHP gemaakt moet worden.

De resultaten uit de risicoanalyse vormen een belangrijke bron voor de instandhoudingsplannen die borgen dat uit te voeren maatregelen ook daadwerkelijk worden uitgevoerd. Deze resultaten worden opgenomen in het p-IHP. Prestatiegestuurde risicoanalyses en de daarop gebaseerde p-IHP's zijn dan ook van onschatbare waarde voor het zo veel mogelijk plannen van de beschikbaarheid en het terugdringen van ongeplande niet-beschikbaarheid van objecten. De handreiking PRA beschrijft welke onderdelen van de risicoanalyse in het instandhoudingsplan moeten worden verwerkt. Ten slotte geeft de handreiking aan hoe prestatiegestuurde risicoanalyses in contracten met opdrachtnemers toe te passen.

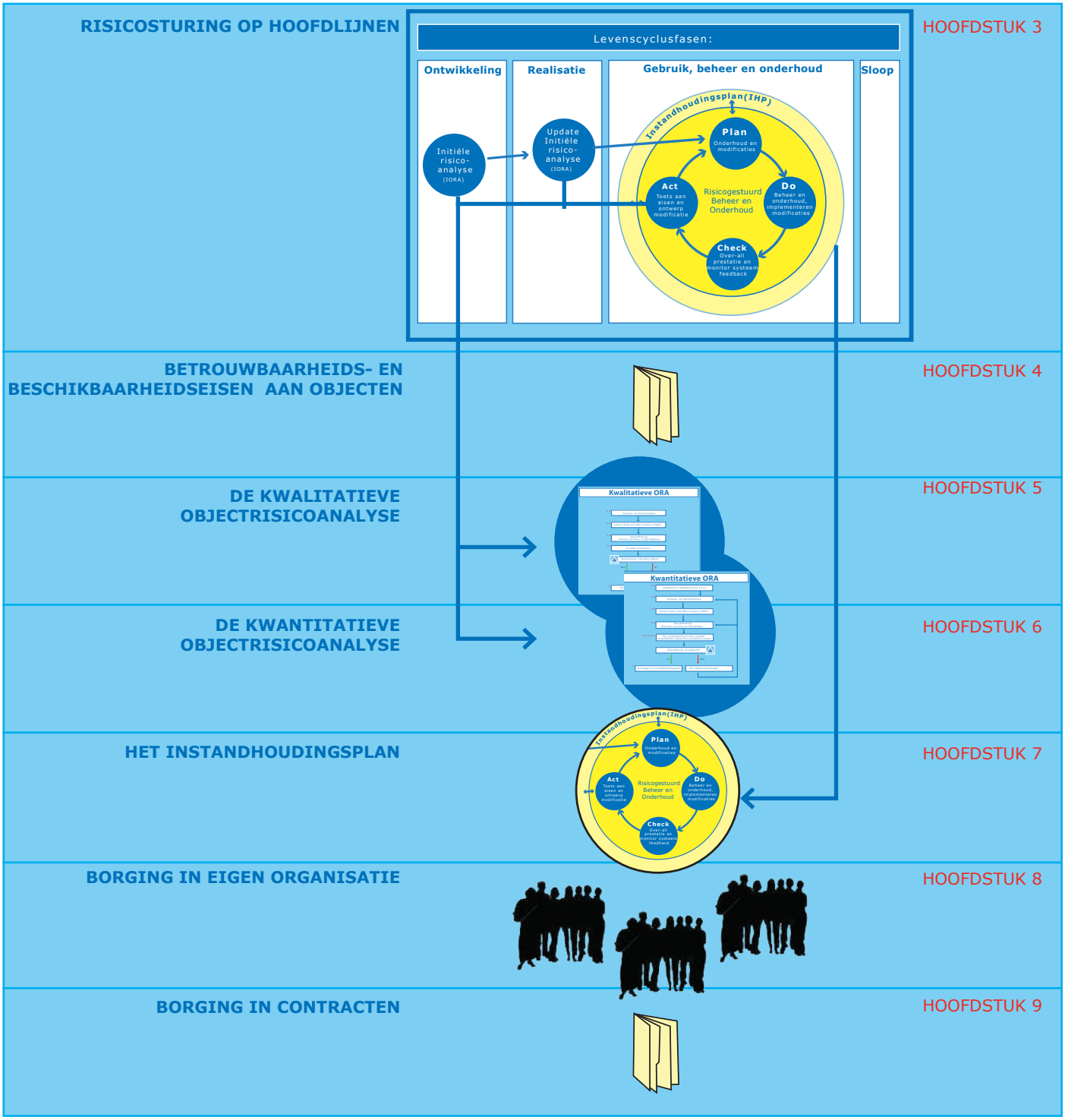
Aan een IHP op basis van ProBO ligt een bijzondere vorm van kwantitatieve risicoanalyse ten grondslag. Het gaat hier om een uitgebreide kwantitatieve variant voor de kritische assets, waarbij strenge eisen maatgevend zijn (foutenboom-methode). Een IHP op basis van ProBO wordt opgesteld voor de vijf stormvloedkeringen die Rijkswaterstaat in beheer heeft (zes vanaf 2018).

Onderstaande infographic over de PRA-processtappen is een onderdeel van de animatie en folder (zie http://corporate.intranet.rws.nl/kennis_en_expertise/kennis_bij_rws/steunpunten/steunpunt_probo/), die deze handreiking flankeren.



Leeswijzer

Deze handreiking beschrijft het proces van prestatiegestuurde risicoanalyses en de daarbij benodigde hulpmiddelen. Zij heeft daarmee een paraplufunctie voor de methoden en hulpmiddelen, die tot in de details van dit proces worden gebruikt. De handreiking gaat niet in op specifieke methoden en hulpmiddelen, maar verwijst er wel naar. Ze zijn in beheer bij Rijkswaterstaat en opvraagbaar bij het steunpunt ProBO.



Hoofdstuk 1 beschrijft als inleiding op de handreiking de belangrijkste kenmerken van risicogestuurd aanleggen, beheren en onderhouden: Wat is dat? Wat zijn nut en noodzaak? Welke relaties heeft risicogestuurd aanleggen, beheren en onderhouden binnen de bredere context van beleid, uitvoering en beheer?

Hoofdstuk 2 gaat in op de grote betekenis van prestatiegestuurde risicoanalyses voor het beleid. Aan de hand van definities en begrippen uit het domein van de systems engineering ontstaat in grote lijn een beeld van het sturingsmodel. Voor de lezer, die nog niet (helemaal) bekend is met de begrippen en termen in het risicogestuurd aanleggen, beheren en onderhouden, geeft dit hoofdstuk ook een toelichting op de meest voorkomende vaktermen.

Hoofstuk 3 schetst op hoofdlijnen de feitelijke risicosturing, het maken van de initiële risicoanalyse en de toepassing ervan in de gebruiksfase. Uitgebreid komt aan de orde welke variant in welke context op zijn plaats is:

- een uitgebreide kwantitatieve variant voor kritische assets, waarbij strenge eisen maatgevend zijn (foutenboom-methode, leidend tot een IHP op basis van ProBO)
- een minder uitgebreide kwantitatieve variant bij assets die een cruciale rol spelen in het presteren van de netwerken (RCM-methode, leidend tot een p-IHP)
- en tot slot een semi-kwantitatieve (kwalitatieve) variant waarmee Rijkswaterstaat de overgrote meerderheid van haar assets beheert en onderhoudt (FMECA, leidend tot een (kwalitatief) IHP).

Hoofdstuk 4 gaat in op de verschillende opties om eisen aan objecten, netwerkschakels of het netwerk te kunnen formuleren. Uiteindelijk zal de wens van de minister van Infrastructuur en Waterstaat een bepalende rol spelen.

Hoofdstuk 5 beschrijft de werkwijze van de kwalitatieve variant en de standaarden die daarbij worden gekozen. In dit hoofdstuk is bij wijze van kader eenduidig vastgelegd hoe Rijkswaterstaat het risicogestuurd beheer en onderhoud via inspecties vormgeeft.

Hoofdstuk 6 heeft dezelfde opzet als hoofdstuk 5, maar nu over de werkwijze van de kwantitatieve variant en de standaarden die daarbij worden gekozen. De kwantitatieve variant resulteert expliciet in een verwachte betrouwbaarheid en/of beschikbaarheid. Dit hoofdstuk is te zien als een kader waarmee Rijkswaterstaat tot deze verwachting komt.

Hoofdstuk 7 handelt over de wijze waarop de resultaten van de risicoanalyses worden verwerkt in een instandhoudingsplan. Ook geeft het aan hoe dit plan de basis vormt voor het uit te voeren onderhoud dat mede randvoorwaarden geeft om de beloofde prestatie te kunnen leveren. De inhoud en vorm van het instandhoudingsplan zelf vallen buiten het blikveld van deze handreiking, maar zijn ook in beheer bij Rijkswaterstaat en opvraagbaar via het steunpunt ProBO.

Hoofdstuk 8 gaat over de organisatie, die nodig is om in de gebruiksfase te borgen dat de beloofde prestatie ook daadwerkelijk zal worden geleverd. Dit gebeurt op basis van de bekende plan-do-check-act-cirkel (PDCA).

Hoofdstuk 9 ten slotte toont welke consequenties de risicosturing heeft voor de diverse contractvormen waarmee Rijkswaterstaat werkt.

1 Risicogestuurd aanleggen, beheren en onderhouden van infrastructuur

1.1 Inleiding

De *Handreiking Prestatiegestuurde Risicoanalyses (PRA)* is opgesteld om het risicogestuurd denken toepasbaar te maken voor de infrastructurele assets die Rijkswaterstaat in beheer heeft. Dit omdat de organisatie het risicogestuurd aanleggen, beheren en onderhouden van infrastructuur ziet als een onontbeerlijk onderdeel van assetmanagement. De handreiking ondersteunt de ontwikkelfase, de realisatiefase en de gebruiksfase van de assets voor het gehele infrastructuursysteem, van tandwielkast tot netwerk en van opdrachtgever tot leverancier. De handreiking integreert en vervangt daarmee de *Leidraad RAMS* en de *Leidraad risicogestuurd beheer en onderhoud*.

De actuele politieke en maatschappelijke beweging in de richting van een kleinere overheid brengt ook een uitdaging met zich mee. Rijkswaterstaat houdt zich minder dan voorheen direct bezig met het bouwen en onderhouden van infrastructuur en concentreert zich vooral op de regierol. Navenant verandert ook de rol van de markt. In deze andere rolverdeling staat het sturen op prestaties meer centraal en komt het aan op goede communicatie en heldere afspraken. De *Handreiking prestatiegestuurde risicoanalyses* draagt hieraan bij doordat de werkwijze en afspraken op het gebied van het sturen op prestaties zijn vastgelegd.

1.2 Wat is risicogestuurd aanleggen, beheren en onderhouden?

Risicogestuurd aanleggen, beheren en onderhouden van objecten houdt een werkwijze in die uitgaat van een berekende of een door expert judgement ingeschatte verwachting, dat objecten voldoen aan gestelde prestatie-eisen. De risicogestuurde werkwijze maakt het ook mogelijk om continu aan te tonen, dat in de verschillende stadia van de levenscyclus van infrastructurele assets daadwerkelijk aan prestatie-eisen wordt voldaan.

Deze handreiking legt een werkwijze vast, inclusief een set methoden om te komen tot prestatiegestuurde risicoanalyses. Zo zorgt de risicogestuurde werkwijze ervoor dat (potentiële) prestaties in samenhang in kaart worden gebracht en ook traceerbaar worden vastgelegd. Daarnaast biedt de werkwijze de mogelijkheid om risico’s op het gebied van prestaties te mitigeren, zwakke plekken in een object te vinden, gericht maatregelen te treffen en alternatieven te vergelijken. Hiermee komt ook de mogelijkheid tot kostenoptimalisatie in zicht.

1.3 Nut en noodzaak van risicogestuurd aanleggen, beheren en onderhouden

Bij de gebruikelijke manier van aanleggen, beheren en onderhouden is er geen transparante relatie tussen enerzijds de gekozen ontwerpen, investeringen en uitvoering van beheer- en onderhoudsactiviteiten, en anderzijds de prestatie-eisen, die impliciet of expliciet aan de functie van een object zijn gesteld. De praktijk wijst dat uit.

De vraag of al dan niet aan de prestatie-eisen wordt voldaan, kan in de praktijk dan ook niet eenvoudig worden beantwoord. Het gevolg kan zijn dat een object onvoldoende of juist bovenmatig presteert en dat het budget niet optimaal over het areaal wordt gebruikt.

Het risicogestuurd denken en de onderliggende methoden zijn erop gericht de relatie tussen prestatie-eisen en het prestatieniveau van het areaal transparant en traceerbaar te maken. Volledige en succesvolle implementatie van risicogestuurd denken stelt de beheerder in staat om:

- blijvend in control te zijn over het areaal, dus zonder grote verrassingen wegens onderhoudskosten of prestatierisico's
- aantoonbaar te voldoen aan wet- en regelgeving en *service level agreements* (SLA's)
- te beschikken over een eenduidig middel voor communicatie met de opdrachtnemer (en indirect de gebruiker), om voor sturing op afstand diens prestaties inzichtelijk te maken
- kosten en opbrengsten van onderhoud te optimaliseren op object- en netwerkniveau.

Deze kwaliteiten maken dat het risicogestuurd denken een goede invulling geeft aan het *publieksgericht netwerkmanagement*, één van de kernaandachtsgebieden van Rijkswaterstaat. Het risicogestuurd denken zorgt immers voor een optimale balans tussen investeringen van publieke gelden en het prestatieniveau van de infrastructuur. Daarnaast kunnen direct belanghebbenden op objectieve en rationele gronden worden geïnformeerd en worden betrokken bij keuzes over de invulling van de infrastructuur.

1.4 Context van risicogestuurd aanleggen, beheren en onderhouden

De overgang naar risicogestuurd aanleg, beheer en onderhoud speelt zich af binnen een context van beleidvorming, methoden en werkwijzen in de uitvoering, de relatie met de beheerder, diverse IPM-rollen in grote projecten, bestaande wet- en regelgeving en de relaties met marktpartijen. Daarom gaat deze paragraaf in op wat de prestatiegestuurde risicoanalyse betekent voor de belangrijkste entiteiten in deze context.

Relatie met het beleid

De minister van Infrastructuur en Waterstaat stelt beleidsdoelen op voor de netwerken die Rijkswaterstaat beheert. De risicogestuurde werkwijze is van grote waarde bij het realiseren van beleidswensen en maakt de kosten daarvan transparant.

Beleidsthema's voor bereikbaarheid, veiligheid en leefbaarheid werken vooral door in het aanlegprogramma en het programma Vervanging en Renovatie, zoals beschreven in het *Meerjarenprogramma Infrastructuur, Ruimte en Transport* (MIRT).

Afspraken over beheer en onderhoud worden gemaakt in de *service level agreement* (SLA). In deze overeenkomst leggen de secretaris-generaal van het ministerie van Infrastructuur en Waterstaat en de directeur-generaal van Rijkswaterstaat vast welke prestaties Rijkswaterstaat zal leveren en wat de kosten daarvan zijn. Bij het realiseren van de afspraken speelt risicogestuurd beheren en onderhouden een cruciale rol. Bij aanlegprojecten worden (nog) geen afspraken gemaakt over de verwachte prestatie in termen van betrouwbaarheid en

beschikbaarheid. Dat komt onder meer doordat de prestatie van infrastructurele netwerken niet alleen afhangt van de aanleg, het beheer en het onderhoud, maar ook van het verkeers- en watermanagement en het incidentmanagement. Deze handreiking gaat alleen over aanleg, beheer en onderhoud.

Relatie met assetmanagement

Assetmanagement zorgt voor optimale benutting van de netwerken van Rijkswaterstaat. Een juist evenwicht tussen prestaties en kosten is hierbij essentieel. Risicogestuurd aanleggen, beheren en onderhouden is een onderdeel van het assetmanagement. Het verscherpt het inzicht in de bijdrage van ieder afzonderlijk object aan het functioneren en presteren van het gehele netwerk. Hier is dus sprake van een koppeling tussen verschillende niveaus van onderhoud en de gevolgen daarvan voor de prestatie(s) van het netwerk. Wat gebeurt er met die prestaties als de komende vier of tien jaar geen onderhoud wordt gepleegd? Wat zijn de gevolgen als voor alternatieve onderhoudsniveaus wordt gekozen? Hoe groot moet de beschikbaarheid zijn van de aan te leggen nieuwe brug? Heeft die beschikbaarheid het gewenste effect op het netwerk? Dit soort vragen illustreert hoe sterk de verwevenheid is van de prestatiegestuurde risicoanalyse met assetmanagement.

Het risicogestuurd denken kan worden aangewend in elke fase van de levenscyclus van een bepaald deel van het netwerk. In combinatie met *life cycle costing* (LCC) weet Rijkswaterstaat precies wanneer concrete risico's ontstaan voor de prestaties van het desbetreffende netwerk. Dit inzicht maakt het mogelijk om, in combinatie met de kennis van de kosten van aanleg en onderhoud, een optimale balans te vinden tussen het prestatieniveau van het areaal en de kosten om dit prestatieniveau in stand te houden, of – waar nodig – te verbeteren. Het risicogestuurd denken koppelt dus de operationele beslissingen over aanleg, beheer en onderhoud aan de tactische en strategische doelstellingen van de organisatie. Het is daarom een belangrijke pijler van het assetmanagement [2].

Relatie met systems engineering

Systems engineering (SE) is een gestructureerde werkwijze om goed presterende systemen te bouwen. 'Goed presterend' heeft onder meer te maken met de aspecten betrouwbaarheid en beschikbaarheid van het systeem. Het werken met deze aspecten wordt dan ook uitgebreid behandeld in de *Leidraad systems engineering* [3]. Deze handreiking moet worden gezien als de concrete invulling van bepaalde analysemethoden die in de *Leidraad systems engineering* zijn genoemd. Zo wordt tevens validatie en verificatie van prestaties mogelijk.

Relatie met life cycle costing

Risicogestuurd aanleggen, beheren en onderhouden doet uitspraken over de toekomst: hoe zal het systeem naar verwachting en gegeven de manier van aanleggen en/of onderhouden, functioneren? De rechtstreekse koppeling tussen wijze van aanleggen en/of onderhouden en de te verwachten prestaties, geeft ook het handvat om de toekomstige kosten in beeld te brengen. Ook voor life cycle costing is de risicogestuurde werkwijze onontbeerlijk.

Relatie met wet- en regelgeving

Eigen aan de risicogestuurde werkwijze is dat aan functies prestatie-eisen worden gesteld. Deze zijn veelal gebaseerd op wet- en regelgeving. Twee bekende voorbeelden zijn de *Waterwet* en de *Wet aanvullende regels veiligheid wegtunnels*.

Overigens is het *Bouwbesluit* al decennialang gestoeld op normen die uitgaan van een kwantitatieve prestatie-eis. In de Eurocodes, die via het *Bouwbesluit* verplicht moeten worden toegepast bij het ontwerpen van bouwwerken, worden maximaal toelaatbare faalkansen per referentieperiode geëist.

Relatie met de operationele beheerder

De regionale organisatieonderdelen van Rijkswaterstaat stellen prestatie- en risicogestuurde instandhoudingsplannen op aan de hand van locatie- en objectgebonden informatie. Daarbij maken zij mede gebruik van risicoanalyses van de objecten, die worden gemaakt en geactualiseerd volgens de systematiek die in deze handreiking is beschreven. De instandhoudingsplannen zijn de basis voor het uit te voeren beheer en onderhoud. Zij borgen de afspraken over de prestaties die de objecten zullen leveren. (Zie voor meer informatie over de rol van het instandhoudingsplan hoofdstuk 7 en voor de organisatorische aspecten, waarmee vooral de beheerder te maken heeft, hoofdstuk 8).

Relatie met de (technisch) manager

Rijkswaterstaat voert aanleg- en grootschalige renovatieprojecten uit met een team dat is samengesteld volgens het integraal projectmanagementmodel (IPM). Zijn aan een te bouwen of te renoveren object betrouwbaarheids- en/of beschikbaarheidseisen gesteld, dan zal het IPM-team die eisen moeten formuleren, contractueel voorschrijven en toetsen op de verwachting dat ze zullen worden waargemaakt. De technisch manager moet over voldoende kennis beschikken om deze activiteiten te begeleiden.

Relatie met de opdrachtnemer

Als bij een aanleg- of onderhoudsproject de risicoanalyse is uitbesteed, moet de opdrachtnemer daadwerkelijk een objectrisicoanalyse (ORA) kunnen maken en blijven actualiseren. De objectrisicoanalyse hoort bij het object en wordt/blijft eigendom van Rijkswaterstaat. Ze moet dus ook beschikbaar, bruikbaar en toegankelijk zijn voor Rijkswaterstaat. De opdrachtnemer heeft de contractuele verplichting om dit gestandaardiseerd te doen en zal daarnaast deze handreiking als hulpmiddel en informatiedrager kunnen gebruiken.

2 Van beleid naar aanleg en onderhoud

Rijkswaterstaat ontwikkelt, beheert en onderhoudt drie Nederlandse netwerken:

- het hoofdwegennetwerk (HWN)
- het hoofdvaarwegennetwerk (HVWN) en
- het hoofdwatersysteem (HWS).

Om te kunnen sturen op prestaties van deze netwerken is op alle niveaus binnen de organisatie risicogestuurd denken noodzakelijk. Op het hoogste, strategische niveau wordt het beleid bepaald dat – samen met vigerende wetgeving en eventueel bestuurlijke afspraken – bepalend is voor aanleg, beheer en onderhoud.

Bij het sturen op tactisch niveau worden de beleidswensen met betrekking tot een hoofdsysteem of netwerk vertaald naar objecten. Het gaat dan om de functie(s) die de verschillende objecten vervullen, en de prestatie-eisen die hieraan worden gekoppeld. Vanzelfsprekend dient bij deze vertaalslag het geheel van de prestaties van objecten en deelsystemen te blijven voldoen aan de beleidsdoelstellingen en aan wet- en regelgeving.

Op operationeel niveau krijgen aanleg, beheer en onderhoud concreet gestalte. Dit gebeurt zodanig dat de afgesproken prestaties daadwerkelijk worden geleverd en dat duidelijk wordt welke kosten hiermee zijn gemoeid.

Een voorbeeld van de wijze waarop prestatie-eisen, beleidsdoelen en wet- en regelgeving op elkaar zijn afgestemd, is te vinden in de Waterwet. De Waterwet stelt voor elke dijkring een veiligheidsnorm. Het beleidsdoel daarvan is het beschermen van het achterland tegen hoog water. De bestuurlijke afspraken zijn dat de waterschappen de dijkringen beheren en zorgplicht hebben voor het voldoen aan de veiligheidsnorm, terwijl de provincies en het ministerie van Infrastructuur en Waterstaat toezicht houden. De eis aan de infrastructuur is dat deze bestand moet zijn tegen een waterstand die een kleine kans per jaar van voorkomen heeft. Dit is een eis aan de betrouwbaarheid.

Een ander voorbeeld: het probleem dat een weg te weinig capaciteit heeft, kan worden opgelost door de weg te verbreden. De capaciteit wordt dan uitgebreid. Het primaire proces ‘aanleg’ draagt bij aan het behalen van de beleidsdoelen. Ook verkeersmanagement kan oplossingen bieden. Denk aan toeritdosering, snelheidsverlaging of omrijroutes. Eisen aan de betrouwbaarheid en de beschikbaarheid beïnvloeden de kwaliteit van de nieuwe delen van het netwerk.

Geplande werkzaamheden aan wegen en vaarwegen (op voorhand bekend) en ongeplande werkzaamheden (onverwacht) zijn een noodzakelijk kwaad. De hoeveelheid werkzaamheden en daarmee de niet-beschikbaarheid, is te beïnvloeden door slimmer onderhoud, meer gebruik van duurzame materialen, kortere herstelperioden et cetera.

Op deze manier draagt het slim uitvoeren van onderhoud bij aan de netwerkprestatie. Gevolgen van niet-beschikbaarheid kunnen worden verminderd door verkeersmanagement: aankondiging van het onderhoud met omrij- en omvaarroutes, maar ook door 's nachts te werken in plaats van overdag.

Als laatste voorbeeld het incidentmanagement. Beter incidentmanagement zorgt ervoor dat de weg snel weer vrij en volledig beschikbaar is, wat resulteert in minder filevorming. Daarmee draagt incidentmanagement bij aan een beleidsdoel van het ministerie van Infrastructuur en Waterstaat.

2.1 Beleidsdoelen

Voorbeelden van beleidsdoelen voor de drie netwerken die Rijkswaterstaat beheert:

Hoofdwegennetwerk:
- De gemiddelde reistijd op snelwegen tussen de steden mag in de spits maximaal anderhalf keer zo lang zijn als buiten de spits.
- De gemiddelde reistijd op snelwegen rond de steden en op niet-autosnelwegen die onderdeel zijn van het HWN, mag in de spits maximaal twee keer zo lang zijn als buiten de spits.

Hoofdvaarwegennetwerk:
- Vervoer over de vaarwegen moet zo betrouwbaar, efficiënt, veilig en duurzaam als mogelijk zijn. Het ministerie van Infrastructuur en Waterstaat stelt dit doel op strategisch niveau. 'Als mogelijk' geeft aan dat de vier genoemde aspecten nooit in absolute zin haalbaar zijn.
- Dit streven in de doelstelling werkt door op tactisch en operationeel niveau. Rijkswaterstaat streeft naar een eenduidig, transparant en doelmatig (nautisch en technisch) beheer van de vaarweg. Speerpunten zijn: zo betrouwbaar mogelijke reistijden, goede bereikbaarheid en continuering van een hoge graad van veiligheid van het vervoer over water.

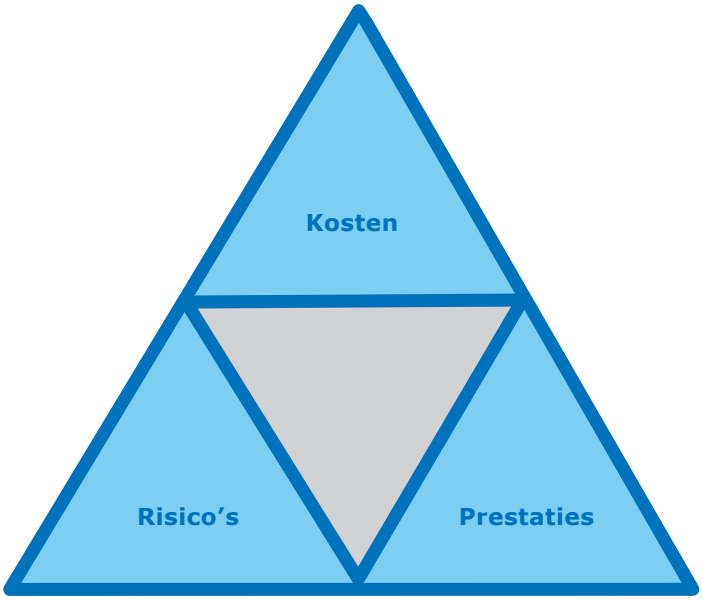
Hoofdwatersysteem:
- *Waterveiligheid*. Het land achter de zeewering en de primaire waterkeringen moet zijn beschermd tegen overstromingen. Op tactisch en operationeel niveau werkt dit beleidsdoel door in het handhaven van de kustlijn, de zorg voor de waterkeringen langs de grote rivieren en meren en de zorg voor het waterafvoerend en waterbergend vermogen van het hoofdwatersysteem.
- *Zoetwater*. Zoetwater moet in voldoende mate beschikbaar zijn voor alle functies, inclusief voor de natuur. In droge tijden moet het beschikbare zoetwater in het hoofdwatersysteem evenwichtig worden verdeeld, met prioriteit voor de meest vitale functies.
- *Waterkwaliteit*. Het water van het hoofdwatersysteem moet voldoende schoon en gezond zijn voor alle gebruiksfuncties, maar vooral voor drinkwaterinname, recreatie en ecologische functies.

Rijkswaterstaat beheert en onderhoudt de netwerken in opdracht van het ministerie van Infrastructuur en Waterstaat. Anders gezegd (in de taal van het assetmanagement): het ministerie van Infrastructuur en Waterstaat is de 'asset owner' en Rijkswaterstaat de 'asset manager'.

Rijkswaterstaat sluit een *service level agreement* (SLA) met het ministerie van Infrastructuur en Waterstaat voor beheer, onderhoud en ontwikkeling (BOO) en voor verkeers- en watermanagement. In de SLA staan verschillende soorten afspraken, onder andere:

- afspraken gerelateerd aan de beschikbaarheid van functies van het infrasysteem
- afspraken gerelateerd aan betrouwbaarheid waarmee de functies worden vervuld.

Er is een verband tussen prestaties, risico's en kosten: hoe lager de risico's en hoe beter de prestaties, hoe hoger de kosten. Het is aan de beleidsmakers om te kiezen welke risico's acceptabel en welke prestatieniveaus met bijbehorende kosten wenselijk zijn. De minister van Infrastructuur en Waterstaat stelt budget beschikbaar en Rijkswaterstaat zorgt voor een optimaal gebruik van dat budget voor het presteren van haar assets.



Figuur 2.1. Relatie tussen risico's, prestaties en kosten

2.2 Systemen, functies, en eisen

Voor een goed begrip van wat deze handreiking uiteenzet over prestatiegestuurde risicoanalyses, is het van belang een aantal sleutelbegrippen kort toe te lichten. Een aantal voor deze handreiking essentiële begrippen is ontleend aan het domein van systems engineering [3].

Systeem
Een systeem is een samenhangend geheel van (fysieke) onderdelen dat is bedoeld om een bepaalde functie te vervullen. De drie netwerken die Rijkswaterstaat onderhoudt, hebben de status van 'hoofdsysteem'. De componenten waaruit de hoofdsystemen zijn opgebouwd, zoals de verbinding tussen A en B, worden deelsystemen of ook wel systeemelementen genoemd. Deelsystemen op hun beurt bestaan uit nog kleinere systeemelementen, zoals wegvakken, knooppunten en bruggen.

Alle systeemelementen samen bepalen het al dan niet goed functioneren van een systeem als geheel. 'Samen' betekent hier niet alleen 'de som der delen', maar ook nadrukkelijk 'in onderlinge samenhang'. Daarnaast is ook de kwaliteit van elk

van de systeemelementen afzonderlijk van directe invloed op de kwaliteit van de netwerken waar ze deel van uitmaken.

Bij Rijkswaterstaat wordt, conform de NEN 2767 [4], de volgende indeling toegepast. De drie netwerken die Rijkswaterstaat onderhoudt, worden de *hoofdsystemen* genoemd. De componenten, waaruit de hoofdsystemen zijn opgebouwd, worden *systemen* genoemd, zoals Rijksweg 1 in het HWN. De systemen op hun beurt zijn opgebouwd uit *systeemdelen*, zoals de verbinding tussen A en B. De systeemdelen bestaan uit *beheerobjecten*, zoals wegen, kanalen, schutsluizen en bruggen. De componenten hiervan worden *elementen* genoemd en deze vallen weer uiteen in *bouwdelen*. Zo kan een goede decompositie worden opgemaakt, welke wezenlijk van belang is binnen de risicoanalyse. De decompositie wordt ook opgenomen in de instandhoudingsplannen van de beheerder.

Functie
Een functie is de (beoogde) werking en/of verrichting van een systeem en een taak die wordt uitgevoerd. Systemen bestaan omdat ze functies uitvoeren. Zo heeft het hoofdwegennet – simpel verwoord – de functie 'het mogelijk maken per voertuig van A naar B te komen'. Een sluis heeft als functie om een schip over een waterstandsverschil te transporteren. Een accu heeft als functie elektrische energie op te slaan en gecontroleerd weer terug te leveren, enzovoorts.

Functies hebben doorgaans een hiërarchische ordening (afgebeeld als functiebomen). Binnen zo'n hiërarchie vallen functies uiteen in sub- of deelfuncties. Zo is bijvoorbeeld het managen van verkeer een subfunctie van de transportnetwerken van Rijkswaterstaat (Hoofdwegen en Hoofdvaarwegen).

Systeemeisen
Systeemeisen is de verzamelnaam voor alle eisen die worden gesteld aan het systeem. Rijkswaterstaat noemt het geheel van de functionele eisen, de aspecteisen en de raakvlakeisen: 'de eisen'. Voor de duidelijkheid is in deze handreiking gekozen voor het onderscheidende begrip systeemeisen.

Functionele eis
De functionele eis is een primaire eis aan de functie. Er is in vervat wat het systeem moet kunnen. Vaak heeft een functionele eis betrekking op de capaciteit die een systeem moet leveren bij het vervullen van de functie. Denk aan de hoeveelheid verkeer die het hoofdwegennet moet kunnen verwerken, of de grootte van de schepen die een sluis moet kunnen schutten, of het waterstandsverschil waarover de sluis schepen moet kunnen transporteren, of de hoeveelheid stroom die een accu kan opslaan.

Aspecteis
Een aspecteis beschrijft de randvoorwaarde(n) waaronder het systeem zijn functies moet vervullen. Voorbeelden zijn: beschikbaarheid, betrouwbaarheid, onderhoudbaarheid, veiligheid, duurzaamheid, gezondheid. Kortom, eisen op het gebied van RAMSSHE€P (zie voor dit acroniem paragraaf 2.3). Een sluis kan groot genoeg zijn en in staat om voldoende waterstandsverschil te overbruggen, maar als hij niet voldoet aan de randvoorwaarde beschikbaarheid (bijvoorbeeld als gevolg van een technisch defect), dan is de kwaliteit van zijn functioneren op dat moment nihil en op jaarbasis mogelijk minder dan was verwacht.

Raakvlakeis
Dit type eis aan een systeem is het resultaat van een raakvlakkenanalyse. Een dergelijke analyse inventariseert de eisen, die de omgeving van het systeem aan het systeem stelt.

Falen

Er is sprake van falen wanneer als gevolg van een gebeurtenis, of een verzameling gebeurtenissen, een systeem zijn functie niet meer kan vervullen. Het systeem voldoet dan niet meer aan de functionele eisen. Dit is een wezenlijk punt, omdat de notie 'falen' vaak wordt gekoppeld aan systemen. Het heet dan 'dat het systeem faalt', maar in feite is van belang dat de functie die het systeem uitvoert niet meer wordt vervuld.

Er kunnen meerdere en uiteenlopende oorzaken zijn waardoor een systeem zijn functie niet meer kan vervullen. Slechts een beperkt deel daarvan kan worden beïnvloed door aanleg, beheer of onderhoud. Er is bijvoorbeeld geen sprake van falen als een systeem zijn functie niet vervult door capaciteitsgebrek. In dit geval wordt het systeem gebruikt op een manier waarvoor het niet is ontworpen.

Faaldefinitie

Er is dus duidelijk een faaldefinitie nodig, een afspraak over wanneer wel of niet sprake is van falen. Een faaldefinitie legt de relatie vast tussen het falen van (de functie van) een deelsysteem en de consequenties daarvan voor het systeem. Als bijvoorbeeld een veiligheidssysteem (deelsysteem) faalt, is de veiligheid van het systeem niet meer voldoende geborgd. De noodzakelijke maatregelen, welke niet altijd het afbreken van de hoofdfunctie behelzen, worden vastgelegd in de faaldefinitie. Meestal is het evident wanneer van falen sprake is. Als een sluisdeur niet meer open of dicht wil, heeft de functie 'schutten' van de sluis gefaald.

Falen van deelsystemen hoeft niet te leiden tot algeheel falen van de hoofdfunctie. Als de hoofdfunctie niet volledig wegvalt, veroorzaakt het falen van een deelsysteem meestal een beperking van de functie van het systeem. En als bij bediening op afstand een of meerdere camera's falen, geeft de faaldefinitie aan hoeveel en welke camera's mogen falen, voordat sprake is van het falen van de functie 'zicht hebben'. Falen er dan méér of specifieke camera's, dan moet de functie 'zicht hebben' als gefaald worden beschouwd. Het proces (het uitvoeren van de functie) moet dan worden gestopt.

Voorbeelden van de relatie tussen beleidsdoelen en de eisen aan functies

Het hoofdwegennet

Het ministerie van Infrastructuur en Waterstaat wenst dat de gemiddelde reistijd op snelwegen tussen de steden in de spits maximaal anderhalf keer zo lang is als buiten de spits. Deze wens heeft betrekking op de functie 'afwikkelen wegverkeer'. De functionele eis aan het wegvak zou kunnen luiden: 'bij een verkeersaanbod kleiner dan of gelijk aan de ontwerpcapaciteit moeten minimaal 4.500 voertuigen per uur met een snelheid van 100 km/uur kunnen passeren'.

Een daarbij behorende aspecteis zou kunnen zijn: 'de beschikbaarheid moet ten minste 99 procent zijn'. Dat betekent dat ten minste 99 procent van de tijd 4.500 voertuigen met een snelheid van 100 km/uur kunnen rijden. Als, bijvoorbeeld door een gat in de weg, minder dan 4.500 voertuigen per uur bij een snelheid van 100 km/uur kunnen passeren, is sprake van falen.

Het hoofdvaarwegennet

Het ministerie van Infrastructuur en Waterstaat wil dat het vervoer over water vlot, betrouwbaar, efficiënt, veilig en duurzaam is. De bijbehorende functie is 'afwikkelen scheepvaartverkeer'. Een functionele eis die hierbij past, is dat een sluis in het netwerk een schip over een

waterstandsverschil van 6 meter moet kunnen transporteren. Een randvoorwaarde aan deze functionaliteit kan zijn: 'de beschikbaarheid (aspecteis) moet ten minste 99 procent zijn'. Dat betekent dat gedurende ten minste 99 procent van de tijd de sluis in staat moet zijn om een schip over een waterstandsverschil van 6 meter te transporteren.

Het hoofdwatersysteem
Het beleid vraagt dat tijdens extreem droge perioden voldoende zoet water aanwezig is voor drinkwater, scheepvaart en industrie (koelwater). De functie is hier 'zoetwater aanvoeren'. Een functionele eis aan de stuw bij Driel, die de waterverdeling over de IJssel en de Lek regelt, zou kunnen zijn: 'de waterafvoer via de IJssel moet ten minste 55 m^3/s zijn'. Een bijbehorende aspecteis voor de stuw is dan: 'de beschikbaarheid van de stuw moet ten minste 99,5 procent zijn'. Gedurende ten minste 99,5 procent van de tijd zal dan de rivierafvoer van de IJssel ten minste het minimale debiet bedragen. Het systeem heeft gefaald als het debiet minder is dan 55 m^3/s. Als in droge tijden, bijvoorbeeld, de Rijn minder dan 1.000 m^3/s water afvoert, is de stuw bij Driel niet in staat de gevraagde 55 m^3/s afvoer via de IJssel te bewerkstelligen. Het systeem is niet ontworpen om ook onder deze omstandigheden zijn functie uit te voeren. In dit geval is daarom geen sprake van falen.

2.3 De aspecten RAMSSHE€P

RAMSSHE€P is een acroniem voor betrouwbaarheid (R, *reliability*), beschikbaarheid (A, *availability*), onderhoudbaarheid (M, *maintainability*), veiligheid (S, *safety*), beveiliging (S, *security*), gezondheid (H, *health*), omgeving en milieu (E, *environment*), kosten (€, *economics*) en imago (P, *politics*). Het zijn alle aspecten van het systeem.

De aspecten betrouwbaarheid en beschikbaarheid zijn indicatoren van de verwachte prestatie van het systeem. Paragraaf 2.4 gaat daar verder op in. De overige aspecten manifesteren zich als (meestal ongewenste) bijwerkingen of mogelijke gevolgen. Eisen aan deze aspecten fungeren als randvoorwaarden voor de werking van het systeem. De voorwaardenscheppende aspecten worden hieronder kort geïntroduceerd, in hoofdstuk 5 over de kwalitatieve objectrisicoanalyse komen ze terug.

Onderhoudbaarheid *(M, maintainability)*
Dit aspect wordt meestal gedefinieerd als de kans dat een systeem (of systeemelement) binnen een specifiek tijdsinterval en onder gegeven omstandigheden, kan worden geïnspecteerd, gerepareerd, of preventief onderhouden. De voorwaardelijke bepaling 'specifiek tijdsinterval', anders gezegd: de herstelduur of de inspectietijd, is ook een belangrijke component van het aspect 'beschikbaarheid'.

Onderhoudbaarheid, volgens deze definitie, wordt (nog) weinig in de praktijk gebruikt, zeker bij Rijkswaterstaat. Rijkswaterstaat interpreteert onderhoudbaarheid vaak als randvoorwaarde aan bereikbaarheid van

systeemelementen, of het hebben van voldoende en juist gereedschap enzovoorts. Dat zijn factoren die de herstel-, vervangings- of inspectietijd bekorten, wat tot een hogere beschikbaarheid leidt.

Veiligheid *(S, safety)*
Dit aspect is de kans dat een systeem gedurende een bepaalde periode, en onder gegeven omstandigheden, geen menselijk letsel (gewonden, doden) veroorzaakt. Deze definitie is gelijk aan die van betrouwbaarheid (zie paragraaf 2.4), met dit verschil dat bij het aspect 'veiligheid' de gevolgen worden uitgedrukt in potentiële slachtoffers en bij 'betrouwbaarheid' in potentiële 'schade'. Rijkswaterstaat vat onder potentiële slachtoffers de gebruikers van het systeem, het bedienings- en onderhoudspersoneel en de omwonenden. Het begrip 'Arbo-veiligheid' valt ook onder deze noemer. Denk aan een brug om een beeld te krijgen van hoe het aspect 'veiligheid' werkt. De mate van veiligheid hangt onder meer af van de kans dat de brug instort. De door Rijkwaterstaat gehanteerde voorschriften (mits goed toegepast) zorgen ervoor dat de kans op instorten van een brug ten hoogste 0,0001 per 50 jaar is. Het systeem (de brug) is hiermee voldoende veilig.

Security *(S, security)*
Het aspect security staat voor de veiligheid van een systeem met betrekking tot bewust onveilig menselijk handelen, zoals vandalisme, terrorisme en cybercrime. Rijkswaterstaat hanteert voor het begrip 'security' de term 'integrale beveiliging'.

Gezondheid *(H, health)*
Het aspect gezondheid is te omschrijven als het lichamelijk, geestelijk en/of maatschappelijk welzijn, zonder dat sprake is van falen of van acute veiligheidsrisico's. Dit welzijn heeft betrekking op gebruikers van de infrastructuur, op personen die op of aan de infrastructuur werken en – voor zover van toepassing – op de infrastructuur zelf. Denk bijvoorbeeld aan de invloeden die uitgaan van ergonomie of gevaarlijke stoffen. Het verschil tussen de aspecten gezondheid en veiligheid is soms wat arbitrair. Gezond werken valt bijvoorbeeld ook onder Arbo-veiligheid. Een voorbeeld hiervan wordt verderop in deze paragraaf gegeven.

Omgeving en Milieu *(E, environment)*
Dit aspect betreft de relatie met de fysieke omgeving. Het kan dan gaan om de inpassing van infrastructuur, maar ook om de (mogelijke) beïnvloeding van de omgeving door de infrastructuur. Denk aan de gevolgen voor de milieukwaliteit en de doorwerking daarvan op flora, fauna, en hinder (geluid, fijnstof) voor mensen. Ook het onderscheid tussen gezondheid en milieu kan enigszins arbitrair zijn.

Kosten *(€, euro's, economics)*
Het aspect 'kosten' omvat het geheel van de financiële gevolgen, zoals kosten van aanleg, kosten van onderhoud, claims en boetes. Het kostenaspect is onlosmakelijk verbonden met de overige RAMSSHE€P-aspecten, omdat het verhogen of verlagen van de prestaties op die aspecten altijd consequenties heeft voor de kosten. Deze wetmatigheid geldt voor alle fasen in de levenscyclus van systemen en komt in de *life cycle cost* (LCC)-benadering [5] expliciet naar voren. Risicogestuurd aanleggen, beheren en onderhouden maakt de relatie tussen kosten en de overige RAMSSHE€P-aspecten transparant. Het verhogen of verlagen van RAMSSHE€P-prestaties worden vaak uitgedrukt in maatschappelijke kosten.

Imago *(P, politics)*
In het aspect 'imago' komen politiek-bestuurlijke en maatschappelijke gevolgen tot uiting. Dat kunnen bijvoorbeeld effecten op het imago van de beheerorganisatie zijn of gevolgen voor de reputatie van de politiek/bestuurlijk verantwoordelijken.

De MSSHE€P-aspecten (dus niet de aspecten beschikbaarheid en betrouwbaarheid) worden vaak geformuleerd als harde randvoorwaarden aan de functie, zoals:

- de geluidsrandvoorwaarde bij een weg (bijvoorbeeld een geluidsscherm plaatsen)
- de fijnstofrandvoorwaarde (schermen plaatsen of tunnelmonden afschermen)
- de beveiligingseisen aan het gebruik van terreinen (hekken plaatsen).

Voor sommige MSSHE€P-aspecten kunnen op hoog abstractieniveau eisen worden gesteld, zoals de maximaal toelaatbare hoeveelheid geluid naast een weg. Andere MSSHE€P-aspecten moeten instrumenteel worden geëist, zoals een beveiligingsconcept.

Voorbeeld

Vanuit het aspect 'gezondheid' wordt de eis gesteld dat naast een wegvak de geluidhinder moet worden beperkt. Daarom zullen geluidsschermen worden geplaatst. Dat zijn dan 'functievervullers' voor de subfunctie 'beperken overdracht geluid'. Aan deze subfunctie kunnen functionele eisen worden gesteld, zoals: 'maximaal x dBA op de achterliggende gevel'. Ook kunnen eisen van beschikbaarheid of betrouwbaarheid worden gesteld aan de kwaliteit waarmee deze subfunctie wordt vervuld, bijvoorbeeld: 'in 2 procent van de tijd mag het geluidsniveau hoger zijn dan x dBA op de achterliggende gevel'. Dit is dan een beschikbaarheidseis aan het geluidsscherm, terwijl het geluidsscherm zelf voortkomt uit een aspecteis aan het hoger liggend systeem (het wegvak).

Dit voorbeeld geeft aan dat aan MSSHE€P-aspecten ook eisen met betrekking tot betrouwbaarheid en beschikbaarheid kunnen zijn verbonden.

2.4 De aspecten betrouwbaarheid en beschikbaarheid

Om de prestaties van de netwerken uit te drukken, gebruikt Rijkswaterstaat de begrippen R (*reliability*) en A (*availability*). Deze bepalen de mate van functioneren van het systeem.

Door eisen te stellen aan deze R- en A-aspecten beperkt Rijkswaterstaat de kans op falen van een systeem en borgt daarmee de mate waarin de functies worden vervuld. Zo'n eis kan bijvoorbeeld luiden: 'De functie mag niet meer dan gemiddeld vier keer per jaar falen', of: 'Als de functie faalt, moet ze binnen 4 uur worden hervat'. Deze eisen geven (uit het oogpunt van betrouwbaarheid) aan hoe vaak falen nog acceptabel wordt gevonden en (uit het oogpunt van beschikbaarheid) hoe lang een functie verstoord mag zijn.

Het totaal van functievervulling en de mate waarin dat gebeurt, wordt de **prestatie** van het netwerk, of van het (deel)systeem, genoemd. Rijkswaterstaat wil als netwerkbeheerder weten welke prestaties de systemen tegen welke prijs moeten leveren. Daarvoor is het nodig te weten:

- welke functionele eisen aan een systeem worden gesteld en welke prestatie-eisen daarvoor gelden
- welke prestaties nu worden geleverd, gegeven de staat van onderhoud en de vigerende onderhoudsafspraken
- wat wanneer nodig is om de gevraagde prestaties te leveren en wat dat kost.

De begrippen betrouwbaarheid en beschikbaarheid zijn direct in getallen uit te drukken, in tegenstelling tot, bijvoorbeeld, het aspect gezondheid. De definitie van **betrouwbaarheid** is:

Betrouwbaarheid is de kans dat een systeem zonder falen zijn functie vervult, gedurende een bepaalde periode, en onder gegeven omstandigheden.

In de praktijk wordt bijna altijd het complement van betrouwbaarheid gebruikt: de onbetrouwbaarheid, ofwel de kans dat een systeem in een bepaalde periode, onder gegeven omstandigheden, faalt. Betrouwbaarheid is dimensieloos per tijdseenheid [-/tijdseenheid]. Een kans per tijdseenheid is in feite een frequentie, waarbij er een relatie is tussen de kans per tijdseenheid en het aantal keren per tijdseenheid. Paragraaf 6.3 gaat hier verder op in.

Denk voor een voorbeeld van het aspect (on)betrouwbaarheid aan de kans per jaar dat het verkeersmanagement faalt, zonder te verwachten menselijk letsel en met alleen schade in de vorm van langere files dan normaal. Als wél menselijk letsel denkbaar is, valt het falen onder het aspect veiligheid. (Zie hierover ook paragraaf 2.3 veiligheid)
Een ander voorbeeld is de kans dat een stuw faalt. Ook hier is die kans gekoppeld aan een tijdsspanne (bijvoorbeeld één jaar). Als dit gebeurt, ontstaat 'alleen maar' schade.

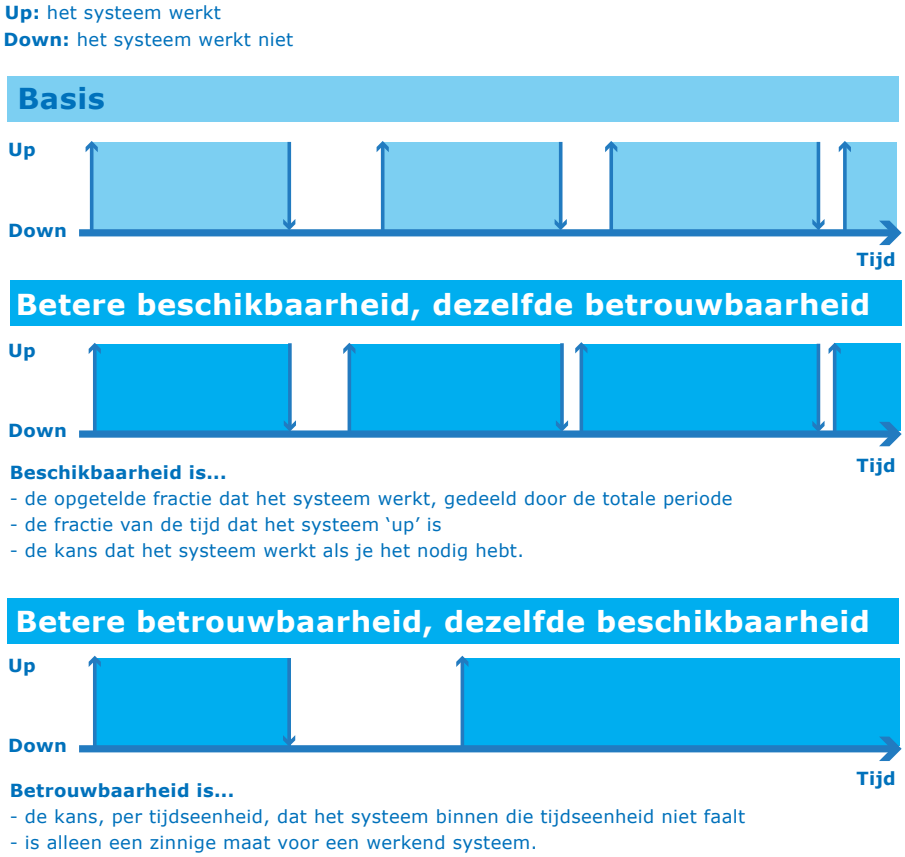
Betrouwbaarheid heeft dus betrekking op systemen die continu werken (functioneren), met schade als gevolg van het falen van het systeem.

De definitie van **beschikbaarheid** is:

1) Beschikbaarheid is de verwachte fractie van de totale tijd dat een systeem, onder gegeven omstandigheden, functioneert.
2) Beschikbaarheid is (ook) de kans dat een systeem, onder gegeven omstandigheden, functioneert wanneer het op een willekeurig tijdstip wordt aangesproken.

Op het oog lijken dit twee compleet verschillende definities van beschikbaarheid. Bij nadere beschouwing blijken het twee verschijningsvormen te zijn van hetzelfde principe. Immers: de verhouding tussen de intervallen waarin gedurende een bepaalde tijdseenheid een systeem werkt (eerste definitie) en de intervallen waarin het systeem niet werkt (faalt), is gelijk aan de kans dat het systeem beschikbaar is wanneer het wordt aangesproken (tweede definitie).

Het verschil tussen betrouwbaarheid en beschikbaarheid wordt nog eens duidelijk gemaakt in figuur 2.2.



Figuur 2.2. Betrouwbaarheid en beschikbaarheid

Het aantal keren down is 4 bij de bovenste twee tijdbalken en 2 bij de onderste (zie figuur 2.2). De oppervlakte is in alle gevallen gelijk, maar de onderste tijdbalk laat minder faalmomenten zien. Een tijdbalk geeft de (gemeten of verwachte) werking van een systeem aan. Bij gelijkblijvende betrouwbaarheid en toenemende beschikbaarheid, blijft het aantal faalmomenten gelijk, maar neemt de totale herstelperiode af (vergelijking bovenste met de middelste tijdbalk). Bij toenemende betrouwbaarheid en gelijkblijvende beschikbaarheid neemt het aantal faalmomenten af, maar blijft de totale hersteltijd gelijk (vergelijking bovenste en onderste tijdbalk).

Als voorbeeld van beschikbaarheid is te denken aan de fractie van de tijd dat een wegvak of een tunnel in gebruik is. Rijkswaterstaat eist vaak van zijn opdrachtnemers dat zijn objecten niet meer dan een bepaalde tijd, bijvoorbeeld maximaal 45 uur per jaar, gestremd mogen zijn. Er wordt dan een beschikbaarheidseis gesteld van (8760 uur {=aantal uren in 1 jaar} - 45 uur) / 8760 uur ≈ 99,5 procent. In termen van niet-beschikbaarheid is de eis dus dat de niet-beschikbaarheid van het systeem maximaal 0,5 procent mag zijn.

Een ander voorbeeld van niet-beschikbaarheid: de kans dat de Maeslantkering onverhoopt niet sluit in geval van een stormvloed mag ten hoogste 0,01 zijn, dus 1 procent. Die eis volgt uit de Waterwet. Er moet dus worden voldaan aan een niet-beschikbaarheidseis van 0,01.

Essentieel is dat voor de beide aspecten R en A het begrip ‘kans’ wordt gehanteerd. Aan de hand van het kansbegrip zijn de verwachte toekomstige betrouwbaarheid en beschikbaarheid van een systeem te berekenen. Door hier eisen aan te stellen heeft Rijkswaterstaat vóóraf grip op de kwaliteit van de gevraagde functies van een systeem. Paragraaf 6.3 gaat dieper in op het begrip kans.

Ook voor het aspect beschikbaarheid wordt vaak het complement gehanteerd. De niet-beschikbaarheid van een systeem is dan de fractie van de tijd dat het systeem ‘down’ is of de kans dat het systeem niet werkt als dat nodig is. Het begrip beschikbaarheid is dimensieloos. Vaak wordt beschikbaarheid in een percentage uitgedrukt, soms in een aantal uren per jaar. In het dagelijkse taalgebruik lopen de begrippen beschikbaarheid en betrouwbaarheid vaak door elkaar. Zo wordt een tunneltechnische veiligheidsinstallatie, of een object als de Maeslantkering veelvuldig ‘betrouwbaar’ genoemd, terwijl het gaat om ‘beschikbaarheid’, namelijk de kans dat de systemen werken als ze nodig zijn.

Het verschil tussen betrouwbaarheid en beschikbaarheid wordt nog eens duidelijk gemaakt in figuur 2.2.

2.5 Geplande versus ongeplande niet-beschikbaarheid

In de vorige paragraaf is de niet-beschikbaarheid gedefinieerd als de fractie van de tijd waarin een systeem niet functioneert, of de kans op niet-functioneren als het systeem op een willekeurig tijdstip wordt aangesproken. De aanleiding voor het niet functioneren van het systeem is geen onderdeel van de definitie, maar wel van groot praktisch belang.

Ongeplande niet-beschikbaarheid die het gevolg is van een storing, wordt als veel ernstiger ervaren dan geplande niet-beschikbaarheid. Ook hebben onverwachte stremmingen een veel grotere (negatieve) invloed op het imago van Rijkswaterstaat dan geplande stremmingen. Voor niet-beschikbaarheid die is gepland en tevoren aangekondigd, is het mogelijk mitigerende maatregelen te nemen, zoals kiezen voor rustige tijden, alternatieven verzorgen, gebruikers informeren over een omrij- of omvaarroute of de transportplanning aanpassen. De schade, die de niet-beschikbaarheid veroorzaakt, is dus bij geplande niet-beschikbaarheid geringer, dan wanneer het niet-functioneren als een verrassing komt. Differentiatie in de eisen is dan ook noodzakelijk. Daar komt bij dat de manier om de verwachte niet-beschikbaarheid te bepalen, afhangt van de aanleiding.

Geplande niet-beschikbaarheid wordt in twee categorieën gesplitst:

- geplande niet-beschikbaarheid wegens inspecties of preventieve onderhoudswerkzaamheden
- geplande niet-beschikbaarheid door niet bedienen van het object. Deze vorm speelt uiteraard alleen bij bediende objecten, zoals beweegbare bruggen en sluizen.

Ook ongeplande niet-beschikbaarheid kent twee verschillende oorzaken:

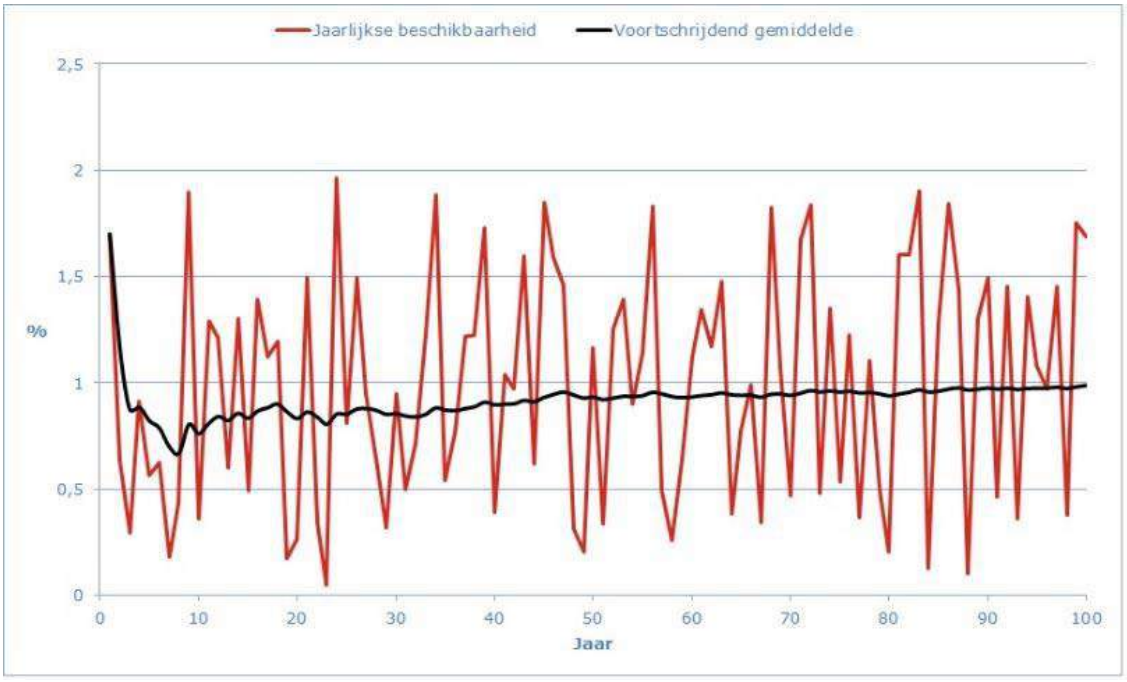
- ongeplande niet-beschikbaarheid door storingen, falen van het object, waarna (correctief) onderhoud nodig is
- ongeplande niet-beschikbaarheid ten gevolge van natuurlijke omstandigheden zoals hoge en lage waterstanden, ijs, wind of mist.

In geval van ongeplande niet-beschikbaarheid kan geen redelijke eis worden gesteld aan de maximaal toelaatbare niet-beschikbaarheid. Immers, de kans op storingen met hele lange herstelduren mag niet geheel worden uitgesloten (met kans 0, dus). Wel kan een eis worden gesteld aan de *gemiddelde* ongeplande niet-beschikbaarheid. Hieronder een figuur (2.3) met een mogelijk verloop van de ongeplande niet-beschikbaarheid, gegeven een verwachting van 1 procent.

Meten achteraf

In sommige gevallen kunnen de prestaties van functies achteraf worden gemeten. Voor het aspect (on)betrouwbaarheid kan dat door te tellen hoe vaak een systeem in een bepaalde periode heeft gefaald. Voor het aspect beschikbaarheid kan het door de fractie van de totale tijd dat een systeem heeft gefunctioneerd te meten, of het aantal keren te tellen dat een systeem heeft gefunctioneerd toen het op een willekeurig tijdstip werd aangesproken. Aan de hand van deze metingen zijn de aannamen te verifiëren die zijn gedaan in het model dat de betrouwbaarheid en beschikbaarheid berekent.

Meten is alleen mogelijk als een systeem of functie werkelijk faalt, zoals bij de niet-beschikbaarheid van een schutsluis. Maar als de kans op falen heel klein is, zoals de kans dat de Maeslantkering niet sluit bij storm of de kans dat de Van Brienenoordbrug bezwijkt, valt er niets te meten. In deze gevallen moet worden uitgegaan van het model dat de verwachte betrouwbaarheid of beschikbaarheid berekent. Uiteraard kan in veel gevallen wel aan deelsystemen worden gemeten, waarmee het model is te verbeteren.



Figuur 2.3. Voorbeeld van actuele, jaarlijkse ongeplande niet-beschikbaarheid (rood) en het voortschrijdende gemiddelde daarvan (zwart). Uitgegaan is van uniform verdeelde niet-beschikbaarheid met grenzen 0 en 2 procent. Het gemiddelde is dus 1 procent.

2.6 Levenscyclus van een systeem

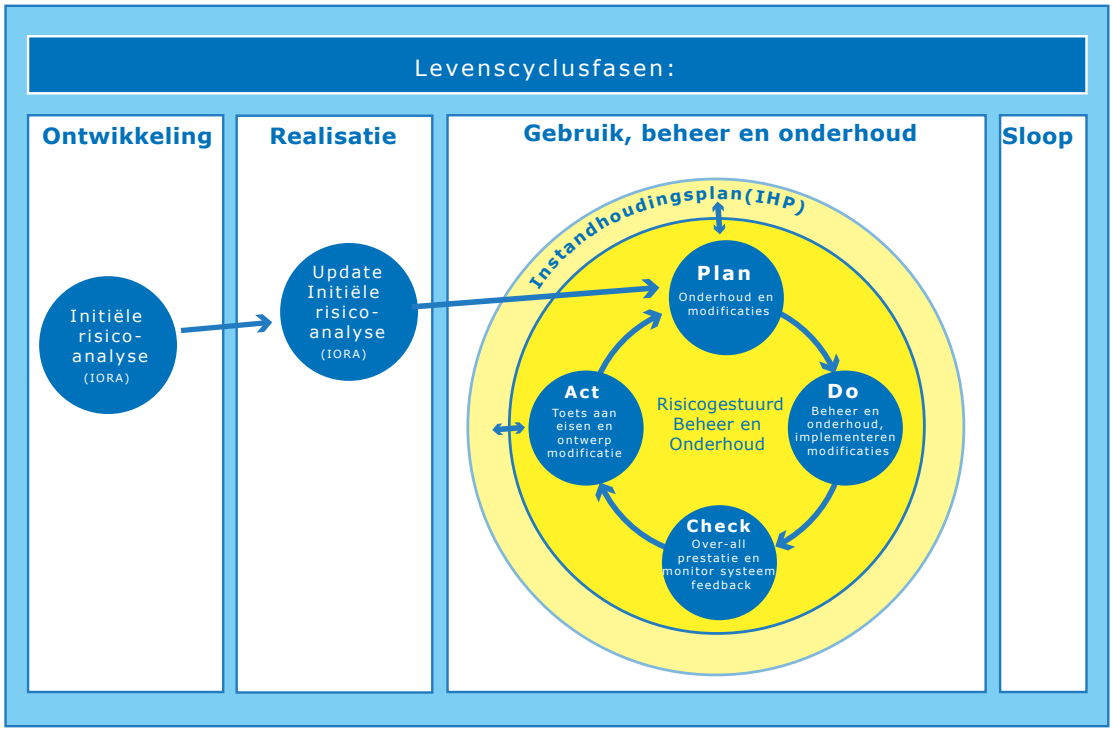
In de levenscyclus van infrastructuur worden vijf fasen onderscheiden [3]:
1) Concept
2) Ontwikkeling
3) Realisatie
4) Gebruik, Beheer en Onderhoud Onderhoud (hieronder vallen ook vervanging en renovatie VenR)
5) Sloop

Figuur 2.4 is een bewerking van het V-model uit de *Leidraad systems engineering*. Links staan de fasen ontwikkeling en realisatie in de levenscyclus. Vervolgens zijn de beheer- en onderhoudsfasen middels een PDCA-cirkel aangegeven tot en met het moment van sloop.

In de ontwikkelfase van het systeem wordt vanaf het begin een risicoanalyse opgebouwd. Zo wordt al bij het ontwerp rekening gehouden met de vereiste betrouwbaarheid en beschikbaarheid. Als de realisatiefase afwijkt van het ontwerp, wordt dat ook tot uiting gebracht in de risicoanalyse, zodat bij de oplevering van het systeem de verwachting van de betrouwbaarheid en de beschikbaarheid is gebaseerd op de juiste gegevens.

Na de realisatiefase volgt de gebruiksfase waarin de beheerder het systeem openstelt voor gebruik en het in stand houdt. Indien mogelijk worden de prestaties van het systeem gemonitord.

Rijkswaterstaat streeft ernaar bij al zijn objecten tijdens de gebruiksfase de PDCA-cirkel te volgen en daarbij voortdurend de prestaties van de objecten, in termen van RAMSSHE€P, te monitoren. Met onderhoud aan of vervanging van deelsystemen kan de beheerder de prestaties van objecten op voldoende niveau houden. Als de functie van het systeem niet meer nodig is, kan het systeem worden gesloopt.



Figuur 2.4. Prestatieborging in de gehele levenscyclus

3 Risicosturing op hoofdlijnen

3.1 Inleiding

De risicosturing op basis van prestatie-eisen aan een object gebeurt aan de hand van een risicoanalyse. Het object en de eisen die daaraan worden gesteld, bepalen de aard en diepgang van de analyse. Deze risicoanalyse wordt een objectrisicoanalyse (ORA) genoemd. Projectrisico's, zoals die bij Rijkswaterstaat worden beheerst met Risicomanagement, vallen buiten de scope van deze handreiking.

Rijkswaterstaat voert de ORA uit voor alle objecten, te beginnen met het kwalitatieve deel en waar nodig uitgebreid met een kwantitatief deel. De kwalitatieve variant beschouwt zowel onverwachte storingen die van grote invloed zijn op de prestatie van de netwerken, als de maatregelen die nodig zijn om de netwerken op langere termijn in stand te houden. Deze variant beperkt zich niet tot de aspecten betrouwbaarheid en beschikbaarheid, maar richt zich expliciet op álle RAMSSHE€P-aspecten van het object. Daarnaast beschouwt de kwalitatieve ORA ook risico's, die weliswaar verwaarloosbaar kunnen zijn op de korte termijn, maar die op den duur uiterst kostbaar kunnen worden, wanneer het standaard verzorgend onderhoud (SVO) niet wordt uitgevoerd. Dit SVO omvat onder meer conserveren, bodembescherming herstellen en lekkages dichten.

Een essentieel verschil tussen de kwalitatieve en de kwantitatieve ORA is dat de kwalitatieve ORA géén uitspraak doet over de verwachte prestatie in termen van betrouwbaarheid en beschikbaarheid van het object. Daarom volstaat de kwalitatieve aanpak alleen bij objecten waarvan de aspecten betrouwbaarheid en (ongeplande) beschikbaarheid een verwaarloosbare invloed hebben op het netwerk. Dat is het geval bij veel onderdelen van de netwerken, zoals lijnobjecten (wegdelen en vaarwegbakken), maar ook vaste bruggen, viaducten en dergelijke objecten. Dit soort objecten kent een klein risico op ongeplande niet-beschikbaarheid. Slechts een beperkte groep objecten heeft wél een bepalende invloed op de prestatie van het netwerk. Voor objecten binnen deze groep wordt dan ook de kwantitatieve variant toegepast (lees meer over deze objecten in paragraaf 3.4). Op de kwalitatieve ORA wordt in hoofdstuk 5 dieper ingegaan.

Het kwantitatieve deel van de ORA richt zich specifiek op de aspecten betrouwbaarheid en/of beschikbaarheid. Deze kan meer of minder nauwkeurig worden uitgevoerd. Kritikaliteit en aard van de objecten bepalen de nauwkeurigheid. De meest nauwkeurige werkwijze is ook bekend onder de verouderde namen 'ProBO volledig' of 'ProBO geavanceerd' Zo'n werkwijze blijkt noodzakelijk om bijvoorbeeld stormvloedkeringen of tunnels aan de wettelijke eisen te laten voldoen. Voor minder kritische objecten is het mogelijk de werkwijze te vereenvoudigen. De risicoanalyse levert een conservatieve inschatting op van de daadwerkelijke prestatie van een object. Dit is essentieel voor de risicosturing.

Doordat - afhankelijk van de aard van de objecten – veel en veelsoortige vereenvoudigingen mogelijk zijn, is in deze handreiking de aparte naamgeving voor verschillende nauwkeurigheidsniveaus bij kwantitatieve risicoanalyses verlaten. Er blijft alleen een principieel verschil tussen de kwalitatieve en de

kwantitatieve risicoanalyse. Op de kwantitatieve ORA wordt in hoofdstuk 6 dieper ingegaan.

In de dagelijkse praktijk van Rijkswaterstaat wordt meestal een driedeling van risicoanalyses gehanteerd:

- IHP

In deze handreiking komt dit overeen met de kwalitatieve risicoanalyse. Daarbij wordt de tool FMECA gebruikt, en wordt voornamelijk toegepast bij vaste kunstwerken en lijnobjecten.

- P-IHP

Dit is een variant die in deze handreiking een kwantitatieve risicoanalyse wordt genoemd, gebaseerd op de RCM-methode. Deze risicoanalyse wordt voornamelijk toegepast bij beheer en onderhoud van de kritische beweegbare objecten en tunnels.

- IHP o.b.v. ProBO

Dit is de meest uitgebreide kwantitatieve risicoanalyse toegepast bij beheer en onderhoud van stormvloedkeringen en de aanleg van tunnels en waterkerende objecten. Hierbij worden foutenbomen gebruikt.

Omdat de P-IHP en IHP op basis van ProBO inhoudelijk veel overlap hebben, worden in deze handreiking deze twee varianten behandeld onder de noemer kwantitatieve risicoanalyse.

Rijkswaterstaat past de kwantitatieve risicoanalyse toe bij de aanleg van een object. Dit biedt namelijk de mogelijkheid om voldoende vertrouwen te krijgen in de kwaliteit waarmee de desbetreffende functie zal worden vervuld. Het is een manier om eisen te stellen aan de kwaliteit van de onderdelen, die de opdrachtnemer ontwerpt, zonder zijn ontwerpvrijheid aan te tasten. Een opdrachtnemer is in principe vrij in zijn ontwerpkeuze. Rijkswaterstaat ontwerpt niet meer zelf, maar dient wel aan te tonen dat het systeem betrouwbaar en/of voldoende beschikbaar zal zijn en (dus) uit deugdelijke componenten wordt samengesteld. In de ontwerpfase is de ORA dus sturend.

Het is niet zinvol om een ORA uit te voeren in een te vroeg (conceptueel) stadium van een ontwerp. De onzekerheid van de uitkomst is dan te groot. Wel is in een vroeg stadium al een uitspraak mogelijk over het verschil in betrouwbaarheid of beschikbaarheid van verschillende alternatieve ontwerpen. Niet de absolute maar de relatieve nauwkeurigheid is dan van belang. Een kwantitatieve ORA aan het eind van de ontwerpfase geeft wél inzicht in de prestatie van het ontwerp in termen van de te verwachten betrouwbaarheid en beschikbaarheid.

Tijdens de gebruiksfase wordt de ORA met een bepaalde regelmaat aangepast aan de actuele toestand. Componenten verouderen, omstandigheden (zoals de mate van belasting) veranderen, er zijn renovaties uitgevoerd et cetera. Dit soort gebeurtenissen beïnvloedt de betrouwbaarheid en/of de beschikbaarheid van het object en daarmee de prestatie van het netwerk. De kwalitatieve ORA geeft dan antwoord op de vraag in welke mate het object nog voldoet aan de gestelde RAMSSHE€P-eisen, terwijl de kwantitatieve ORA aangeeft of het object nog voldoende betrouwbaar en/of beschikbaar is. Mocht het systeem niet meer (redelijk) goed presteren, dan tonen beide delen van de ORA's de zwakke plekken in het systeem en waar efficiënt verbeteringen mogelijk zijn, zodat het systeem weer aan de beloofde prestatie voldoet. De ORA is dus ook in de gebruiksfase sturend.

Belangrijk: de kwantitatieve risicoanalyse berekent een verwachting van de ongeplande niet-beschikbaarheid. Voor het berekenen van deze verwachtingswaarde zijn aannamen nodig met betrekking tot het onderhoud. Deze aannamen bepalen dus mede de geplande niet-beschikbaarheid.

Concluderend: de ORA is de spil van de risicosturing. De volgende paragrafen beschrijven op hoofdlijnen het gebruik van de risicoanalyse voor zowel aanleg als beheer en onderhoud.

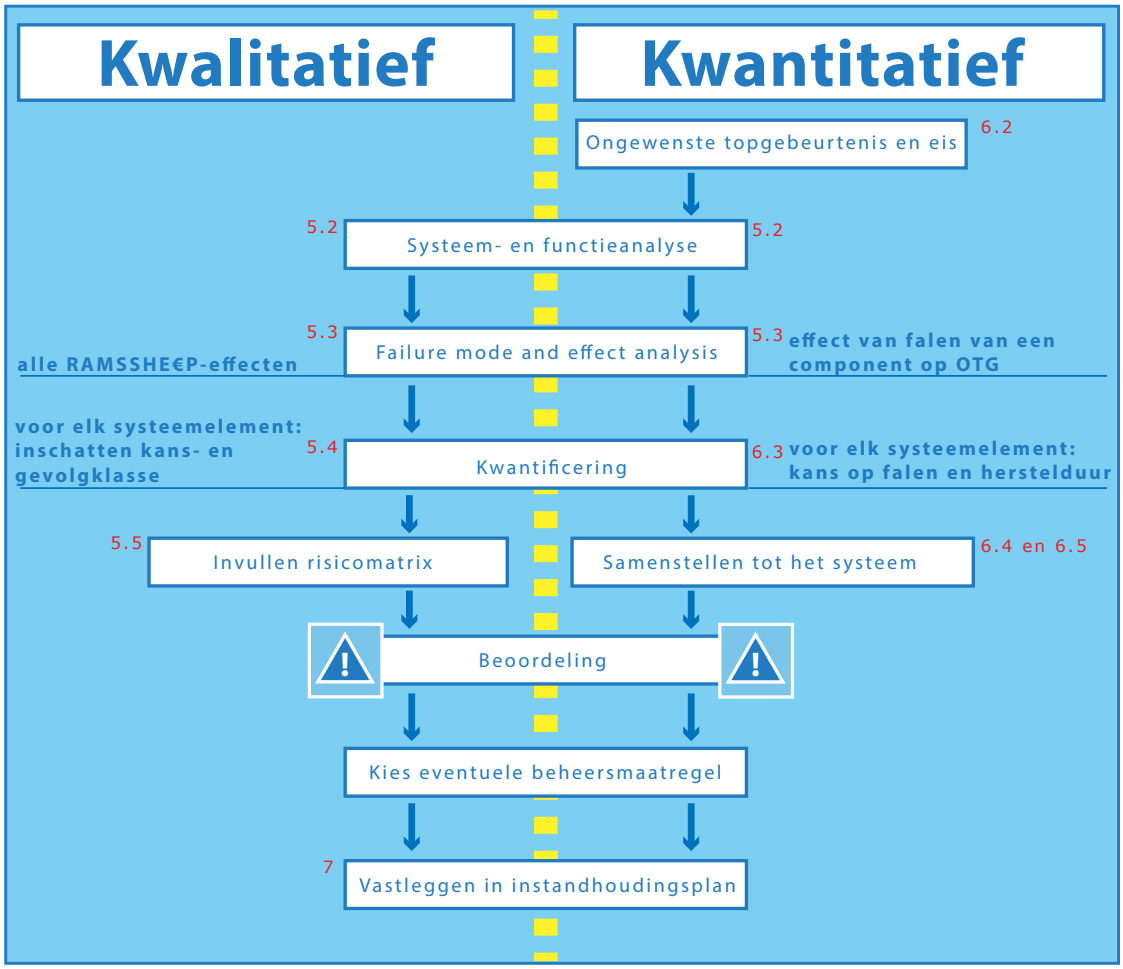
3.2 De risicoanalyse bij aanleg, beheer en onderhoud

De ORA maakt objectief en transparant duidelijk welke risico's, welke elementen (componenten) in welke situaties, het functioneren van het systeem bedreigen. **De kwalitatieve risicoanalyse** van risicogestuurd aanleggen, beheren en onderhouden kent altijd de volgende stappen (zie figuur 3.1):

- systeem- en functieanalyse
- *failure mode and effect analysis*
- inschatten van kans- en gevolgklassen
- invullen van de risicomatrix
- formuleren van maatregelen (afhankelijk van de vorige stap).

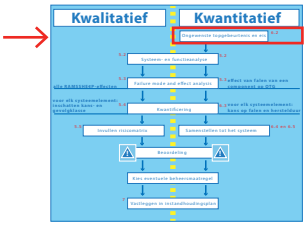
De kwantitatieve risicoanalyse berekent de betrouwbaarheid en/of de (on-) geplande niet-beschikbaarheid en bestaat uit de volgende stappen (zie figuur 3.1):

- bepalen van de ongewenste topgebeurtenis (OTG) en vaststellen van de eis aan de functie
- systeem- en functieanalyse
- *failure mode and effect analysis*
- faaldata bepalen
- samenstellen tot het systeem
- resultaat vergelijken met de eis.



Figuur 3.1. De stappen bij een kwalitatieve en kwantitatieve ORA. De nummers verwijzen naar de paragrafen die dieper op deze stappen ingaan.

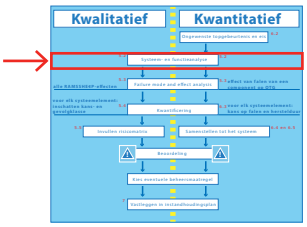
De stappen ‘systeem- en functieanalyse’ en ‘*failure mode and effect analysis*’ (FMEA) zijn in beide risicoanalyses gelijk. De gereedschappen voor de FMEA (gestandaardiseerde spreadsheets) lopen echter uiteen, omdat ook de volgende stap, het (semi-)kwantificeren, onderdeel is van de spreadsheets. De overige onderdelen verschillen. Beide analyses resulteren in een toets om vast te stellen of het systeem voldoet of dat additionele maatregelen nodig zijn.



3.2.1 Het bepalen van de ongewenste topgebeurtenis

De kwantitatieve variant van de ORA begint met het bepalen van de functies waarvoor de risicoanalyse moet worden gemaakt. Dat is nodig omdat een kwantitatieve risicoanalyse altijd betrekking heeft op één functie. Objecten in de infrastructuur hebben soms maar één functie, bijvoorbeeld het keren van hoog water (stormvloedkering), of het overbruggen van een waterstandsverschil (schutsluis), of het omhoogpompen van water (gemaal). Vaak heeft een object meerdere functies. Een schutsluis kan behalve de functie ‘overbruggen waterstandsverschil’ ook de functie ‘hoogwater keren’ hebben. De betrouwbaarheid of beschikbaarheid van elke functie apart wordt berekend en getoetst aan de eis die voor die ene functie geldt. Als een object twee belangrijke functies vervult, waarvoor (dus) twee eisen gelden, zijn twee risicoanalyses noodzakelijk. Het falen van de functie wordt de ongewenste topgebeurtenis (OTG) genoemd en in feite berekent de ORA de kans op de OTG.

Voor de kwalitatieve variant van de ORA is deze eerste stap niet nodig. Deze variant beschouwt alle elementen van het systeem, ongeacht aan welke functie zij een bijdrage leveren. Door daarbij ook álle aspecten van RAMSSHE€P te betrekken, kijkt de kwalitatieve variant niet alleen naar het falen van de primaire functie van het systeem, maar ook naar de effecten (de gevolgen) van falen van (elementen van) het systeem.



3.2.2 Systeem- en functieanalyse

De systeem- en functieanalyse heeft tot doel een beschrijving te bieden van wat het systeem (object) is en welke deelfunctie(s) de subsystemen van het systeem moeten kunnen vervullen. De volgende vragen zijn daarbij aan de orde:

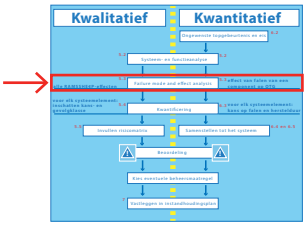
- Hoe functioneert het systeem?
- Welke subsystemen spelen daarin een rol?
- Wat zijn de functies van de desbetreffende subsystemen?

De producten van de systeembeschouwing zijn:

- een systeembeschrijving
- de fysieke decompositie
- soms een functionele decompositie.

Het systeem moet met een brede scope worden bezien. Alle elementen die bijdragen aan de functie(s) van het systeem moeten in kaart worden gebracht. Hieronder wordt verstaan hardware, software, menselijk handelen, externe gebeurtenissen en relevante processen.

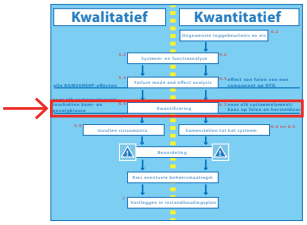
Dit is een van de redenen waarom het belangrijk is de systeemgrenzen zorgvuldig te bepalen, af te wegen en vast te leggen.



3.2.3 Failure mode and effect analysis

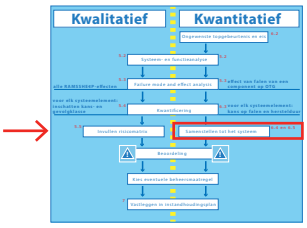
De *failure mode and effect analysis* (FMEA) is een techniek om alle mogelijke afwijkingen van het functioneren van elementen van het systeem te bepalen en de gevolgen van het falen van die elementen voor het systeem vast te leggen. Dit gebeurt op een gestandaardiseerde manier, aan de hand van de resultaten uit de vorige stap.

De kwantitatieve analyse beschouwt alleen het effect van falen van een component op de OTG (falen van de beschouwde functie), de kwalitatieve analyse schat álle RAMSSHE€P-effecten in. Ook het begrip 'component' moet breed worden opgevat: dus naast hardware zijn ook software en menselijk handelen componenten van het systeem.
Tevens worden in deze fase de externe gebeurtenissen geïnventariseerd waarvan de oorzaak weliswaar buiten het systeem ligt, maar die toch het falen van het systeem kunnen veroorzaken. Aanvaring en blikseminslag zijn hiervan typische voorbeelden.



3.2.4 Kwantificering: faaldata bepalen en kans-/gevolgklasse schatten

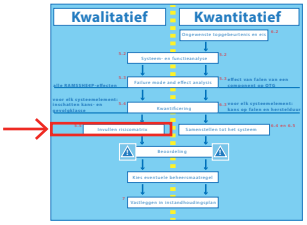
Bij een kwantitatieve analyse wordt voor elk element van het systeem de kans op falen (soms als functie van de tijd) en de herstelduur ingeschat. Bij een kwalitatieve analyse gaat het – eveneens voor elk element – om de inschatting van de kans op falen in een *kansklasse* en het gevolg ervan in een *gevolgklasse.* Indien bij de screening externe gebeurtenissen van toepassing worden verklaard, worden die in deze stap ook meegenomen.



3.2.5 Van element naar systeem

De resultaten van een kwantitatieve analyse van alle afzonderlijke elementen worden samengesteld tot één beeld van de betrouwbaarheid en/of de beschikbaarheid van de gevraagde functie van het systeem. Doordat met een niet in de tijd variërende faalkans wordt gerekend, geeft deze aanpak de verwachte betrouwbaarheid en/of beschikbaarheid voor de korte termijn.

Bij gecompliceerdere vormen kan de foutenboomtechniek worden gebruikt, soms in combinatie met de gebeurtenissenboomtechniek. Bij de meer eenvoudige varianten van de analyse (bijvoorbeeld bij *Reliability Centered Maintenance*, RCM) bestaat de samenstelling uit een optelling.



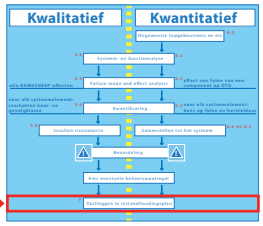
3.2.6 Risicomatrix vullen

Bij de kwalitatieve analyse worden de resultaten uit de vorige stap (de kwantificering) ingevuld in een risicomatrix, zie figuur 3.2. Maatregelen ter verbetering hangen af van de positie in de risicomatrix. Uitgangspunt is dat risico's in het rode gebied direct moeten worden weggenomen door maatregelen. Van risico's in het gele gebied moet worden nagegaan hoe snel ze moeten worden aangepakt (een en ander is afhankelijk van de aard en kritikaliteit van het object) en risico's in het groene gebied zijn acceptabel.

Bij een kwantitatieve analyse wordt de berekende betrouwbaarheid en/of beschikbaarheid getoetst aan de gestelde eis. Blijkt de score onvoldoende, dan moet het systeem worden verbeterd. De ORA geeft een overzicht van de zwakke plekken, ofwel de elementen van het systeem die belangrijk bijdragen aan de onbetrouwbaarheid of de niet-beschikbaarheid.

RISICOMATRIX		GEVOLG			
		1: VERWAAR-LOOSBAAR	2: BEPERKT	3: GROOT	4: ERNSTIG
KANS	1: VERWAARLOOSBAAR	Acceptabel	Acceptabel	Acceptabel	Acceptabel
	2: KLEIN	Acceptabel	Acceptabel	Ongewenst	Ongewenst
	3: GEMIDDELD	Acceptabel	Ongewenst	Ongewenst	Ongewenst
	4: GROOT	Acceptabel	Ongewenst	Ongewenst	Onacceptabel
	5: ZEKER	Ongewenst	Ongewenst	Onacceptabel	Onacceptabel

Figuur 3.2. De risicomatrix



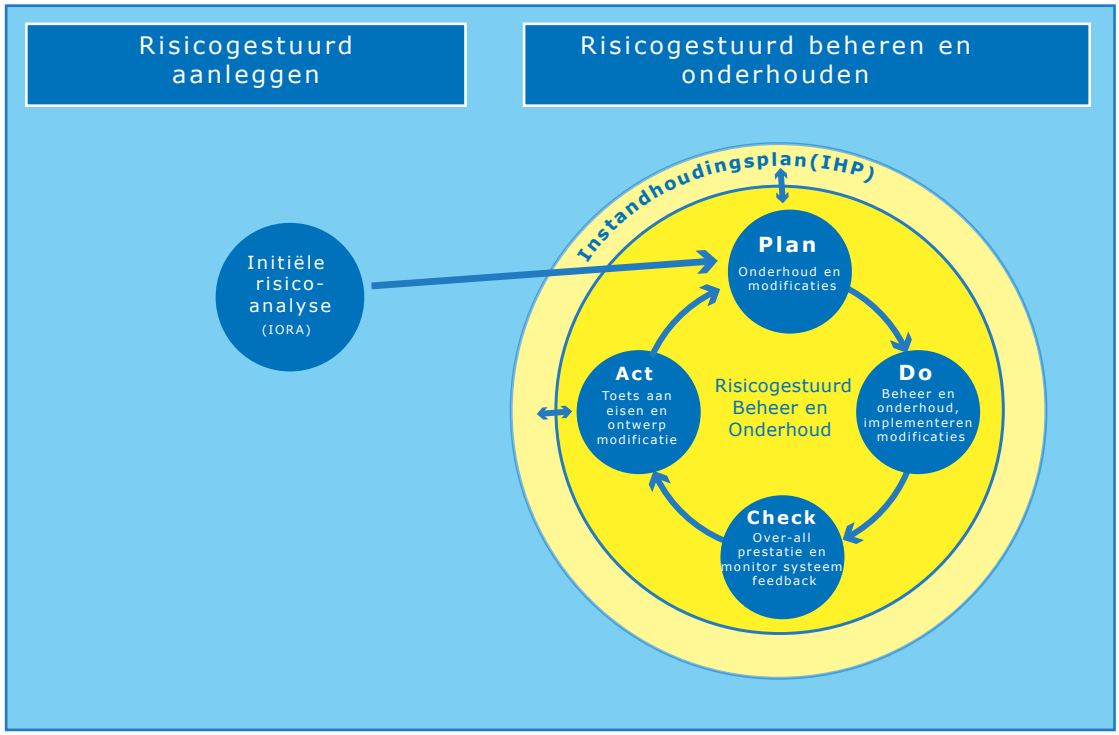
3.2.7 Vastleggen in het instandhoudingsplan

Uit de ORA volgen, naast de mogelijk te nemen maatregelen, een aantal randvoorwaarden betreffende het onderhoud, die nodig zijn om kansen en risico's te kunnen berekenen. Deze aannamen moeten aantoonbaar worden geborgd. Alleen dan is de risicoanalyse valide en is de verwachte prestatie correct. Het borgen dat dit onderhoud ook werkelijk wordt uitgevoerd, gebeurt door de randvoorwaarden en de check op de uitvoering vast te leggen in het instandhoudingsplan. De randvoorwaarden die volgen uit de kwalitatieve analyse worden vastgelegd in een (kwalitatief) IHP. De randvoorwaarden uit de kwantitatieve analyse worden opgeslagen in het p-IHP en de randvoorwaarden uit de meest nauwkeurige kwantitatieve analyse in een IHP o.b.v. ProBO.

Het preventieve onderhoud, dat nodig is om de prestatie van de elementen van het systeem te verzekeren, kan leiden tot geplande niet-beschikbaarheid. De ongeplande niet-beschikbaarheid en een deel van de geplande niet-beschikbaarheid volgen dus beide uit de ORA.

3.3 Het actualiseren van de risicoanalyse

De sturing op basis van de prestatie van een object staat centraal. Dat betekent dat niet alleen bij oplevering van een object de verwachte prestatie bekend moet zijn, maar ook dat deze op elk gewenst moment aantoonbaar deel uitmaakt van beslissingen die te maken hebben met het beheer van het object.
Rijkswaterstaat voert risicogestuurd beheer en onderhoud uit volgens de PDCA-cyclus (plan, do, check, act). Zoals in de inleiding van dit hoofdstuk is beschreven, is voor elk object een initiële risicoanalyse nodig. Vanuit de ORA worden acties geformuleerd die in het instandhoudingsplan komen (*plan*). Het uitvoeren van de activiteiten uit het instandhoudingsplan (*do*) zorgt ervoor dat het object voldoet aan de vooraf bepaalde prestatie. In het gebruik dient de werkelijke prestatie van zowel het object als de uitgevoerde maatregelen te worden gemeten (*check*).
De resultaten hiervan worden vervolgens verwerkt in de ORA (*act*), waarna het instandhoudingsplan wordt aangepast en de PDCA-cyclus zich herhaalt. In figuur 3.3 is dit proces grafisch weergegeven. Hoofdstuk 8 gaat dieper in op deze PDCA-cyclus.



Figuur 3.3. De initiële ORA bij aanleg en de PDCA-cirkel bij beheer en onderhoud

3.4 Wanneer een kwantitatieve risicoanalyse?

In het voorgaande is geschetst dat Rijkswaterstaat twee verschillende objectrisicoanalyses hanteert, de kwantitatieve variant en de kwalitatieve (semi-kwantitatieve) variant, die altijd wordt toegepast in de gebruiksfase.
Van alle objecten dient een kwalitatieve risicoanalyse te worden gemaakt. Soms is het nodig om aanvullend een kwantitatieve risicoanalyse te maken.
De keuze voor de kwantitatieve risicoanalyse is afhankelijk van de eisen aan het desbetreffende object. Als de eis kwantitatief is, zal een kwantitatieve risicoanalyse nodig zijn. Voorbeelden hiervan zijn eisen aan de waterkeringen, die volgen uit de *Waterwet*. Maar ook als aan de betrouwbaarheid of beschikbaarheid van een object geen (wettelijke) kwantitatieve eisen worden gesteld, kan een kwantitatieve risicoanalyse wenselijk zijn. Dit is het geval bij alle objecten die kritisch bijdragen aan de functionaliteit van de netwerken. Dit zijn vrijwel alle objecten die relatief vaak falen én waarvan het falen een grote impact heeft op het functioneren van de infrastructuur als geheel. Denk aan de grote beweegbare bruggen in het hoofdwegennet, de schutsluizen in het hoofdvaarwegennet en aan de tunnels die Rijkswaterstaat in beheer heeft. Deze objecten functioneren door een complex samenstel van werktuigbouwkundige, hydraulische, elektrotechnische en softwarematige deelsystemen, in combinatie met menselijk handelen.

Zuiver statische objecten, zoals een vaste brug of viaduct, oevers, bodems en geluidwerende voorzieningen, falen vrijwel nooit onverwacht. Voor deze objecten volstaat een kwalitatieve ORA, met relatief eenvoudige invulling van kans(en) en gevolgen van risico’s en gebaseerd op generieke uitgangspunten en inspecties.

Het bestuur van Rijkswaterstaat heeft, met deze gedachte als uitgangspunt, bepaald welke objecten op basis van een kwantitatieve ORA moeten worden beheerd en onderhouden [1], middels een p-IHP of IHP o.b.v. ProBO. Een afweging aan de hand van een afwegingskader, is daardoor niet meer nodig.

4 Prestatie-eisen aan objecten

4.1 Inleiding

In hoofdstuk 2 is gesteld dat de minister van Infrastructuur en Waterstaat door middel van SLA's afspraken maakt met Rijkswaterstaat over de prestaties van de drie netwerken. De mate waarin de netwerken presteren is onder meer afhankelijk van de betrouwbaarheid en de beschikbaarheid van de onderdelen van deze netwerken. Maar de prestatie van een netwerk is niet goed uit te drukken in alléén de betrouwbaarheid en de beschikbaarheid van de onderdelen. Ook de kwaliteit van het verkeers- en watermanagement, het incidentmanagement en de capaciteit speelt een belangrijke rol. De registratie van *gelabelde voer- en vaartuigverliesuren* (vvu's) biedt wellicht meer mogelijkheden om het effect van verkeers- en watermanagement, incidentmanagement en capaciteitstekort te kwantificeren.

Als een onderdeel (object) van een netwerk niet beschikbaar is, hangt het effect daarvan op de prestatie van het netwerk af van de belangrijkheid van het object in het netwerk. Die belangrijkheid wordt bepaald door het aantal en het type vaar- of voertuigen die van het object gebruikmaken, en van de beschikbaarheid van alternatieven voor omrijden of omvaren, maar ook van de redundantie in het netwerk. Rijkswaterstaat maakt dan ook onderscheid tussen hoofd- en gewone transportassen, tussen routes waarlangs wél of niet gevaarlijke stoffen mogen worden vervoerd, en meer van dergelijke opties. Dit zijn voorbeelden uit de beide transportnetwerken, maar in een iets andere vorm maakt Rijkswaterstaat een dergelijk onderscheid ook voor het HWS.

Omdat de beschikbaarheid en betrouwbaarheid van een object maar gedeeltelijk de prestatie van het hele netwerk bepalen, is het (nu nog) niet mogelijk om een directe vertaling te maken van de afspraken in de SLA's naar een eis aan de betrouwbaarheid of beschikbaarheid van een object. Op dit moment wordt onderzocht of dat via een methode gebaseerd op voer- en vaartuigverliesuren wél kan. De betekenis van een object voor het netwerk wordt in ieder geval beter tot uitdrukking gebracht.

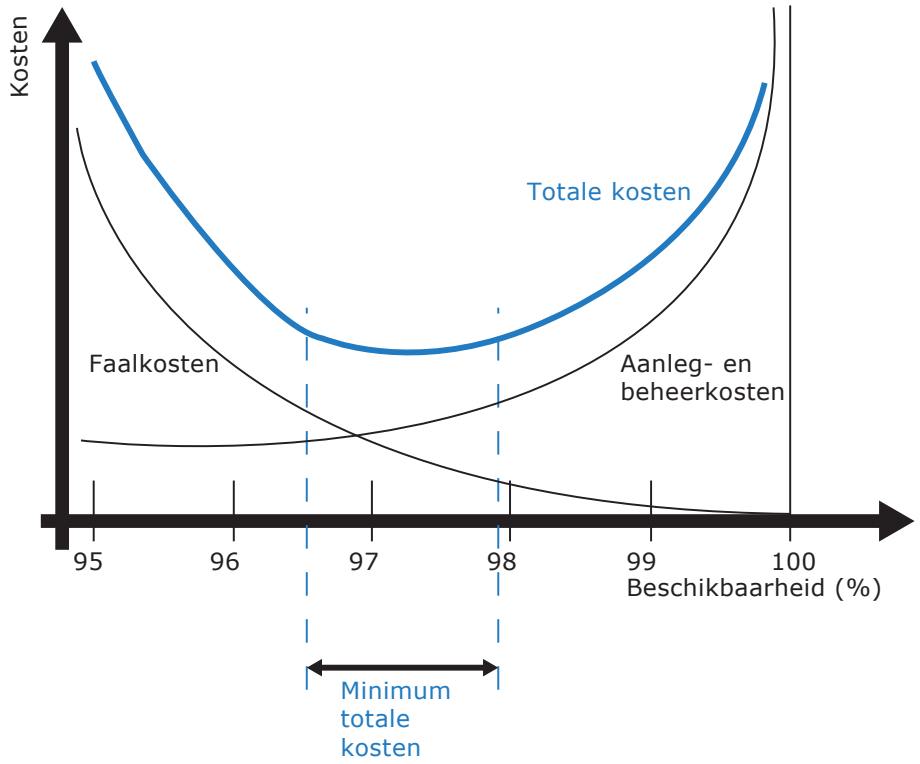
4.2 Methoden voor eisen

Zolang een directe, kwantitatieve relatie met de SLA's niet is te maken, moeten andere manieren worden gehanteerd om recht te doen aan de geest van de SLA's: strenge eisen aan belangrijke objecten en minder strenge eisen aan minder belangrijke objecten. Voor het opstellen van deze betrouwbaarheids- of beschikbaarheidseis (R/A) is een aantal methoden voorhanden.

4.2.1 Economische optimalisatie

De meest rationele manier om een R-/A-eis op te stellen is om met behulp van een maatschappelijke kosten-batenanalyse (MKBA) het evenwicht te zoeken tussen de schade die wordt ondervonden door de niet-beschikbaarheid van het object en de (life cycle) kosten die het vergt om de gewenste beschikbaarheid te realiseren. De schade (faalkosten) wordt gevormd door de directe kosten van de herstelacties en de maatschappelijke schade. Ingeval van het falen

van transportnetwerken van Rijkswaterstaat kan dan worden gedacht aan het kapitaliseren van vaar- en voertuigverliesuren. In figuur 4.1 is deze gedachte grafisch weergegeven.



Figuur 4.1 Economische optimalisatie

Naarmate de (verwachte) beschikbaarheid toeneemt, dalen de faalkosten, tot 0 euro in de denkbeeldige, maar onhaalbare toestand van 100 procent beschikbaarheid. De kosten om deze beschikbaarheid te bereiken nemen echter exponentieel toe. De totale kosten (die overigens niet door één partij hoeven te worden gedragen), zijn de som van beide. Omdat de twee kostenposten tegengesteld aan elkaar toenemen, is voor de totale kosten altijd een minimum te vinden. Meestal is dit een vlak minimum, in het voorbeeld tussen de 96,5 en 98 procent.

De procedure van economische optimalisatie levert dus een basis voor de eis aan het object (het systeemelement van het netwerk). Deze procedure is illustratief en transparant, maar ook kostbaar en specifiek voor het desbetreffende object. Ook is het resultaat niet goed te generaliseren naar vergelijkbare objecten, omdat de faalkosten afhankelijk zijn van de betekenis van het object voor het netwerk.

Een meer concrete uitwerking van deze aanpak voor de functie schutten van een sluis is gegeven in [6]. Uit de bijbehorende, realistische casestudie werd gevonden dat een eis van (ten hoogste) 1 à 1,5 procent ongeplande niet-beschikbaarheid voor de schutfunctie economisch optimaal was.

4.2.2 Eisen volgend uit wet- en regelgeving

Als R-/A-eisen voortvloeien uit wet- of regelgeving is alles veel eenvoudiger. Dat is bijvoorbeeld het geval voor de (natte) kunstwerken in (primaire) waterkeringen waarvoor de *Waterwet* eisen dicteert, voor wat de functie 'keren hoogwater' betreft.

Er zijn meer wettelijke kaders die een bron vormen voor eisen aan objecten. Zo stelt de *Woningwet*, via het *Bouwbesluit* en de Eurocodes, betrouwbaarheidseisen aan bouwwerken in relatie tot de functie 'belastingen weerstaan' (dat zijn dus eisen aan de sterkte). En in de *Landelijke tunnelstandaard* [7] worden expliciet eisen gesteld aan de betrouwbaarheid en beschikbaarheid van tunnelsystemen van Rijkswaterstaat. Zo stelt deze standaard voor de functie 'volledig doorstromen' een beschikbaarheidseis van 93 procent. Gedurende 5 procent van de tijd mag de tunnel slechts beperkt beschikbaar zijn (beperkte doorstroming) en de overige 2 procent mag de tunnel geheel buiten gebruik zijn (geen doorstroming). Hiermee is de tunnel dus (gemiddeld) 98 procent van de tijd beschikbaar voor de weggebruiker, waarvan maximaal 5 procent met beperkte doorstroming. Ook aan de frequenties van storingen (ongepland onderhoud) stelt de Landelijke tunnelstandaard eisen. Het mag bijvoorbeeld maar gemiddeld één keer per jaar gebeuren dat als gevolg van een storing de hele tunnel moet worden gestremd (gebaseerd op vigerende versie Landelijke tunnelstandaard 2016).

4.2.3 Eisen volgend uit het verleden

Prestaties die in het verleden door objecten zijn geleverd, kunnen een basis vormen voor het opstellen van eisen bij grootschalige renovaties of voor eisen aan nieuw te bouwen vergelijkbare objecten. Dat geldt ook voor prestaties in het verleden die niet voldoende werden bevonden. Deze kunnen helpen bij het formuleren van een scherpere eis.

Hierbij past echter de kanttekening dat de perceptie van de betrouwbaarheid en beschikbaarheid van een bestaand object veelal in positieve zin afwijkt van de feitelijke betrouwbaarheid en beschikbaarheid en, in nog sterkere mate, van de berekende betrouwbaarheid en/of beschikbaarheid. Dit komt doordat kleine storingen soms onbelangrijk worden geacht (vooral in het HVWN en het HWS) en grote storingen maar heel sporadisch voorkomen. Maar beide type storingen zijn wel onderdeel van de risicoanalyse. Ook het werken met oude faalgegevens maakt de risicoanalyse meestal pessimistischer (conservatiever) dan de 'werkelijkheid' zoals die wordt ervaren.

4.2.4 Eisen volgend uit een referentieontwerp

Als voor een aanbesteding een referentieontwerp wordt gemaakt, levert een risicoanalyse van dat ontwerp realistische eisen voor het te bouwen object. In dat geval kan ook worden bestudeerd wat de meerkosten zijn die strengere eisen met zich meebrengen en hoeveel er mogelijk kan worden bespaard door minder strenge eisen te stellen. De economische optimalisatie, zoals beschreven in paragraaf 4.2.1, komt dan onder handbereik. Als variant hierop kan worden gekeken naar bestaande, vergelijkbare objecten. Welke eisen zijn daaraan gesteld? En zijn die overdraagbaar?

4.3 Afsluitende opmerkingen

In het algemeen geldt dat uitbreiding van de geplande niet-beschikbaarheid de ongeplande niet-beschikbaarheid doet afnemen, en vice versa. Bij een strenge eis omtrent de ongeplande niet-beschikbaarheid hoort dus een ruime eis voor de geplande niet-beschikbaarheid. Maar zo'n situatie is ook duurder dan zijn tegenpool: weinig gepland onderhoud en veel ongeplande niet-beschikbaarheid, althans als de faalkosten niet in rekening worden gebracht. Het is dus zaak evenwichtig te specificeren.

Soms is het zinvol om zowel aan de betrouwbaarheid als aan de beschikbaarheid een eis te stellen. Dat voorkomt dat systemen die weinig falen erg lange hersteltijd nodig hebben wanneer ze falen. Of andersom, dat systemen frequent falen met korte herstelduren. De tweede optie is gewenst in situaties waarin zich wachtrijen kunnen opbouwen, zoals bij tunnels of beweegbare bruggen. Het totaal van vele korte onderbrekingen is minder ernstig dan één heel lange onderbreking, doordat bij een lange onderbreking de wachttijden kwadratisch toenemen.

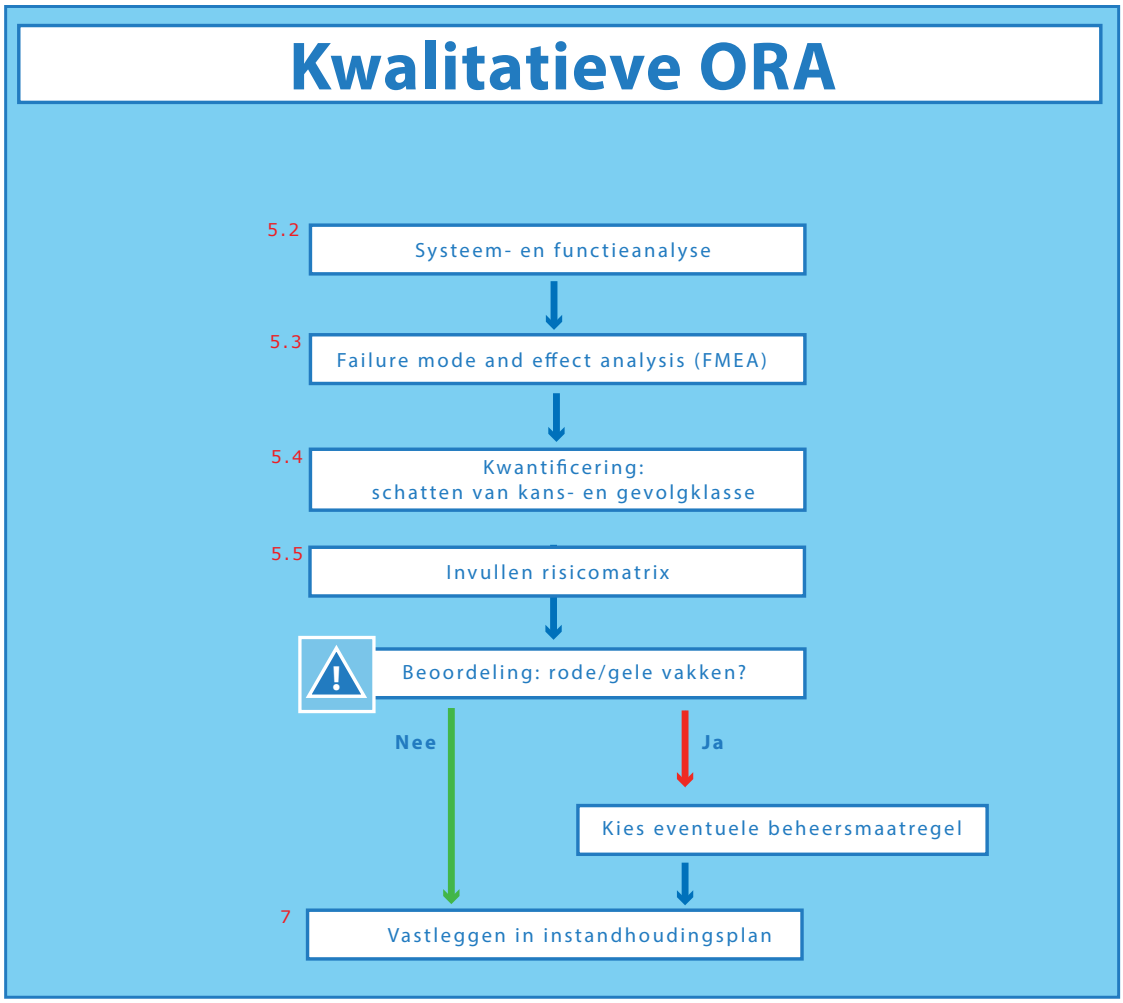
Het is van belang dat eisen aan functies en systemen realistisch zijn. Als deze eisen nog niet goed zijn vastgelegd, dan moet dat gebeuren in het instandhoudingsplan van dat object. De systemen moeten maakbaar en onderhoudbaar zijn. Zoals in paragraaf 4.2.3 al is aangegeven, lopen perceptie, statistiek en berekening uiteen. Als de eis door berekening wordt geverifieerd (een kwantitatieve eis dus), moet daarmee rekening worden gehouden.
Ook een eis aan ongepland onderhoud moet op realisme zijn gestoeld. Het is bijvoorbeeld niet mogelijk een eis te stellen aan de maximale duur. De risicoanalyse berekent weliswaar de gemiddelde niet-beschikbaarheid, maar het precieze tijdstip en hoe lang het herstel zal duren, is niet te voorspellen.

5 De kwalitatieve objectrisicoanalyse

5.1 Inleiding

In de voorgaande hoofdstukken is een beeld geschetst van de kenmerken en toepassingen van de kwalitatieve en de kwantitatieve variant van de objectrisicoanalyse (ORA). Dit hoofdstuk gaat dieper in op de **kwalitatieve objectrisicoanalyse**. In de onderstaande figuur verwijzen de nummers bij de opeenvolgende processtappen naar de paragrafen waarin deze worden behandeld.

Dit hoofdstuk maakt gebruik van het format FMECA van de eenvoudige objectrisicoanalyse versie 2.1.1 uit de WW RWS nummer 1560. Voor de meest recente versie daarvan inclusief de werkwijzer wordt naar WW RWS verwezen.



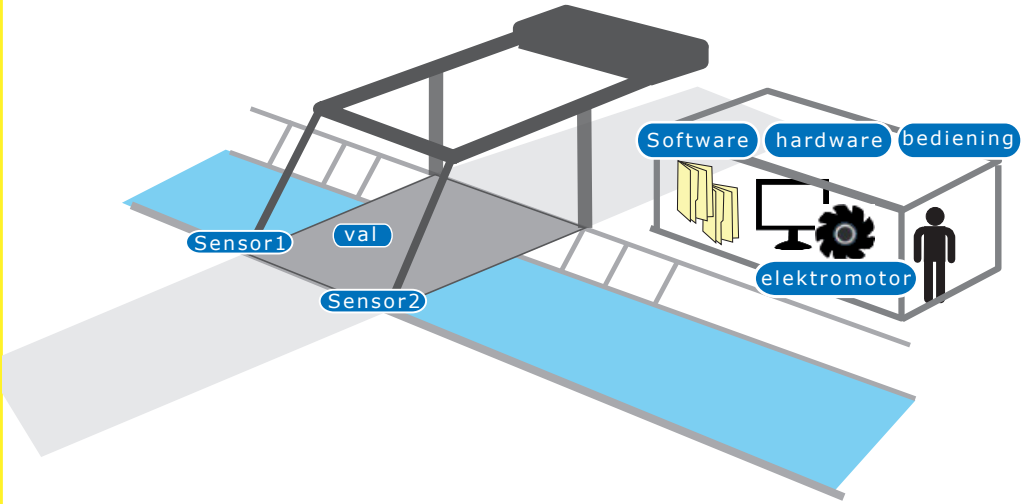
Figuur 5.1. Stappen in de kwalitatieve ORA

In onderstaande beschrijvingen zijn de opeenvolgende stappen geïllustreerd aan de hand van een beweegbare brug. De beweegbare brug zal als voorbeeld dienen voor de komende hoofdstukken.

Voorbeeld: een ophaalbrug

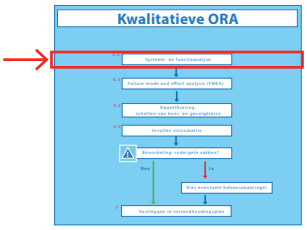
De focus ligt in dit voorbeeld van een beweegbare brug op het aspect niet-beschikbaarheid. Het bepalen van de betrouwbaarheid verloopt op een vergelijkbare wijze.

De beweegbare brug is van het type 'ophaalbrug', die bestaat uit een val (het beweegbare brugdek), een bewegingswerk waarvan voor de eenvoud alleen de elektromotor wordt beschouwd, een bediengebouw met daarin een bedienaar, een computer met besturingssoftware en twee sensoren, die beiden aangeven of het brugdek na een brugopening in zijn ruststand is gekomen. Zie figuur 5.2.



Figuur 5.2: Ophaalbrug

De brug overspant als onderdeel van een autosnelweg een lokale vaarweg. In rust maakt de brug landverkeer mogelijk, in geopende toestand verkeer over water, dat te hoog is om te kunnen passeren tijdens de ruststand. Wanneer de brug moet worden geopend, zorgt de bedienaar er volgens een voorgeschreven procedure voor dat de brug verkeersvrij is. Vervolgens stelt hij veelal middels hardware (computer) en speciale software (besturingssysteem) het bewegingswerk (elektromotor) in werking. Het bewegingswerk opent de brug. Bij het sluiten van de brug test het besturingssysteem via de beide sensoren of het brugdek weer in de positie is om landverkeer toe te laten. Het mechanisme is redundant uitgevoerd: bij het falen van één sensor kan worden vertrouwd op de andere. Pas als het besturingssysteem aangeeft dat het val in de juiste positie is, kan de bedienaar de autosnelweg weer vrijgeven.



5.2 Processtap: systeem- en functieanalyse

Risicogestuurd aanleggen, beheren en onderhouden vraagt om een functionele benadering, waarbij naast functionele eisen ook prestatie-eisen worden gesteld op basis van alle RAMSSHE€P-termen. Voorafgaand aan de initiële ORA is een goede beschrijving van het object noodzakelijk in termen van systems engineering. Deze systeem- en functiebeschrijving is belangrijk om de werking van het systeem te kennen. Bij complexe objecten is een functionele decompositie aan te bevelen, die definities geeft van verschillende deelfuncties.

Een object heeft één (of meerdere) primaire functie(s). Een (beweegbare) waterkering beschermt het achterland tegen hoogwater. Is de waterkering beweegbaar, dan kan een tweede primaire functie zijn het laten passeren van schepen. Een stuw helpt het waterpeil in een rivier beheersen. Een tunnel is bedoeld om van A naar B te komen en daarmee het wegverkeer te laten doorstromen, bijvoorbeeld bij het kruisen van een (water)weg. Een corridor van stuwen en sluizen in een waterweg combineert een primaire functie voor het waterbeheer met de functie 'transport van waterverkeer'.

Naast primaire functie(s) heeft een object meestal meerdere nevenfuncties, zoals bijvoorbeeld het realiseren van een ecologische verbinding bij een kering door fauna te laten passeren. Om de gewenste prestaties van een object goed te kunnen beschouwen, kan het noodzakelijk zijn om de primaire functies op te splitsen in deelfuncties. Zo is de primaire functie van een beweegbare waterkering onder te verdelen in sluiten en keren. Het openen van een kering is een belangrijke functionaliteit om de functie van de waterweg te herstellen (scheepvaart en/of afvoer van water).

Tot slot nog een kanttekening bij het begrip veiligheid, dat vaak wordt gezien als primaire functie. Dat is correct als het gaat om een beweegbare waterkering die primair een veiligheidsfunctie heeft. Bij de meeste andere objecten is veiligheid weliswaar belangrijk, maar geen functie. Een tunnel bijvoorbeeld heeft niet als functie de veiligheid te bevorderen. In de terminologie van systems engineering is veiligheid een aspecteis. Toegepast op een tunnel betekent dit dat het wegverkeer op een veilige manier doorstroomt. De primaire functie van een tunnel is doorstroming onder de randvoorwaarde (aspecteis) dat dit veilig gebeurt. Het aspect veiligheid stelt dan extra eisen aan het systeem.

Systeem- en functiebeschrijving

Een systeem- en functiebeschrijving geeft op overzichtelijke wijze weer:

- hoe het systeem functioneert
- welke subsystemen daarin een rol spelen
- wat de functies zijn van de subsystemen.

Voor bestaande objecten wordt een systeem- en functiebeschrijving bij voorkeur gemaakt aan de hand van beschikbare ontwerp- en *as-built*-gegevens. Deze beschrijving bestaat gewoonlijk uit teksten en schema's, die de opbouw van het systeem overzichtelijk weergeven.
Voor (nog) niet bestaande objecten worden de ontwerpdocumenten gehanteerd. Zie ook [3] en [8].

De systeembeschrijving moet zó in elkaar zitten, dat het mogelijk is om de werking van het systeem en de functies van de elementen ervan volledig te doorgronden. Elementen kunnen hardwarecomponenten, softwaremodulen en menselijk handelen zijn. De term 'componenten' heeft in deze handreiking betrekking op hardwarecomponenten.

Om een risicoanalyse te kunnen maken, moeten de systeemgrenzen van het object duidelijk worden vastgelegd. Voorts is het belangrijk dat de beheerder weet waarvoor het object – in samenhang met andere objecten – is bedoeld. De beschrijving van het systeem moet – conform de systems engineeringaanpak – objectief en volledig informatie geven over de functie(s) van het systeem. Het maakt immers nogal verschil of bijvoorbeeld een stuw binnen 1 of 4 uur moet kunnen worden gestreken. In de systeem- en functiebeschrijving moeten de succescriteria zo worden geformuleerd dat ze meetbaar zijn. Deze criteria zijn immers gerelateerd aan de faalcriteria, die op hun beurt zijn verbonden aan de prestatie-eisen.

Systeemdecompositie

Door objecten en functies te decomponeren en als losse onderdelen te koppelen, ontstaan zichtbare relaties tussen de functies en de fysieke delen van het object. Deze relaties zijn essentieel voor de risicoanalyse, want de samenhang in het falen van onderdelen moet worden vertaald naar mogelijk falen van de functie van het object.

Voor de decompositie van het object is het uitgangspunt dat dit gebeurt volgens een *system breakdown structure* (SBS) met behulp van de NEN 2767-4. Cruciaal daarbij is een eenduidige weergave van de fysieke samenhang van de onderdelen binnen het gehele object. Van elk SBS-element moet de functie zijn gedefinieerd. De functionele samenhang tussen de verschillende SBS-elementen is weer te geven door middel van blokdiagrammen of blokschema's, waarmee tevens globaal de samenstelling en werking in beeld worden gebracht. Ook de in- en uitvoer van de verschillende blokken moet duidelijk zijn, met speciale aandacht voor de koppelingen tussen verschillende blokschema's (interfaces van het systeem).

Zeker bij meer complexe systemen is het belangrijk de relatie tussen de systeemdelen en functies goed in kaart te brengen. Hierbij ontstaat een matrix, met op de ene as een onderverdeling in systeemdelen (tot op systeemelementniveau) en op de andere as een onderverdeling in deelfuncties. De decompositie is geen doel op zich, maar een hulpmiddel en goede basis om te komen tot een risicoanalyse en een integrale beschouwing van het gehele beheer en onderhoud (B&O). Dit maakt optimalisaties in het B&O-proces mogelijk.

Decompositieniveau

Op de vraag tot op welk detailniveau een decompositie moet worden uitgevoerd, luidt het algemene antwoord: tot op niveau van het systeemelement (bouwdeelniveau) – en in dit geval de hardwarecomponent – die als aparte eenheid onderworpen is aan onderhoud, vervanging of revisie.

Vooruitlopend op de behandeling van de kwantitatieve analyse (hoofdstuk 6) is voor het decompositieniveau ook het bepalen van de faalfrequentie en de herstelduur van belang. Een pomp bijvoorbeeld wordt in zijn geheel vervangen als hij faalt. Verdere decompositie in onderdelen is dus niet nodig of wenselijk. De faalfrequentie van een pomp is op te halen uit databoeken. Dat geldt niet voor een complete voedingsinstallatie. Die moet verder worden uitgesplitst naar onderdelen die elk een eigen faalfrequentie hebben, zoals het noodstroomaggregaat, de netvoeding en de verbindende onderdelen.

Bij software systeemelementen gaat de decompositie tot aan modulen (zie paragraaf 6.3.2). Menselijk handelen wordt gedecomponeerd tot het niveau waarop het OPSCHEP-model kan worden toegepast (zie paragraaf 6.3.3).

NEN 2767-4

De richtlijnen, die bindend zijn voor systeemdecompositie, zijn vastgelegd in de NEN 2767-4. Hiermee is geborgd dat gelijksoortige objecten op uniforme wijze worden beschreven. Bovendien kan efficiënt gebruik worden gemaakt van eventueel beschikbare bibliotheken van faalwijzen en -definities en van *best practices* van eerder beschreven en geanalyseerde objecten. Het gebruik van de in de norm gehanteerde codering maakt het mogelijk om gelijksoortige objecten onderling beter te kunnen vergelijken en beoordelen.

Een kanttekening: het laagste niveau dat de NEN 2767-4 hanteert is het niveau van bouw- of installatiedeel. In veel gevallen zal de benodigde decompositie waarschijnlijk verder gaan dan dat niveau. Voor die lagere niveaus is geen naamgeving en codering voorgeschreven, maar het ligt voor de hand dat te doen in de lijn van de NEN.

Voorbeeld: de ophaalbrug

De scope van de analyse wordt bepaald door het, in de vorige paragraaf beschreven, systeem. Dat betekent bijvoorbeeld dat de voorhaven, met zijn afmeerplaatsen, niet in de scope zit en dus niet in de analyse hoeft terug te komen.

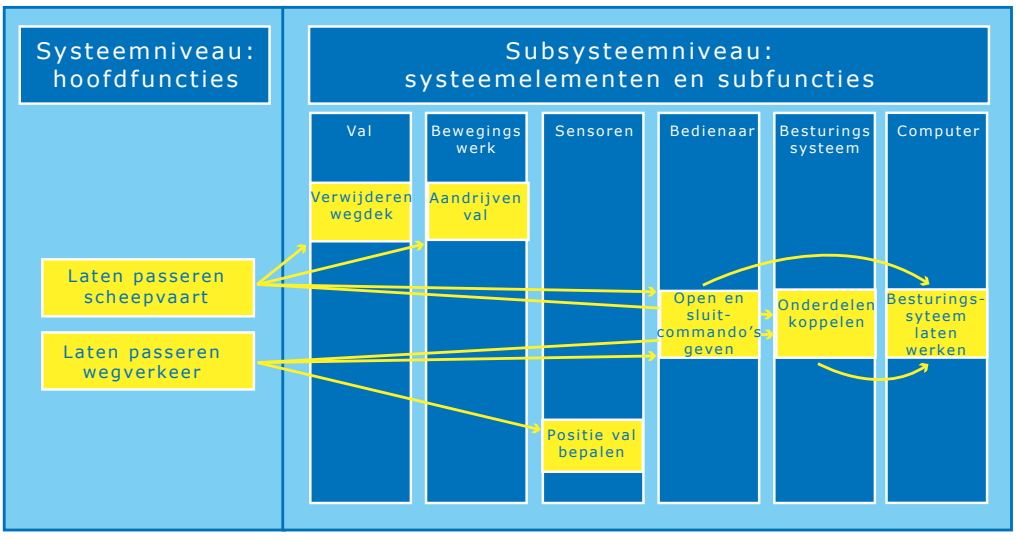
In het voorbeeld van de ophaalbrug is bewust de scope beperkt en de decompositie vereenvoudigd tot de systeemelementen:
- val
- bewegingswerk
- computer (hardware)
- sensoren (2 stuks)
- bedienaar
- besturingssysteem (software)

In werkelijkheid zullen de systeemelementen 'bewegingswerk' en 'computer', verder worden gedecomponeerd. Het is immers niet mogelijk de faalkans te vinden voor 'een' bewegingswerk. Van zo'n samengesteld onderdeel zijn er te veel verschillende soorten. Ook wordt het onderhoud van het bewegingswerk op onderdelen gedaan.

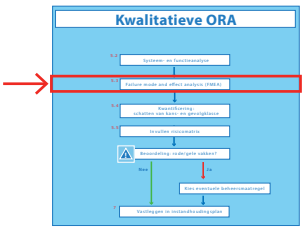
Een vereenvoudigde decompositie, volgens NEN 2767-4, voor beweegbare bruggen bestaat uit:
- 1461 Hoofddraagconstructie (val)
- 1182 Aandrijving en bewegingswerk, elektromotor
- 1431 Bedienings- en Besturingsinstallatie, PLC (computer, hardware)
- 1490 Meetinstallatie, sensor.

De bediening door de bedienaar en de software worden door de NEN 2767-4 niet ingedeeld.

Ook de functieanalyse is bij dit simpele voorbeeld eenvoudig. De brug heeft twee functies: het laten passeren van wegverkeer en het laten passeren van scheepvaart. Figuur 5.3 toont de relatie tussen functies, systeemelementen en subfuncties.



Figuur 5.3. Functionele analyse en allocatie



5.3 Processtap: FMEA

Failure mode and effect analysis (FMEA) is een techniek om alle mogelijke afwijkingen van het functioneren van een systeemelement te bepalen en de gevolgen van dat falen voor het systeem vast te leggen. De techniek is gestandaardiseerd in [9].

Bij de systeemanalyse (zie 0) is vastgelegd hoe het systeem is opgebouwd en hoe het werkt. Het systeem is gedecomponeerd in een objectenboom, volgens NEN 2767-4 [4] en eventueel een functieboom, volgens de SE-werkwijze [3, 8].

Vervolgens wordt, in een setting met experts op het gebied van het systeem, per systeemelement bepaald op welke manier het systeemelement kan falen (*failure modes*) met welke gevolgen (effect). Dit gebeurt gestructureerd aan de hand van een lijst van (standaard) gidswoorden. Zie tabel 5.1.

De resultaten van deze analyse worden vastgelegd in een tabel of spreadsheet. Rijkswaterstaat heeft hiervoor een gestandaardiseerd Excel template [10].

GIDSWOORD	TOEPASSING
GEEN of NIET	De toegedachte functie ontbreekt geheel.
MEER of HOGER of LATER of SNELLER	Er is een kwantitatieve toename van de toegedachte functie. Afhankelijk van de aard van de afwijking wordt het meest passende gidswoord gekozen.
MINDER of LAGER of EERDER of LANGZAMER	Er is een kwantitatieve afname van de toegedachte functie. Afhankelijk van de aard van de afwijking wordt het meest passende gidswoord gekozen.
ONVOLDOENDE	De toegedachte functie wordt onvoldoende gerealiseerd.
VERKEERD	In plaats van de toegedachte functie wordt een verkeerde functie gerealiseerd.
GEDEELTELIJK	De toegedachte functie wordt slechts voor een deel verwezenlijkt.
ONREGELMATIG	De toegedachte functie wordt onregelmatig verwezenlijkt.
EVENALS	De toegedachte functie voldoet, terwijl er ook een additioneel effect optreedt.
ONTERECHT	De toegedachte functie wordt op de juiste manier gerealiseerd, echter ten onrechte omdat deze functie niet had moeten plaatshebben.
OMGEKEERD	De toegedachte functie vindt niet plaats maar juist het tegengestelde effect of richting vindt plaats.
ANDERS DAN of WAAR ANDERS	De toegedachte functie wordt helemaal niet gerealiseerd. Er gebeurt iets volkomen anders, mogelijk zelfs op een andere locatie.

Tabel 5.1. De meest voorkomende gidswoorden met hun toepassing voor een FMEA

Voorbeeld: de ophaalbrug

De decompositie uit paragraaf 5.2 vormt de basis voor de FMEA. Per systeemelement wordt, met behulp van de gidswoorden, systematisch onderzocht of niet-functioneren gevolgen heeft voor het systeem. In deze fase beperken we ons tot de verschillende faalwijzen en de impact van het falen op de functie. In figuur 5.4 is het resultaat van de FMEA samengevat.

Objectrisicoanalyse (ORA)

Beheerobject code:				**Datum:**	20-11-2015	**Opgesteld do**	S.E. van Manen		
Naam volgens DISK:		Voorbeeld Beweegbare Brug		**Versie:**	1.0.0	**Adviesbureau**	RWS		
Naam anders (evt.):				**DISK clustercode:**		**Contractcode**			

Fase 1: Bureaustudie: processtappen informatieoverdracht en I-ORA

Element/bouwdeel		Code Element/bouwdeel	Functie van het onderdeel	Functioneel falen	Faalwijze	Code Faalwize	Faalmechanisme	Oorzaak van falen	Bron van falen	Gevolg van falen	Direct merkbaar?	Laten passeren wegverkeer	Laten passeren scheepvaart
Hoofddraagconstructie													
1461	Val	V	Wegverkeer dragen	Is niet in staat het wegverkeer te dragen	Bezwijken	B	Instorten	Vermoeiings-scheur	Onjuiste detaillering bij ontwerp	Mogelijk doden en gewonden, kostbare reparatie en lange reparatieduur	Ja	Ja	Ja
Aandrijving- en bewegingswer													
1182	Elektromotor	EM	In beweging brengen van het val	Val kan niet gelicht worden	Motor start niet	SN	Veroudering Trilling Slijtage Vrijving	Externe invloed	Onderhoud	Scheepvaart kan niet passeren	Nee	Nee	Ja
					Motor stopt voortijdig	SV	Veroudering Verhitting Slijtage	Overbelasting	N.v.t	Zowel scheepvaart als wegeverkeer kan niet passeren	Ja	Ja	Ja
Bedienings- en besturingsinstallatie													
1431	PLC	BB	Aansturen van de diverse onderdelen	De brug kan niet geheven worden	Valt uit	SV	Trilling Aantasting	Externe invloed	N.v.t.	Scheepvaart kan niet passeren	Ja	Nee	Ja
Meetinstallatie													
●●	**Sensor nr 1**	S	Bepalen of het val op de juiste positie is	De brug kan niet vrijgegeven worden voor het wegverkeer	Valt uit	SV	Aantasting Vervuiling Slijtage	Externe invloed	N.v.t.	Brug blijft gesloten voor het wegverkeer	Nee	Ja	Nee
●●	**Sensor nr 2**	S	Bepalen of het val op de juiste positie is	De brug kan niet vrijgegeven worden voor het wegverkeer	Valt uit	SV	Aantasting Vervuiling Slijtage	Externe invloed	N.v.t.	Brug blijft gesloten voor het wegverkeer	Nee	Ja	Nee

Figuur 5.4. FMEA ophaalbrug

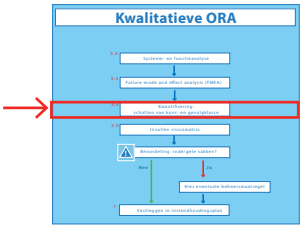
Formeel moeten alle gidswoorden uit tabel 5.1 worden toegepast op de functie van alle componenten. Zo geldt voor de functie van het val: 'Geen', 'onvoldoende' of 'gedeeltelijk'. De overige afwijkingen van de functie zijn niet van toepassing, ze zijn in feite ondenkbaar. Het 'meer dragen van het wegverkeer', of het 'langzamer dragen van het wegverkeer' hebben geen zinnige betekenis.

'Geen', 'onvoldoende' of 'gedeeltelijk' kunnen apart als faalmechanisme worden meegenomen. 'Geen' kan bezwijken betekenen, 'onvoldoende' kan staan voor onveilig (het val functioneert nog wel, maar de sterkte is onvoldoende om echt grote verkeerslasten te dragen) en bij 'gedeeltelijk' kan men denken aan gedeeltelijk bezwijken. Omwille van de eenvoud is in het voorbeeld verder alleen de faalwijze 'geen dragen van het wegverkeer' meegenomen, wat betekent dat de brug is bezweken.

Bij de elektromotor is sprake van twee mogelijke faalwijzen: de motor start niet (gidswoord 'geen') of hij stokt halverwege (gidswoord 'later'). Uiteraard is uitbreiding mogelijk met 'onregelmatig' et cetera. Zo worden voor de ophaalbrug de volgende faalmechanismen gevonden:

SYSTEEMELEMENT	GIDSWOORD	FAALMECHANISME
VAL	Geen	Bezwijken
ELEKTROMOTOR	Niet	Start niet
ELEKTROMOTOR	Later	Stopt voortijdig
PLC	Niet, Verkeerd	Valt uit
SENSOREN (2 STUKS)	Niet, Onterecht	Valt uit

Merk op dat de bedienaar, met functie 'bedienen' en het besturingssysteem, met functie 'aansturen van de onderdelen', niet in de FMEA terugkomen. Bij de kwantitatieve analyse komen ze wel terug.



5.4 Processtap: schatten van kans- en gevolgklassen

Bij toepassing van de kwalitatieve variant van de objectrisicoanalyse wordt de FMEA uitgebreid met kans- en gevolgklassen. In feite is de kwalitatieve variant daarmee een semi-kwantitatieve variant, immers de range waarin de faalkansen liggen, wordt geschat en in een getalsmatige verhouding uitgedrukt. Ook de gevolgklassen zijn — waar mogelijk — kwantitatief. In feite wordt de FMEA uitgebreid tot een FMECA (*failure mode, effect and criticality analysis*). De FMECA resulteert in maatregelen die de geconstateerde risico's reduceren. In de realisatiefase wordt de FMECA niet expliciet gebruikt, omdat als uitgangspunt geldt dat de risico's al worden beheerst met adequate maatregelen die grotendeels in de *klant-eisenspecificatie* (KES) zijn meegenomen.

Van alle faalwijzen van alle systeemelementen uit de FMEA (paragraaf 5.3) worden de kans van optreden en de gevolgen ingeschat. Op basis van het totaal van inschattingen is de grootte van het risico te bepalen.

5.4.1 De kansscore

Het uitgangspunt bij de kansschatting is dat het huidige standaard verzorgend onderhoud wordt uitgevoerd. Bij deze inschatting moet ook de bron worden vermeld (bijvoorbeeld 'Rijkswaterstaat referentiekader beheer en onderhoud' [11], leveranciersinformatie of expertmening).

De kans op een bepaalde faalwijze van een element van een systeem wordt ingevuld op basis van expertmening en soms leveranciersinformatie. De daarbij gebruikte maat is een 'levensduur', of gemiddelde tijd tot falen ofwel *mean time to failure* (MTTF). De MTTF wordt in het algemeen korter naarmate het systeemelement ouder is. Als de technische levensduur van een onderdeel (bijna) is bereikt zal de kans op falen groter zijn dan bij een nieuw onderdeel. In bijzondere gevallen veroudert een systeem nauwelijks en blijft de faalsnelheid constant.

De MTTF wordt vervolgens in een kansklasse ondergebracht. De grenzen van de kansklassen (de tijdsvensters) zijn gekozen op basis van een 6-jaarlijkse instandhoudingsinspectie.

De volgende kansscores gelden voor veroudering in de model-risicomatrix (hierbij is t het moment waarop het eerstvolgende falen wordt verwacht).

1. *Verwaarloosbaar (20 jr < t)*
   Het falen wordt niet in de komende 20 jaar verwacht.
2. *Klein (6 jr < t ≤ 20 jr)*
   Het falen wordt tussen 6 en 20 jaar na nu verwacht.
3. *Middelmatig (2 jr < t ≤ 6 jr)*
   Het falen wordt tussen 2 en 6 jaar na nu verwacht.
4. *Groot (½ jr < t ≤ 2 jr)*
   Het falen wordt tussen 6 maanden en 2 jaar na nu verwacht.
5. *Zeker (t ≤ ½ jr)*
   Het falen is al gebeurd of wordt in de komende 6 maanden verwacht.

Als de faalkans in de tijd constant blijft, moeten de gegeven kansscores worden gezien als gemiddelde frequenties:

1. *Verwaarloosbaar*
   Het falen treedt gemiddeld minder vaak dan eens per 20 jaar op.
2. *Klein (6 jr < t ≤ 20 jr)*
   Het falen treedt gemiddeld eens per 20 jaar op of vaker, maar minder vaak dan eens per 6 jaar.
3. *Middelmatig (2 jr < t ≤ 6 jr)*
   Het falen treedt gemiddeld eens per 6 jaar op of vaker, maar minder vaak dan eens per 2 jaar.
4. *Groot (½ jr < t ≤ 2 jr)*
   Het falen treedt gemiddeld eens per 2 jaar op of vaker, maar minder vaak dan eens per ½ jaar.
5. *Zeker (t ≤ ½ jr)*
   Het falen treedt gemiddeld eens per ½ jaar op of vaker.

5.4.2 De gevolgscore

De kwalitatieve risicoanalyse beschouwt de gevolgen voor alle RAMSSHE€P-aspecten. Het aspect betrouwbaarheid (R) staat voor de kans, die in deze processtap in kansklassen is ingedeeld. Voor de overige aspecten wordt met behulp van onderstaande tabel (tabel 5.2) per aspect de gevolgscore bepaald. Per faalwijze geldt de hoogste gevolgscore over alle aspecten voor het bepalen van de totale risicoscore.
Rijkswaterstaat heeft ervoor gekozen om de ongewenste gevolgen te groeperen in vier categorieën:

1. Verwaarloosbaar
2. Beperkt
3. Groot
4. Ernstig

Daarnaast wordt de gevolgscore 0 toegekend als er geen gevolg voor een aspect is. De gevolgscore hangt samen met het gewenste prestatieniveau van het desbetreffende object. Bij beschikbaarheid, of hinder (A), wordt gewerkt met een vooraf vast te stellen onder- en bovengrens. Hinder die korter duurt dan de ondergrens krijgt de gevolgscore ‘Beperkt’ (2). Hinder die langer duurt dan de bovengrens krijgt de gevolgscore ‘Ernstig’ (4). Hinder tussen de onder- en bovengrens krijgt de gevolgscore ‘Groot’ (3). Voor de overige RAMSSHE€P-aspecten wordt in tabel 5.2 aangegeven wat onder ‘Verwaarloosbaar’, ‘Beperkt’, Groot’ en ‘Ernstig’ wordt verstaan.

		GEVOLG			
		1: VERWAARLOOSBAAR	**2: BEPERKT**	**3: GROOT**	**4: ERNSTIG**
RAMSSHEEP	**A**	Zeer kortdurende hinder voor primaire functies van object; geen hinder voor netwerk	Hinder voor netwerk is korter dan ondergrens voor alle functiecategorieën: 1. wegverkeer 2. scheepvaart 3. waterhuishouding	Hinder voor netwerk is korter dan bovengrens in alle functiecategorieën, maar langer dan ondergrens in één of meer van de functiecategorieën: 1. wegverkeer 2. scheepvaart 3. waterhuishouding	Hinder voor netwerk is langer dan bovengrens in één of meer van de functiecategorieën: 1. wegverkeer 2. scheepvaart 3. waterhuishouding
	M	Lokaal herstel, eenvoudig uitvoerbaar	Herstel met extra inspanning (bijvoorbeeld door speciaal gereedschap, of wachten op reservedelen)	Herstel met veel inspanning (bijvoorbeeld door het forceren van toegang voor uitvoeren onderhoud of wachten op speciaal te fabriceren reservedelen of vergunningen)	Herstel weegt niet meer op tegen de economische levensduur van het object; andersoortige maatregelen zijn noodzakelijk (bijvoorbeeld grootscheepse vervanging)
	S	Het falen leidt direct of indirect tot ongelukken met niet-blijvend letsel zonder verzuim bij één of meer personen	Het falen leidt direct of indirect tot ongelukken met niet-blijvend letsel met medische assistentie/ ziekenhuisopname bij één of meer personen	Het falen leidt direct of indirect tot ongelukken met blijvend letsel bij één persoon	Het falen leidt direct of indirect tot ongelukken met: - blijvend letsel bij meer personen, of - fataal letsel bij één of meer personen
	SE	Ongewenst menselijk handelen mogelijk met kleine gevolgen zoals graffiti	Ongewenst menselijk handelen mogelijk met beperkte gevolgen zoals toegang tot een onbelangrijke ruimte	Ongewenst menselijk handelen mogelijk met grote gevolgen zoals digitale/fysieke toegang tot vertrouwelijke informatie	Ongewenst menselijk handelen mogelijk met ernstige gevolgen zoals digitale/fysieke toegang tot de (nood-)besturing van het object
	H	Op termijn gezondheidshinder bij één of meer personen	Op termijn tijdelijke gezondheidsschade bij één of meer personen	Op termijn blijvende gezondheidsschade bij één persoon	Op termijn: - blijvende gezondheidsschade bij meer personen - fatale gezondheidsschade bij één of meer personen
	E	Verwaarloosbare gevolgen voor flora en fauna	Beperkte gevolgen voor flora en/of fauna; geen maatregel nodig, het lost vanzelf op	Grote gevolgen voor flora en/of fauna; maatregelen nodig om erger te voorkomen	Ernstige, langdurige gevolgen voor flora en fauna; grootscheepse maatregelen noodzakelijk
	€	Gevolgkosten tussen €100,- en €10.000,-	Gevolgkosten tussen €10.000,-en €100.000,-	Gevolgkosten tussen €100.000,-en €500.000,-	Gevolgkosten > €500.000,-
	P	Klachten	Imagoverlies lokaal	Imagoverlies regionaal	Imagoverlies landelijk

Tabel 5.2. De classificatie van mogelijke gevolgen

Voorbeeld: de ophaalbrug

Bij de kwalitatieve risicoanalyse wordt de FMEA aangevuld tot een FMECA. In de initiële bureaustudie wordt voor elke gevonden faalwijze een inschatting gedaan van de kans- en de gevolgklasse.

De ophaalbrug is in 1995 gebouwd. Falen van het val is direct merkbaar en heeft gevolgen voor zowel het wegverkeer als het scheepvaartverkeer. Voor de hoofdfunctie 'laten passeren wegverkeer' (LPW) wordt voor hinder 1 dag als ondergrens en 1 week als bovengrens gesteld. Voor de functie 'laten passeren scheepvaart' (LPS) wordt 2 dagen als ondergrens en 1 maand als bovengrens gekozen.

Voor het val wordt ingeschat dat de gemiddelde levensduur gelijk is aan de geplande levensduur namelijk 100 jaar. Dit is een pessimistische inschatting. Deze inschatting plaatst het val in kansklasse 1 (zie tabel 5.2).

De gevolgen van het falen van het val voor de RAMSSHE€P-aspecten (minus betrouwbaarheid) zijn bij deze aannamen:

ASPECT	GEVOLG	GEVOLGKLASSE
BESCHIKBAARHEID (HINDER)	Ernstig, groter dan 1 maand	4
ONDERHOUDBAARHEID	Geen	0
VEILIGHEID	Ernstig	4
SECURITY	Geen	0
GEZONDHEID	Geen	0
OMGEVING EN MILIEU	Geen	0
KOSTEN	Ernstig, meer dan € 500.000	4
IMAGO	Landelijk imagoverlies	4

Informatie over de faalfrequentie van de elektromotor staat in een database. Voor dit voorbeeld is de aanname dat de motor relatief vaak faalt, namelijk 1 keer per jaar. Daarmee komt hij in kansklasse 4.
Ook dit is een pessimistische inschatting want in de praktijk faalt de elektromotor (veel) minder. De elektromotor kan binnen één dag (ca. 12 uur) worden gerepareerd. De gevolgen bij deze aanname zijn dan:

ASPECT	GEVOLG	GEVOLGKLASSE
BESCHIKBAARHEID (HINDER)	Korter dan de ondergrens	2
KOSTEN	Tussen € 100 en € 10.000	1
IMAGO	Klachten	1

De overige gevolgen zijn niet van toepassing en dienen dus als zodanig vermeld te worden.

De PLC faalt gemiddeld eens in de 5 jaar. Ook dit gegeven komt uit een database. Daarmee zit hij nog net in kansklasse 3. Het falen kan binnen een dag worden verholpen. Daarmee worden de gevolgen bij deze aanname:

ASPECT	GEVOLG	GEVOLGKLASSE
BESCHIKBAARHEID (HINDER)	Korter dan de ondergrens	2
KOSTEN	Tussen € 100 en € 10.000	1
IMAGO	Klachten	1

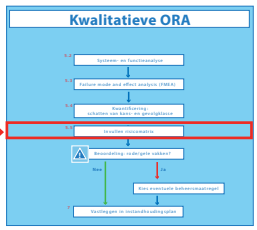
Een sensor faalt gemiddeld eens in de 10 jaar. Dat komt overeen met kansklasse 2. Het falen is niet eerder merkbaar dan bij het weer neerlaten van het val. De herstelduur is (slechts) 4 uur doordat de tweede sensor de back-up is waarmee de brug kan blijven functioneren. Reparatie heeft geen gevolgen voor de beschikbaarheid. De gevolgen van deze aannamen worden daarmee:

ASPECT	GEVOLG	GEVOLGKLASSE
BESCHIKBAARHEID (HINDER)	Verwaarloosbaar	1
KOSTEN	Tussen € 100 en € 10.000	1
SECURITY	Ongewenst menselijk handelen mogelijk, vandalisme	1
IMAGO	Klachten	1

Alle aannamen en gevonden waarden uit het voorbeeld ‘ophaalbrug’ zijn samengevat in figuur 5.5.

Element/bouwdeel		(In)bouwjaar	MTTF [jaar]	Kansscore	Hinder	M	S	Se	H	E	€	P	Maximale gevolgscore	Risicoscore	Risiconiveau	Toelichting, bronvermelding
Hoofddraagconstructie																
1461	Val	1995	100	1	4	0	4	0	0	0	4	4	4	4	Acceptabel	Ontwerpdocumenten, Eurocode
Aandrijving- en bewegingswerk																
1182	Elektromotor	1995	1	4	2	0	0	0	0	0	1	1	2	8	Ongewenst	RWS Database voor opdrachtnemers
			1	4	2	0	0	0	0	0	1	1	2	8	Ongewenst	RWS Database voor opdrachtnemers
Bedienings- en besturingsinstallatie																
1431	PLC	2005	5	3	2	0	0	0	0	0	1	1	2	6	Ongewenst	RWS Database voor opdrachtnemers
Meetinstallatie																
1490	Sensor nr 1	2005	10	2	1	0	0	1	0	0	1	1	1	2	Acceptabel	RWS Database voor opdrachtnemers - sensor positieteller
1490	Sensor nr 2	2005	10	2	1	0	0	1	0	0	1	1	1	2	Acceptabel	RWS Database voor opdrachtnemers - sensor positieteller

Figuur 5.5. Inschatting kans- en gevolgklassen in de initiële analyse, de bureaustudie



5.5 Processtap: invullen risicomatrix

De risicomatrix (tabel 5.3) maakt bij een gegeven faalwijze met een kansklasse en een gevolgklasse direct inzichtelijk hoe noodzakelijk een beheersmaatregel is. De matrix werkt met een kleurcode voor drie niveaus: rood, oranje of groen.

1. Rood = onacceptabel
   Er moet een maatregel worden getroffen om het risico te beheersen. Er kunnen tevens redenen zijn om het vaste onderhoud te herzien of om een variabel-onderhoudsmaatregel of zelfs redesign voor te stellen.

2. Oranje = ongewenst
   Er moet ofwel een maatregel worden getroffen om het risico te beheersen ofwel worden aangetoond waarom dit niet haalbaar/noodzakelijk is. Tevens kan het noodzakelijk zijn het standaard verzorgend onderhoud te herzien of een var iabel-onderhoudsmaatregel toe te voegen.

3. Groen = acceptabel
   Er hoeft geen maatregel te worden getroffen om het risico te beheersen. Als de faalwijze zich voordoet, worden de gebruikelijke acties ondernomen voor (functie-)herstel. Merk op dat ook een laag risico nog steeds reden kan zijn om het standaard verzorgend onderhoud te herzien, maar nu omdat mogelijk minder activiteiten nodig zijn.

RISICOMATRIX		GEVOLG			
		1: VERWAAR-LOOSBAAR	2: BEPERKT	3: GROOT	4: ERNSTIG
KANS	1: VERWAARLOOSBAAR	Acceptabel	Acceptabel	Acceptabel	Acceptabel
	2: KLEIN	Acceptabel	Acceptabel	Ongewenst	Ongewenst
	3: GEMIDDELD	Acceptabel	Ongewenst	Ongewenst	Ongewenst
	4: GROOT	Acceptabel	Ongewenst	Ongewenst	Onacceptabel
	5: ZEKER	Ongewenst	Ongewenst	Onacceptabel	Onacceptabel

Tabel 5.3. Risicomatrix

Risicoprofiel van het systeem

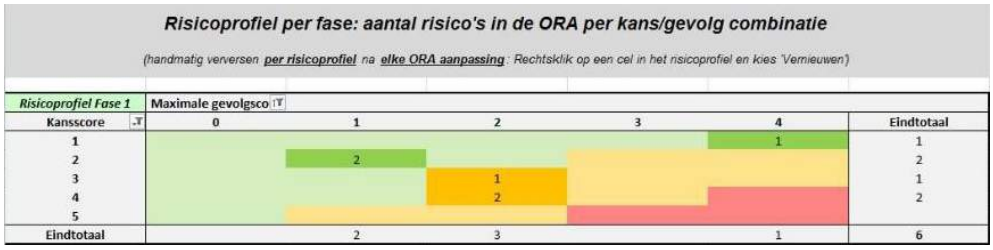
De kansklassen, gevolgklassen en hun onderlinge relaties zijn vastgelegd in de risicomatrix. Het totaal van alle faalwijzen van alle systeemelementen is vervolgens uit te drukken in een risicoprofiel. De risicomatrix wordt daartoe gevuld met het aantal risico's voor elke afzonderlijke kans-gevolgcombinatie in het desbetreffende object.

De kwalitatieve variant van de objectrisicoanalyse heeft, net als de kwantitatieve variant, een cyclisch plan-do-check-act-karakter. Na uitvoering van de initiële bureaustudie, zoals in dit hoofdstuk is beschreven, volgt een inspectie (check). Afwijkingen ten opzichte van de initiële analyse worden op dezelfde manier vastgelegd (act). Op basis daarvan volgt een instandhoudingsadvies (plan) voor de te nemen maatregelen (do). Ook het verwachte effect van deze maatregelen komt via de risicomatrix tot uiting. Het uiteindelijke doel is dat alle risico's zich in het 'groene' gebied bevinden.

Een en ander zal ook in het instandhoudingsplan voor dat object worden opgenomen en vastgelegd.

Voorbeeld: de ophaalbrug

De kans- en gevolginschattingen, zoals die in de vorige paragraaf zijn gemaakt, worden in de risicomatrix geplot. Daarmee ontstaat het risicoprofiel, zie figuur 5.6.



Risicoprofiel per fase: aantal risico's in de ORA per kans/gevolg combinatie

*(handmatig verversen **per risicoprofiel** na **elke ORA aanpassing**: Rechtsklik op een cel in het risicoprofiel en kies 'Vernieuwen')*

Risicoprofiel Fase 1	Maximale gevolgsco				
Kansscore	0	1	2	3	4	Eindtotaal
1					1	1
2		2				2
3			1			1
4			2			2
5						
Eindtotaal		2	3		1	6

Figuur 5.6. Risicoprofiel na bureaustudie

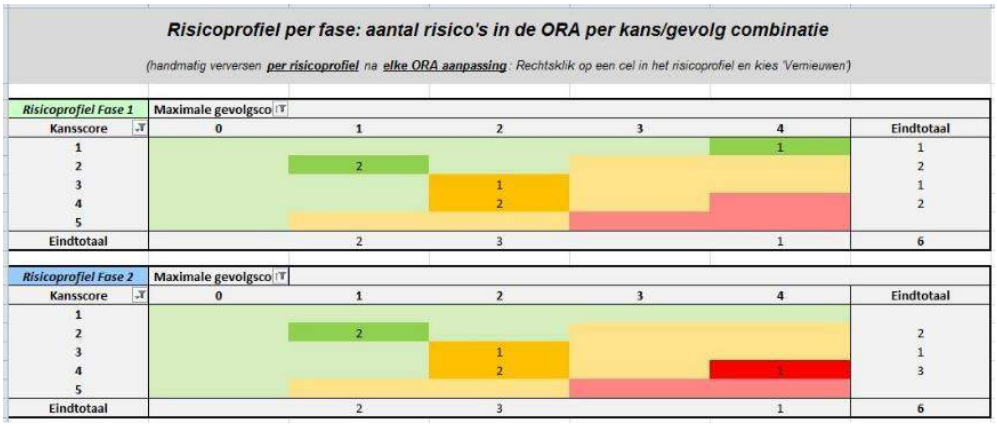
Er zijn drie mogelijke gebeurtenissen die geen zorg vereisen, maar ook drie gebeurtenissen die ongewenst zijn. Het gaat om de elektromotor en de PLC. Zoals al is aangegeven, zijn de kansen op falen van deze componenten pessimistisch ingeschat. Zolang de praktijk geen frequent falen laat zien, zijn specifieke maatregelen (nog) niet nodig.

Tijdens een inspectie op alle onderdelen worden grote langsscheuren in het rijdek geconstateerd. De kans op falen van het val is groot geworden en valt nu in klasse 4. Bij de overige componenten worden geen bijzonderheden waargenomen. De FMECA wordt aangepast en geeft het beeld van figuur 5.7.

		Fase 2: Inspectie (aangepaste ORA)												
Element/bouwdeel		Inspectie-bevinding	MTTF	Kansscore	Hinder	MS	Se	H	E	€	P	Maximale gevolgscore	Risicoscore	Risiconiveau
Hoofddraagconstructie														
1461	Val	Langsscheur van 2 meter	2	4	4	0	4	0	0	0	4	4	4	16	Onacceptabel
Aandrijving- en bewegingswerk														
1182	Elektromotor	Geen bijzonderheden	1	4	2	0	0	0	0	0	1	1	2	8	Ongewenst
		Idem	1	4	2	0	0	0	0	0	1	1	2	8	Ongewenst
Bedienings- en besturingsinstallatie														
1431	PLC	Geen bijzonderheden	5	3	2	0	0	0	0	0	1	1	2	6	Ongewenst
Meetinstallatie														
1490	Sensor nr 1	Net vernieuwd	10	2	1	0	0	1	0	0	1	1	1	2	Acceptabel
1490	Sensor nr 2	Net vernieuwd	10	2	1	0	0	1	0	0	1	1	1	2	Acceptabel

Figuur 5.7. Inschatting kans- en gevolgklassen na inspectie

De gevolgen zijn onveranderd, waardoor het risico 'Bezwijken van het val' nu onacceptabel groot is. Er moet direct actie worden ondernomen. Het risicoprofiel na inspectie is gegeven in figuur 5.8.



Risicoprofiel per fase: aantal risico's in de ORA per kans/gevolg combinatie

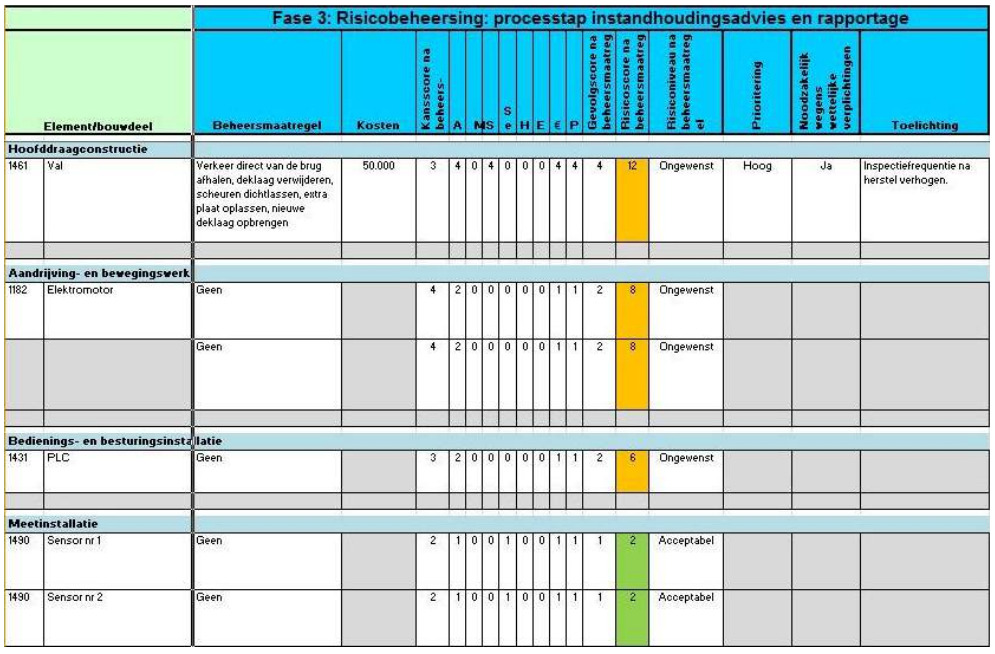
*(handmatig verversen **per risicoprofiel** na **elke ORA aanpassing**: Rechtsklik op een cel in het risicoprofiel en kies 'Vernieuwen')*

Risicoprofiel Fase 1	Maximale gevolgsco				
Kansscore	0	1	2	3	4	Eindtotaal
1					1	1
2		2				2
3			1			1
4			2			2
5						
Eindtotaal		2	3		1	6

Risicoprofiel Fase 2	Maximale gevolgsco				
Kansscore	0	1	2	3	4	Eindtotaal
1						
2		2				2
3			1			1
4			2		1	3
5						
Eindtotaal		2	3		1	6

Figuur 5.8. Risicoprofiel na inspectie

Het val komt nu in het rood en er moeten direct maatregelen worden genomen. Deze bestaan uit het van de brug halen van het verkeer, de deklaag verwijderen, de scheuren dichtlassen, mogelijk een extra plaat oplassen en nieuwe deklaag opbrengen. Na de genomen maatregelen ziet de FMECA er als volgt uit (figuur 5.9):



		Fase 3: Risicobeheersing: processtap instandhoudingsadvies en rapportage															
Element/bouwdeel		Beheersmaatregel	Kosten	Kansscore na beheers-	A	NS	Se	H	E	€	P	Gevolgscore na beheersmaatreg	Risicoscore na beheersmaatreg	Risiconiveau na beheersmaatregel	Prioritering	Noodzakelijk wegens wettelijke verplichtingen	Toelichting
Hoofddraagconstructie																	
1461	Val	Verkeer direct van de brug afhalen, deklaag verwijderen, scheuren dichtlassen, extra plaat oplassen, nieuwe deklaag opbrengen	50.000	3	4	0	4	0	0	0	4	4	4	12	Ongewenst	Hoog	Ja	Inspectiefrequentie na herstel verhogen.
Aandrijving- en bewegingswerk																	
1182	Elektromotor	Geen		4	2	0	0	0	0	0	1	1	2	8	Ongewenst			
		Geen		4	2	0	0	0	0	0	1	1	2	8	Ongewenst			
Bedienings- en besturingsinstallatie																	
1431	PLC	Geen		3	2	0	0	0	0	0	1	1	2	6	Ongewenst			
Meetinstallatie																	
1490	Sensor nr 1	Geen		2	1	0	0	1	0	0	1	1	1	2	Acceptabel			
1490	Sensor nr 2	Geen		2	1	0	0	1	0	0	1	1	1	2	Acceptabel			

Figuur 5.9. Inschatting kans- en gevolgklassen na herstel van het val

Het risico is gemitigeerd, maar blijft ongewenst. Een mogelijke maatregel is het verhogen van de inspectiefrequentie. Het resterende risicoprofiel is gegeven in figuur 5.10.

Risicoprofiel Fase 1	Maximale gevolgsco					
Kansscore	0	1	2	3	4	Eindtotaal
1					1	1
2		2				2
3			1			1
4			2			2
5						
Eindtotaal		2	3		1	6

Risicoprofiel Fase 2	Maximale gevolgsco					
Kansscore	0	1	2	3	4	Eindtotaal
1						
2		2				2
3			1			1
4			2		1	3
5						
Eindtotaal		2	3		1	6

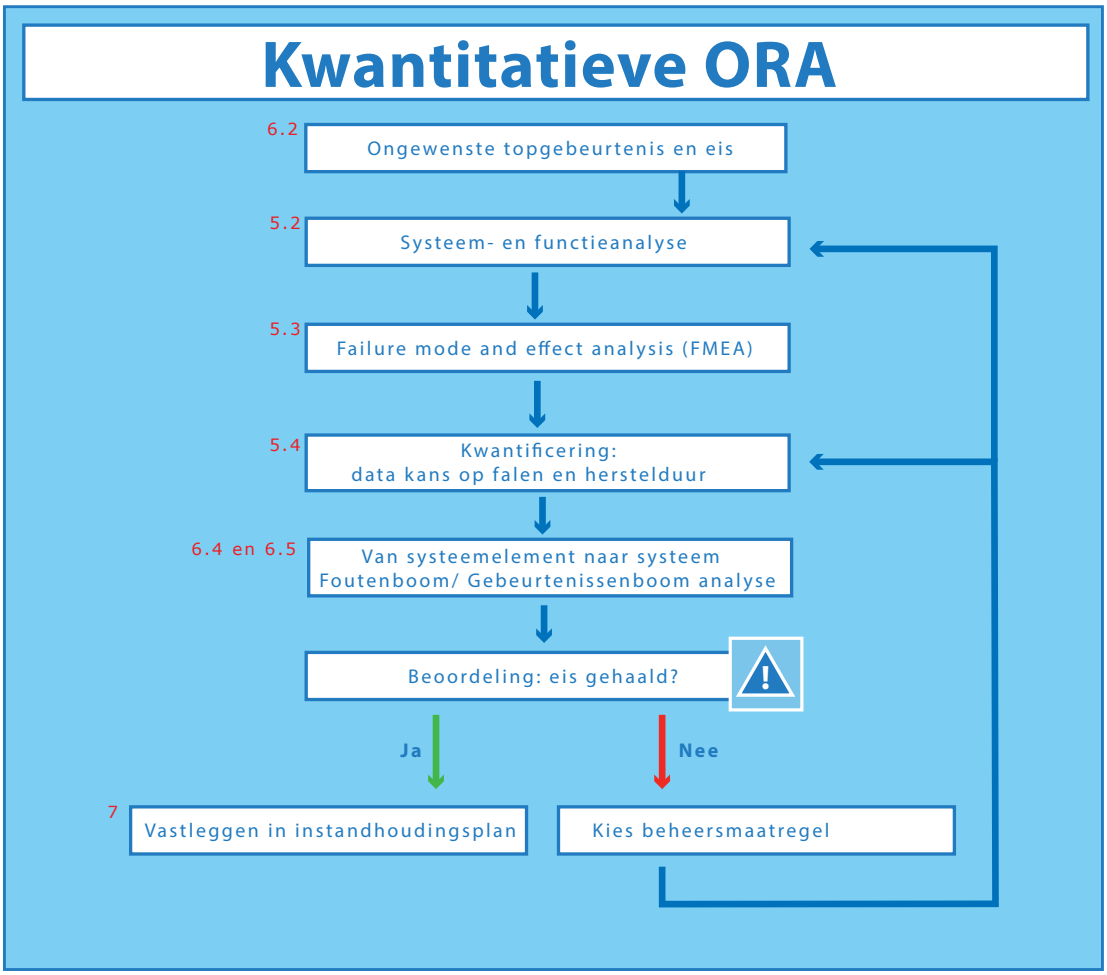
Risicoprofiel Fase 3	Maximale gevolgscore na beheersmaatregi					
Kansscore na beheersmaatregel	0	1	2	3	4	Eindtotaal
1						
2		2				2
3			1		1	2
4			2			2
5						
Eindtotaal		2	3		1	6

Figuur 5.10. Het resterende risicoprofiel

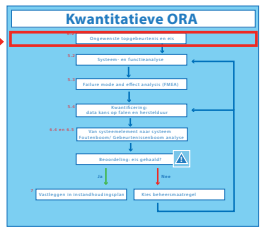
6 De kwantitatieve objectrisicoanalyse

6.1 Inleiding

Dit hoofdstuk beschrijft de kwantitatieve objectrisicoanalyse (ORA) in detail. In de onderstaande figuur verwijzen de nummers bij de opeenvolgende processtappen naar de paragrafen waarin deze worden behandeld. Omdat de 'systeem- en functieanalyse' en 'FMEA' gelijk zijn aan die bij de kwalitatieve risicoanalyse, verwijzen deze stappen in de figuur naar de paragrafen 5.2 en 5.3.



Figuur 6.1. Stappen in de kwantitatieve ORA



6.2 Processtap: ongewenste topgebeurtenis en eis

Een kwantitatieve ORA beschouwt per analyse slechts één gevolg van falen en berekent zo goed mogelijk de kans dat de ongewenste topgebeurtenis zich voordoet. Deze ongewenste topgebeurtenis (OTG) moet worden gedefinieerd. Veelal gaat het om gebeurtenissen als 'keren hoog water faalt' (stormvloedkering), of 'laten passeren wegverkeer faalt' (tunnel of beweegbare brug), of 'afvoeren water faalt' (spuicomplex).

Soms kent een object meerdere OTG's van uiteenlopende aard. Bij een beweegbare brug bijvoorbeeld kan een OTG het falen van de functie 'laten passeren scheepvaart' zijn en een andere het falen van 'laten passeren wegverkeer'. Ook is het denkbaar dat de OTG de mate van falen uitdrukt. Bij een sluiscomplex met twee kolken kan sprake zijn van drie OTG's: kolk 1 faalt, kolk 2 faalt en beide kolken falen. Of, nog wat lastiger, bij een tunnel met twee rijstroken per tunnelbuis kan één tunnelbuis niet beschikbaar zijn (beide rijstroken), of voor één rijstrook kan een snelheidsbeperking gelden, of kan er een snelheidslimiet zijn ingesteld bij het falen van de verlichting. Dat zijn drie verschillende ongewenste topgebeurtenissen, die elk kunnen worden veroorzaakt door verschillende falende elementen van een systeem en die elk een eigen beschikbaarheids- of betrouwbaarheidseis kunnen hebben.

Het ligt voor de hand om voor elke OTG een eis te formuleren: de acceptabele niet-beschikbaarheid of de acceptabele onbetrouwbaarheid. Maar ook zonder eis is een kwantitatieve ORA zinvol. Hij geeft dan aan welke betrouwbaarheid en beschikbaarheid van het object kunnen worden verwacht en waar, wat deze aspecten betreft, de knelpunten, maar ook de optimalisaties in het systeem zitten. Is er ook een eis gesteld, dan kunnen tevens zinvolle maatregelen worden geformuleerd voor het geval dat niet aan de eis wordt voldaan.

Voorbeeld: de ophaalbrug

De ophaalbrug heeft twee hoofdfuncties: het laten passeren van wegverkeer en het laten passeren van scheepvaart. De ongewenste topgebeurtenissen zijn daar direct uit af te leiden:

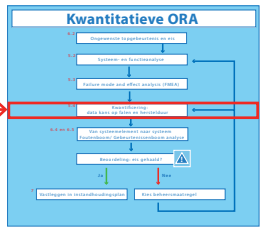
1. De ophaalbrug opent niet (passeren scheepvaart faalt).
2. De ophaalbrug sluit niet (passeren wegverkeer faalt).

Beide hoofdfuncties moeten voldoen aan de Rijkswaterstaatmissie voor vlotte en veilige doorstroming.

Vlotte doorstroming kan worden gerealiseerd door een eis te stellen aan de beschikbaarheid. Veronderstel dat – als afgeleide van de afspraken met de minister van IenM in de SLA – is afgesproken dat de ongeplande niet-beschikbaarheid van de brug voor de functie LPS gemiddeld 1 procent mag bedragen. Dat komt neer op ongeveer 90 uur per jaar (IPM-teams en beheerders hebben een voorkeur voor het denken in uren per jaar).

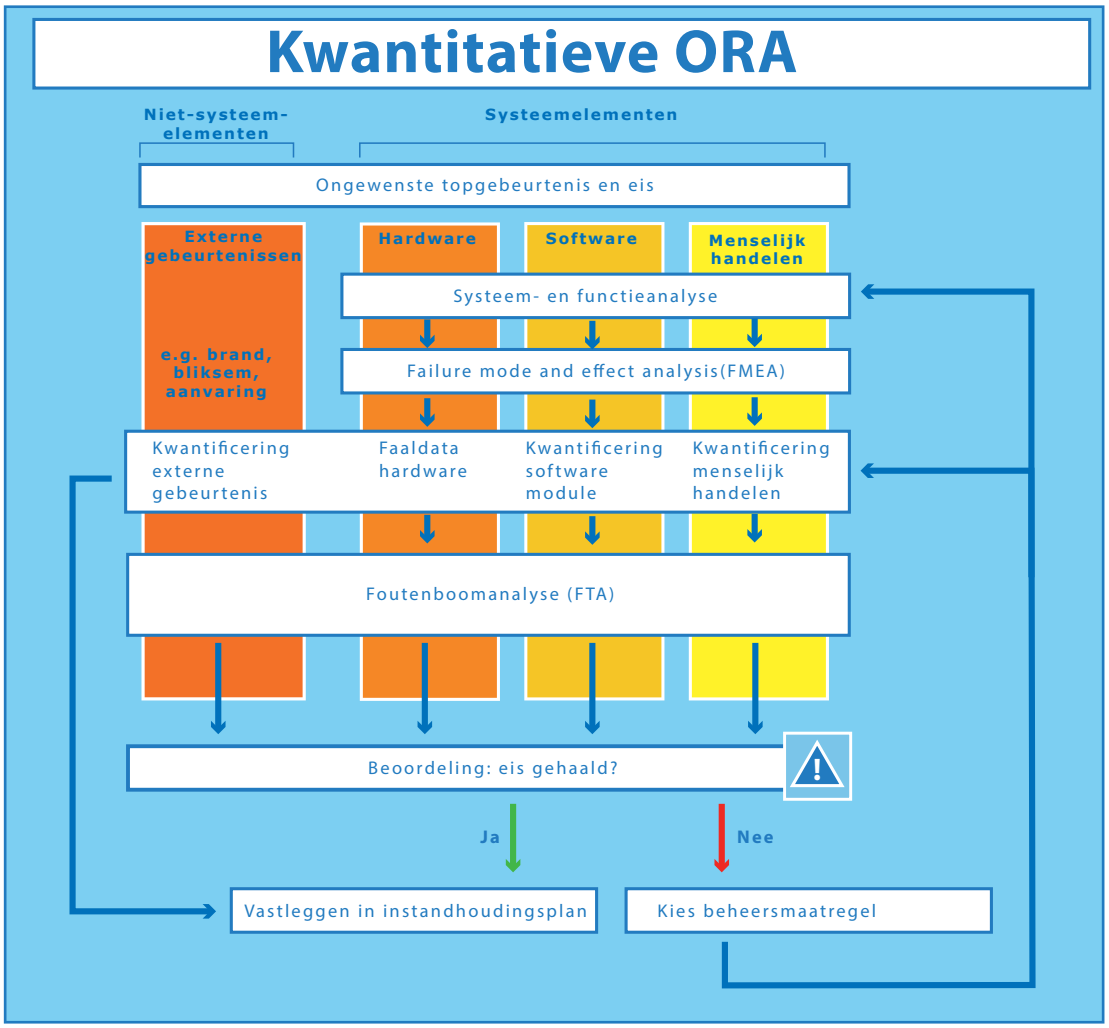
In de vraagspecificatie kan dan de volgende eis zijn opgenomen:

ID	GEMIDDELDE ONGEPLANDE NIET-BESCHIKBAARHEID LPS	BOVEN-LIGGEND	ONDER-LIGGEND
EIS Z	Infrastructuur RWS dient de functie 'Laten passeren scheepvaart' te vervullen met een ongeplande niet-beschikbaarheid van niet hoger dan, gemiddeld, 90 uur per jaar, gerekend over de levensduur.	Eis W	
VERIFICATIE-FASE	**VERIFICATIEMETHODE**	**BESCHRIJVING VERIFICATIE-METHODE**	
ONTWERP EN BOUW	Verificatiemethode Betrouwbaarheid en Beschikbaarheid, 18 juni 2015, versie 1.0.4	Er wordt een kwantitatieve beschikbaarheidsanalyse gevraagd, waarbij het denkbaar is dat sommige risico's door RWS worden gedragen. In dat geval hoeven ze niet in rekening te worden gebracht door de opdrachtnemer.	



6.3 Processtap: dataverzameling

Bij de kwantitatieve variant van de objectrisicoanalyse wordt de FMEA uitgebreid met het bepalen van faalkansen en herstelduren. Een overzicht van deze variant is gegeven in figuur 6.2.



Figuur 6.2. De stappen en datastromen bij de kwantitatieve ORA

Na de kwalitatieve modellering, beschreven in de paragrafen 0 en 5.3, volgt de kwantitatieve modellering. Alle elementen van een systeem die gevolgen kunnen hebben voor de OTG, worden in deze analyse betrokken.

Er zijn drie typen systeemelementen en daarnaast één type niet-systeemelement: externe gebeurtenissen, alle met een eigen aanpak voor het kwantificeren:

1. **hardware**, bijvoorbeeld een motor, het elektriciteitsnet of een hydraulische cilinder
2. **software**, bijvoorbeeld van het besturingssysteem of de software die wordt gebruikt bij de communicatie tussen bedienaar en systeem
3. **menselijk handelen**, bijvoorbeeld bedienfouten leidend tot storingen, onderhoudsfouten leidend tot latent falen, of onjuiste herstelacties, alsnog leidend tot falen
4. **externe gebeurtenissen**, oorzaken van falen van het systeem, die buiten het normaal functioneren van het systeem ontstaan. Te denken valt aan brand, blikseminslag en scheepsaanvaring. Ook niet-beschikbaarheid door natuurlijke randvoorwaarden (ijs, te harde wind, te hoog water) hoort hier bij.

Alle dragen bij aan het mogelijk falen van het systeem. Daarmee zijn ze onderdelen van de risicoanalyse. Van deze onderdelen moeten twee eigenschappen worden bepaald: de kans op falen, en bij hardware, software en externe gebeurtenissen ook de herstelduur. Beide begrippen worden hieronder nader toegelicht.

Het kansbegrip

In het voorgaande is al veel gesproken over kansen en frequenties, maar een duidelijke definitie is niet gegeven. Kans is een genormeerde maat voor de waarschijnlijkheid van uitkomsten van experimenten, gebeurtenissen genaamd. Het kansbegrip zoals we dat nu kennen, is als eerste gebruikt bij experimenten die, uit symmetrieoverwegingen, statistisch voorspelbare uitkomsten gaven. Voorbeelden hiervan zijn het gooien van een zuivere munt of dobbelsteen, of het willekeurig trekken van een kaart bij een kaartspel. Daarbij werd er al vanuit gegaan dat de som van de kansen op alle mogelijke uitkomsten van het experiment 1 is en dat de kans op een onmogelijke uitkomst 0 is. Deze aannamen vormen een belangrijk axioma: $0 \leq p \leq 1$.

Een kans ligt altijd tussen 0 en 1. Op die manier is onmiddellijk vast te stellen dat de kans op kop bij het gooien van een zuivere munt ½ is en dat de kans op het trekken van klaverenaas uit een kaartspel van 52 kaarten 1/52 is.

Als dit experiment echt wordt uitgevoerd, bijvoorbeeld het 10.000 keer gooien van een zuivere munt, dan zal de relatieve frequentie van kop of munt ook vrijwel exact ½ zijn: 5000 keer kop en 5000 keer munt.

De frequentistische notie van kans ligt dan ook voor de hand: $p=n/M$, waarbij n het aantal gebeurtenissen is waarvan de kans wordt bepaald en M het totaal aantal experimenten.

Met deze definitie als basis kan het kansbegrip ook iemands gevoel van waarschijnlijkheid op een gebeurtenis onder woorden brengen, ook al is er geen sprake van symmetrie en zijn herhaalde experimenten onmogelijk. Uitspraken als ‘de kans dat het morgen niet regent is 0,8 (80 procent)’ vallen onder deze categorie. Op basis van allerlei informatie, opgedaan in het verleden, is zo’n uitspraak mogelijk. De kans is dan niet alleen een eigenschap van het systeem, maar ook van degene die de uitspraak doet. Dit subjectieve kansbegrip wordt het Bayesiaanse kansbegrip genoemd. Het wordt gehanteerd bij het oplossen van vrijwel alle praktische problemen, inclusief het kansbegrip wat ons in staat stelt risicogestuurd aan te leggen, te beheren en te onderhouden.

Kans versus frequentie

In deze handreiking staat veelvuldig de term frequentie, als kans op een gebeurtenis in een tijdsinterval. Onbetrouwbaarheid zoals gedefinieerd in paragraaf 2.4 is daarvan een voorbeeld, namelijk de kans op falen in een bepaalde tijdsspanne. Is de kans in zo’n tijdseenheid groot, dan is het ook waarschijnlijk dat de gebeurtenis meerdere keren optreedt. In dat geval is het praktischer om over te stappen van ‘kans op falen’ op de notie ‘aantal faalgebeurtenissen in een tijdsinterval’.

De relatie is eenvoudig en te bewijzen door het tijdsinterval (oneindig) klein te maken: $p=1-e^{-\lambda}$, waarbij p de kans is dat de gebeurtenis 1 of meerdere keren optreedt en λ het verwachte aantal gebeurtenissen, beide in hetzelfde tijdsinterval. Uitgangspunt bij deze formule is dat λ constant is.

Herstelduur

Voor hardwaresysteemelementen en voor externe gebeurtenissen is de faalfrequentie niet voldoende om de ongeplande niet-beschikbaarheid van de component, en dus van het systeem, te bepalen. De niet-beschikbaarheid is immers een kans per vraag die, voor continu werkende systemen, bestaat uit het product van faalfrequentie en herstelduur. Voor een beschikbaarheidsanalyse zijn dus ook hersteltijden nodig.

De herstelduur is de totale tijd die het vergt om het systeemelement weer werkend te krijgen. Het is dus de tijdsspanne tussen het moment van opmerken van een storing en het moment van vrijgave voor gebruik van de herstelde component. Deze tijd is in het algemeen veel langer dan de reparatietijd, want ook besteltijd, aanrijtijd, testtijd et cetera zijn onderdeel van de herstelduur.

In de risicoanalyse wordt vrijwel altijd aangenomen dat de component na vervanging of herstel weer dezelfde eigenschappen heeft als het oorspronkelijke element: zo goed als nieuw. Het is echter altijd mogelijk om na herstel een grotere, of juist kleinere faalfrequentie aan te nemen.

6.3.1 Hardwarefalen

Componenten functioneren in twee fundamenteel verschillende situaties:

- continu, zoals de energievoorziening via het hoofdnet
- in stand-by mode staand, zoals een noodstroomvoorziening, bijvoorbeeld de nooddiesel.

In het eerste geval wordt falen direct gemerkt, in het tweede geval niet. Het falen van een in stand-by mode staande component wordt pas opgemerkt als de component wordt aangesproken: hij wil niet starten. Bij een component in stand-by mode is dus sprake van een faalkans per vraag. Om dit onmerkbaar falen eerder te ontdekken is een functionele test nodig. Hoe vaker een functionele test wordt uitgevoerd, hoe kleiner de kans is dat de component in de tussentijd (onopgemerkt) faalt. Daarmee wordt de beschikbaarheid van het systeemelement groter, ervan uitgaande dat de inspectie zelf geen (geplande) niet-beschikbaarheid oplevert. Het tijdsinterval voor een functionele test volgt uit een economische optimalisatie en het resultaat van de test wordt gehanteerd in de ORA.
Het spreekt voor zich dat zo'n testinterval ook in het instandhoudingsplan terug moet komen en dat de tests daadwerkelijk moeten worden uitgevoerd.

Het faalgedrag van continu draaiende componenten wordt bepaald door de faalfrequentie (λ) [-/tijd]. Als tijdseenheid wordt veelal een uur gebruikt, heel soms een jaar. Ook wordt wel gewerkt met *mean time between failures* (MTBF), een parameter die gelijk is aan $1/\lambda$, waarbij impliciet wordt verondersteld dat de faalfrequentie niet toeneemt in de tijd.

Het faalgedrag van stand-by componenten wordt bepaald door de faalfrequentie (λ), de herstelduur (θ) en het testinterval (τ) [tijd]. De faalfrequentie betreft dan het onmerkbare falen gedurende de stand-by periode. Hoe langer deze stand-by periode, hoe groter de kans dat de component niet werkt als er aanspraak op wordt gedaan. Periodiek testen (en indien noodzakelijk repareren of vervangen) verkleint de kans dat de component blijkt te falen wanneer hij wordt aangesproken.

Maar let op: zodra een component die normaal in de stand-by modus staat, gaat werken, verandert de kans op falen en dus ook de faalfrequentie. Vrijwel altijd is deze groter dan in de stand-by modus. Zo'n component kent dan ook twee faalfrequenties, één tijdens stand-by en één tijdens de missie.

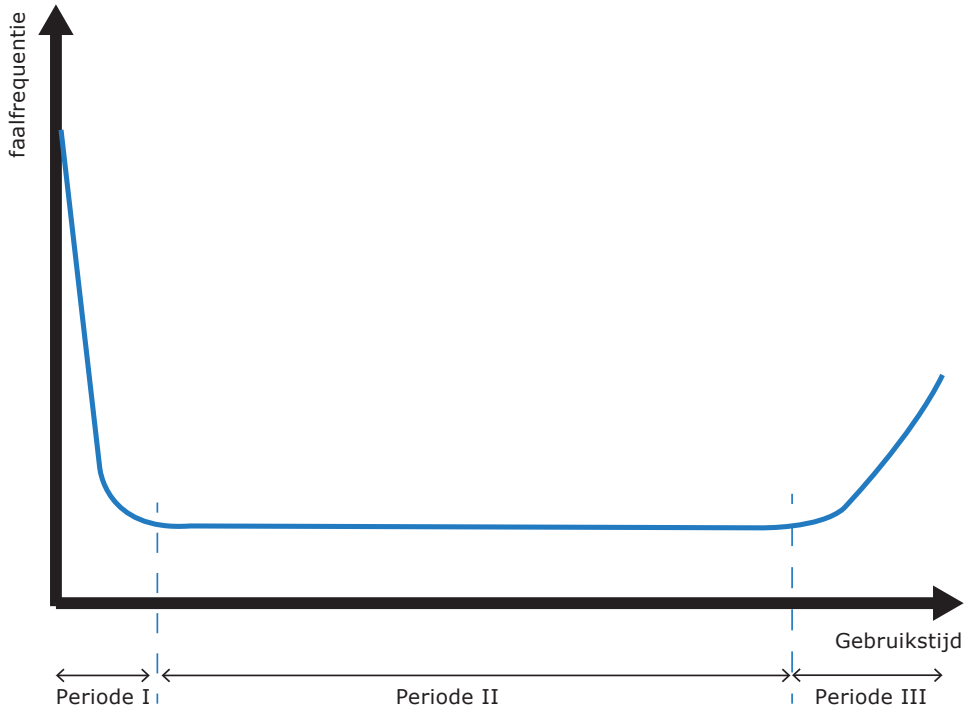
De onderhoudsanalyse

Tijdens het gebruik van een systeem of component is de faalfrequentie niet constant, doordat verschillende perioden in het gebruik ook verschillende oorzaken van falen met zich meebrengen. De faalfrequentie is grofweg in te delen in drie kenmerkende perioden. Figuur 6.3 toont de kenmerkende karakteristiek van de faalfrequentie in de opeenvolgende perioden. Deze karakteristiek staat bekend als de 'badkuipkromme'.

Periode I: Falen door kinderziektes.
Als een component nieuw op de markt komt en vlak na de inbedrijfstelling storingen vertoont, worden deze vaak beschouwd als kinderziektes. Meestal is dan sprake van ontwerp-, fabrieks-, of installatiefouten. Naarmate een component ouder wordt, neemt de kans op dergelijke storingen af.

Periode II: Constant faaltempo.
Na de periode van kinderziektes en voordat de component onderhevig is aan veroudering, is er een periode waarin leeftijd minder relevant is voor de faalfrequentie. Eventuele storingen treden min of meer op willekeurige tijdstippen op en hebben vaak niets te maken met de toestand of de leeftijd van de component.

Periode III: Falen door ouderdom.
Na een bepaalde periode krijgt de leeftijd van een component wél meer invloed op het faalgedrag. In deze periode neemt de kans op storingen toe met het ouder worden van de component. De degradatie van een component wordt dan de dominante oorzaak van falen.



Figuur 6.3: Vereenvoudigde weergave van faalfrequentie in de tijd

Of componenten alle perioden doorlopen en wat de tijdsduur van elke periode is, hangt af van verschillende factoren. De constante faalfrequentie, die bij foutenbomen wordt aangenomen in de *korte termijn kwantitatieve risicoanalyses*, is het faaltempo dat hoort bij periode II. Aan het eind van periode II moet de component dus worden gereviseerd of vervangen.

Met behulp van een gedetailleerde onderhoudsanalyse, die ook rekening houdt met de fasen I en III, wordt de effectieve onderhoudsstrategie vastgesteld. Voor een goed begrip van de toepassing van deze strategie in de opeenvolgende gebruiksperioden volgt eerst een toelichting op de aard en mogelijkheden van 'de onderhoudsstrategie'.

Er zijn drie onderhoudsstrategieën: storingsafhankelijk onderhoud (SAO), gebruiksafhankelijk onderhoud (GAO) en toestandsafhankelijk onderhoud (TAO). Een onderhoudsstrategie wordt toegepast op een element (component) van het systeem, in feite dus een systeemelement van de objecten.

Bij storingsafhankelijk onderhoud (SAO) wordt gewacht tot het systeemelement faalt. Op dat moment, of op het moment waarop blijkt dat het systeem (in stand-by mode) al eerder faalde, wordt het systeemelement vervangen of gerepareerd. Bij gebruiksafhankelijk onderhoud (GAO) wordt de component vervangen of gereviseerd na een bepaalde kalendertijd, of na een bepaalde gebruiksduur, of na een gegeven aantal aanspraken. Het gebruik bepaalt dus de vervanging. Toestandsafhankelijk onderhoud (TAO) houdt in dat metingen uitwijzen wat de toestand van de component is en dat deze wordt vervangen of gereviseerd als de gemeten parameter — storingsvoorspellende grootheid (SVG) genoemd — een bepaalde grens overschrijdt.

De keuze van het type onderhoud gebeurt op basis van kosten en technische (on)mogelijkheden. Kosten zijn de directe onderhoudskosten en de verwachte, maatschappelijke faalkosten. Ook technische mogelijkheden spelen een belangrijke rol: als bijvoorbeeld niets kán worden gemeten, is toestandsafhankelijk onderhoud niet mogelijk.

Dat betekent een keuze voor **storingsafhankelijk onderhoud** (SAO) als sprake is van lage faalkosten en/of slechte voorspelbaarheid (een constante faalfrequentie). Een goed voorbeeld van SAO is het onderhoud aan de lampen van een auto. Dat gebeurt pas als ze (de componenten) falen. Bij componenten die stand-by staan, wordt dat falen niet opgemerkt, ze worden immers niet aangesproken.

Gebruiksafhankelijk onderhoud (GAO) wordt toegepast bij componenten waarvan het aanbreken van periode III (zie figuur 6.3) op basis van het gebruik goed is te voorspellen terwijl de faalkosten hoog zijn. Met de auto weer als voorbeeld, is het vervangen van de distributieriem in de motor, op basis van het aantal kilometers, een goed voorbeeld van GAO. Het is op basis van het gebruik goed mogelijk de kwaliteitsafname te voorspellen en de faalkosten zijn (erg) hoog, namelijk onherstelbare schade aan het hele motorblok. Bij GAO wordt alleen vervangen of gereviseerd. Dit is periodiek en preserverend, of conserverend onderhoud. Het te kiezen interval volgt uit een economische optimalisatie.

Het is overigens niet uitgesloten dat de component toch voortijdig faalt. Die kans wordt (soms) 'restkans' genoemd. De betrouwbaarheid en/of de beschikbaarheid van een component is nooit 100 procent. Ook bij GAO moet het vervangingsinterval onderdeel worden van het instandhoudingsplan en worden geëffectueerd. De aanname van de faalkans van de component is immers gebaseerd op dit interval.

Toestandsafhankelijk onderhoud (TAO) is mogelijk als er iets te meten is waarmee het begin van periode III (zie figuur 6.3) nauwkeurig(er) is te voorspellen en als die meting relatief goedkoop is. Met de auto als voorbeeld is de bandenslijtage een goed voorbeeld van TAO. De diepte van het profiel is nauwkeurig en goedkoop te meten, terwijl de grenstoestand (aantal millimeter

profiel) is voorgeschreven. Bij het eerdere GAO-voorbeeld (vervangen van de distributieriem) is de kwaliteit van de riem ook wel te meten, maar die handeling is erg duur, zodat in dit geval GAO goedkoper is dan TAO.

Bij TAO speelt de inspectie dus de hoofdrol, maar ook de inspectie geeft geen volledige garantie voor feilloos functioneren. Apart van de onmogelijkheid om een 100 procent beschikbaarheid te garanderen, spelen ook de kans op detectie en de nauwkeurigheid van de meting een rol. Het inspectie-interval en de grens waarop wordt afgekeurd, volgen uit een economische optimalisatie en worden gebruikt in de ORA. Ook deze parameters zijn dus uitgangspunten, die in het instandhoudingsplan worden opgenomen. Er kunnen nog andere ontwerpen zijn, een en ander zou in de faaldefinities moeten terugkomen.

Optimalisatie

Een economische optimalisatie op componentniveau blijkt de basis voor de te hanteren parameters: testintervallen, vervangingsintervallen en inspectie-intervallen. Uit deze optimalisatie volgt óók de bijbehorende faalfrequentie van de component.

Er zijn diverse hulpmiddelen om deze economische optimalisatie uit te voeren, bijvoorbeeld het LVO-model van Rijkswaterstaat [12] of RCM-Cost van Isograph [13]. Deze hulpmiddelen maken een afweging op basis van minimale levensduurkosten (LCC). Ze resulteren in de goedkoopste strategie, inclusief de bijbehorende parameters, waaronder dus de faalfrequentie. Ook is het mogelijk om bij het toepassen van RCM-Cost uit te gaan van een gegeven prestatie-eis aan het systeem. Er wordt bijvoorbeeld een faalfrequentie geëist die kleiner is dan de goedkoopste strategie op systeemniveau aangeeft. Als aan deze eis wordt voldaan door suboptimalisatie op elementniveau, geeft het model in het verlengde daarvan een kleiner inspectie-interval of vervangingsinterval.

De hulpmiddelen om de optimale onderhoudsstrategie te bepalen, maken gebruik van een benadering van de faalsnelheid als functie van de tijd, zoals getoond in figuur 6.3.

Daarbij zijn twee situaties van belang: componenten die een constante faalsnelheid hebben, en componenten die onderhevig zijn aan veroudering. Van de eerste groep moet de faalsnelheid (λ) worden geschat. Voor de tweede groep is een schatting van de levensduur (MTBF) en een schatting van de spreiding daaromheen nodig. Op basis hiervan wordt een kansverdeling samengesteld, meestal een *Weibull-verdeling*, maar soms ook een normale verdeling. Meestal wordt de eerste tak van de badkuipkromme, de ‘kinderziektes’, niet gemodelleerd.

Bepalen faalfrequentie

Er zijn drie manieren om de faalfrequentie (λ), of de faalkans per vraag (Q), van een faalmechanisme van een hardwarecomponent te bepalen:

1. statistiek
2. expertmening
3. berekening.

1. Statistiek

Het faalgedrag van hardware, dat wil zeggen van fysieke elementen zoals een pomp of een elektromotor, wordt bijgehouden en verwerkt tot faalkansen. De faalfrequentie of de kans op falen per vraag wordt bijgehouden in generieke databases. Vooral in de offshore industrie en in kernenergiegebonden sectoren zijn veel faalgegevens verzameld, zodat over veel hardwarecomponenten betrouwbare gegevens beschikbaar zijn. Een leverancier kan gegevens aanleveren over de faalfrequentie of faalkans, maar ook over herstelduur, testintervallen, vervangingsintervallen en inspectie-intervallen.

Rijkswaterstaat beheert een database, waarin conservatieve (hoge) faalgetallen zijn verzameld [14]. Voor de systemen, die Rijkswaterstaat laat bouwen en beheren, mogen deze hoge faalgetallen zonder meer worden gebruikt. Als een opdrachtnemer meer betrouwbare componenten gebruikt en dus lagere faalgetallen in zijn analyse wil opnemen, dan moet hij deze betere betrouwbaarheid onderbouwen. De data in de Rijkswaterstaat-database zijn overigens gebaseerd op generieke databases. Het is denkbaar dat Rijkswaterstaat op termijn de faalgetallen aanpast op basis van eigen ervaring.

Het is altijd zaak om te controleren of een component in kwestie wel voldoende vergelijkbaar is met de component in de generieke database waaraan de gegevens worden ontleend en of hij op gelijke wijze wordt gebruikt als deze component. Ook de keuze van bovengenoemde onderhoudsstrategieën speelt een rol. Als GAO wordt toegepast, hangt de faalkans af van het vervangingsinterval. In de praktijk wordt meestal het voorschrift van de leverancier gevolgd, maar door clustering van onderhoud of andere specifieke invloeden, kan de vervanging of renovatie wel eens wat later worden uitgevoerd. Bij die keuze moet dan wel de overweging worden meegenomen en vastgelegd dat de faalkans van de component toeneemt. Iets vergelijkbaars gebeurt bij het vergroten van de inspectie-intervallen bij TAO. De hulpmiddelen LVO-model en RCM-Cost ondersteunen het berekenen van de faalkans.

2. Expertmening
Als geen statistiek voorhanden is, bijvoorbeeld omdat een geheel nieuwe component wordt toegepast, of in een situatie waarvoor de beschikbare generieke data niet geldig zijn, wordt gebruikgemaakt van expertmening. Op grond van ervaring met vergelijkbare componenten in vergelijkbare situaties kan een expert een uitspraak doen over de naar zijn oordeel verwachte faalkans of faalfrequentie. Bij het combineren van de meningen van meerdere experts kan beoordeling van de experts (kalibratie) ertoe leiden dat de mening van een goede expert meer gewicht heeft dan de mening van een minder goede. Een uitgebreide verhandeling hierover is gegeven in [15].

3. Berekening
Ten slotte is het soms mogelijk de faalkans van een component te berekenen, uitgaande van een model van de werking van de component en random invoer van de gegevens in dat model. Deze *structural analysis* wordt vooral toegepast bij componenten die bezwijken door degradatie of (te hoge) belastingen. In Nederland wordt deze vorm van probabilistiek 'Probabilistisch Ontwerpen' genoemd.

Voorbeeld: de ophaalbrug

De ophaalbrug kent de volgende hardware componenten:
- val
- bewegingswerk (elektromotor)
- computer (PLC)
- sensoren (2 stuks).

De drie eerste hardwarecomponenten spelen een cruciale rol bij de hoofdfunctie LPS. De sensoren bepalen of er weer wegverkeer over de brug kan en hebben geen effect op het niet kunnen openen van de brug. Zij spelen een rol bij LPW. Zie ook figuur 5.4.

Het val is een component met een – mits goed onderhouden – erg kleine faalkans, die geleidelijk toeneemt in de tijd. TAO is voor deze component de aangewezen onderhoudsstrategie, met als storingsvoorspellende grootheid (SVG) een detecteerbare scheur. Buiten de scheurdetectie is de kans op falen van het val af te leiden van de voorschriften in de Eurocode, die zijn gehanteerd bij het ontwerpen. De Eurocode, aangewezen door *Woningwet* en *Bouwbesluit*, eist dat bouwkundige onderdelen een faalkans hebben van ten hoogste $8{,}5.10^{-6}$ (0,0000085) per geplande levensduur. In het geval van de ophaalbrug is dat 100 jaar. Als de ontwerp- en bouwprocedures van de Eurocode worden gevolgd, is het aannemelijk dat aan deze eis wordt voldaan. Dat betekent een faalsnelheid van ca. 1.10^{-11} per uur. De hersteltijd van een bezweken val is lang, ten minste een half jaar. Conservatief wordt uitgegaan van 1 jaar.

De elektromotor faalt binnen de geplande levensduur. De faalsnelheid is constant en vindbaar in bestaande databases. De onderhoudsstrategie is GAO. Op gezette tijden worden onderdelen vervangen of gereviseerd, volgens opgave van de fabrikant. Voor het bepalen van de faalsnelheid van de elektromotor in dit voorbeeld is gebruikgemaakt van de RWS-Faaldatabase opdrachtnemersversie [14]. Hierin is gevonden dat de motor in stand-by situatie een faalsnelheid heeft van: $\lambda=1{,}1\cdot10^{-4}$ per uur. In werking is de faalsnelheid ook $\lambda=1{,}1\cdot10^{-4}$ per uur. Blijkbaar is in deze situatie geen significant verschil in faalsnelheid gevonden tussen de werkende en de niet-werkende fase. Voor de hersteltijd van de motor wordt 12 uur (inclusief wacht-, reparatie-, test- en aanrijtijd) aangehouden, wat contractueel is vastgelegd met een onderhoudsbedrijf.

De onderhoudsstrategie van de computer, voor de eenvoud voorgesteld als één PLC, is SAO. Er zijn geen speciale onderhoudsacties voorzien en de PLC wordt vervangen als hij faalt of omdat hij functioneel niet meer voldoet. De faalsnelheid is volgens [14], $\lambda=2{,}08\cdot10^{-5}$ per uur. Het uitvallen is direct merkbaar en herstel duurt minder dan 8 uur.

Ook de sensoren worden onderhouden met SAO. De faalsnelheid is $\lambda=1{,}13\cdot10^{-5}$ per uur, wederom afkomstig uit [14]. Volgens aanname faalt een sensor onmerkbaar, maar wordt dit onmiddellijk geconstateerd bij het weer laten zakken van het val. De herstelduur wordt geschat op 24 uur.

De resultaten zijn samengevat in figuur 6.4.

Element/bouwdeel	Gevolg voor *Laten Passeren Scheepvaart*? [ja/nee]	Type falen - merkbaar - niet-merkbaar - falen per vraag - falen tijdens missie	Faalfrequentie λ [-/uur]	Faalkans per vraag Q [-]	Onderbouwing λ, Q [bronvermelding / verwijzing]	Reparatieduur θ [uur]	Testinterval [uur]	Gekozen OM-strategie	Common Cause Falen (CCF) Groep	Common Cause Falen (CCF) Model	Common Cause Falen (CCF) Parameters	Eventuele opmerkingen
Hoofddraagconstructie												
1401 Val	Ja	Merkbaar, falen tijdens missie	1,00E-11	-	Eurocode	8760	n.v.t.	TAO	n.v.t.	n.v.t.	n.v.t.	
Aandrijving- en beweegingswerk												
1102 Elektromotor	Ja	Niet-merkbaar	1,10E-04	-	RWS Faalgatabase Opdrachtnemers-versie	12	n.v.t.	SAO	n.v.t.	n.v.t.	n.v.t.	
	Ja	Merkbaar, falen tijdens missie	1,10E-04	-	RWS Faalgatabase Opdrachtnemers-versie	12	n.v.t.	SAO	n.v.t.	n.v.t.	n.v.t.	
Bedienings- en besturingsinstallatie												
1431 PLC	Ja	Niet-merkbaar	2,00E-06	-	RWS Faalgatabase Opdrachtnemers-versie	0	n.v.t.	SAO	n.v.t.	n.v.t.	n.v.t.	
Meetinstallatie												
1400 Sensor nr 1	Nee	Niet-merkbaar	1,13E-05	-	RWS Faalgatabase Opdrachtnemers-versie	0	n.v.t.	SAO	Groep 1	Beta	0,1	Gezamenlijk falen herstelduur 24 uur
1400 Sensor nr 2	Nee	Niet-merkbaar	1,13E-05	-	RWS Faalgatabase Opdrachtnemers-versie	0	n.v.t.	SAO	Groep 1	Beta	0,1	Gezamenlijk falen herstelduur 24 uur

Figuur 6.4. Gegevens voor de kwantitatieve analyse

Bayesiaans updaten

Als van een specifieke component zelf gegevens voorhanden zijn of zullen komen, is het zinvol om ook deze in de risicoanalyse mee te nemen. De update van oude data met de nieuwe gegevens kan leiden tot een nieuwe verbeterde schatting van de faalgetallen. Een belangrijke methode van updaten is het 'Bayesiaans updaten'. Zie [16] voor een complete verhandeling van deze aanpak.

Afhankelijk falen (CCF) en redundantie

Afhankelijk falen (*common cause failure, CCF*) is aan de orde als twee of meer gebeurtenissen niet onafhankelijk van elkaar optreden. In dat geval gaat de productregel niet op die geldt voor onafhankelijke gebeurtenissen:

$$\Pr\{A \cap B\} \neq \Pr\{A\} \cdot \Pr\{B\}$$

waarbij Pr {A} de kans is op gebeurtenis A en Pr{A ∩ B} de kans op gebeurtenis A én B. De kans op A én B wordt, door afhankelijkheid, groter dan het product.

Het fenomeen afhankelijk falen speelt een essentiële rol bij redundantie. Redundant ontwerpen betekent het zodanig meervoudig uitvoeren van onderdelen, dat het systeem goed blijft functioneren wanneer één of meerdere onderdelen falen. Dit is een goede manier om de betrouwbaarheid van het systeem te vergroten, mits men rekening houdt met de factor afhankelijkheid. Het simpelweg vermenigvuldigen geeft een te gunstig resultaat. Indien de factor afhankelijkheid meespeelt, zal de werkelijke betrouwbaarheid lager uitvallen. En juist bij het meervoudig uitvoeren van dezelfde onderdelen speelt afhankelijkheid vrijwel altijd een rol. Het is daarom van cruciaal belang om bij een faalkansanalyse de mogelijke afhankelijkheden te identificeren, te analyseren en kwantitatief op de juiste manier in de analyse te verwerken.

Er zijn verschillende bronnen van afhankelijkheid:

1. **Een gemeenschappelijke component**, zoals een voeding.

2. **Fysische interactie**, bijvoorbeeld bij falen als gevolg van hoge temperatuur. Als de desbetreffende componenten zich beide in dezelfde ruimte bevinden, falen ze allebei als de temperatuur te hoog wordt.

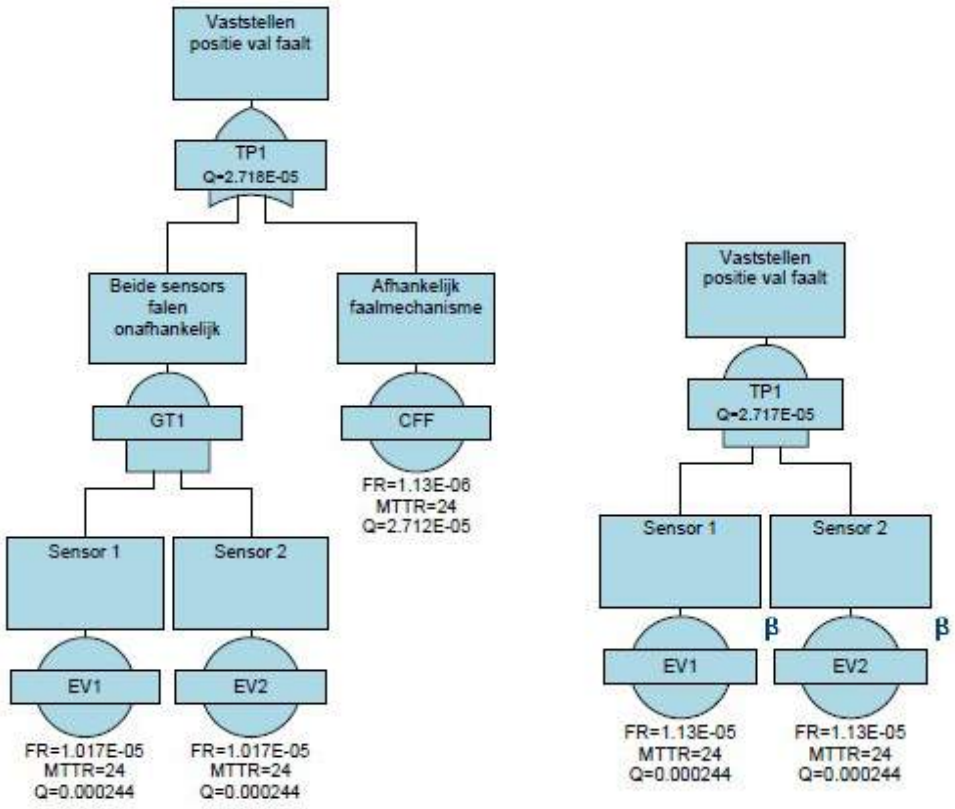
3. **Een gemeenschappelijke productielijn**. Fouten in het ontwerp of bij de fabricage en montage die niet eerder zijn ontdekt, zitten in alle componenten van deze productielijn. Als één component daardoor faalt, wordt het heel waarschijnlijk dat de naastliggend geproduceerde component ook zal falen.

4. **Gemeenschappelijk onderhoud**. Als het onderhoud door één bedrijf wordt uitgevoerd, zullen foutjes bij het onderhoud, bijvoorbeeld door onwetendheid van de onderhoudsmonteur of in het onderhoudsvoorschrift, of het gebruik van onjuiste onderhoudsmaterialen, bij alle vergelijkbare componenten hetzelfde effect sorteren. De eerste bron is eenvoudig te modelleren met de foutenboommethode. Falen van de gemeenschappelijke component betekent falen van het systeem. Bij de overige bronnen is dat moeilijker, doordat de precieze oorzaak niet expliciet is te benoemen en te kwantificeren. Dat betekent in de praktijk dat CCF op basis van statistiek en expertmening wordt verdisconteerd.

Bij Rijkswaterstaat worden twee modellen gebruikt om CCF te verdisconteren. De meest bekende is het β-factormodel. Dit model gaat ervan uit dat er bij alle afhankelijke componenten slechts één faaloorzaak bestaat, waardoor direct alle componenten falen indien deze faaloorzaak optreedt.

Het gezamenlijk falen van een deelverzameling van de afhankelijke componenten wordt dus niet beschreven met het model. Eén component faalt of alle componenten falen.

Een deel van de faalkans van een component wordt dus bepaald door een verschijnsel dat bij alle componenten gelijk is. In feite is dit niets anders dan het expliciet modelleren van een aparte 'virtuele' component, die een gezamenlijk deel is van alle componenten in de groep. Deze virtuele component is dan ook als een separate en expliciete bijdrage in een foutenboom te modelleren. Deze constatering loopt vooruit op de beschrijving van de 'foutenboom' (zie figuur 6.5) en de 'foutenboomanalyse'. Zie daarvoor paragraaf 6.5.



Figuur 6.5. Expliciete (links) en impliciete (rechts) modellering van afhankelijk falen (lees meer in paragraaf 6.5)

Het 'afhankelijke' deel van de faalkans, of bij werkende componenten de faalfrequentie, is de fractie β. De faalfrequentie van deze virtuele component is:

$\lambda_{c,d}=\beta\cdot\lambda_c$

waarin:

β = de fractie afhankelijk falen,
λ_c = de faalsnelheid van een component, veelal te vinden in databases en
$\lambda_{c,d}$ = het afhankelijke deel van de faalsnelheid van een component.

In veel gevallen wordt voor de fractie afhankelijk falen de waarde β=0,1 gekozen. Dat betekent dat 10 procent van de faalfrequentie van de component een faalwijze is waarbij alle componenten falen.

Het tweede model dat Rijkswaterstaat hanteert, is het *Binomial failure rate model* (BFR). Dit model gaat ervan uit dat elke component een onafhankelijke kans p heeft om te falen als gevolg van een gebeurtenis die met een frequentie van μ optreedt. Bij zo'n gebeurtenis faalt dus naar verwachting een deel van de totale groep componenten, maar ze falen hoogstwaarschijnlijk niet allemaal. Deze gebeurtenis wordt een niet-dodelijke shock (*non-lethal shock*) genoemd. Daarnaast wordt een tweede gebeurtenis aangenomen, die met een frequentie ω voorkomt, waarbij alle componenten tegelijk falen. Deze gebeurtenis wordt een *lethal shock* genoemd.

Generieke waarden die vaak worden gebruikt voor de parameters p, μ en ω zijn:

p = 1/3
μ = $0{,}4\cdot\lambda_c$
ω = $0{,}005\cdot\lambda_c$

Het eenvoudige β-factor model beschouwt een CCF-groep als één geheel: alle componenten falen gegarandeerd zodra de afhankelijke gebeurtenis plaatsvindt. Deze modellering leidt bij afhankelijkheid van meer dan twee componenten tot een te pessimistische schatting van de faalkans. Het BFR-model geeft een meer waarschijnlijk beeld van de kans en is in staat om de kans op het uitvallen van enkele in plaats van alle componenten te bepalen. Vandaar dat het β-factor model wordt toegepast bij één, of hooguit twee dezelfde componenten, en dat het BFR-model wordt toegepast als meer dan twee componenten afhankelijk worden geacht.

Een voorbeeld van het toepassen van het β-factor model is het hydraulische bewegingswerk in de keersluis bij Heumen. Deze is geheel enkelvoudig redundant uitgevoerd, waarbij de afhankelijkheid van beide systemen met behulp van het β-factor model is gemodelleerd. Hierbij is β=0,1 aangehouden.

Een voorbeeld van het toepassen van het BFR-model zijn de kleppen en de pompen in de Maeslantkering. Daar is het van groot belang dat slechts een aantal van het totale aantal componenten kan falen. Het functioneren van de kering wordt dan weliswaar vertraagd, maar dat hoeft niet direct tot het falen van de totale kering te leiden. De bovengenoemde waarden van de parameters p, μ en ω zijn in de analyse voor de Maeslantkering gebruikt.

Voorbeeld: de ophaalbrug

De sensoren, die vaststellen dat het val in de juiste positie is, zijn elkaars back-up, ze zijn redundant uitgevoerd. In dat geval moet gekeken worden naar mogelijk afhankelijk falen. In dit voorbeeld zijn beiden sensoren gelijk, komen van dezelfde fabrikant uit waarschijnlijk dezelfde productiebatch en worden tegelijkertijd door één bedrijf onderhouden. Dat genereert afhankelijkheid.

In het voorbeeld is de faalkans van een sensor: $\lambda_c=1{,}13\cdot10^{-5}$ per uur. Indien wordt aangenomen dat het afhankelijk deel 10 procent is van de totale faalkans ($\beta=0{,}1$), dan volgt:

$\lambda_{c,d}=\beta\cdot\lambda_c=1{,}13\cdot10^{-6}$ per uur
$\lambda_{c,i}=(1-\beta)\cdot\lambda_c=1{,}017\cdot10^{-5}$ per uur.

Als hersteltijd was 24 uur aangenomen. De niet-beschikbaarheid van de sensor door het afhankelijke deel wordt daarmee:

$Q_d=\lambda_{c,d}\cdot\theta=2{,}712\cdot10^{-5}$ per vraag

en voor het onafhankelijke deel:

$Q_i=\lambda_{c,i}\cdot\theta=2{,}441\cdot10^{-4}$ per vraag.

De kans dat het systeem faalt is nu uit te rekenen met de formule:

$Q_{systeem}=Q_d+Q_i\cdot Q_i=2{,}718\cdot10^{-5}$ per vraag.

Dit is dus de kans dat beide sensoren defect blijken te zijn wanneer de bedienaar de brug weer laat zakken. Op dat moment ontstaat niet-beschikbaarheid van de brug, die aanhoudt tot de sensoren zijn hersteld of vervangen. Het bovenstaande voorbeeld is ook uitgerekend met behulp van FaultTree+ en het resultaat is weergegeven in figuur 6.5.

6.3.2 Softwarefalen

Het schatten van de kans op falen van software gebeurt met de TOPAAS-methode. Het acroniem TOPAAS staat voor *Task oriented probability of abnormalities analysis for software*. De methode wordt uitgevoerd door onafhankelijke experts, die de scores bepalen op basis van informatie die door de leverancier wordt verstrekt. Deze methode kijkt naar het proces van totstandkoming, het product, de mate van traceerbaarheid en verificatie, de mate waarin het product is getest en de omgeving waarin het product werkt. De methode bestaat globaal uit het vaststellen van de verschillende softwaremodules en de bepaling van de faalkans daarvan. Voor een verdere detailuitwerking wordt verwezen naar het document [17].

Voorbeeld: de ophaalbrug

De communicatie tussen onderdelen van de ophaalbrug verloopt via een besturingssysteem dat bestaat uit hard- en software. De hardware (PLC) is al eerder aan de orde geweest. Voor dit voorbeeld wordt verondersteld dat het besturingssysteem bestaat uit één module. Tabel 6.1 geeft een realistisch beeld van het communicatieproces. In de tweede kolom staan de vragen, in de derde de gegeven antwoorden en in de vierde kolom de toegekende waardering van de gegeven antwoorden. Een antwoord dat rood scoort verhoogt de faalkans, de antwoorden die groen scoren verlagen de faalkans en de wit scorende antwoorden geven een neutraal beeld van de kwaliteit van de software.

TOTSTANDKOMINGSPROCES			
1	Het ontwikkelproces voldoet aan een van de SIL-levels van de IEC 61508	Onbekend	0
2	Gebruik van Inspecties	Inspecties op ontwerpen en code uitgevoerd	0
3	Hoeveelheid wijzigingen ten opzichte van het originele ontwerp/eisenpakket	Zeer frequente of enkele fundamentele wijzigingen	2/3
4	Cultuur en samenwerking	Zelflerende organisatie	-1/2
5	Opleidingsniveau en ervaring ontwikkelaars	Uitstekende kennis en veel ervaring met systeemontwikkeling voor het specifieke domein (onbewust bekwaam)	-1/2
6	Samenwerking met opdrachtgever	Sterk betrokken opdrachtgever met voldoende kennis, met open dialoog en een systems engineeringaanpak.	-1/2
PRODUCT			
7	Complexiteit beslissingslogica	Beslissingslogica en foutherkenning zijn erg eenvoudig, MacCabe Index kleiner dan 10	-1/2
8	Omvang softwaremodule (Lines of code)	Minder dan 1000	-1/2
9	Helderheid gebruikte architectuurconcepten	Er is een scherp benoemde scheiding van taken en verantwoordelijkheden voor componenten beschreven, welke het principe van 'maximale cohesie en minimale koppeling respecteert', en deze is actief bewaakt tijdens het ontwikkelproces	-1/2
10	Gebruik van een certified compiler	Gebruik van een compiler waar men langdurige ervaring mee heeft	0
REQUIREMENTS TRACEABILITY/VERIFIEERBAARHEID			
11	Traceerbaarheid van requirements door het proces heen	Traceerbaar naar architectuur en testen	-1/3

TESTEN			
12	Testtechnieken en dekkingsgraad	Wel testen gedocumenteerd, geen formele testtechnieken gehanteerd; dekkingsgraad onbekend	-1/3
EXECUTIEOMGEVING/GEBRUIK			
13	Multiprocesomgeving	Dedicated CPU en memory op geen, triviaal of Proven OS	-1/3
14	Aanwezigheid representatieve velddata gedurende missie	Beperkte gegevens aanwezig uit eigen draaiperiode	0
15	Monitoring	Langdurige monitoring, maar infrequent missiegebruik	-1/3
		SOMMATIE	**-3 2/3**

Tabel 6.1. Resultaat van een TOPAAS-analyse

De faalkans van de software is 10 tot de macht van de sommatie van de antwoorden. In dit geval dus:

$Q_s = 1 \cdot 10^{-3,667} = 2,15 \cdot 10^{-4}$ per vraag

De software heeft in eerste instantie een belangrijk aandeel in de faalkans. Bij het besturingssysteem van een ophaalbrug zal de invoer van de software na een aantal maanden niet veel meer veranderen. De software volgt vrijwel altijd hetzelfde pad. Fouten die in dat pad zaten zijn verbeterd. Daarmee is de faalkans aanzienlijk gedaald. TOPAAS is (dus) vooral goed in het voorspellen van de faalkans van weinig gebruikte software, zoals veiligheidssoftware.

Reparatie van de software neemt over het algemeen een vrij lange tijd in beslag. Het verbeterprotocol zal zorgvuldig moeten worden nagelopen en alle tests moeten worden herhaald. Verondersteld wordt dat na 24 uur de brug weer kan worden bediend, wellicht onder speciale omstandigheden.

6.3.3 Falen door menselijk handelen

Voor het berekenen van faalkansen ten gevolge van menselijke handelingen is het zogenoemde OPSCHEP-model ontwikkeld. 'OPSCHEP' staat voor 'Ontwikkeling keringen Europoort Project software for the calculation of human error probabilities'. De titel refereert naar de Europoortkering, omdat het model in eerste instantie daarvoor is ontwikkeld. Het OPSCHEP-model is gericht op de kwantificering van menselijke fouten, ofwel de bijdrage van menselijk handelen aan de niet-beschikbaarheid van een (sub)systeem.

Het OPSCHEP-model wordt beheerd door Rijkswaterstaat. Een verdere detailuitwerking is te vinden in [18].

Voorbeeld: de ophaalbrug

De ophaalbrug wordt bediend door een bedienaar en die kan fouten maken. Door zo'n fout kan de veiligheid in het geding komen, maar ook de beschikbaarheid van een of beide hoofdfuncties van de brug. Middels een 'proces-FMEA', ook wel HAZOP (*Hazard and operability analysis*) genoemd, moet formeel worden onderzocht welke fouten de bedienaar zou kunnen maken en welke gevolgen dat heeft. Dit eenvoudige voorbeeld beperkt zich tot één fout: het per ongeluk indrukken van de noodstop. De consequenties daarvan zijn dat de brug vanaf dat moment voor beide hoofdfuncties is gestremd en dat moet worden gewacht op een bevoegde monteur om de noodvergrendeling op te heffen. De herstelduur wordt enigszins pessimistisch geschat op 4 uur.

De kans dat een bedienaar per ongeluk de noodstop bedient, wordt bepaald door het OPSCHEP-model dat Rijkswaterstaat specifiek voor zijn objecten heeft ontwikkeld. De gemaakte fout in dit voorbeeld is een 'uitvoeringsfout', in het OPSCHEP-model P3 genoemd. Er zijn diverse factoren die deze fout beïnvloeden, zie figuur 6.6.

Factor P3 (keuzefout)

Aspect	Waardering	Factor
Wel of geen gebruik van werkinstructies	Voor de taak zijn werkinstructies niet van belang	1,00E+00
Wel of geen nabijheid van componenten	Andere component direct in de buurt maar lijkt er niet op	2,00E+00
Labellen van componenten	Goede labelling	1,00E+00
Mogelijkheden voor het instellen of verstellen van een component in meerdere posities	Maar een positie mogelijk	1,00E+00
Complexiteit	(Zeer) eenvoudige taak	3,33E-01
Het wel of niet werken vanuit een ongemakkelijke werkhouding	Normale werkhouding	1,00E+00
Tijdsdruk	Geen tijdsdruk	1,00E+00
Mate van kennis vaardigheden	Voldoende kennis en ervaring	1,00E+00
Het al dan niet moeten herhalen van handelingen	Het moeten herhalen van handelingen waardoor de scherpte afneemt	3,00E+00
Afhankelijkheid tussen menselijke handelingen	Geen afhankelijkheid	1,00E+00

Motivatie: de omstandigheden bij brugbediening

Basiswaarde:	3,00E-04
Correctiefactor:	2,00E+00
Resultaat P3:	**6,00E-04**

Figuur 6.6. Kwantificering keuzefout door het OPSCHEP-model

Het resultaat, dat wil zeggen de kans dat de bedienaar op de noodstop drukt, is dus $Q_m = 6 \cdot 10^{-4}$ per vraag. De brug gaat vier keer per dag open, dat is ongeveer 1500 keer per jaar. Dat betekent dat volgens het model gemiddeld bijna één keer per jaar per ongeluk op de noodstop wordt gedrukt. Dat is duidelijk te vaak, want in de praktijk gebeurt het per ongeluk op de noodstop drukken hooguit één keer in de levensduur van de brug. Op basis van de bewezen praktijk moet de berekende kans een factor 100 worden gereduceerd: $Q_m = 6 \cdot 10^{-6}$ per vraag. Het OPSCHEP-model is hier te pessimistisch en nodigt expliciet uit om antwoorden te controleren. In dit geval moet het antwoord dus worden bijgesteld.

6.3.4 Falen door externe gebeurtenissen

Een afzonderlijke analyse is nodig om een overzicht te krijgen van externe gebeurtenissen die een bedreiging vormen voor, of direct invloed hebben op prestaties van een object. Onder een externe gebeurtenis wordt een ongewenste gebeurtenis verstaan die buiten het normaal functioneren van het beschouwde systeem ligt, maar toch het falen van het systeem tot gevolg kan hebben. Voorbeelden van externe gebeurtenissen zijn brand, blikseminslag, aanvaring en overstroming.

Met een uitputtende lijst van potentieel bedreigende externe gebeurtenissen wordt een screening uitgevoerd om te bepalen welke specifieke gebeurtenissen een bedreiging vormen voor het functioneren van het object [19]. Voor de analyse van de impact van diverse externe gebeurtenissen zijn deelmethoden voor bliksemrisico [20], brandrisico [21] en aanvaarrisico [22] beschikbaar.

Voorbeeld: de ophaalbrug

Om te bepalen welke externe gebeurtenissen nader moeten worden geanalyseerd, is de *screening externe gebeurtenissen* ontwikkeld. Deze screening beoordeelt of potentieel bedreigende externe gebeurtenissen voor de ophaalbrug ook daadwerkelijk een bedreiging vormen. De screening tool bevat een vaste set van externe, mogelijk bedreigende gebeurtenissen.

De screening geeft aan dat voor de ophaalbrug in het voorbeeld de volgende gebeurtenissen nader moeten worden geanalyseerd:

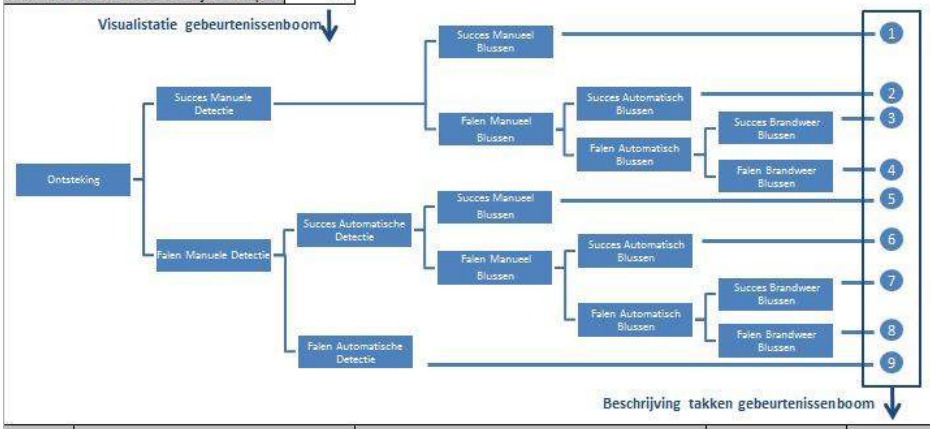
- blikseminslag
- brand
- aanvaring van pijlers, brugdek en brugval
- aanrijding met afsluitbomen
- incident met giftige gassen of chemicaliën naar aanleiding van een transportongeval
- uitval elektriciteitstoevoer.

Voor deze brug is de brandanalyse nader uitgewerkt. Rijkswaterstaat heeft voor de externe gebeurtenis brand het 'brandrisicomodel' ontwikkeld dat in de vorm van een spreadsheet beschikbaar is. Het model heeft als invoer gegevens nodig over de ruimten en scheidingswanden in het object en over de brandgevaarlijke inhoud van de ruimten. Aan de hand van standaard ontstekingskansen wordt de kans op brand in elke ruimte bepaald. De mogelijkheid dat de brand zich uitbreidt, wordt bepaald door de aanwezige detectie- en brandblussystemen en door de brandwerendheid van de tussenwanden. Het model berekent voor elke ruimte waarin zich een ontstekingsbron bevindt de ontstekingsfrequentie en geeft op basis van de door de gebruiker aangegeven herstelduren de niet-beschikbaarheid.

Het resultaat voor de bedienruimte van de brug is gegeven in figuur 6.7. De niet-beschikbaarheid, die door brand wordt veroorzaakt is naar verwachting $Q_b=2{,}24\cdot10^{-4}$. Omdat de machinekamer ook een bijdrage heeft (hier niet getoond) is in het vervolg van dit voorbeeld $Q_b=2{,}29\cdot10^{-4}$ gehanteerd.

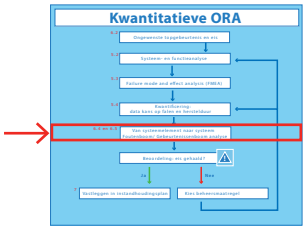
Resultaten

Gemiddelde niet-beschikbaarheid als gevolg van brand in Bedienruimte	2,24E-04
Ontstekingsfrequentie (-/uur):	3,37E-07
Gemiddelde herstelduur bij brand (uur	663



Tak #	Beschrijving situatie	Beschrijving gevolg	Kans (%) op tak, gegeven ontsteking	Herstelduur (uur)
1	Succesvolle manuele detectie en blusactie	Brand beperkt tot component	1,9%	41
2	Succesvolle manuele detectie en succesvolle automatische blusactie	Brand beperkt tot component. Eventuele additionele schade door blussysteem	0,0%	41
3	Succesvolle manuele detectie en succesvolle professionele blusactie	Brand beperkt tot ruimte, of tot gebouw, afhankelijk strategie brandweer	13,1%	730
4	Succesvolle manuele detectie maar alle blusacties falen	Brand wordt niet actief beheerst	1,5%	730
5	Succesvolle automatische detectie en succesvolle manuele blusactie	Brand beperkt tot component	7,8%	41
6	Succesvolle automatische detectie en blusactie	Brand beperkt tot component. Eventuele additionele schade door blussysteem	0,0%	41
7	Succesvolle automatische detectie en succesvolle professionele blusactie	Brand beperkt tot ruimte, of tot gebouw, afhankelijk strategie brandweer	53,1%	730
8	Succesvolle automatische detectie maar alle blusacties falen	Brand wordt niet actief beheerst	5,9%	730
9	Alle detectiemogelijkheden falen, dus geen blusacties	Brand wordt niet actief beheerst	16,7%	730

Figuur 6.7. Resultaat brandanalyse



6.4 Processtap: van systeemelement naar systeem

In de vorige paragraaf zijn de factoren beschreven, die de betrouwbaarheid en beschikbaarheid bepalen op het niveau van elementen van een systeem.

Deze beschrijving op systeemelementniveau geeft nog geen beeld van de performance van het systeem als geheel. Soms is dit voldoende, maar vaak is een beeld van de verwachte betrouwbaarheid en beschikbaarheid van het totale systeem nodig, bijvoorbeeld om te voldoen aan wettelijke eisen of aan afspraken met het ministerie van Infrastructuur en Waterstaat (zie hoofdstuk 2). Er is dus nog een stap nodig van de R- en A-eigenschappen van elementen naar de betrouwbaarheid en/of de beschikbaarheid van het gehele systeem.

Om deze stap te kunnen zetten, is eerst een belangrijke tussenstap nodig, namelijk de bundeling van optimale onderhoudsscenario's tot werkpakketten. Hierbij wordt het werk zodanig gepland dat de uitvoeringskosten van tests en metingen worden geoptimaliseerd. Dat leidt er meestal toe dat inspectie- en testintervallen enigszins gaan afwijken van de optimale situatie op componentniveau en dat de kans op falen en de faalfrequentie toenemen. Deze wijziging zal moeten worden verdisconteerd in de R- en A-eigenschappen van

de systeemelementen. De bundeling van het werk maakt de extra faalkosten als gevolg deze suboptimalisatie echter vrijwel altijd meer dan goed.
Optellen is de meest eenvoudige manier om de R- en A-eigenschappen van de systeemelementen te combineren tot de aspecten betrouwbaarheid en beschikbaarheid van het systeem.

Als van de systeemelementen, die falen van het object kunnen veroorzaken, de faalfrequenties worden opgeteld, geeft dat een conservatief resultaat voor de faalfrequentie λ van het systeem ofwel, de betrouwbaarheid van het systeem. In formulevorm: $\lambda_{systeem} \approx \Sigma \lambda_{systeemelement}$

Hetzelfde geldt voor de beschikbaarheid *U*: de som van de producten van faalfrequentie en hersteltijd van de systeemelementen is een conservatieve schatting van de niet-beschikbaarheid van het systeem:

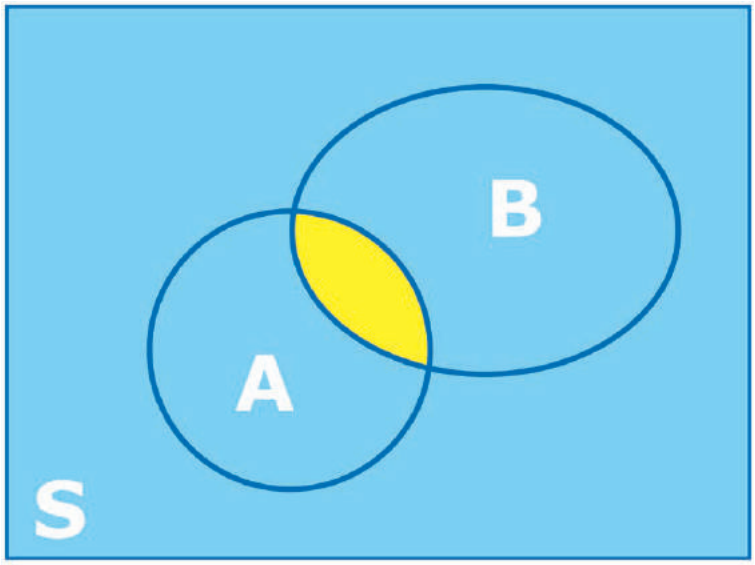
$$U_{systeem} = \Sigma\, \lambda_{systeemelement} \cdot \theta_{systeemelement}$$

waarin θ de hersteltijd is, dus de tijd tussen het opmerken van de storing en het weer functioneren van het systeemelement.

De benadering is conservatief omdat redundantie en afhankelijkheid worden verwaarloosd en omdat de berekening zelf conservatief is. Een optelling is namelijk niet de exacte manier om de faalkans van een systeem te bepalen:

$$p_{systeem} = p_A + p_B - p_A \cdot p_B$$

Bij een optelling wordt de term $p_A \cdot p_B$ verwaarloosd.



Figuur 6.8 Venndiagram faalkans systeem, waarin A een gebeurtenis is uit S (systeem) met kenmerk A, en B een gebeurtenis is uit S met kenmerk B, binnen de verzameling mogelijke gebeurtenissen. Het gele gedeelte wordt dubbel geteld en moet dus weer van de faalkans worden afgetrokken.

Deze conservatieve resultaten worden met behulp van een foutenboomanalyse (FTA) (zie paragraaf 6.5) geëlimineerd.

Voorbeeld: de ophaalbrug

In het voorgaande zijn alle systeemelementen van de ophaalbrug gekwantificeerd. In samenvatting:

- val
- elektromotor
- computer (hardware)
- sensoren (2 stuks)
- bedienaar
- besturingssysteem (software)
- brand

In paragraaf 6.3.1 is vastgesteld dat het val een faalkans heeft van ca. 1.10^{-11} per uur en een herstelduur van een jaar (8760 uur). Hoewel in de praktijk het scheepvaartverkeer weer redelijk snel op gang zou kunnen komen (het bezweken val wordt verwijderd en het nieuwe val wordt elders gefabriceerd), is in dit voorbeeld aangenomen dat het falen van de beide functies LPW en LPS een vol jaar duurt.

Het bewegingswerk is in dit eenvoudige voorbeeld de elektromotor die stand-by en in missie kan falen met dezelfde faalfrequentie van $1,1.10^{-4}$ per uur. Falen tijdens missie betekent falen van zowel LPW als LPS. Falen in stand-by betekent alleen falen van LPS, de brug kan immers niet meer worden geopend. Omdat de missieduur kort is ten opzichte van de stand-byduur, is voor dit eenvoudige voorbeeld het falen gedurende missie verwaarloosd.

De faalfrequentie van de PLC is $2,08.10^{-5}$ per uur en de herstelduur is 8 uur. Falen van de PLC laat LPS falen.

Beide sensoren hebben een faalfrequentie van $1,13.10^{-5}$ per uur en een herstelduur van 24 uur. Falen van beide sensoren betekent dat onbekend is of de brug goed is dichtgegaan. Dat betekent dus falen LPW.

De software faalt met een kans van $2,15.10^{-4}$ per vraag, zie paragraaf 6.3.2. Indien de brug vier keer per dag geopend wordt, betekent dit dus:

$\lambda = 4 \cdot 2,15 \cdot 10^{-4}$ in 24 uur $= (4 \cdot 2,15 \cdot 10^{-4})/24 = 3,58 \cdot 10^{-5}$ per uur

Zoals eerder is opgemerkt, is dit een conservatieve waarde indien de brug enige tijd in gebruik is geweest (en eventuele fouten in de geprogrammeerde routine al zijn verholpen). Reparatie van de software kost 24 uur en falen heeft alleen gevolgen voor LPS.

Ook een bedienfout wordt gemodelleerd via een kans per vraag. In paragraaf 6.3.3 is afgeleid dat deze ongeveer 6.10^{-6} per vraag is. Voor de herstelduur was 4 uur aangenomen. De fout heeft zowel gevolgen voor LPW als LPS.

Ten slotte is het effect van brand berekend (paragraaf 6.3.4). Het resultaat daarvan is al direct in niet-beschikbaarheid uitgedrukt: $2,29.10^{-4}$.

In tabel 6.2 (volgende bladzijde) is dit overzicht nog eens samengevat.

FAALOOR-ZAAK	KANS PER VRAAG	AANTAL VRAGEN PER UUR	FRACTIE VAN DE TIJD	FREQUENTIE PER UUR	HERSTEL-DUUR [UUR]	NIET-BESCHIK-BAARHEID LPS	NIET-BESCHIK-BAARHEID LPW	LPW MET REDUN-DANTIE
RIJBAAN (VAL) BEZWIJKT				1,00E-11	8760	8,760E-08	8,76E-08	8,76E-08
ELEKTROMO-TOR START NIET			9,58E-01	1,10E-04	12	1,265E-03		
ELEKTROMO-TOR STOPT VOORTIJDIG			4,17E-02	1,10E-04	12	5,500E-05	5,500E-05	5,500E-05
PLC FAALT				2,08E-05	8	1,664E-04		
SENSOR 1 FAALT				1,13E-05	24		2,71E-04	2,72E-05
SENSOR 2 FAALT				1,13E-05	24		2,71E-04	
SOFTWARE FAALT	2,15E-04	0,167		3,58E-05	24	8,600E-04		
BEDIENFOUT	6,00E-06	0,167		1,00E-06	4	4,000E-06	4,00E-06	4,00E-06
BRAND						2,290E-04	2,29E-04	2,29E-04
					TOTAAL	0,00258	0,00083	0,00032
					PERCEN-TAGE	0,26%	0,08%	0,03%
					UUR PER JAAR	22,6	7,3	2,8

Tabel 6.2. Eenvoudige optelling niet-beschikbaarheid componenten beweegbare brug

Voor de functie LPS volgt dus een niet-beschikbaarheid van 0,26 procent, ofwel 22,6 uur per jaar. De eis van 1 procent, of 90 uur per jaar, die is geformuleerd in paragraaf 6.2, wordt dus ruimschoots gehaald. Een nauwkeuriger analyse is daarom niet nodig.

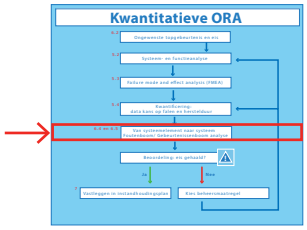
De niet-beschikbaarheid van het wegverkeer is 0,08 procent, wat overeenkomt met gemiddeld 7,3 uur per jaar. Maar de faalkans van beide sensoren is hier opgeteld, terwijl ze in werkelijkheid elkaars back-up zijn, waardoor rekening moet worden gehouden met de 'redundancy (en eventueel afhankelijk falen)'. De juiste wijze van modelleren gebeurt door middel van een FTA.

Dit resultaat van deze analyse voor het object 'ophaalbrug' is ter vergelijking ook berekend met behulp van het programma RCM-Cost van Isograph [13]. Dit programma maakt gebruik van simulatie om de betrouwbaarheid en beschikbaarheid te berekenen (paragraaf 6.5). Het aantal simulaties is een maat voor de betrouwbaarheid van het resultaat. In tabel 6.3 (volgende pagina) zijn bovenstaande resultaten vergeleken met de resultaten uit RCM-Cost bij 10.000 en 10.000.000 simulaties.

FAALOORZAAK	NIET-BESCHIKBAAR-HEID LPS	NIET-BESCHIKBAAR-HEID LPW	RCM-COST LPS	RCM-COST LPW	RCM-COST LPS	RCM-COST LPW
AANTAL SIMULA-TIES	Analytisch		10.000		10.000.000	
VAL BEZWIJKT	8,760E-08	8,76E-08	0	0	3,78E-08	3,78E-08
ELEKTROMOTOR START NIET	1,265E-03		1,28E-03		1,26E-03	
ELEKTROMOTOR STOPT VOORTIJ-DIG	5,500E-05	5,500E-05	5,25E-05	5,25E-05	5,49E-05	5,49E-05
PLC FAALT	1,664E-04		1,66E-04		1,67E-04	
SENSOR 1 FAALT		2,71E-04		2,72E-04		2,71E-04
SENSOR 2 FAALT		2,71E-04		2,72E-04		2,71E-04
SOFTWARE FAALT	8,600E-04		8,52E-04		8,55E-04	
BEDIENFOUT	4,000E-06	4,00E-06	4,43E-06	4,43E-06	4,00E-06	4,00E-06
BRAND	2,290E-04	2,29E-04	2,46E-04	2,46E-04	2,26E-04	2,26E-04
TOTAAL	0,00258	0,00083	0,00260	0,00085	0,00257	0,00083
PERCENTAGE	0,26%	0,08%	0,26%	0,08%	0,26%	0,08%
UREN PER JAAR	22,60	7,28	22,75	7,42	22,50	7,24

Tabel 6.3. Vergelijking niet-beschikbaarheid van het systeem beweegbare brug

Merk op dat de 10.000 simulaties de waarden die uit de analytische berekening komen al dicht benaderen.



6.5 Processtap: foutenboomanalyse

Een foutenboomanalyse (*Fault tree analysis*, FTA) is een analyse, die de kans op falen van het systeem (de kans op de OTG) berekent door uit te gaan van de kansen op falen van de afzonderlijke systeemelementen. Het verschil met de methode 'optellen', die in de vorige paragraaf is beschreven, is dat de FTA kansberekening correct toepast en de factoren redundantie en afhankelijkheid op de juiste wijze verdisconteert. Dit leidt tot een minder conservatief resultaat dan het sec optellen van de gegevens van systeemelementen. De FTA geeft ook een beter inzicht in de zwakke punten van een systeem dan mogelijk is met de methode 'optellen'.

Een FTA kenmerkt zich door de 'foutenboom', een grafische representatie van de samenhang tussen het falen van de verschillende systeemelementen die kunnen leiden tot een OTG.

Een foutenboom bestaat uit één topgebeurtenis (OTG) met daaronder verscheidene basisgebeurtenissen ('*basic events*'). Basisgebeurtenissen beschrijven het falen van systeemelementen. Dit kan het falen zijn van een fysiek systeemelement, maar ook van een softwaremodule, een fout bij menselijk handelen, of het optreden van een externe gebeurtenis. Een basisgebeurtenis of combinatie van basisgebeurtenissen, die nodig maar ook voldoende is voor het optreden van de topgebeurtenis, heet een 'minimale deelverzameling' (of cut set). Een minimale deelverzameling met één basisgebeurtenis is een '*single point of failure*'. Een minimale deelverzameling waarbij twee basisgebeurtenissen moeten optreden om de OTG te veroorzaken, wordt een 2de orde minimale deelverzameling genoemd, et cetera.

Door de kans op elke minimale deelverzameling uit te rekenen ontstaat ook een waarde voor de kans op de OTG. Dit kan, afhankelijk van het type analyse, een faalkans of een frequentie zijn. Als de hersteltijden worden meegerekend, resulteert de analyse in de ongeplande niet-beschikbaarheid van het systeem, wat in feite ook een faalkans is, zoals toegelicht in paragraaf 6.3.1.

De basisgebeurtenissen zijn via logische 'poorten' gekoppeld aan de topgebeurtenis. Er zijn veel poorten mogelijk, maar de belangrijkste zijn:

- EN-poorten (*AND*-gates): voor het koppelen van onderliggende gebeurtenissen die alleen als ze **allemaal** optreden de (sub)topgebeurtenis veroorzaken.
- OF-poorten (*OR*-gates): voor het koppelen van onderliggende gebeurtenissen waarvan er **ten minste één** moet optreden om de (sub)topgebeurtenis te veroorzaken.
- K-uit-N poorten (*Voting OR* gates): voor het koppelen van onderliggende gebeurtenissen waarvan **ten minste K van de N** moet optreden om de (sub) topgebeurtenis te veroorzaken. Deze poort is in feite een samenstelling van EN- en OF-poorten.

Voor het opzetten van een foutenboom geldt een aantal belangrijke regels.

- De topgebeurtenis is altijd het niet voldoen aan een functionele eis of het falen van een systeem. In een foutenboom komen geen 'positieve' gebeurtenissen voor.
- Een foutenboom wordt van boven naar beneden opgezet, tegen de procesflow in. De topgebeurtenis wordt via tussenstappen steeds verder gedecomponeerd tot het niveau van de basisgebeurtenissen.

Het kwantificeren van de basisgebeurtenissen gebeurt met de resultaten van de processtap 'dataverzameling' (paragraaf 6.3). Een FTA gaat uit van een constante

faalsnelheid, ofwel het vlakke deel van de 'badkuipkromme' (zie figuur 6.3). Deze vereenvoudiging betekent dat het berekeningsresultaat voor de te verwachten betrouwbaarheid en/of beschikbaarheid geldt voor de korte termijn, namelijk tot op het moment dat de stijgende tak van de kromme in figuur 6.3 wordt bereikt.

Het berekenen van de faalkans of de faalfrequentie van een systeem is meestal een complexe aangelegenheid. Ook de grafische representatie van het systeem is niet eenvoudig zonder hulpmiddelen te maken. Rijkswaterstaat eist daarom dat een FTA met behulp van een (inter)nationaal erkend programma wordt uitgevoerd. Daarbij moeten de samenhang van de systeemelementen en – per systeemelement – de relevante faalgegevens worden ingevoerd. Het programma verwerkt vervolgens de ingevoerde gegevens tot de minimale deelverzamelingen en de kansen daarop, de kans op de OTG en de grafische representatie van het geheel.

Nadat de foutenboom is gekwantificeerd, moeten enkele controles worden uitgevoerd. De grootste fouten die eventueel bij het modelleren van een foutenboom zijn gemaakt, komen al snel naar boven door de minimale deelverzamelingen met de grootste kans van optreden na te lopen en te doorzien.

Gevoeligheidsanalyse

Daarnaast zijn de faalgegevens die voor de systeemelementen worden gebruikt altijd een schatting. Door een gevoeligheidsanalyse uit te voeren, ontstaat een indruk van de belangrijkheid van de parameters die de betrouwbaarheid en de beschikbaarheid van het systeem bepalen. Hiermee kan dan een optimalisatieslag worden gemaakt. Als bijvoorbeeld het testinterval een grote invloed heeft op de einduitkomst, zal een kortere testinterval de betrouwbaarheid en de beschikbaarheid van het systeem vergroten. Als het testinterval van een component slechts minimale invloed heeft, kan het een overweging zijn het testinterval te verlengen, zonder dat de einduitkomst wezenlijk verslechtert.

De gebruikte programmatuur heeft vrijwel altijd een optie om deze gevoeligheidsanalyse automatisch uit te voeren en er is een aantal indices, die een indruk geven van de belangrijkheid van de systeemelementen in het systeem. De bekendste indices zijn de *Birnbaum importance* en de *Fussell-Vesely importance*.

De *Birnbaum importance* geeft weer hoe gevoelig het systeem is voor de betrouwbaarheid of beschikbaarheid van een systeemelement, ofwel $(\partial Q_{sys})/(\partial q_i)$. Dit is de afgeleide naar het systeemelement. In de formule staat Q_{sys} voor de faalkans van het totale systeem als functie van de tijd, of voor de niet-beschikbaarheid van het totale systeem, terwijl q_i de faalkans of niet-beschikbaarheid van het systeemelement weergeeft. De *Fussell-Vesely importance* geeft het effect op de betrouwbaarheid of beschikbaarheid van het systeem weer als een systeemelement verondersteld wordt perfect te zijn: Q_{sys} indien $q_i=0$.

Simulatietechniek

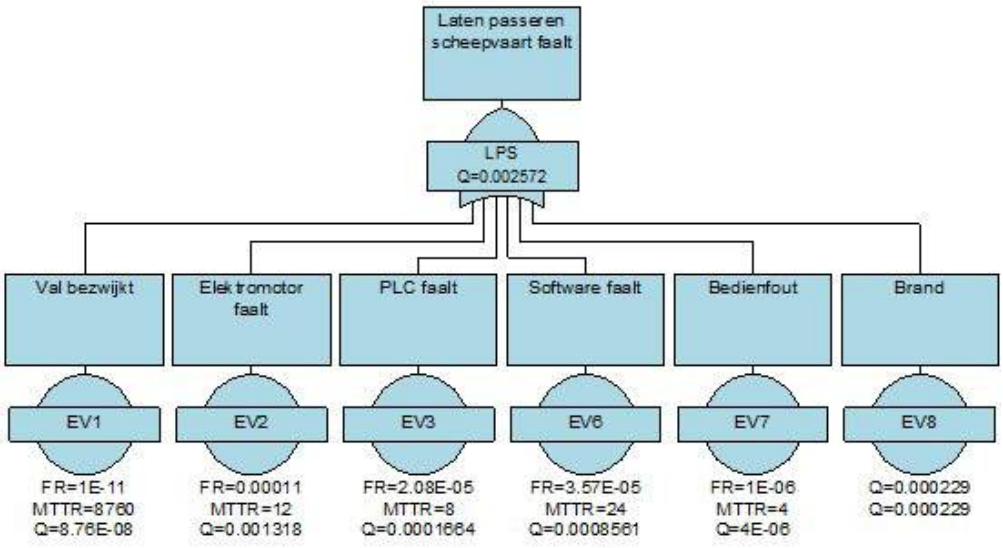
Een interessante ontwikkeling is het voorspellen met behulp van simulaties van de combinatie van betrouwbaarheid en beschikbaarheid én kosten. De verwachte betrouwbaarheid en beschikbaarheid en de verwachte kosten worden dan berekend uit de gemiddelden van vele 'realisaties'. De levensloop van een systeem wordt als het ware nagespeeld. Naarmate meer simulaties worden beschouwd, neemt de nauwkeurigheid van de berekende gemiddelden toe. Ook wordt het met deze simulatietechniek mogelijk verder in de toekomst te kijken. Het resultaat van een FTA geldt voor de korte termijn, tot aan het moment dat de faalfrequentie van een of meerdere componenten gaat toenemen. Maar met de methode van simulatie is het mogelijk de toename van de faalkans als

functie van de tijd te verdisconteren. In combinatie met de kosten van inspecties, reparaties en vervangingen kan voor de nabije toekomst een realistisch beeld worden verkregen van de verwachte prestatie én de verwachte daarmee gemoeide kosten.

Het programma RCM-Cost van Isograph [13] faciliteert een dergelijke berekening. De hoeveelheid benodigde gegevens moet echter niet worden onderschat.

Voorbeeld: de ophaalbrug

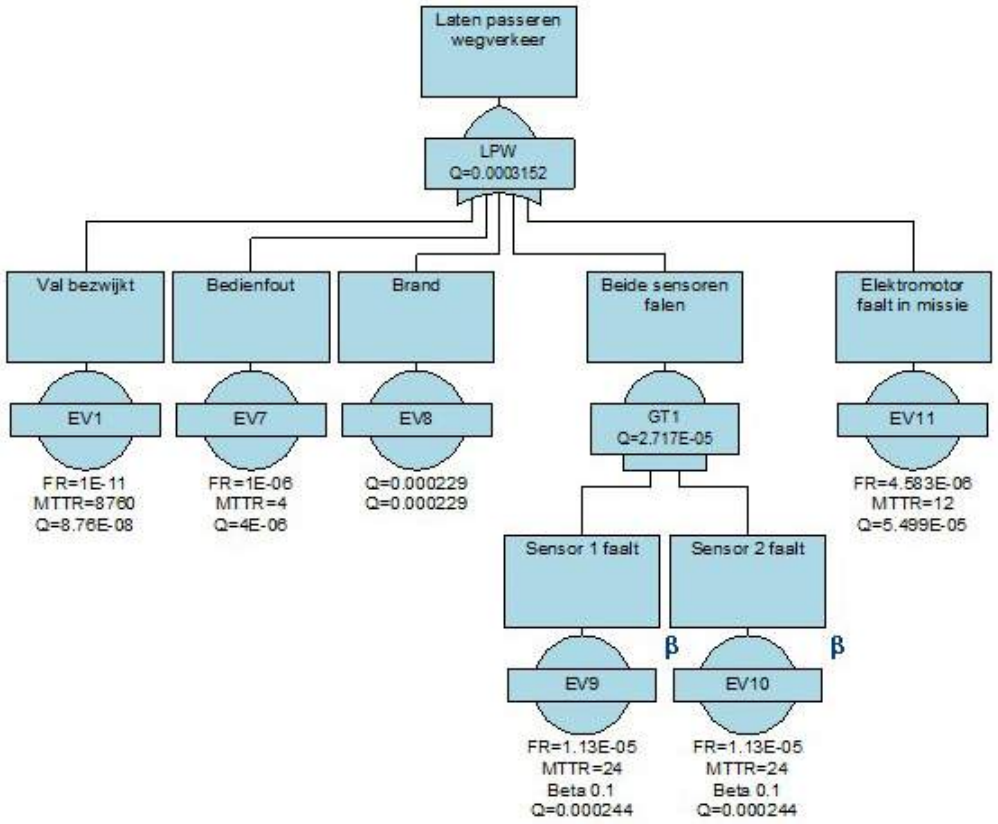
In figuren 6.8 en 6.9 is het resultaat van de foutenboommodellering gegeven voor LPW en LPS. De figuren en het rekenresultaat zijn verkregen met een Fault Tree+ berekening. FR staat voor faalfrequentie, MTTR voor de (gemiddelde) herstelduur en Q voor de niet-beschikbaarheid.



Figuur 6.9. Foutenboom 'laten passeren scheepvaart'

Figuur 6.9 geeft de foutenboom met resultaat voor 'laten passeren scheepvaart'. De sensoren spelen geen rol en het falen van alle overige systeemelementen betekent direct falen van het systeem. Ze zijn met een 'of-poort' gemodelleerd. Het resultaat is een niet-beschikbaarheid van het systeem van 0,002572, conform het resultaat van de vorige paragraaf.

Figuur 6.10 (volgende pagina) geeft de foutenboom met resultaat voor 'laten passeren wegverkeer'. De beide sensoren worden gemodelleerd met een 'en-poort', ze moeten immers beide falen om het systeem, dat de positie van het val registreert, te doen falen. Ze vormen een tweede-orde minimale deelverzameling. De afhankelijkheid tussen beide sensoren is gemodelleerd met het β-factor-model, met β = 0,1. Alle overige systeemelementen zijn zelfstandig in staat de ongewenste topgebeurtenis te veroorzaken. Ze worden in de foutenboom met een 'of-poort' gemodelleerd.



Figuur 6.10. Foutenboom 'laten passeren wegverkeer'

Het resultaat voor LPW is een niet-beschikbaarheid van 0,0003152. Dat is aanzienlijk beter dan de 0,00083 uit de vorige paragraaf. De oorzaak van dit verschil ligt in het modelleren van de redundante sensoren. In de foutenboom is dit wél correct gedaan. De *Fussell-Vesely importance*, zowel analytisch als het resultaat uit FaultTree+ is gegeven in tabel 6.4.

FAALOORZAAK	FUSSELL-VESELY LPS	FUSSELL-VESELY LPS FAULTTREE+	FUSSELL-VESELY LPW	FUSSELL-VESELY LPW FAULTTREE+
VAL BEZWIJKT	3,40E-05	3,40E-05	2,78E-04	2,78E-04
ELEKTROMOTOR START NIET	0,4904			
ELEKTROMOTOR STOPT VOORTIJDIG	0,0213		0,1745	0,1744
PLC FAALT	0,0645	0,0646		
SENSOR 1 FAALT			0,0862	0,0862
SENSOR 2 FAALT				
SOFTWARE FAALT	0,3334	0,3326		
BEDIENFOUT	0,0016	0,0016	0,0127	0,0127
BRAND	0,0888	0,0890	0,7264	0,7264
TOTAAL	1,0000		1,0000	

Tabel 6.4. Fussell-Vesely Importance

Bij de ongewenste topgebeurtenis voor de functie 'laten passeren scheepvaart' zijn de elektromotor, de software en de PLC de belangrijkste verwachte oorzaken van falen. Bij 'laten passeren wegverkeer' is brand de grootste verwachte faaloorzaak.

6.6 Processtap: gebeurtenissenboomanalyse

In de vorige paragrafen is voortdurend sprake geweest van een enkelvoudige relatie tussen een gebeurtenis en het gevolg daarvan voor een systeemelement of het falen van een object. In werkelijkheid kunnen, na een bepaalde (start) gebeurtenis, meerdere andere gebeurtenissen volgen, die bij wijze van een scenario uitmonden in het uiteindelijke effect op het functioneren van het object. De gebeurtenissenboomanalyse (*Event tree analysis*, ETA) is dan behulpzaam bij het in kaart brengen en berekenen van de kans op verschillende gevolgen als resultaat van een gegeven (start)gebeurtenis.

Net als bij een foutenboom is het bijzonder illustratief om een gebeurtenissenboom grafisch te presenteren. Vandaar ook hier de naam 'boom'. De mogelijke scenario's, die kunnen optreden na een gegeven, meestal ongewenste, startgebeurtenis worden door deze visualisatie inzichtelijk. Net als bij een foutenboom kan aan een gebeurtenissenboom de kans op deze scenario's worden toegevoegd.

Een gebeurtenissenboom begint altijd met een startgebeurtenis. Gebeurtenissen die hierop volgen, worden volggebeurtenissen genoemd.

Een gebeurtenissenboom biedt een paar belangrijke extra's:
- Alle vervolggebeurtenissen, die voort kunnen komen uit één specifieke gebeurtenis zijn op een overzichtelijke wijze geordend.
- Een gebeurtenissenboom maakt de situatie transparant en is daarmee in te zetten als communicatiemiddel. Zodra de startgebeurtenis is vastgelegd, kan iedereen inzien en begrijpen waarom bepaalde vervolggebeurtenissen plaatsvinden en waarom andere (combinaties van) gebeurtenissen juist niet plaatsvinden.
- Van de verschillende scenario's is traceerbaar en transparant wat de kans op het optreden van de gebeurtenis is en hoe deze verder kan worden beïnvloed.

De opbouw van een gebeurtenissenboom —uitgaande van een startgebeurtenis— begint met de verzameling van alle relevante volggebeurtenissen. Vervolgens moeten deze in de juiste volgorde worden gezet. Vaak is dat een chronologische volgorde, die samenhangt met de activering van verscheidene (veiligheids)-systemen of fysieke processen die na de startgebeurtenis kunnen plaatsvinden. Vanaf de startgebeurtenis kunnen door middel van aftakkingen per relevante volggebeurtenis scenario's worden ontwikkeld. In veel gevallen is een grote hoeveelheid verschillende scenario's mogelijk, maar deze leiden in de praktijk meestal maar tot een beperkt aantal verschillende gevolgen, zie figuur 6.10.

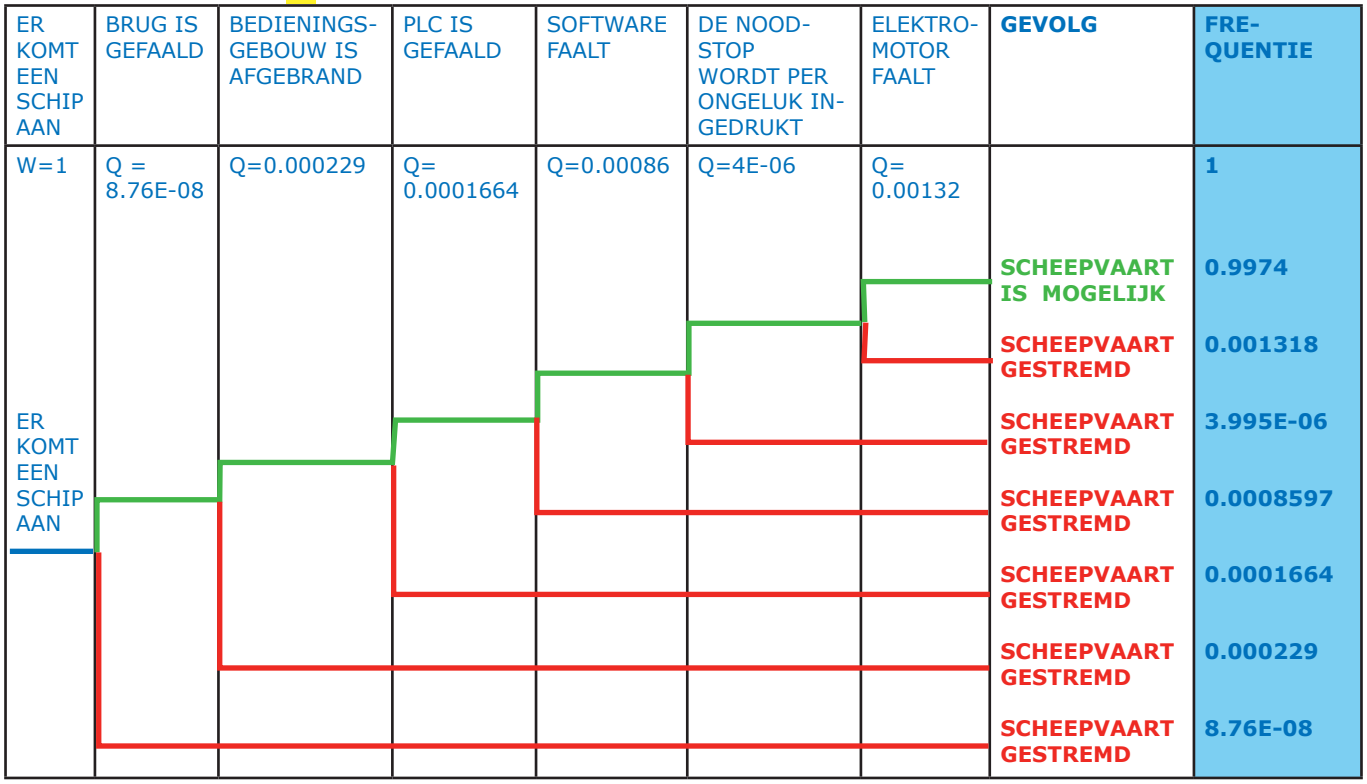
Als de kwalitatieve modellering is afgerond en alle scenario's zijn geïdentificeerd, kan iedere volggebeurtenis worden voorzien van een conditionele kans op optreden. De voorwaarde is dat de voorgaande gebeurtenis heeft plaatsgevonden. De kans op elk scenario wordt bepaald door vermenigvuldiging van de kansen van optreden van de voorgaande volggebeurtenissen, die samen het scenario bepalen. Omdat alle scenario's worden beschreven en de startgebeurtenis een gegeven is met een kans gelijk aan 1, is op elk moment de som van de kansen op de diverse scenario's ook 1. Dit gegeven is een belangrijk controlemiddel bij het kwantificeren.

In paragraaf 6.3 worden mogelijke bronnen voor deze conditionele kansen genoemd. In sommige gevallen is het noodzakelijk om de kans vast te stellen middels een FTA. In dat geval ontstaat er een combinatie van een

FTA (om de kans op een ongewenste gebeurtenis te bepalen) en een gebeurtenissenboomanalyse (om de kansen op de gevolgen te bepalen). De meest bijzondere verschijning hiervan is het vlinderdasmodel, waarbij de initiële gebeurtenis van de gebeurtenissenboom tevens de ongewenste topgebeurtenis van de foutenboom is.

Voorbeeld: de ophaalbrug

In figuur 6.11 is het resultaat van de gebeurtenissenboommodellering gegeven voor de hoofdfunctie LPS.



Figuur 6.11. Gebeurtenissenboom laten passeren scheepvaart

De startgebeurtenis is dat er een schip aankomt. De verdere gebeurtenissen zijn enigszins in tijdsvolgorde geplaatst, maar dat is in dit voorbeeld ietwat geforceerd en voor het resultaat ook niet nodig. De niet-beschikbaarheid heeft hier de notie van kans gekregen, bijvoorbeeld de kans dat het bedieningsgebouw is afgebrand.

Elke tak is een scenario. De kans dat deze voorkomt, is in de rechterkolom gegeven. De optelsom van de kansen van de scenario's die 'Scheepvaart gestremd' opleveren, bedraagt $2{,}577.10^{-3}$. Dit is het complement van de kans van de tak waarbij scheepvaart mogelijk is: 0,9974. Zie ook figuur 6.12, een deel van een rapport van FaultTree+.

RWB V12.0

Consequence Confidence Re

Laten Passeren Scheepvaart

ID	Description	Mean frequency
CQ1	Scheepvaart gestremd	2.577e-3
CQ2	Scheepvaart is mogelijk	9.974e-1

Figuur 6.12. De resultaten van de gebeurtissenboom laten passeren scheepvaart

6.7 Processtap: additionele beheersmaatregelen

6.7.1 Actie voor herstel bij falen door de mens

Eén van de mogelijkheden om de berekende prestatie te verbeteren, is het introduceren van herstelacties. Anders dan het gebruik van redundantie of menselijk falen, gaat het hierbij om een menselijke actie die expliciet wordt meegenomen als herstelmaatregel.

Het idee is dat als een deel van het systeem faalt, een herstelactie kan worden verricht, die ervoor zorgt dat de functie alsnog wordt uitgevoerd. Denk bijvoorbeeld aan het handmatig overhalen van een schakelaar bij het falen van een automatische laagspanningsverdeler of aan het doorknippen van de lier bij de Maeslantkering. Een dergelijke herstelactie kan meestal niet direct in de foutenboom worden gemodelleerd, omdat er meerdere systeemdelen bij betrokken zijn en de actie wellicht tijdsafhankelijk is.

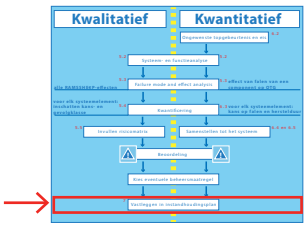
De procedure is dan ook dat eerst de foutenboom zonder herstelacties wordt doorgerekend, waarna voor elke minimale deelverzameling een correctiefactor wordt aangegeven, die de bijdrage van die verzameling aan de totale faalkans reduceert. Voor de Maeslantkering is hiertoe een hersteldatabase en MS-Access applicatie opgesteld, die de minimale deelverzamelingen koppelt en factoren meeweegt zoals uitvoerbaarheid en kans op succes. Vanzelfsprekend moeten de voorgestelde herstelacties praktisch uitvoerbaar zijn en worden geoefend.

6.7.2 Reservedelen

Een andere mogelijkheid om de berekende prestatie te verbeteren, is het gebruik van reservedelen. Dat voorkomt lange hersteltijd wanneer de component niet voorradig is, ook niet bij de leverancier. Het kan dus zinvol zijn om een reservedeel, of zelfs meerdere delen aan te schaffen en deze stand-by te houden. Vooral in een systeem met meerdere dezelfde componenten is het denkbaar dat dit reserveonderdeel wordt ingezet voor een eerder gefaalde component. Dan wordt alsnog misgegrepen, met lange hersteltijd tot gevolg. Het kan ook uit kostenoverwegingen efficiënt zijn om één of meerdere reservedelen in voorraad te hebben.

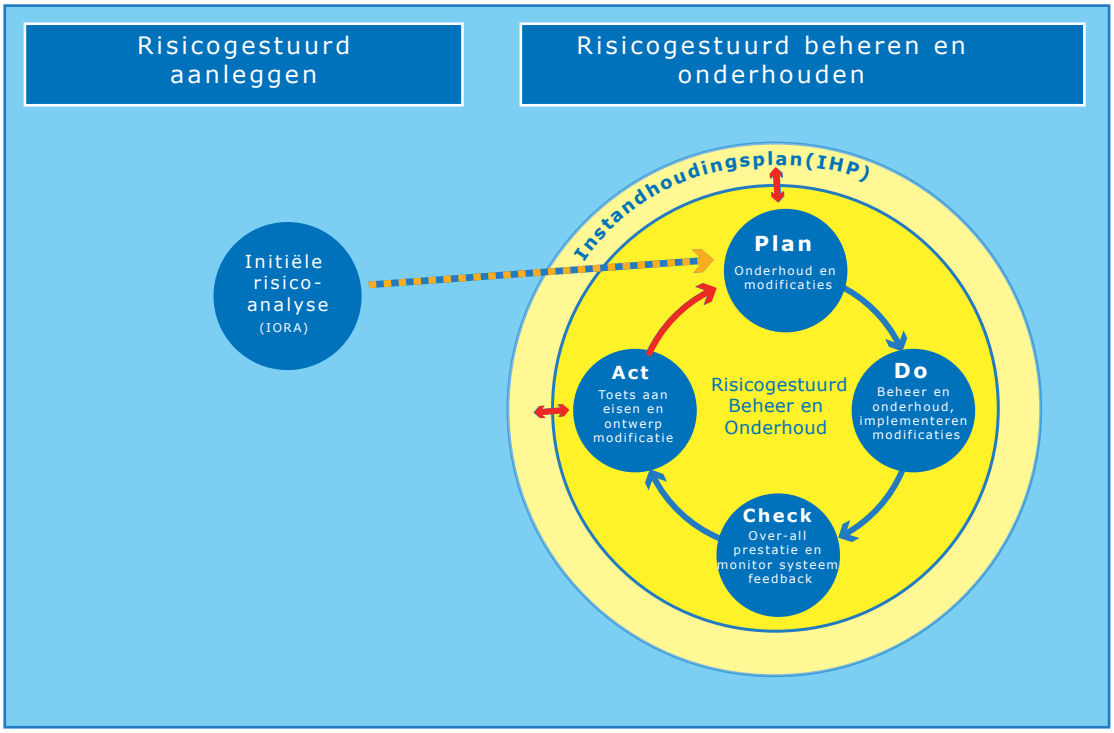
Er is een (analytisch) verband tussen het misgrijpen (geen component voorradig), de lengte van de aanvultijd, het aantal componenten in het systeem en het aantal aanwezige reservedelen. Op basis daarvan is een uitspraak mogelijk over het minimum benodigde aantal reservedelen. Deze analyse wordt beschreven in de handreiking Basismodel Reservedelen [23].

7 De relatie van de objectrisicoanalyse met het instandhoudingsplan



7.1 Inleiding

Dit hoofdstuk beschrijft het vastleggen van de resultaten van de ORA in het instandhoudingsplan (IHP). Deze stap is essentieel omdat de aannamen en randvoorwaarden die in de ORA zijn gehanteerd, moeten worden geborgd in het risicogestuurde beheer- en onderhoudsproces. Zonder deze stap is de verwachting van de prestatie van het object onjuist. In de PDCA-cirkel (zie paragraaf 3.3) gaat het om de stap van 'act' (het aanpassen van de ORA) naar 'plan' (het plannen en programmeren van het noodzakelijke onderhoud). Na aanleg moet de opdrachtnemer de aannamen en uitgangspunten van de initiële risicoanalyse in het instandhoudingsplan aanleveren, waarbij de rode pijlen de acties in de PDCA-cirkel zijn en zodoende een relatie aangeven tussen de ORA en het IHP. Zie figuur 7.1.



Figuur 7.1. De informatie van ORA naar IHP

De aandachtspunten die hiermee samenhangen, komen in dit hoofdstuk aan de orde. Eerst in het kort de functie van een IHP, daarna de wijze waarop de kwalitatieve en de kwantitatieve ORA input leveren voor de instandhoudingsplannen. Ten slotte zijn er enkele aandachtspunten over de borging van het IHP.

7.2 Het instandhoudingsplan

Een instandhoudingsplan (IHP) is een dynamisch document dat door of namens de beheerder wordt opgesteld en periodiek wordt geactualiseerd. Het IHP beschrijft algemene zaken zoals objectgegevens, geldende prestatie-eisen en functies op basis van vigerende wet- en regelgeving, van belang zijnde omgevingsaspecten en de prestatie die het object naar verwachting zal leveren conform de beheer- en onderhoudsmaatregelen, die eveneens in het IHP worden opgenomen. Het IHP dient meerdere doelen. De ORA is één van de bronnen. De overige zaken, die in het IHP worden opgenomen, vallen buiten de scope van deze handreiking, omdat ze niet risicogestuurd zijn. Informatie hoe een IHP op te stellen, is verkrijgbaar bij het steunpunt ProBo.

De ORA kan zowel kwalitatief als kwantitatief worden uitgevoerd (hoofdstuk 3). In beide gevallen resulteert de risicoanalyse in een set beheer- en onderhoudsmaatregelen, waarvan de uitvoering middels het IHP wordt geborgd. De twee varianten van de ORA resulteren in verschillende typen maatregelen. Een kwalitatieve ORA resulteert na periodieke inspectie in een set van onderhoudsmaatregelen die in de aansluitende periode moeten worden genomen. Een IHP dat is gebaseerd op een kwalitatieve ORA, wordt een **(kwalitatief) IHP** genoemd.

Een kwantitatieve ORA geeft, behalve voor deze directe onderhoudsmaatregelen, aanwijzingen voor tussentijdse, gerichte inspecties en uit te voeren tests. Daarbij moet ook een storingsvoorspellende grootheid worden gemeten. Ook kan de herstelduur die in de ORA de vorm heeft van een aanname, in het IHP worden vastgelegd. Een IHP dat is gebaseerd op een kwantitatieve ORA, wordt een **p-IHP (prestatiegestuurd IHP)** of **IHP op basis van ProBO** genoemd.

7.2.1 De kwalitatieve ORA en het IHP

De kwalitatieve ORA bepaalt op basis van inspectie de conditie van de bouwdelen en geeft vervolgens een indicatie van de risico's die een beheerder loopt op alle RAMSSHE€P-aspecten. In risicosessies kunnen risico's in de risicomatrix worden ingevuld, door middel van een combinatie van kans- en gevolgklassen. Op basis van de scores zullen beheer- en/of onderhoudsmaatregelen worden geformuleerd. Voor een nadere invulling, zie paragraaf 5.5.

Deze maatregelen worden in het IHP nader afgewogen, waarbij onderwerpen als versobering, prioritering en/of bestuurlijke afspraken als andere bronnen kunnen fungeren.

Randvoorwaarde is daarbij wel dat transparant blijft wat de risico's zijn van het object en dat het uitblijven van maatregelen leidt tot een toename van risico's en dus in de ORA dient te worden verwerkt.

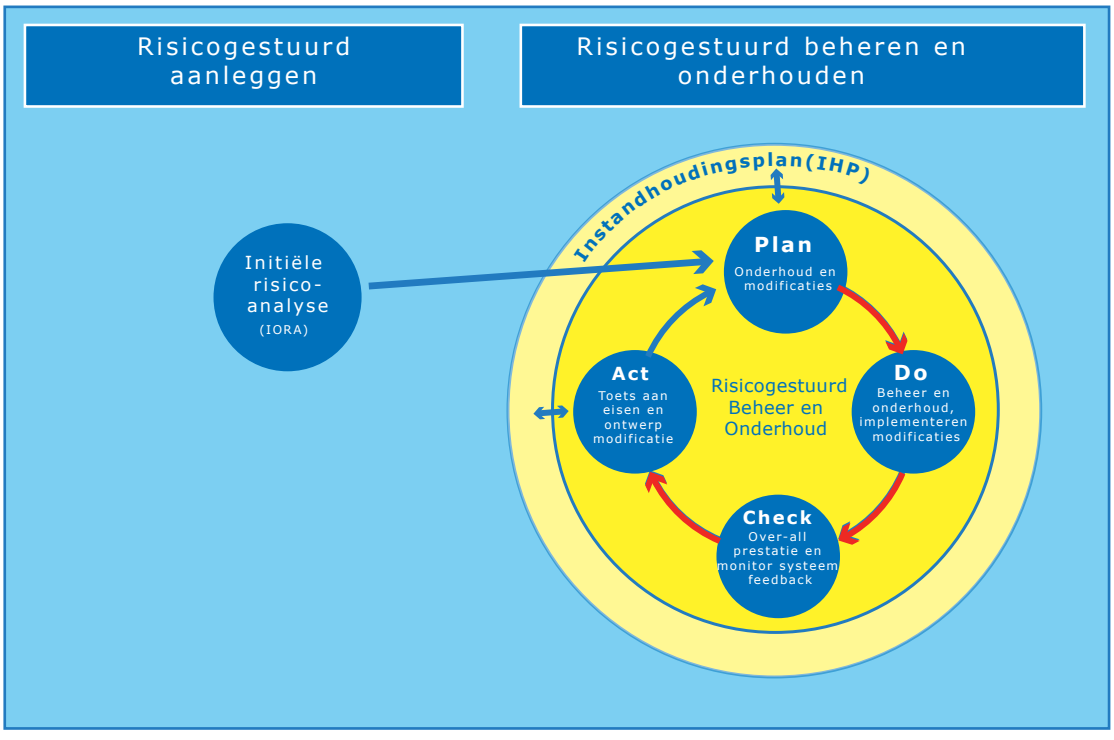
De beheer- en onderhoudsmaatregelen worden in het IHP vastgelegd en voorzien van kosten. Dit is dan de zogeheten *onderhoudsbehoefte* van het object, dat zodoende zal voldoen aan de gestelde eisen en normen vanuit Rijkswaterstaat.

7.2.2 De kwantitatieve ORA en het IHP

Een kwantitatieve ORA geeft de te verwachten prestatie van een object in termen van betrouwbaarheid en beschikbaarheid, gegeven dat het standaard verzorgend onderhoud wordt uitgevoerd volgens de onderhoudsanalyse die als input voor de ORA is gebruikt (zie hoofdstuk 6). Het gaat dan om randvoorwaarden uit de hardware-analyse, zoals taakstellende herstelduren, test- en inspectie-intervallen en de faalfrequentie van systeemelementen in een bepaalde fase van hun levensduur.

De software-analyse kan tot randvoorwaarden leiden. Bij de analyse menselijk handelen liggen die in de sfeer van opleidingsniveau, de frequentie van trainingen, aanwezigheid, gebruik en kwaliteit van werkinstructies en zo meer. De analyse externe gebeurtenissen kan tot randvoorwaarden leiden op het gebied van monitoringsfrequentie, aanwezigheid van een gecertificeerd brandbestrijdingssysteem, gecertificeerde brandcompartimentering, gecertificeerde bliksembeveiligingsinstallaties, onderhoud van omliggend groen en dergelijke. Als het onderhoud dat uit de ORA volgt, niet wordt geprogrammeerd en in het IHP wordt opgenomen, moet net als bij de kwalitatieve ORA de risicoanalyse worden aangepast. Het object zal dan, naar verwachting, een andere (vrijwel altijd mindere) prestatie leveren. De nieuwe prestatieverwachting moet dan ook worden verwerkt in de verwachtingen voor het desbetreffende netwerk en worden getoetst aan de afspraken in de SLA (hoofdstuk 2).

Ook hierbij kan de onderhoudsbehoefte van dat object worden bepaald. De beheer- en onderhoudsmaatregelen worden vastgelegd in een IHP.



Figuur 7.2. Het bijstellen van de ORA naar aanleiding van aanpassingen aan het gewenste onderhoud

7.3 Aandachtspunten bij de borging van beheer- en onderhoudsmaatregelen in het IHP

De beheer- en onderhoudsmaatregelen die voortkomen uit de ORA, moeten worden geborgd in het instandhoudingsplan. Valt het besluit om de maatregelen niet in het IHP op te nemen, dan moet dat expliciet in het IHP worden vermeld, inclusief de argumenten voor deze keuze, het risico dat het gevolg is van de keuze en de onderbouwing waarom dat risico in dit geval toch acceptabel is. Zo zijn bij de eerstvolgende actualisatie van de ORA de niet-genomen maatregel, het genomen risico en de motivatie daarvoor direct weer in beeld.

Anders dan bij de maatregelen uit de kwalitatieve ORA, heeft het niet overnemen van beheer- en onderhoudsmaatregelen uit de kwantitatieve ORA, een directe invloed op de verwachte prestatie van het object. Ook hier zal dan in het IHP worden vermeld met argumenten waarom tot deze keuze is gekomen en wat daarvan de gevolgen en risico's zijn voor dat object.

De monitoring van het gedrag van het object (de 'check' in de PDCA) is vaak uitgebreider dan bij de kwalitatieve variant, omdat kwantitatief meer aspecten moeten worden gemeten. De wijze van monitoring van deze aspecten wordt dan ook in het IHP vastgelegd.

Onderdeel van de kwantitatieve ORA is een (kwantitatieve) onderhoudsanalyse. Hierin is, gegeven het systeem, een optimum bepaald tussen de onderhoudsinspanning en de daarmee verwachte prestatie van het object. De onderhoudsinspanning is taakstellend (verplicht, anders wordt de verwachte prestatie van het object niet meer geleverd) en omvat onder meer:

- onderhoudsintervallen
- herstelduur bij storingen
- testintervallen
- inspectie-intervallen
- grenswaarden van storingsvoorspellende grootheden (SVG)
- vervangingsintervallen.

De genoemde intervallen mogen wel kleiner zijn, maar niet groter dan uit de ORA volgt. Het zijn dus maxima. Dit geldt ook voor de verwachte herstelduur bij storingen. Het is (nog) niet gebruikelijk, maar het blijkt veelal noodzakelijk te zijn om de herstelduur expliciet in de contracten vast te leggen en met enige regelmaat te controleren of de gecontracteerde hersteldurен ook daadwerkelijk worden gerealiseerd.

Ook de maatregel die moet worden genomen bij het overschrijden van een grenswaarde van een 'storingsvoorspellende grootheid' (SVG), moet in het IHP worden opgenomen. Als bijvoorbeeld is besloten dat een scheur in een brugdek wordt gerepareerd als hij groter is dan 10 cm, moet dit uitgangspunt in het IHP zijn vermeld en zal het in de ORA een rol spelen bij het bepalen van de kans op falen van het brugdek.

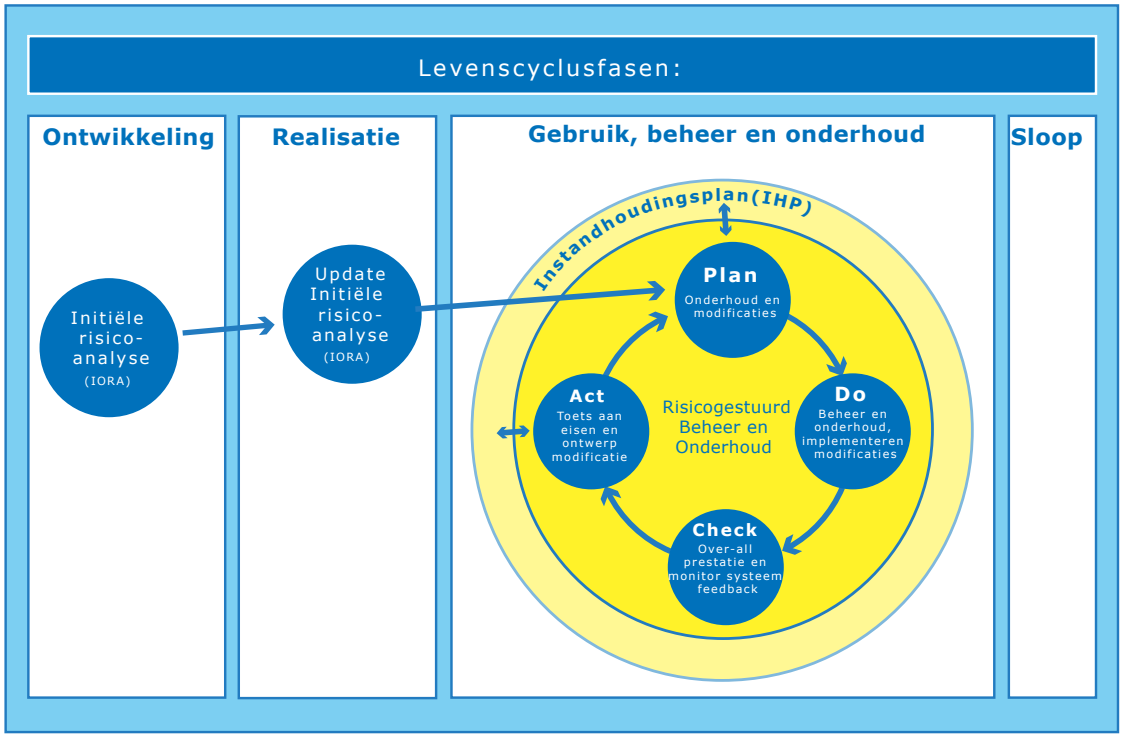
8 Het borgen van risicogestuurd aanleggen, beheren en onderhouden in de eigen organisatie

8.1 Inleiding

Een risicoanalyse is, net als een sterkteberekening, een ontwerphulpmiddel om het gewenste doel te behalen, in dit geval voldoende betrouwbaarheid en/of beschikbaarheid. Bij de aanleg, of bij een grootschalige renovatie van een object, wordt een eerste risicoanalyse opgesteld. Deze moet tijdens het ontwerp- en bouwproces up-to-date blijven en dient achteraf als verificatie van het ontwerp. Zo ontstaat bij oplevering van het object een '*as-is*'-ORA: een risicoanalyse die de werkelijkheid zo goed mogelijk modelleert.

Vanuit de eerste risicoanalyse start een cyclus van continue beheersing van het prestatieniveau van het object. De noodzakelijke beheer- en onderhoudsactiviteiten die uit de risicoanalyse volgen (act), worden in het IHP geborgd (plan), uitgevoerd (do) en gemeten (check). Vervolgens wordt het verschil tussen eisen en gemeten prestaties vastgesteld en wordt de ORA geüpdatet (act). Waar nodig volgen verbeteracties en mogelijke optimalisaties (plan). Daarmee wordt de PDCA-cirkel opnieuw doorlopen (zie figuur 8.1).

Als van een bestaand object geen initiële risicoanalyse is gemaakt, dan dient dat alsnog te gebeuren. Het resultaat is dan niet het gewenste, maar het aanwezige prestatieniveau. Vaak zijn ook beheer- of onderhoudsmaatregelen benoemd en in de ORA verwerkt, zodat er zicht is op de mogelijke prestatie van het object. Ook kan de ORA dan worden gebruikt om verbeteringen in het bestaande ontwerp te realiseren. In beide gevallen is deze ORA het startpunt voor het beheer en onderhoud in de gebruiksfase.



Figuur 8.1. PDCA-cyclus na de eerste objectrisicoanalyse

In die beheer- en onderhoudsfase is de ORA een onmisbaar onderdeel om de prestaties van het object continu te beheersen, dus om duurzaam in de organisatie te borgen dat het object aan de prestatie-eisen blijft voldoen. Binnen de randvoorwaarde dat wordt voldaan aan de vigerende prestatie-eisen, kunnen de onderhoudskosten over de levensduur worden geminimaliseerd. Als een organisatie dit proces onder de knie heeft en voor haar objecten op elk moment kan aantonen dat aan de prestatie-eisen wordt voldaan, is de organisatie 'in control' met betrekking tot de prestaties van haar assets en de daarvoor nodige investeringen.

Het blijkt in de praktijk niet vanzelfsprekend te zijn dat de status 'in control' na de initiële implementatie van het risicogestuurde werken actueel blijft. Onder invloed van de werkdruk, reorganisaties en het verloop van betrokken medewerkers verzwakt de aandacht voor het transparante procesmatige werken en het aantoonbaar vastleggen van (deel)resultaten. Dit hoeft niet te betekenen dat de organisatie niet meer in staat is de prestatie van het object vast te houden, maar wel dat dit niet meer aantoonbaar is. Om de status 'in control' te borgen, moeten de processen niet alleen tijdens de implementatie worden ingericht, maar blijvend in de PDCA-cirkel worden geëvalueerd.

Dit hoofdstuk beschrijft de randvoorwaarden voor de organisatie van het risicogestuurde aanleggen, beheren en onderhouden. In een aantal gevallen is die aanpak al in de organisatie geborgd. Zo stelt de *Landelijke tunnelstandaard* [7], die door het Bestuur van Rijkswaterstaat is vastgesteld als dé standaard voor tunnels van Rijkswaterstaat, ook eisen aan de processen en de beheerorganisatie van een tunnel. Het beleggen van de rollen draagt bij aan het borgen van de kwaliteit van het beheer- en onderhoudsproces. Het is zaak om de rollen die nodig zijn voor de risicogestuurde werkwijze op verstandige wijze te combineren met de rollen die de *Landelijke tunnelstandaard* noodzakelijk acht.

8.2 Borging risicogestuurd aanleggen

Bij de aanleg, of bij grootschalige renovatie van een object, hanteert Rijkswaterstaat het integraal projectmanagementmodel (IPM-model). De kwaliteit van de initiële risicoanalyse wordt in eerste instantie bepaald door het kwaliteitssysteem van de opdrachtnemer. De technisch manager toetst met behulp van systeemgerichte contractbeheersing (SCB) het werk van de opdrachtnemer. Dit kan nog wel eens afwijken met wat voor beheer en/of de beheerder van belang is. Het is dus zaak om in zo'n vroeg mogelijk stadium, als de beheerder bekend is, daarmee nader af te stemmen. Afhankelijk van de specifieke aard en omvang van de analyse wordt de hulp van adviseurs ingeroepen.

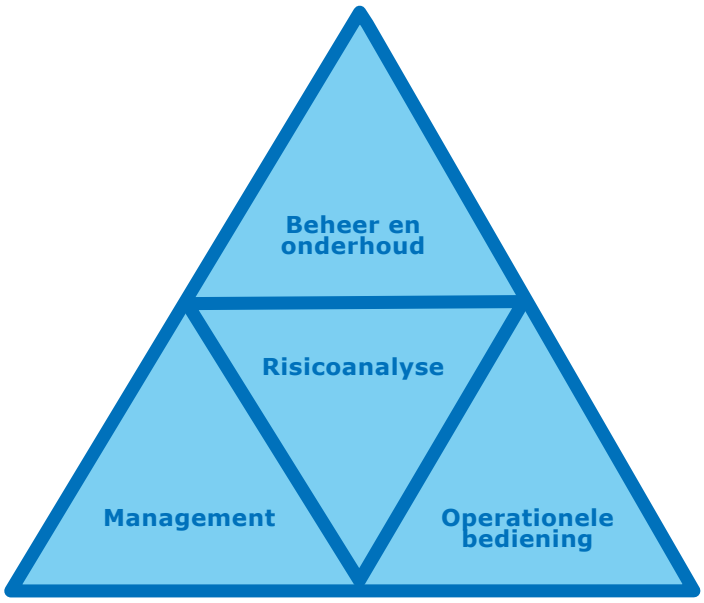
In sommige gevallen kan de technisch manager specifieke wensen (zoals externe reviews) hebben voor de borging van de kwaliteit van de initiële risicoanalyse. Dit wordt dan altijd in samenspraak met de betrokken adviseur vooraf vastgelegd in het zogenaamde productkwaliteitsplan.

8.3 Borging risicogestuurd beheren en onderhouden

In de beheer- en onderhoudsfase is behalve techniek ook een passende organisatie nodig om het beheer en onderhoud op een beheerst niveau te houden. Het aantoonbaar 'in control' zijn (de essentie van risicogestuurd beheer en onderhoud) vraagt een procesgerichte manier van werken met de ORA als hart van de risicosturing. De daarvoor noodzakelijke processen liggen in de sfeer van:

- de inrichting van de organisatie (structuur, taken, verantwoordelijkheden en bevoegdheden, sturingslijnen)
- kennis en ervaring (functieprofielen, opleidingen, ontwikkeling) en
- bedrijfscultuur (gedrag, relevante competenties, bijvoorbeeld op het gebied van veiligheid).

Drie processen beïnvloeden het prestatieniveau van het object direct: het beheer- en onderhoudsproces, het bedienproces en het managementproces, zoals gevisualiseerd in figuur 8.2.



Figuur 8.2. Processen die de risicogestuurde werkwijze beïnvloeden

8.3.1 Het beheer- en onderhoudsproces

De objecten van Rijkswaterstaat zijn onderhevig aan veroudering, slijtage en veranderende omstandigheden. Onderhoud, renovatie en vervanging of uitbreiding zijn essentieel om blijvend te voldoen aan de prestatie-eisen. Het risicogestuurde onderhoudsproces voorziet hierin volgens een PDCA-cirkel.

Planfase

Kenmerkend voor de 'plan'-fase is het omzetten naar concrete plannen van beheer- en onderhoudsactiviteiten (aangenomen in de kwantitatieve ORA) of maatregelen (volgend uit de kwalitatieve ORA). Samengevat worden de concrete plannen toe- en/of ingevoegd aan het instandhoudingsplan. Deze stap omvat alle beheer- en onderhoudsactiviteiten (strategie, duur, frequentie, aantallen, kwaliteit, kosten) en ook de werkwijzen bij het gebruik van het object (procedures, werkinstructies).

De activiteiten, die in het instandhoudingsplan zijn opgenomen, moeten uitvoerbaar worden gemaakt door de organisatie (taken, bevoegdheden, verantwoordelijkheden, in- en uitbesteding/contractering). De concrete plannen worden in een planning uitgezet en in de 'do'-fase uitgevoerd. Soms impliceert dat geplande niet-beschikbaarheid van het object.

De producten uit de 'plan'-fase zijn:
- een bijgesteld, actueel instandhoudingsplan
- aangepaste contracten, in lijn met het aangepaste IHP.

Do-fase

Kenmerkend voor de 'do'-fase is de daadwerkelijke uitvoering van werkzaamheden en maatregelen, die in de 'plan'-fase zijn gedefinieerd en in het instandhoudingsplan zijn vastgelegd. Deze activiteiten zijn taakstellend. Ze *moeten* worden uitgevoerd om de gewenste prestatie van het object te borgen. Hierbij wordt gebruikgemaakt van procedures en werkinstructies. Voor zover activiteiten uit de kwantitatieve ORA voortkomen, spelen ook prestatie-eisen aan systeemelementen, frequenties, doorlooptijden van inspectie-, test- en onderhoudswerkzaamheden en storingshersteltijden een rol. Ook deze parameters kunnen taakstellend uit de ORA volgen. Ze borgen de betrouwbaarheid en beschikbaarheid van de functies van het object.

De mogelijke producten uit de 'do'-fase zijn:
- toegepaste inspectieplanning, inclusief de werkelijke inspectie-intervallen
- inspectierapporten, inclusief het verloop van conditieparameters
- toegepaste testplanning, inclusief de werkelijke testintervallen
- testrapporten, inclusief het aantal defecten of afkeuringen na een test
- storingsdatabase, inclusief opgave werkelijke herstelduren
- *root cause analyses* voor ingrijpende of terugkerende storingen
- opgave van daadwerkelijke beschikbaarheid, inclusief weergave niet-beschikbaarheden ingedeeld naar de oorzaken van:
    - gepland onderhoud
    - inspecties
    - tests
    - storingen (ongepland onderhoud)
- afgetekende procedures en werkinstructies.

Check-fase

De 'check'-fase is bedoeld om de gegevens en informatie uit de 'do'-fase te monitoren en te evalueren. Het is essentieel dat de daarvoor relevante informatie in de 'do'-fase goed wordt geordend en vastgelegd door de beheerder. In essentie richt het monitoringsproces zich op het signaleren en tot bruikbare informatie verwerken van afwijkingen van zowel het proces en de plannen als de technische staat van een object.

Parameters, die kunnen afwijken zijn onder meer:
- storingsfrequentie en faalmechanismen
- herstelduren, test- en inspectieresultaten
- onverwachte trends of meetwaarden in storingsvoorspellende grootheden (SVG, zie hoofdstuk 6)
- visuele afwijkingen aan het object
- afwijkingen in het beheer van reserveonderdelen
- onverwacht menselijk handelen, onverwachte reacties van software
- afwijkingen in getraindheid/opleidingsniveau van de medewerkers.

De mogelijke producten uit de 'check'-fase zijn:
- analyses van afwijkingen
- rapportage van wijzigingen.

Act-fase
In de 'act'-fase volgt de vertaling van de gegevens en voorstellen uit de 'check'-fase naar concrete onderhoudsmaatregelen, inclusief mogelijke systeemwijzigingen. Maatregelen en eventuele systeemwijzigingen worden in de ORA verwerkt, waarmee een nieuw prestatieniveau vast komt te liggen. Ook worden de prestatie-eisen geëvalueerd en zo nodig bijgesteld. Hierbij doet zich de mogelijkheid voor om te optimaliseren.

De producten uit de 'act'-fase zijn:
- indien gewijzigd: een bijgestelde systeembeschrijving
- indien gewijzigd: een bijgestelde fysieke decompositie
- een bijgestelde ORA
- een bijgestelde prestatie.

8.3.2 Het operationele (bedien)proces
Het operationele bedienproces is cruciaal voor het goed functioneren van (een deel van) het areaal en daarmee essentieel voor het voldoen aan de prestatie-eisen. Wanneer de organisatie van de bediening niet goed is belegd, kan dit grote invloed hebben op het uiteindelijke prestatieniveau. In sommige gevallen is de prestatie-eis alleen haalbaar als in de sfeer van opleiding, motivatie, hulpmiddelen en dergelijke specifieke eisen worden gesteld aan het operationele proces. Dit proces moet daarom duidelijk in een draaiboek zijn beschreven, inclusief de structuur van de bedienorganisatie, beredeneerd vanuit de te behalen prestaties [24].

8.3.3 Het managementproces
Een belangrijk aandachtspunt bij de invoering en borging van risicogestuurd beheer en onderhoud is de rol van het management. Daaronder vallen de sturing, de regievoering en de eindverantwoordelijkheid voor het goed functioneren van de objecten. Door de organisatie te ondersteunen, maakt het management de realisatie en duurzame borging van de gewenste situatie (voldoen aan de prestatie-eisen) mogelijk. Tevens heeft het management de voorwaardenscheppende taak om behoeften in termen van budget, capaciteit en dergelijke vanuit de beheer- en onderhoudsprocessen te vertalen naar de behoeften van de organisatie. Deze vertaalslag vereist communicatie met de budgetverstrekkers, het bestuur (en mogelijk de doorwerking daarvan in de politiek) en soms ook de omgeving en de media. Dit geldt zowel voor de regionale beheerder als voor landelijk opererende diensten van Rijkswaterstaat.

Beheer en onderhoud zijn bij Rijkswaterstaat op verschillende niveaus belegd. Een beschrijving van de organisatie van het beheer en onderhoud moet dan ook zijn uitgesplitst naar elk van die niveaus.

Strategisch
Op strategisch niveau worden afwegingen gemaakt over budget, capaciteit en de daarmee te leveren prestaties. Voor- en nadelen van keuzes moeten voor de beslissers helder zijn, zodat zij weloverwogen en goed onderbouwd besluiten kunnen nemen. Alle hiervoor noodzakelijke informatie moet beschikbaar zijn.

Tactisch
De beslissingen, die op strategisch niveau zijn genomen, worden doorvertaald naar de regionale organisatieonderdelen, die, als product van hun programmeerproces, voorstellen doen voor clustering van onderhoud. Ook wordt op dit niveau de inkoop van onderhoudsdiensten geregeld.

Operationeel
De regionale organisatieonderdelen, met name de districten, zijn belast met de verantwoordelijkheid voor de dagelijkse beheer- en onderhoudswerkzaamheden van de objecten. Voor de succesvolle uitvoering van risicogestuurd beheren en onderhouden is een goede invulling van deze verantwoordelijkheid van groot belang: de werkzaamheden hebben een grote invloed op het uiteindelijke prestatieniveau. De regionale organisatieonderdelen beheren de opgestelde ORA's, leggen de aannamen en de resultaten van risicoanalyses samen met de berekende kosten vast in instandhoudingsplannen en zorgen ervoor dat de in deze plannen genoemde maatregelen worden uitgevoerd. Daarnaast wordt de operationele bediening van de objecten door het landelijke organisatieonderdeel Verkeer- en Watermanagement (VWM) uitgevoerd.

De regionale onderhoudsorganisatie en de operationele (bedien-)organisatie spelen een belangrijke rol bij het leveren van de gewenste prestaties van de netwerken. Een belangrijke notie bij de invoering van risicogestuurd aanleggen, beheren en onderhouden is het scheiden van de verantwoordelijkheden van de assetmanager en de prestatiemanager. De assetmanager is verantwoordelijk voor het dagelijks beheer en onderhoud van het object, de prestatiemanager stelt periodiek de prestatie van het object vast. Hij doet dat onafhankelijk van de assetmanager. Rijkswaterstaat vindt het niet wenselijk om deze verantwoordelijkheden te combineren. De scope van de assetmanager is immers veel groter dan alleen de prestaties van de assets. Politieke-, economische- en omgevingsbelangen kunnen strijdig zijn met de gewenste prestatie. De assetmanager maakt daarin een afweging. Vanzelfsprekend is een goede samenwerking en informatiedeling tussen beide managers essentieel.

8.4 Randvoorwaarden aan de beheer- en onderhoudsorganisatie

Om het risicogestuurde beheer en onderhoud te kunnen uitvoeren, moeten de hierboven genoemde processen aan een aantal randvoorwaarden voldoen. De detaillering en diepgang van deze randvoorwaarden variëren voor de verschillende objecttypen en zijn afhankelijk van de complexiteit van het object. De generieke randvoorwaarden laten zich categoriseren naar:
- mensen
- methoden
- middelen

8.4.1 Mensen
De risicogestuurde werkwijze heeft als gevolg dat continu moet zijn geborgd dat de vereiste competenties en vaardigheden in voldoende mate aanwezig zijn. Aspecten, die het prestatieniveau beïnvloeden en minimaal moeten worden beschouwd en periodiek geëvalueerd, zijn:

- de beschikbaarheid van medewerkers met de juiste kennis, competenties en vaardigheden, met het strategische HRM-plan als belangrijk hulpmiddel voor borging
- het duidelijk en transparant vastleggen van de taken, verantwoordelijkheden en bevoegdheden van medewerkers, waarbij de RASCI-methode een belangrijk hulpmiddel is
- de kennis en ervaring van de medewerkers, waarvoor het HRM- en opleidingsplan belangrijke hulpmiddelen zijn
- een beschrijving van de trainingen en opleidingen voor huidige en nieuwe medewerkers.

8.4.2 Methoden

In de ORA zijn uitgangspunten verwerkt over hoe het onderhoud en de bediening moeten worden uitgevoerd. Om de objectrisicoanalyse valide te laten zijn, moet conform deze uitgangspunten worden gehandeld.

Hiervoor is onder meer het volgende nodig:

- methoden, waarmee de prestatie wordt gemeten en vastgelegd
- inspectie- en testprotocollen
- procedures en/of werkinstructies voor onderhouds- en herstelacties
- planning van inspecties, tests en onderhoud
- registratiemethoden ter evaluatie van het onderhoudsproces
- draaiboeken voor de operationele fase
- procedures en/of werkinstructies voor bedieningshandelingen
- registratiemethoden voor de evaluatie van het operationele bedienproces.

8.4.3 Middelen

In de ORA worden ook aannamen gedaan met betrekking tot de beschikbare middelen. Het ontbreken van deze middelen zal leiden tot het niet volledig realiseren van gestelde hersteldurен, herstelmogelijkheden enzovoorts. Onder 'middelen' wordt onder andere het volgende verstaan:

- voldoende budget om de maatregelen, die uit de ORA volgen, uit te voeren
- ondersteunende systemen voor de ORA, zoals sjablonen ter ondersteuning van de FMECA en computerprogrammatuur voor RCM of foutenbomen
- de ondersteunende systemen voor het onderhoud, inclusief de registratie, zoals een onderhoudsmanagementsysteem (OMS)
- de noodzakelijke meetapparatuur voor onderhoudshandelingen
- de noodzakelijke reservedelen en gereedschappen voor onderhoud en herstel
- de benodigde veiligheidsmiddelen voor onderhouds- en herstelacties
- de ondersteunende systemen voor de bediening, zoals beslisprotocollen
- de ondersteunende informatiesystemen voor bediening en onderhoud
- de beschikbaarheid van een kwaliteitssysteem
- de aanwezigheid van een evaluatiestructuur, waarbij vaststaat wat en wanneer moet worden geëvalueerd en gerapporteerd.

8.5 Kwaliteitsborging

De precieze inrichting van de organisatie om tot een beheerst en geborgd beheer- en onderhoudsproces te komen of dit te behouden, valt grotendeels buiten de scope van deze handreiking. Wel zijn er – vanuit algemeen aanvaarde en beschikbare ISO-normen voor kwaliteitsborging – criteria en randvoorwaarden af te leiden, die een oordeel geven over de mate waarin de B&O-organisatie in staat is het gewenste proces op een voldoende niveau uit te voeren.

Net als technisch falen niet volledig is te voorkomen, is in een organisatie het maken van fouten niet uit te sluiten. Het kwaliteitssysteem is erop gericht deze fouten zoveel mogelijk te voorkomen en, wanneer mogelijk en zinvol, tijdig te herstellen. Daarmee wordt de kans op onvoldoende kwaliteit op een acceptabel laag niveau gebracht.

Belangrijk is dat er een algemeen vertrouwen is dat het kwaliteitssysteem voldoende functioneert. Blijkt in de praktijk regelmatig sprake te zijn van 'verrassingen', dan is het kwaliteitssysteem nog niet verankerd in de kwaliteitscultuur. Uiteraard moet ook het kwaliteitssysteem periodiek worden geëvalueerd en zo nodig aangepast.

Een internationaal opgestelde en geaccepteerde norm voor kwaliteitsmanagement is de NEN-EN-ISO 9000 [25] of een daarvan afgeleide norm, zoals de ISO 55000 voor assetmanagement [26], voorheen PAS55. Deze normen bieden voldoende aanknopingspunten voor het inrichten van een kwaliteitssysteem voor de beheer- en onderhoudsorganisatie of voor de operationele organisatie. De normen schrijven ten behoeve van het kwaliteitsmanagement onder andere het volgende voor:

- het vastleggen van producten, processen, rolhouders en verantwoordelijkheden
- het periodiek evalueren van de producten, processen, rolhouders en verantwoordelijkheden
- het integreren van risicomanagement in de processen.

De inhoudelijke aspecten, die vanuit het risicogestuurde werken in de verschillende processen moeten zijn geborgd, worden in bovenstaande paragraaf generiek uitgewerkt en toegelicht. Bij Rijkswaterstaat is een hulpmiddel ontwikkeld dat de processen op deze aspecten beoordeelt en daarmee de risicoanalyse valideert: ‘het Kompas’. Momenteel is het Kompas alleen nog voor de kwantitatieve risicoanalyse voor de stormvloedkeringen uitgewerkt.
Voor andere typen objecten en voor de kwalitatieve ORA is een dergelijk instrument in principe ook toepasbaar, maar zullen enkele inhoudelijke aspecten ingrijpend moeten worden aangepast.

9 De borging van risicogestuurd aanleggen, beheren en onderhouden in contracten

9.1 Welke uitgangspunten moeten worden geborgd?

Het gedachtegoed van risicogestuurd aanleggen, beheren en onderhouden moet niet alleen worden geborgd in de eigen organisatie, ook in de contracten zal de risicogestuurde werkwijze moeten landen. Feitelijk maakt het niet uit welke verdeling van taken, verantwoordelijkheden en bevoegdheden middels het contract wordt gemaakt, zolang de ketens rondom het opstellen van de risicoanalyse, het instandhoudingsplan en het beheer van beide maar gesloten blijven. Daartoe moeten de uitgangspunten van het risicogestuurd aanleggen, beheren en onderhouden als randvoorwaarden in de contracten worden meegegeven. Specifieke aandacht moet daarbij uitgaan naar:

- het maken, beheren, configureren en actualiseren van de risicoanalyse (ORA, hoofdstuk 5 en 6)
- het opstellen en actualiseren van het instandhoudingsplan (IHP, hoofdstuk 7)
- het uitvoeren en terugkoppelen van (onderdelen van) het instandhoudingsplan
- het evalueren van de resultaten.

De omvang van de uitbesteding van activiteiten heeft grote invloed op de organisatie-inrichting van de eigen Rijkswaterstaat-beheerorganisatie. De beheerorganisatie moet in staat zijn regie te voeren over de contracten, processen en werkzaamheden en moet de uitbestede werkzaamheden inhoudelijk kunnen (laten) toetsen. Dit betekent dat de juiste competenties en de juiste kennis en kunde niet alleen aan opdrachtnemerskant, maar ook bij Rijkswaterstaat beschikbaar moeten zijn.

9.1.1 De objectrisicoanalyse in contracten

Voor alle contracten is het van belang dat er een risicoanalyse met de juiste diepgang en kwaliteit aan ten grondslag ligt. Deze wordt opgesteld door de beheerder, of door een opdrachtnemer voor of namens de beheerder. Voor het uitvragen van het kwantitatieve deel van een ORA is het document *Verificatiemethode Betrouwbaarheid en Beschikbaarheid* [27] opgesteld. Hierin zijn de eisen samengevat die Rijkswaterstaat aan een ORA stelt.

9.1.2 Het instandhoudingsplan in contracten

De objectrisicoanalyse en het instandhoudingsplan bieden de objectbeheerder de mogelijkheid om het onderhoud te contracteren dat is vereist voor de gemaakte prestatieafspraken. Cruciaal is dat eisen worden gesteld aan het onderhoudsproces en in het bijzonder aan de feedback tijdens het proces. Eisen aan het onderhoudsproces betreffen de test-, vervangings- en inspectie-intervallen en de te realiseren hersteldurен. De feedback stelt de beheerder in staat de objectrisicoanalyse, het instandhoudingsplan en het onderhoudsmanagementsysteem actueel te houden.

De objectbeheerder moet daarom in het contract specificeren dat de juiste informatie wordt verzameld en geregistreerd, bijvoorbeeld test- en inspectieresultaten, gefaalde componenten, inclusief de daarbij aangetroffen

mechanismen, et cetera. Onderstaande opsomming toont, niet uitputtend, een aantal parameters die van belang zijn voor een instandhoudingsplan dat mede gebaseerd is op een kwantitatieve ORA.

Bedrijfsparameters:
- draaiurenregistratie
- aantal aanspraken.

Storingsdata:
- datum/tijdstip storingsmelding
- registratie van bouwdeel/element/component, conform de FMEA
- beschrijving van faalwijze en faaloorzaak
- aantal voorgevallen storingen per component
- wachttijd tussen storingsmelding en overgaan tot werkelijk functieherstel
- de herstelduur vanaf wachttijd tot functieherstel
- herstelduur (som van beide bovenstaande tijden)
- datum/tijdstip storingsafmelding.

Onderhoudsdata:
- datum/tijdstip uitvoeren planmatige onderhoudsactiviteiten
- de testduur per component
- de inspectieduur (toestandsafhankelijke inspecties) per component
- de gemeten storingsvoorspellende grootheden (SVG)
- de duur van het onderhoud per component
- aantal reservedelen van component op voorraad (indien van toepassing).

In de contractering dienen duidelijke afspraken te worden gemaakt over hoe de onderhoudsaannemer deze parameters bijhoudt. Het is belangrijk dat deze onderhoudsinformatie wordt geregistreerd in datasystemen van Rijkswaterstaat, zodat ze ook in de toekomst kan worden gebruikt.

9.1.3 Het uitvoeren van (onderdelen van) het instandhoudingsplan
Het is van belang dat de randvoorwaarden uit de ORA worden geborgd.
Als bijvoorbeeld in de ORA is aangenomen dat de voorraad minimaal twee componenten moet bevatten, of dat de hersteltijd maximaal 24 uur is, zullen deze aannamen als eisen in het contract met de opdrachtnemer moeten staan.

9.1.4 Het evalueren van de resultaten
De gegevens, die gedurende het gebruik van het object worden verzameld en waarvan een deel hierboven is genoemd, moeten worden geïnterpreteerd en verwerkt tot feedback, zoals in paragraaf 9.1.2 is beschreven. Hiermee wordt de PDCA-loop gesloten.

9.2 Borging in de contractvormen van Rijkswaterstaat

Rijkswaterstaat kent verschillende contractvormen met opdrachtnemers. Rijkswaterstaat streeft bij deze contracten naar functionele eisen; getracht wordt te beschrijven welke functies moeten worden gerealiseerd en niet hoe die functies precies moeten worden geleverd of tot stand moeten komen.

Dat streven lukt goed als de oplossingsruimte (de variatie aan mogelijke invullingen van de gevraagde functie) groot is en wordt moeilijker naarmate er meer randvoorwaarden gelden. Dat laatste speelt met name bij onderhoud: de bestaande situatie maakt de *oplossingsruimte* beperkt. Het denken in systeemelementen, zoals dat bij systems engineering gebeurt en ook in dit document wordt voorgesteld, betekent dat componenten kunnen worden vervangen of gereviseerd. In dergelijke situaties kan het zelfs voorkomen dat een product van een specifiek merk moet worden aangeschaft en is er geen enkele oplossingsvrijheid meer. Ook bij de revisie van een bestaand onderdeel bestaat nauwelijks functionele vrijheid voor de opdrachtnemer.

Dat betekent dat de verschillende contractvormen nogal uiteenlopen. Als er veel oplossingsvrijheid is, wordt er functioneel gespecificeerd en dan is het stellen van prestatie-eisen belangrijk. Is er weinig tot geen oplossingsruimte, dan is de gerealiseerde betrouwbaarheid en/of beschikbaarheid van het gevraagde veeleer een *resultaat* in plaats van een van tevoren gespecificeerde *eis*. In dat geval zal de ORA van het systeem moeten worden aangepast met de gerealiseerde R-/A-eigenschappen van de component.

In de GWW werkt Rijkswaterstaat met de volgende contractvormen:

Engineering & construct (E&C)
De opdrachtnemer voert werk uit met een minimaal aandeel detail-engineering (voornamelijk variabel onderhoud).

Design & construct (D&C)
De opdrachtnemer is verantwoordelijk voor het ontwerp en de uitvoering daarvan. Het gaat veelal om aanleg of renovatie.

Prestatiecontracten
De opdrachtnemer is gedurende enkele jaren verantwoordelijk voor het onderhoud van een deel van het netwerk.

Design, build, finance & maintain (DBFM)
De opdrachtnemer is niet alleen verantwoordelijk voor het ontwerp en de bouw van het project, maar ook voor de financiering en het totale onderhoud.

Samenwerkingsovereenkomst ingenieursdiensten
Afgesproken voorwaarden voor het uitvragen van diensten aan een geselecteerde groep ingenieursbureaus.

Marktplaatsmodel voor project- en technisch personeel
Methode om de meest geschikte kandidaat te selecteren voor het inhuren van project- en technisch personeel.

De laatste twee contractvormen gaan niet over contracten waarin (deel)systemen worden opgeleverd en worden hier verder niet behandeld.

9.2.1 E&C-contract

Engineering & construct-contracten (E&C) worden doorgaans gebruikt voor aanlegprojecten en variabel-onderhoudsprojecten, die geen of slechts een kleine ontwerpcomponent kennen. Het ontwerpwerk beperkt zich tot een minimaal aandeel detail-engineering. Een voorbeeld van een E&C-contract is het aanbrengen van nieuwe deklagen asfalt op bestaande rijbanen.

Rijkswaterstaat tracht een zoveel mogelijk functioneel gespecificeerde uitvraag op te stellen. Omdat de ontwerpruimte beperkt is, liggen de functionele eisen doorgaans op een laag abstractieniveau. Het bepalen welke werkzaamheden de opdrachtnemer moet verrichten om het gevraagde te leveren blijft de verantwoordelijkheid van de opdrachtnemer.

Omdat de opdrachtnemer zich bezighoudt met slechts een deel van het object, een subsysteem dus, kunnen slechts RAMSSHE€P-eisen worden gesteld aan dit deel. Eisen aan de betrouwbaarheid of beschikbaarheid moeten dus van toepassing zijn op het subsysteem en niet op het hele object. Met behulp van de ORA van het object is het mogelijk te bepalen welke betrouwbaarheid en beschikbaarheid het subsysteem voorheen had. Hiermee kunnen zinvolle R-/A-eisen aan het te onderhouden (vervangen, reviseren) subsysteem worden geformuleerd.

Soms is de ontwerpvrijheid zó beperkt, dat moet worden geaccepteerd dat het nieuwe subsysteem een bepaalde betrouwbaarheid of beschikbaarheid heeft en niet kan voldoen aan strengere eisen. In dat geval moet de ORA van het object worden aangepast en moet opnieuw worden bekeken of het object nog voldoet aan de gestelde eisen. Dit is dan onderdeel van het actualiseren van de ORA, zoals in paragraaf 3.3 is beschreven.

9.2.2 D&C-contract

Bij Design & construct-contracten (D&C) is de opdrachtnemer verantwoordelijk voor het ontwerp van infrastructuur en de uitvoering van de aanleg daarvan. Rijkswaterstaat stelt een functioneel gespecificeerde uitvraag op. De opdrachtnemer krijgt de ruimte om innovaties toe te passen in het ontwerp en de uitvoering. Ook moeten deze beide fasen zo goed mogelijk op elkaar worden afgestemd.

D&C-contracten zijn er vooral voor projecten in de aanlegsector en grote renovaties. Voorbeelden zijn het wegvak A4 Delft-Schiedam (aanleg) en het herstel van damwanden langs het Amsterdam-Rijnkanaal (onderhoud).

D&C-contracten lenen zich goed voor functioneel specificeren: het uitvragen van een functie in plaats van een systeem. De kwaliteit van de geleverde functie wordt geëist door de eisen aan de RAMSSHE€P-aspecten. De eisen aan de mate waarin de functie moet worden vervuld, komen tot uiting in kwantitatieve eisen aan de betrouwbaarheid en de beschikbaarheid van de functie. Omdat de verantwoordelijkheid van de opdrachtnemer eindigt bij het opleveren van het systeem, is het bij D&C absoluut noodzakelijk met behulp van een ORA aannemelijk te maken dat het object na oplevering aan de gestelde eisen zal voldoen. Als het over de betrouwbaarheid van een brug gaat, doet de opdrachtnemer dat door zich gedocumenteerd aan de (internationale) ontwerpvoorschriften te houden. Als het gaat om de beschikbaarheid van een sluis wordt dat geborgd door een kwantitatieve risicoanalyse te maken, conform de voorschriften van Rijkswaterstaat [24].

9.2.3 Prestatiecontract

Voor meerjarig onderhoud gebruikt Rijkswaterstaat prestatiecontracten. Bij deze contractvorm is de opdrachtnemer verantwoordelijk voor het onderhouden van een object. Het object moet tijdens de looptijd van het contract aan alle vooraf gestelde eisen voldoen. In de opdrachtomschrijving van het prestatiecontract ligt het accent vooral op het handhaven van het 'dagelijks functioneren en presteren' van het areaal en het beheersen van de risico's in het areaal, naast 'het in stand houden van de toestand'.

De opdrachtnemer levert gegevens voor de ORA en het IHP. Aan de opdrachtnemer wordt gevraagd om het object (het areaal) meerjarig in stand te houden, te monitoren en de opdrachtgever te informeren over de toestand. De opdrachtgever wenst daarbij te sturen op prestaties en op kwaliteit, in plaats van op concrete activiteiten, hoewel specifiek benoemde activiteiten niet zijn uitgesloten. In het algemeen draagt de opdrachtgever (de beheerder) zelf zorg voor het updaten van de ORA en het IHP.

In de praktijk werkt de opdrachtnemer nog niet vaak risicogestuurd. Het vereiste onderhoud wordt taakstellend uitgevraagd. In dat geval is het van belang te zorgen dat de uitvraag past bij de ORA, waaruit volgt dat aan de onderliggende prestatie-eisen wordt voldaan. De beheerder zal vervolgens bij het periodiek doorlopen van zijn beheercyclus moeten toetsen of de opdrachtnemer inderdaad voldoet aan de randvoorwaarden uit de risicoanalyse. Dit kan enerzijds door het nagaan van een verplichte terugkoppeling vanuit de opdrachtnemer (bijvoorbeeld behaalde herstelduren) en anderzijds door het toetsen van zijn processen (bijvoorbeeld het opleidingsproces van medewerkers).

9.2.4 DBFM-contract

Bij een *Design, build, finance and maintain-contract* (DBFM) is de opdrachtnemer zowel verantwoordelijk voor het ontwerp en de bouw van het project, als voor de financiering en het totale onderhoud voor een vastgelegd aantal jaren. Het is dus een geïntegreerde contractvorm. Zo krijgt de opdrachtnemer maximale ruimte om zijn kennis en creativiteit toe te passen, inclusief in de gebruiksfase. Bij D&C-contracten ontbreekt die fase. De gedachte is dat de opdrachtnemer in termen van *life cycle* zal denken bij de aanleg: hij optimaliseert de som van stichtingskosten en onderhoudskosten. Afhankelijk van het contract is de opdrachtnemer na de realisatiefase nog 20 of 30 jaar verantwoordelijk voor het onderhoud.

Een ander uitgangspunt bij een DBFM-contract is dat risico's en verantwoordelijkheden worden belegd bij de partij die deze het beste kan beheersen en dragen. De betaling aan de opdrachtnemer gebeurt periodiek na de bouw, op basis van geleverde diensten. Als de afgesproken diensten niet worden geleverd, treden boeteclausules in werking. De winstdoelstelling van het consortium en de private financiers zorgt ervoor dat de som van opgelopen boetes en de kosten tot een minimum zullen worden beperkt.

Bij een D&C-contract koopt Rijkswaterstaat een product in: bijvoorbeeld een rijksweg met 2x2 rijstroken. Bij een DBFM-contract neemt de opdrachtgever echter een dienst af: een beschikbare rijksweg. Eén van de eerste voorbeelden van een DBFM-project is de Tweede Coentunnel (aanbesteding 2005).

Ook bij deze contractvorm is het essentieel prestatie-eisen mee te geven. Enerzijds omdat daarmee richting wordt gegeven aan het ontwerpproces en de noodzaak aantoonbaar te maken dat het object zal gaan voldoen aan (wettelijke) eisen, anderzijds ook omdat sommige eigenschappen niet in de praktijk meetbaar zijn, waardoor de opdrachtnemer daar dus niet op 'af te rekenen' is.

Een voorbeeld hiervan zijn eisen die de *Waterwet* stelt. De functie 'keren hoogwater' kent in het algemeen een strenge beschikbaarheidseis, terwijl het systeem de functie slechts incidenteel hoeft te vervullen. Daarom is voor de functie 'keren hoogwater' in het algemeen niet via metingen vast te stellen of de geëiste prestatie wordt gehaald en wordt ervoor gekozen om de geëiste prestatie met behulp van een risicoanalyse aan te tonen. Deze ORA zal op regelmatige basis aan de veranderingen van het systeem moeten worden aangepast om op die manier ook in de loop van de gebruiksfase aan te tonen dat aan de gestelde eisen wordt voldaan.

Maar ook als de kwaliteit van de functie die wordt geleverd in de gebruiksfase wél kan worden gemeten, zal de opdrachtnemer vanwege het beboeten (het afrekenen) een economisch optimum zoeken. Dat hoeft niet per se samen te vallen met de eisen die maatschappelijk gewenst zijn. Uiteraard kan door het kiezen van het juiste boeteregime het gewenste effect worden bereikt, maar de opdrachtgever zal dan een (heel) goed beeld moeten hebben van de kosten die met de te behalen prestaties zijn gemoeid.

In de praktijk betekent dit dat Rijkswaterstaat RAMSSHE€P-eisen stelt aan de hoofdfuncties en dat de opdrachtnemer bij oplevering (beschikbaarheidsdatum) met behulp van een ORA en het daaruit resulterende IHP aannemelijk maakt dat het object aan de gestelde eisen zal voldoen. Voor de functies waarvan de eigenschappen in de gebruiksfase niet meetbaar zijn, zal de opdrachtnemer de ORA regelmatig moeten actualiseren, conform paragraaf 3.3. Voor de functies waarvan de eigenschappen wel meetbaar zijn, denk bijvoorbeeld aan de functie 'Laten Passeren Wegverkeer' bij een tunnel, kan een passend boeteregime de kwaliteit borgen.

10 Referenties

[1] Struik, P.
Business case risicogestuurd onderhoud, bijlage 1
Nota Bestuur RWS, Nummer RWS-2013/33552, 27 juni 2013
Goedgekeurd RWS Bestuursvergadering nr. 18, 5 juli 2013

[2] Velde, Jenne van der en Henrik Hooimeijer
Assetmanagement binnen Rijkswaterstaat, Een kennismaking op hoofdlijnen
Rijkswaterstaat, november 2010

[3] Werkgroep Leidraad systems engineering
Leidraad voor systems engineering binnen de GWW-sector, versie 3
Rijkswaterstaat, november 2013

[4] NEN 2767-4-1
Conditiemeting - Deel 4: Infrastructuur - Deel 1: Methodiek
Nederlands Normalisatie-instituut, juli 2011

[5] *Kader Life Cycle Cost (LCC) 2014*
ww-nummer #1485
Rijkswaterstaat, december 2002

[6] Beem, R.C.A., editor
Richtlijn Waterkerings- en Beschikbaarheidseisen – Consequenties van eisen aan Waterkering, Spuien en Verkeer te land en te water voor het ontwerp van Kunstwerken in de Natte Infrastructuur
Rijkswaterstaat, september 1998

[7] *Landelijke tunnelstandaard*
Rijkswaterstaat, oktober 2012

[8] *Uitvoeren functie analyse, Werkwijzebeschrijving systems engineering, WWB-SE-0022*
ww-nummer #849
Rijkswaterstaat , april 2017

[9] NEN-EN-IEC 60812
Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA)
Nederlands Normalisatie-instituut, mei 2006

[10] *Template eenvoudige ORA beweegbare kunstwerken*
ww-nummer #1560
Rijkswaterstaat, november 2017

[11] *Referentiekader beheer en onderhoud (RBO 2015)*
ww-nummer #3041
Rijkswaterstaat, juli 2015

[12] *Handleiding voor het LVO-model (Modelversie 1.4.1)*
Stijnen, J.W., J.M. van Noortwijk en M.J. Kallen, februari 2011

[13] *Availability workbench*
Isograph, 2013

[14] *Handreiking Faaldatabase - Generieke, pessimistische faalgegevens, te gebruiken door opdrachtnemers, versie 1.0.1*
ww-nummer #5499
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[15] Cooke, R.M.
Experts in uncertainty
Oxford University Press, New York, 1991

[16] *Handreiking Bayesiaanse update – Het aanpassen van faaldata op basis van metingen, versie 1.0.1*
ww-nummer #5500
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[17] *Handleiding TOPAAS - Een structurele aanpak voor faalkansanalyse van software intensieve systemen, versie 0.7*
ww-nummer #1319
Rijkswaterstaat, januari 2013
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[18] *Handreiking Kwantificering menselijk handelen met gebruik van het OPSCHEPmodel, versie 1.0.2*
ww-nummer #5532
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[19] *Handreiking externe gebeurtenissen – Screening, versie 1.0.1*
ww-nummer #5501
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[20] *Handreiking kwantitatieve analyse van bliksemrisico, versie 2.0.2*
ww-nummer #5534
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[21] *Handreiking Externe gebeurtenis – Brand, versie 1.0.1*
ww-nummer #5502
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[22] *Handreiking kwantificering aanvaarrisico, versie 1.0.1*
ww-nummer #5555
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[23] *Handreiking Basismodel Reservedelen, versie 1.0.1*
ww-nummer #5534
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

[24] *LBS Landelijke bruggen en sluizen – kaders bediening en besturing beweegbare objecten, release 3.1*
ww-kader #1334
Rijkswaterstaat, september 2016

[25] NEN-EN-ISO 9000
Kwaliteitsmanagementsystemen
Nederlands Normalisatie-instituut, oktober 2015

[26] NEN-ISO 55000
Assetmanagement
Nederlands Normalisatie-instituut, februari 2014

[27] *Handreiking Verificatiemethode Betrouwbaarheid en Beschikbaarheid, versie 1.0.7*
ww-nummer #1567
Rijkswaterstaat, november 2017
(zie Werkwijzer Rijkswaterstaat voor vigerende versie)

Bijlage A: Begrippen en definities

Areaal: het geheel aan deelsystemen waarmee de drie netwerken van Rijkswaterstaat (HWN, HVWN en HWS) zijn opgebouwd: wegen, vaarwegen, bruggen, sluizen, viaducten, stuwen, gemalen, hoogwaterkeringen et cetera.

Assetmanagement: systematische en gecoördineerde activiteiten en werkwijze, waarmee Rijkswaterstaat optimaal en duurzaam haar netwerken, met de bijbehorende prestaties, risico's en uitgaven over de levensduur beheert, zodat aan de afspraken met het ministerie van Infrastructuur en Waterstaat wordt voldaan.

Aspect: specifieke eigenschap van een (nog te ontwikkelen) systeem.

Aspecteis: beschrijft de randvoorwaarde waaronder een systeem zijn functies dient te vervullen. Voorbeelden zijn: beschikbaarheid, betrouwbaarheid, onderhoudbaarheid en veiligheid.

Basisgebeurtenis: het falen van een deelsysteem, waarbij het deelsysteem niet verder wordt gedecomponeerd om de faalkans te bepalen.

Bedrijfszekerheid: synoniem van betrouwbaarheid.

Beheren: het geheel van activiteiten dat erop gericht is om de functies van een systeem gedurende de levensduur in voldoende mate te laten vervullen. Het gaat hier dan met name om de organisatorische aspecten: het zorgen voor onderhoud, het zorgen voor de juiste bedienprocedures, et cetera.

Beschikbaarheid heeft twee definities:

1. de verwachte fractie van de totale tijd dat een systeem, onder gegeven omstandigheden, functioneert
2. de kans dat een systeem, onder gegeven omstandigheden, functioneert wanneer het op een willekeurig tijdstip wordt aangesproken.

Betrouwbaarheid: de kans dat een systeem gedurende een bepaalde periode zonder falen zijn functie vervult, onder gegeven omstandigheden.

Capaciteit: maximum hoeveelheid of het grootste aantal dat kan worden ontvangen of bevat door een systeem. Bij Rijkswaterstaat moet dan worden gedacht aan bijvoorbeeld het maximum aantal vaar- of voertuigen per tijdseenheid, dat een (vaar)wegvak kan passeren. De capaciteit wordt veelal vastgelegd in de functionele eisen.

Common Cause Falen: falen door een gemeenschappelijke oorzaak, wat correlatie tussen componenten veroorzaakt. Dat betekent dat de kans op falen van een component afhankelijk is van het falen van een andere component. De component faalt door een mechanisme (*cause*) dat ook in de andere component tot falen kan leiden. Met name in het geval van redundantie, waarbij twee dezelfde componenten elkaars functie kunnen overnemen, is door *Common Cause* Falen de (gezamenlijke) faalkans veel groter dan op grond van onafhankelijkheid zou mogen worden verwacht.

Common Mode Falen: synoniem van *Common Cause Falen*.

Component: hardware systeemelement.

Cut set: minimale deelverzameling.

Deelsysteem: onderdeel van een systeem. Deze onderdelen worden, in de context van het grotere geheel, ook wel systeemelementen genoemd.

Faaldefinitie: een vastgelegde relatie tussen het falen van een functie van een (deel)systeem en de consequenties daarvan voor het functioneren van het systeem. De vastlegging bestaat uit een definitie van falen (wanneer vinden we het (deel)systeem gefaald) en de te nemen maatregelen, indien het systeem volgens de afspraak is gefaald.

Faalfrequentie: het gemiddeld aantal keren per tijdseenheid, dat falen optreedt. Wordt ook faalsnelheid (*failure rate*) genoemd.

Faalkans: kans op falen van de functie van een systeem, waarbij falen is gedefinieerd in een faaldefinitie.

Faalmechanisme: de wijze waarop het systeem faalt, zodat het zijn functie niet meer levert.

Faalsnelheid: het gemiddeld aantal keren per tijdseenheid, dat falen optreedt. Wordt ook *faalfrequentie* genoemd.

Falen: een gebeurtenis, of een verzameling gebeurtenissen, waardoor een systeem zijn functie verliest, c.q. niet meer kan vervullen (voldoet niet meer aan de functie eis). Er wordt niet van falen van het systeem gesproken, indien het systeem zijn functie niet kan vervullen door geplande onderhoudswerkzaamheden of capaciteitsgebrek.

FMEA: *Failure mode and effect analysis.* De FMEA is een methode waarmee op gestructureerde wijze faaloorzaken van een systeem worden geïnventariseerd. Dit gebeurt door systematisch de rol van de systeemelementen waar het systeem uit bestaat, te onderzoeken. Een FMEA levert dus *faalmechanismen* op.

FMECA: *Failure mode, effect and criticality analysis*. Dit is een FMEA, waarbij óók een inschatting wordt gemaakt van de kans op de gevonden faaloorzaak. De kans wordt veelal op basis van expertmening vastgesteld en gespecificeerd in een kansklasse.

Foutenboom: grafische weergave van de relatie tussen het falen van systeemelementen en het falen het systeem, uitgedrukt in de *Ongewenste Topgebeurtenis* (OTG). Deze grafische weergave wordt veelal gefaciliteerd door programmatuur, die tevens de kans op, of de niet-beschikbaarheid van de OTG berekent.

Functie: beoogde werking en/of verrichting van een systeem. Een functie is een taak die wordt uitgevoerd. Systemen bestaan omdat ze functies uitvoeren.

Functionele eis: primaire eis die wordt gesteld aan de functie. Dit geeft het antwoord op de vraag 'wat moet het systeem kunnen?' Een functionele eis heeft veelal betrekking op de capaciteit die een systeem moet leveren bij het vervullen van de functie.

Functionele test: het testen van de werking van de functie van een systeem.

GAO: gebruiksafhankelijk onderhoud. Bij deze onderhoudsstrategie wordt een component op basis van kalendertijd, gebruiksduur of aantal aanvragen vervangen. Deze vorm kent één parameter: het vervangingsinterval. Een bekend voorbeeld is het vervangen van de distributieriem bij een automotor.

Gebeurtenissenboom: grafische weergave van de mogelijke scenario's, gegeven een startgebeurtenis. Het doel van een gebeurtenissenboom is het berekenen van gevolgen. Deze grafische weergave wordt veelal gefaciliteerd door programmatuur, die tevens de kansen van optreden van de verschillende scenario's berekent.

Gepland onderhoud: werkzaamheden aan een systeem die van tevoren bekend zijn. Dit zijn meestal onderhoudswerkzaamheden en meestal beperken ze het functioneren van het systeem. In dat geval hebben ze invloed op de beschikbaarheid. Omdat de geplande niet-beschikbaarheid van het systeem vroegtijdig bekend is bij de gebruikers van het systeem, zijn de gevolgen door de gebruikers te mitigeren en worden deze als veel minder ernstig ervaren dan de tegenhanger: ongepland onderhoud.

Herstelduur: tijdsspanne tussen het moment van opmerken van een storing en het moment van vrijgave voor gebruik van de gefaalde component.

IHP: instandhoudingsplan.

Kunstwerk: civieltechnisch bouwwerk, niet bestemd voor bewoning. De term wordt alleen gebruikt voor de bouwwerken in de infrastructuur. De weg is geen kunstwerk, maar de brug wel. De rivier, of het kanaalpand, is geen kunstwerk, maar een stuw of een sluis wel.

Kwalitatieve ORA: bepalen van kansen en gevolgen van ongewenste gebeurtenissen op basis van ervaring en expertmening, waarbij zowel de kansen als de gevolgen in klassen worden ingedeeld, in plaats van als puntwaarden.

Kwantitatieve ORA: bepalen van de kans op één gevolg (de *Ongewenste Topgebeurtenis*) op basis van numerieke data en wiskundige analyses, waarbij het resultaat een puntwaarde is voor zowel kans als gevolg. Er zijn twee belangrijke kwantitatieve methoden om de kans te bepalen: de '*structural analysis*' en de '*systems analysis*'. Een *structural analysis* gaat uit van een model van de werkelijkheid, waarbij de invoer bestaat uit statistische grootheden: stochasten. Een *systems analysis* gaat uit van systeemelementen waarvan het faalgedrag statistisch bekend is. *Betrouwbaarheid- en beschikbaarheidsanalyses*, zoals die in dit document worden beschreven, zijn op systems analysis gebaseerd.

Minimale deelverzameling: een minimale set van systeemelementen die indien ze allen falen, falen van (een hoofdfunctie van) het systeem tot gevolg heeft. Indien de set uit één systeemelement bestaat wordt het falen van dat systeemelement een 'single point of failure' genoemd. Indien de set uit twee systeemelementen bestaat spreekt men van 'tweede orde deelverzameling', enzovoort.

MTBF: *mean time between failures*, de gemiddelde levensduur. Is dus gelijk aan de MTTF bij een nieuw systeemelement.

MTTF: *mean time to failure*, de gemiddelde tijd tot falen vanaf het moment van beoordelen.

Netwerk: geheel van met elkaar verbonden objecten die gezamenlijk een functie vervullen. Rijkswaterstaat kent drie netwerken: het hoofdwegennetwerk (HWN), het hoofdvaarwegennetwerk (HVWN) en het hoofdwatersysteem (HWS). De eerste twee netwerken hebben één functie: het mogelijk maken om van A naar B te komen, via de weg of via het water. Het hoofdwatersysteem kent meerdere (hoofd-)functies: het verzorgen van voldoende water, het verzorgen van schoon water en het veilig keren van hoog water.

Object: afzonderlijk identificeerbaar onderdeel van een netwerk met een specifieke functie, zoals tunnels, sluizen, stuwen, bruggen, viaducten en geluidschermen. Er is een grote overlap met het begrip kunstwerk, maar ook vaarwegpanden, wegdelen en onderdelen van kustwerken worden wel objecten genoemd.

Onderhoudbaarheid: kans dat een systeem (of systeemelement) binnen een specifiek tijdsinterval kan worden gerepareerd, geïnspecteerd of preventief kan worden onderhouden, onder gegeven omstandigheden. In de praktijk wordt onderhoudbaarheid ook vaak gezien als de lengte zelf van het tijdsinterval waarin onderhoud kan worden gepleegd.

Onderhouden: fysieke activiteiten, die erop gericht zijn om de functies van een systeem gedurende de levensduur in voldoende mate te laten vervullen.

Onderhoudsanalyse: analyse waarmee de optimale onderhoudsstrategie van een component wordt bepaald, inclusief de bijbehorende parameters. Deze analyse is vrijwel altijd op basis van *life cycle costs* (LCC) en resulteert in SAO, GAO of TAO.

Ongewenste gebeurtenis: gebeurtenis die kan bijdragen aan het falen van de functie van een systeem: de *ongewenste topgebeurtenis* (OTG).

Ongewenste Topgebeurtenis: (partieel) functieverlies van een systeem. De ongewenste topgebeurtenis (OTG) is de gebeurtenis, waarvan de kans wordt berekend in een kwantitatieve risicoanalyse. Veelal is dit het falen van de hoofdfuncties van het systeem, zoals hoog water keren, laten passeren scheepvaart, laten passeren wegverkeer, afvoeren water, et cetera.

Ongepland onderhoud: werkzaamheden aan een systeem die onverwacht noodzakelijk zijn en dus niet van tevoren bekend waren. Dit zijn altijd onverwachte storingen die het functioneren van het systeem beperken. Ze bepalen de betrouwbaarheid en hebben invloed op de beschikbaarheid van het systeem. Omdat de beperking van het systeem onverwacht optreedt, zijn gebruikers van het systeem niet in staat de gevolgen hiervan te mitigeren. Het onverwachte karakter brengt vaak ook nog additionele irritatie teweeg. Daarom wordt deze vorm van niet-beschikbaarheid als veel ernstiger ervaren dan de tegenhanger: gepland onderhoud.

ORA: objectrisicoanalyse. Dit begrip is gekozen om duidelijk te maken dat het hier gaat om een risicoanalyse van een fysiek systeem, een object. Dit ter onderscheid met een risicoanalyse op een proces, zoals bij *risicomanagement* wordt gehanteerd.

PDCA-cyclus: Plan, Do, Check, Act kwaliteitscirkel (afkomstig van de Amerikaanse statisticus William Deming), waarmee activiteiten worden beschreven die gericht zijn op verbeteringen in organisaties.

Plateauniveau: het niveau waarop organisatie en objecten zich bevinden indien een systematische en volledig ingeregelde vorm van risicogestuurd beheer en onderhoud wordt toegepast, waarbij op elk moment aantoonbaar is dat aan de prestatie-eisen wordt voldaan.

Prestatie: rendement van een systeem; geeft weer hoe goed het systeem werkt. Soms specifiek in termen van betrouwbaarheid en/of beschikbaarheid.

Prestatieanalyse: een analyse van het rendement van een systeem, in termen van betrouwbaarheid en/of beschikbaarheid en gefocust op de hoofdfuncties die het systeem dient uit te voeren. In de praktijk is prestatieanalyse synoniem aan betrouwbaarheid- of beschikbaarheidsanalyse.

Prestatie-eisen: aan de hoofdfunctie(s) van een object gestelde eisen in termen van *RAMSSHE€P*. Soms specifiek kwantitatieve betrouwbaarheids- en beschikbaarheidseisen.

ProBO: Probabilistisch beheer en onderhoud, een risicogestuurde wijze van beheren en onderhouden van objecten waarmee kan worden aangetoond dat aan een gestelde prestatie-eis wordt voldaan, conform de in dit document voorgestelde werkwijze.

Raakvlakeis: eis aan een systeem die het resultaat is van een raakvlakkenanalyse. Een dergelijke analyse inventariseert de eisen die de omgeving van het systeem aan het systeem stelt.

RASCI-tabellen: een matrix om de relatie tussen rollen, taken en bevoegdheden van personen weer te geven.

RAMSSHE€P: acroniem voor:
- R: *reliability*, betrouwbaarheid;
- A: *availability*, beschikbaarheid;
- M: *maintainability*, onderhoudbaarheid;
- S: *safety*, veiligheid;
- S: *security*, beveiliging;
- H: *health*, gezondheid;
- E: *environment*, milieu;
- €: *economics*, waarde, geld;
- P: *politics*, imago, politieke wensen.

Redundantie: het zodanig meervoudig uitvoeren van onderdelen, dat het geheel goed blijft functioneren wanneer één of meerdere onderdelen falen.

Risico: kans dat een ongewenste gebeurtenis plaatsvindt ‘vermenigvuldigd’ met het ‘gevolg’ van die gebeurtenis. Als het gevolg kwantificeerbaar is, kan dit daadwerkelijk een vermenigvuldiging zijn. Het resultaat is dan de verwachtingswaarde van het gevolg.

Risicoanalyse: een beschouwing van de kans op, en de gevolgen van een ongewenste gebeurtenis. Zie kwalitatieve en kwantitatieve ORA.

Risicogestuurd: uitvoering van een risicogestuurde activiteit is gerelateerd aan het reduceren van de kans op een ongewenste gebeurtenis, of het verminderen van de ernst van de effecten van de ongewenste gebeurtenis. Naarmate de ongewenste gebeurtenis een grotere bedreiging vormt voor de te bereiken prestatie van het systeem, wordt er meer beheersing op gezet. Bij risicosturing krijgen dus de grootste prestatiebedreigingen de meeste aandacht.

Root cause analysis (RCA): een methode waarmee de onderliggende oorzaken van fouten of problemen wordt vastgesteld. Een oorzaak wordt een basisoorzaak (*root cause*) genoemd indien het wegnemen daarvan de fout met zekerheid wegneemt of het probleem met zekerheid oplost.

SAO: storingsafhankelijk onderhoud. Deze onderhoudsstrategie houdt in dat wordt gewacht tot de component faalt en kent geen parameters. Een bekend voorbeeld is het vervangen van een lamp van een auto.

Semi-kwantitatief: gebruikmakend van een indeling in klassen of ordegroottes.

Single point of failure: een enkelvoudig deel van een system dat bij uitval het uitvallen van de functie van het systeem tot gevolg heeft.

Storingsvoorspellende grootheid (SVG): een te meten, fysieke eigenschap van een component, die een maat is voor de toestand van de component en daarmee een maat is voor de kans dat de component binnen een specifiek tijdsinterval zal falen.

SVO: standaard verzorgend onderhoud, ook wel vast onderhoud genoemd.

Subfunctie: een onderdeel van een functie die wordt uitgevoerd door een deelsysteem. Het bewegingswerk van een beweegbare brug is een deelsysteem van een beweegbare brug. De subfunctie is het doen bewegen van het val.

Systeem: samenhangend geheel van fysieke onderdelen dat is bedoeld om een bepaalde functie te vervullen. Anders gezegd: een afhankelijk van het gestelde doel binnen de totale werkelijkheid te onderscheiden verzameling elementen, die onderlinge relaties hebben.
De netwerken van Rijkswaterstaat zijn systemen, maar de onderdelen daarvan ook. Elk systeem is onderdeel van een groter geheel en is dus in feite een deelsysteem. Het hangt dus van de context af waar de grenzen van het systeem worden getrokken. Rijkswaterstaat trekt de grenzen bij zijn hoofdsystemen: Hoofdwegennet (HWN), Hoofdvaarwegennet (HVWN) en het Hoofdwatersysteem (HWS).

Systeemelement: kleinste eenheid van een systeem, waarbij de interne opbouw en relaties niet meer beschouwd worden.

Systeemeis: alle eisen die worden gesteld aan het systeem. De functionele eisen, de aspecteisen en de raakvlakeisen worden bij Rijkswaterstaat gezamenlijk 'de eisen' genoemd. Voor de herkenbaarheid is hier gekozen voor het onderscheidende begrip systeemeis. De belangrijkste bronnen voor een systeemeis zijn: de *functieanalyse*, de *aspectenanalyse* en de r*aakvlakken-analyse.* Deze analyses leveren respectievelijk f*unctionele eisen, aspecteisen* en *raakvlakeisen*.

TAO: toestandsafhankelijk onderhoud. Bij deze onderhoudsstrategie wordt een (of meerdere) *storingsvoorspellende grootheid* (SVG) gemeten en wordt op basis van deze meting besloten te wachten tot een volgende meting of een vervangings- of herstelactie te doen. Een bekend voorbeeld is het meten van het profiel van een autoband.

Veiligheid: de kans dat het systeem gedurende een bepaalde periode geen menselijk letsel (gewonden, doden) veroorzaakt. Indien een systeem alleen maar schade veroorzaakt bij falen, dan wordt van betrouwbaarheid gesproken. De kans op overstroming door hevige regenval, waarbij geen gevaar voor menselijk letsel ontstaat, wordt in het spraakgebruik weliswaar vaak veiligheid genoemd, maar is in feite een kwestie van betrouwbaarheid. Een betrouwbaar systeem voert het water snel af waardoor niet vaak wateroverlast ontstaat, een onbetrouwbaar systeem geeft wel vaak wateroverlast.

Verzorgend onderhoud: onderhoud met als doel om de conditie van een object te handhaven. Hierbij moet worden gedacht aan conserveren, reinigen, schoonmaken, smeren, invetten, bijvullen, aftappen, verversen, ontluchten, kleine revisies (tandwielkast), kleine vervangingen (aansluitklemmen), et cetera.

Dit is een uitgave van

Rijkswaterstaat

www.rijkswaterstaat.nl
0800 - 8002

Maart 2018