Specificatie Veiligheidsfuncties Beweegbare Bruggen en Schutsluizen

Onderdeel van de brug- en sluisstandaard

Datum 9 december 2013
Status Vrijgegeven (versie 2.1)

Uitgegeven door:	
Versie:	2.1
Status:	Vrijgegeven
Opgeleverd door:	Leon Uijttewaal (CIV-PRIA)
	3 december 2013
Vrijgegeven door:	Programmateam LBB
	9 december 2013
Vastgesteld door:	
Beheerd door:	
	088 797 1355
Meer informatie:	
	088 797 1355

Leden van productgroep:

Naam	Dienst
Gerard Appelman	PPO
Alex Groothaert	PPO
Andre Smits	PPO
Peter Janssen	PPO
Henri Vogels	PPO
Guido Vroombout	PPO
Tom Huveneers	CD
Jan Looijen	WNZ
Johan den Toom	GPO
Bas Dietvorst	GPO
Chris Tettero	GPO

Bovenstaande personen hebben het document versie 1.3 getoetst en stemmen in met de in het document gemaakte keuzes.

Revisiehistorie

Versie	Datum	Toelichting	Distributielijst
0.1	01-01-2011	Eerste concept	Productgroep
0.2	01-05-2011	Tweede concept, aanvullingen Nick de With (Fusacon) doorgevoerd.	Productgroep
0.3	01-06-2011	Definitief concept	Productgroep, programma LBB
1.0	01-07-2011	Definitieve versie	Productgroep, programma LBB
1.1	01-09-2011	Definitieve versie, vastgesteld door programma LBB	Productgroep, programma LBB
1.2	01-10-2012	Definitieve versie, opmerkingen uit projecten verwerkt en diverse onderwerpen toegevoegd	Productgroep, programma LBB
1.3	24-01-2013	Definitieve versie, diverse tekstuele wijzigingen doorgevoerd	Productgroep, programma LBB
1.3a	29-07-2013	TBV Definitieve versie, diverse tekstuele wijzigingen doorgevoerd	programma LBB LBB Toetsers
2.0	30-10-2013	Definitieve versie, versie 1.3 is vastgesteld door de Regiegroep werkwijzer Aanleg	programma LBB
2.1	9-12-2013	Vrijgegeven door programmateam LBB	Programmateam LBB

1 Inleiding

Dit kader ‘Specificatie Veiligheidsfuncties Beweegbare Bruggen en Schutsluizen’ maakt deel uit van de brug- en sluisstandaard.

1.0 Beschrijving Brug- en sluisstandaard

De brug- en sluisstandaard bestaat uit documenten die de inrichting van de werk-processen en de functionele en technische eisen aan bruggen en sluizen beschrijven, in het licht van de wetgeving, beleidsdoelstellingen en netwerkmanagement van RWS. Deze documenten hebben betrekking op het gebruik, de bediening en besturing van beweegbare bruggen en schutsluizen (met aandacht voor doelstellingen, organisatie, primaire werkprocessen en de daarvoor gebruikte functionele en technische uitrusting).
De standaard is van toepassing op alle beweegbare bruggen en schutsluizen van RWS.
Bediening is nauw verbonden met de processen aanleg&onderhoud en beheer en ontwikkeling. Daarom worden ook eisen gesteld aan deze processen, daar waar er raakvlakken zijn.

Deze standaard wordt gebruikt bij de inrichting van de bedienprocessen, de inrichting van het beheerprocessen en het opstellen van onderhoudscontracten en aanleg (nieuwbouw/renovatie) van bruggen en sluizen binnen RWS.

1.01 Plaats van dit document in brug- en sluisstandaard

De brug- en sluisstandaard kent 4 lagen:
-de laag strategische documenten, dat het geheel van basisprincipes en uitgangspunten voor de bediening van bruggen en sluizen en de daarvoor benodigde informatievoorziening en inrichting beschrijft.

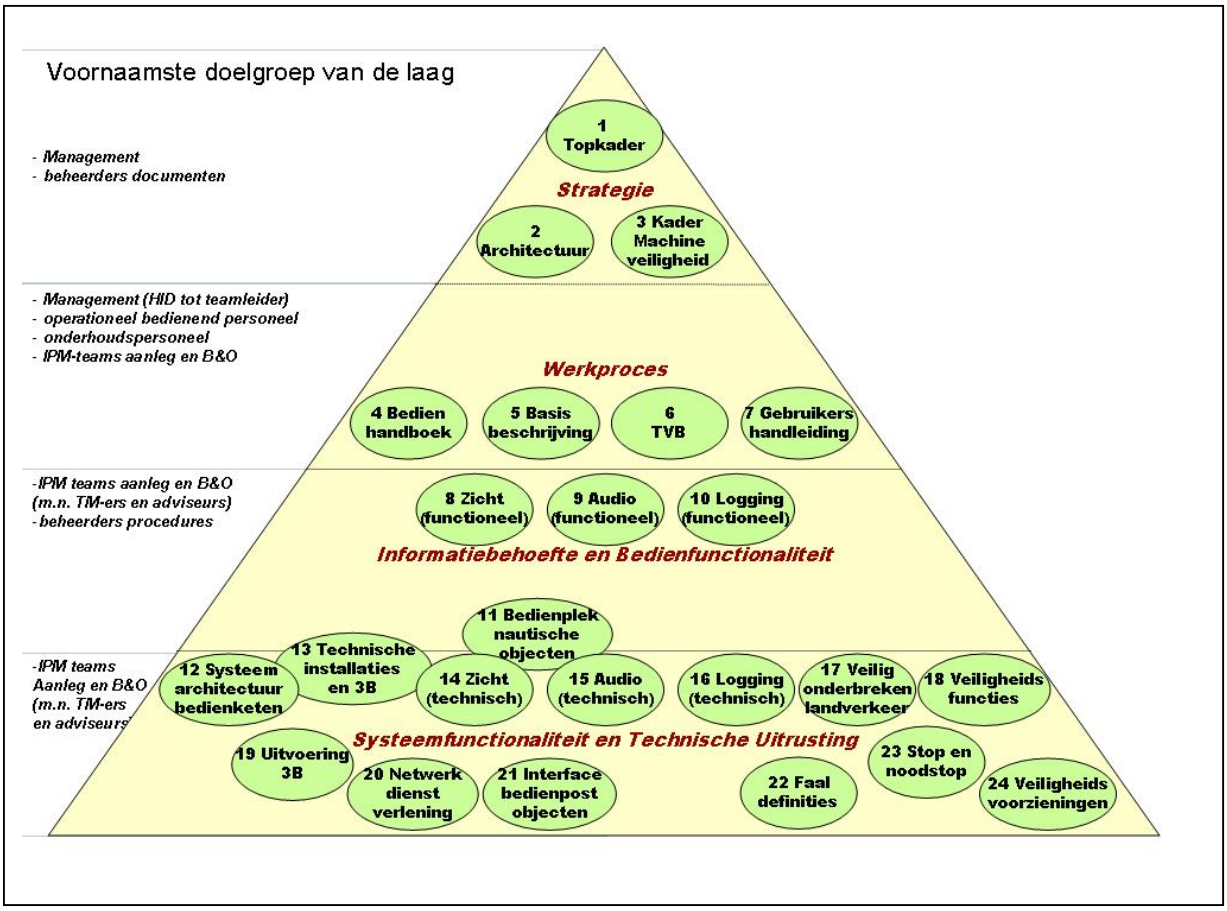
-de laag ‘beschrijving werkproces, taken & verantwoordelijkheden’.
Deze laag bevat de beschrijving van de werkprocessen, de organisatie, de taken & verantwoordelijkheden van medewerkers en de bijbehorende procedures.

-de laag ‘definiëren informatiebehoefte en bedienfunctionaliteit’. De documenten in deze laag beschrijven welke informatie en uitrusting nodig is voor uitvoeren van de werkprocessen.

-de laag ‘beschrijving Systeemfunctionaliteit en Technische Uitrusting’, zie figuur 2. De documenten in deze laag beschrijven de voorwaarden voor en eisen aan de systemen voor audiocommunicatie bij de bediening van beweegbare bruggen en schutsluizen.

In onderstaande piramide ziet men de plek van dit kader en de laag waarin die thuishoort.

Dit document zit in de laag beschrijving Systeemfunctionaliteit en Technische Uitrusting’, zie figuur 2. De documenten in deze laag beschrijven de voorwaarden voor en eisen aan de systemen voor audiocommunicatie bij de bediening van beweegbare bruggen en schutsluizen


Voornaamste doelgroep van de laag
- Management
- beheerders documenten
- Management (HID tot teamleider)
- operationeel bedienend personeel
- onderhoudspersoneel
- IPM-teams aanleg en B&O
-IPM teams aanleg en B&O (m.n. TM-ers en adviseurs)
- beheerders procedures
-IPM teams Aanleg en B&O (m.n. TM-ers en adviseurs
1 Topkader
Strategie
2 Architectuur
3 Kader Machine veiligheid
Werkproces
4 Bedien handboek
5 Basis beschrijving
6 TVB
7 Gebruikers handleiding
8 Zicht (functioneel)
9 Audio (functioneel)
10 Logging (functioneel)
Informatiebehoefte en Bedienfunctionaliteit
11 Bedienplek nautische objecten
12 Systeem architectuur bedienketen
13 Technische installaties en 3B
14 Zicht (technisch)
15 Audio (technisch)
16 Logging (technisch)
17 Veilig onderbreken landverkeer
18 Veiligheids functies
Systeemfunctionaliteit en Technische Uitrusting
19 Uitvoering 3B
20 Netwerk dienst verlening
21 Interface bedienpost objecten
22 Faal definities
23 Stop en noodstop
24 Veiligheids voorzieningen

1.02 Verwijzing waar overige documenten te vinden zijn

De vastgestelde en vrijgegeven (dwz: met succes de kwaliteitstoets doorstaan en dus gereed voor gebruik, maar nog niet vastgesteld door de proceseigenaar of bestuur) onderdelen van de brug- en sluisstandaard zijn te vinden in het configuratieoverzicht op: http://vpr.intranet.rijkswaterstaat.nl/Algemeen/Kaders_Bediening_Bruggen_Sluizen/default.aspx.

Voor vragen over de brug- en sluisstandaard kan men terecht bij loketkaders@rws.nl

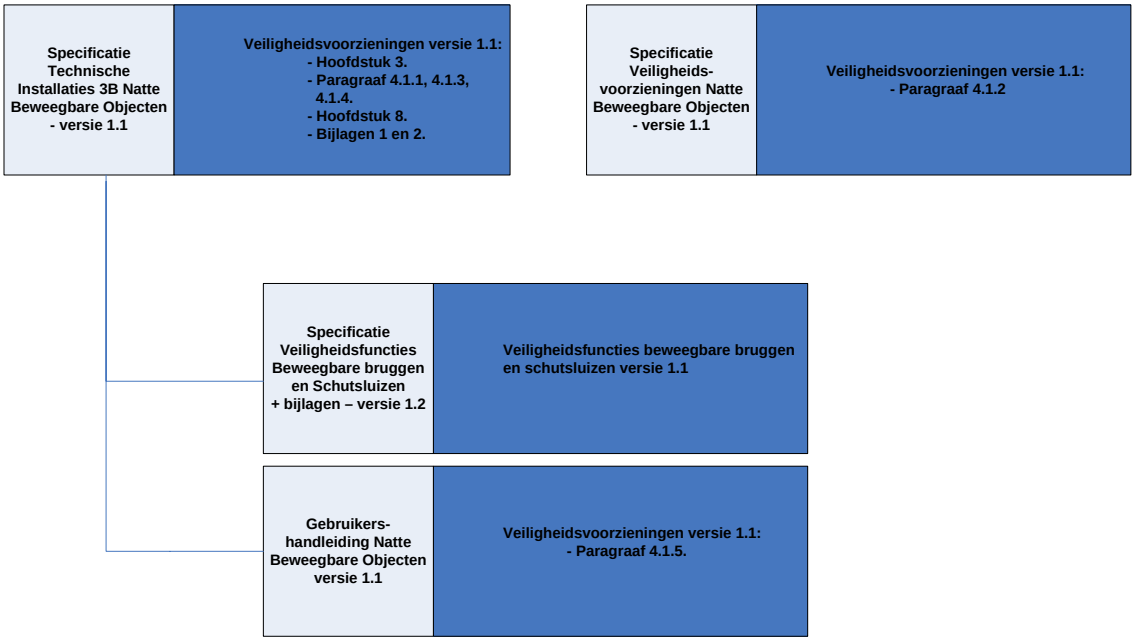
1.03 Openstaande punten

Deze paragraaf gaat in op de openstaande punten bij dit kaderdocument en eventuele oplossingsrichting daarbij. Aanvullend hierop heeft de brug- en sluisstandaard ook nog de zogenaamde known problem-lijst. Deze heeft net zoals de openstaande punten, als doel om de gebruiker van het kader vooraf mee te geven wat er bij het kader speelt en is te vinden op de VPR.

1.1 Doel, doelgroep en scope van dit document

De doelstelling van Rijkswaterstaat is om (vaar)weggebruikers een veilige en vlotte doorstroming van natte beweegbare objecten te bieden. Dit houdt in dat de organisatie, processen en techniek zo ingericht moeten worden dat deze doelstelling behaald wordt. Dit document beschrijft de veiligheidsfuncties welke gerealiseerd dienen te worden in het bediening-, besturing-, en bewakingssysteem van het object en het proces hoe ze tot stand dienen te komen. De lijst van in dit rapport beschreven veiligheidsfuncties is niet limitatief. Uit een risicobeoordeling kan blijken dat additionele veiligheidsfuncties noodzakelijk zijn of dat veiligheidsfuncties dienen te voldoen aan een hoger veiligheidsniveau.
Het doel van dit document is om natte beweegbare objecten op een uniforme en veilige wijze te laten functioneren en is een eerste aanzet tot meer standaardisatie van oplossingen. Dit om de aanleg, renovatie en het beheer en onderhoud van natte beweegbare objecten efficiënter te maken. De eisen in dit document zijn niet afdoende om het gehele object als veilig te bestempelen. Uit de risicobeoordeling kan/zal blijken dat aanvullende maatregelen noodzakelijk zijn.

De scope van dit document beperkt zich tot de besturingstechnische veiligheidsfuncties die in het bediening-, besturing- en bewakingsysteem (3B) gerealiseerd moeten worden, en het proces om deze te realiseren. Dit document dient in samenhang gehanteerd te worden met het document “Technische Installaties 3B Natte Beweegbare Objecten”. Voor onderwerpen die niet direct gerelateerd zijn aan de bediening en besturing, maar wel met veiligheidsvoorzieningen van natte beweegbare objecten, wordt verwezen naar de “Specificatie veiligheidsvoorzieningen natte beweegbare objecten”. Een compleet overzicht van alle documenten en hun samenhang is te vinden in het document “Architectuur voor gebruik, bediening en besturing schutsluis en beweegbare brug”. In Figuur 1 wordt weergegeven hoe de onderliggende documenten (Specificatie Veiligheidsfuncties Beweegbare Bruggen en Schutsluizen, Gebruikershandleiding Natte Beweegbare Objecten) en oude documenten (Veiligheidsvoorzieningen en Veiligheidsfuncties inclusief bijlagen) verwerkt zijn in de nieuwe documenten structuur.



Figuur 1

Dit document is onderdeel van de integrale aanpak om veiligheidsrisico's te beheersen. Het is dan ook geen losstaande oplossing, maar één van de stappen die uitgevoerd dient te worden om de machine (beweegbare brug of schutsluis, zie "Kader Machineveiligheid") te laten voldoen aan de essentiële veiligheid- en gezondheidseisen van de Machinerichtlijn (2006/42/EG) en daarmee in de gebruikersfase aan de Richtlijn Arbeidsmiddelen (2009/104/EG). Daarnaast dient rekening gehouden te worden met de veiligheid van (vaar)weggebruikers en de omgeving waarin de beweegbare objecten zich bevinden.

Het document kan toegepast worden in projecten waar gebruik gemaakt wordt van de Systems Engineering (SE) en de RAMS (Reliability, Availability, Maintainability and Safety) methodiek. De in dit document beschreven processen zijn gebaseerd op het toepassen van het V-model zoals beschreven in de Leidraad SE (in de GWW). De producteisen die in document gesteld worden hebben invloed op alle RAMS aspecten, waarmee rekening gehouden moet worden in het ontwerpproces.

De doelgroep van dit document zijn ontwerpers en adviseurs (van zowel Opdrachtnemer als Opdrachtgever) die betrokken zijn bij het ontwerpen en toetsen van technische installaties van natte beweegbare objecten. De bruikbaarheid van dit document beperkt zich dus tot de projectorganisaties van de processen aanleg en onderhoud.

1.2 Leeswijzer

De expliciete product- en proceseisen in dit document worden aangegeven door middel van de afkorting VF en het bijbehorende eisnummer (voorbeeld: ***VF#001***). In hoofdstuk 8 van dit document is een overzicht gegeven van alle eisen, inclusief de bijbehorende verificatiemethode en de levenscyclusfase waarin de eis geverifieerd dient te worden.

Hoofdstuk 2 van dit document geeft een overzicht van de belangrijkste normen op het gebied van besturingstechniek en alle documenten waarnaar verwezen wordt. In hoofdstuk 3 wordt de context beschreven waarin dit document geplaatst en gebruikt moet worden waarna hoofdstuk 4 een overzicht geeft van de te beheersen risico's. In hoofdstuk 5 en 6 worden de veiligheidsfuncties gedefinieerd die deze risico's moeten beheersen en worden eisen gesteld hoe deze veiligheidsfuncties gerealiseerd dienen te worden. Tenslotte worden in hoofdstuk 7 eisen opgenomen met betrekking tot het tijdelijk overbruggen van veiligheidsfuncties.

Opmerking: In dit document wordt verwezen naar diverse normen. Indien eisen in dit document, of documenten waarnaar verwezen wordt, afwijkend zijn met eisen zoals verwoord in normen, dan zijn de eisen in dit document leidend. Bij afwijkingen is het uitgangspunt dat het behaalde veiligheidsniveau aantoonbaar gelijk is aan dat in de norm en is beargumenteerd waarom er afgeweken is.

2 Aangehaalde documenten

Hieronder volgt een overzicht met interne Rijkswaterstaat documenten waarnaar verwezen wordt, waarbij aangegeven is wat de vigerende versie is.

Titel	Datum / Versie	Organisatie
Specificatie Technische Installaties 3B Natte Beweegbare Objecten	Vigerende	RWS DI - GPO
Specificatie Veiligheidsvoorzieningen Natte Beweegbare Objecten	Vigerende	RWS DI - GPO
Generiek eisen aan de uitvoering van 3B systemen	Vigerende	RWS CIV
Architectuur voor gebruik, bediening en besturing schutsluis en beweegbare brug	Vigerende	RWS CIV
Kader machineveiligheid	Vigerende	RWS DI - GPO

De onderstaande lijst geeft een overzicht van de meeste belangrijke normen ten aanzien van veilige besturingstechniek. Indien van toepassing kunnen deze normen gehanteerd worden tijdens ontwerp en realisatie. Het is toegestaan om geen gebruik te maken van deze normen (tenzij expliciet aangegeven wordt dat een norm gehanteerd moet worden), in dat geval moet aangetoond worden dat met de gekozen oplossing minimaal hetzelfde veiligheidsniveau wordt behaald.

Opmerking: een norm is van toepassing indien de daarin beschreven technieken en methoden gebruikt worden. Voorbeeld: De norm EN-ISO 4413:2010 is van toepassing indien gebruik gemaakt wordt van hydraulische (sub)systemen.

- EN-ISO 12100:2010; Veiligheid van machines – Algemene ontwerpbeginselen – Risicobeoordeling en risicoreductie
- EN 1037:1996; Veiligheid van machines - Voorkoming van onbedoeld starten
- ISO 14119/EN 1088:1996; Blokkeerinrichtingen gekoppeld aan afschermingen - Grondbeginselen voor het ontwerp en de keuze
- EN-IEC 60204-1:2006; Veiligheid van machines - Elektrische uitrusting van machines - Deel 1: Algemene eisen
- EN-IEC 60204-11 2007; Veiligheid van machines - Elektrische uitrusting van machines - Deel 11: Eisen voor hoogspanningsapparatuur voor spanningen hoger dan 1000 V wisselspanning maar niet hoger dan 36 kV
- EN-IEC 61439-1:2011; Laagspanningsschakel- en verdeelinrichtingen - Deel 1: Eisen met gehele of gedeeltelijke typegoedkeuring voor samenstellingen
- EN-IEC 61800-5-2:2007; Regelbare elektrische aandrijfsystemen - Deel 5-2: Veiligheidseisen – Functionele veiligheid
- EN-IEC 61000-6-2:2005; Elektromagnetische compatibiliteit (EMC) - Deel 6-2: Algemene normen - Immuniteitsnorm voor industriële omgevingen
- EN-IEC 61000-6-4:2001; Elektromagnetische compatibiliteit (EMC) - Deel 6-4: Algemene normen - Emissienorm voor industriële omgevingen

- NPR-IEC/TS 61000-1-2:2008; Elektromagnetische compatibiliteit (EMC) - Deel 1-2: Algemeen - Methodologie voor de functionele veiligheid van elektrische en elektronische systemen inclusief apparatuur met betrekking tot elektromagnetische verschijnselen
- EN-ISO 13850; Noodstopvoorzieningen, functionele aspecten. Ontwerpbeginselen
- EN-IEC 62061:2010; Veiligheid van machines - Functionele veiligheid van elektrische, elektronische en programmeerbare systemen met een veiligheidsfunctie
- EN-IEC 61508:2010, deel 1,2 en 3; Functionele veiligheid van elektrische, elektronische en programmeerbare systemen met een veiligheidsfunctie
- IEC/TR 62513:2008; Veiligheid van machines - Richtlijnen voor het gebruik van communicatiesystemen in toepassingen met een veiligheidsfunctie
- EN-ISO 13849-1:2008; Veiligheid van machines - Onderdelen van besturingssystemen met een veiligheidsfunctie - Deel 1: Algemene ontwerpbeginselen
- EN-ISO 13849-2:2008; Veiligheid van machines - Onderdelen van besturingssystemen met een veiligheidsfunctie - Deel 2: Validatie
- EN-ISO 4413:2010; Veiligheid van machines - Algemene regels voor hydraulische systemen
- EN-ISO 4414:2010; Veiligheid van machines - Algemene regels voor pneumatische systemen
- NEN 6787:2003; Het ontwerpen van beweegbare bruggen - Veiligheid

3 Machineveiligheid, risicobeoordeling en –reductie

Machineveiligheid is één van de aspecten die onderdeel uit maakt van integrale veiligheid zoals vastgelegd in de Leidraad Integrale Veiligheid. Onder machineveiligheid wordt verstaan voldoen aan alle essentiële veiligheids- en gezondheidseisen die voortkomen uit het Warenwetbesluit Machines (afgeleid van de Machinerichtlijn 2006/42/EG) en de stand der techniek zoals vastgelegd in de geharmoniseerde normen.

Omdat niet alleen risico's beschouwd worden die direct gerelateerd zijn aan machineveiligheid, maar ook risico's voor de (vaar)weggebruiker en de omgeving die geïntroduceerd worden door het incorrect functioneren van het beweegbare object, wordt ook wel gesproken over systeemveiligheid. Alle risico's gerelateerd aan systeemveiligheid zullen echter via dezelfde methodiek als machine gerelateerde risico's beschouwd en behandeld worden, daarom wordt door dit document heen de term machineveiligheid gehanteerd.

De Machinerichtlijn is een Europese richtlijn welke in de Nederlandse Wetgeving is opgenomen en wel in het Warenwetbesluit Machines. Een fabrikant van een machine dient tijdens het ontwerp en bouw rekening te houden met de wettelijke eisen gesteld door de Machinerichtlijn. De Machinerichtlijn is van toepassing voor de gehele levenscyclus, wat betekent dat de fabrikant van de machine de risico's gedurende de gehele levenscyclus moet hebben beoordeeld en tevens daarvoor maatregelen moet treffen c.q. moet aangeven welke maatregelen door de gebruiker uitgevoerd dienen te worden.

De richtlijn Arbeidsmiddelen 2009/104/EG is ook vastgesteld op Europees niveau en opgenomen in de Nederlandse Arbeidsomstandighedenwet (Arbo-wet) en wel in het Arbobesluit hoofdstuk 7. Zij heeft als doel om een minimum veiligheidsniveau van arbeidsmiddelen te realiseren tijdens de gebruiksfase. Deze sociale richtlijn wordt niet nader beschouwd in dit document omdat de Arbo-wet bij het ontwerpen en realiseren van de machine geen additionele eisen stelt aan machines ten opzichte van de Machinerichtlijn op het gebied van functionele veiligheid.

De Machinerichtlijn schrijft voor dat een risicobeoordeling uitgevoerd moet worden, waarmee begonnen moet worden tijdens het ontwerp, om de essentiële veiligheids- en gezondheidsrisico's in kaart te brengen. Deze risicobeoordeling zal uitgevoerd moeten worden conform de norm NEN-EN-ISO 12100 (voorheen NEN-EN-ISO 14121-1 / NEN-EN 1050) welke geharmoniseerd is onder de Machinerichtlijn. De ontwerper dient elk gevaar, elke gevaarlijke situatie of elke gevaarlijke gebeurtenis die aan de machine is verbonden, te identificeren en te documenteren.

De risico's verbonden aan deze gevaren dienen voor alle hieronder genoemde fasen van de levenscyclus van een machine te worden bepaald:

- transport, opbouw en installatie;
- ingebruikname;
- gebruik, onderhoud en wijzigen;
- uit gebruik nemen, ontmanteling en verwijdering.

Bij het uitvoeren van een risicobeoordeling volgens de norm NEN-EN-ISO 12100 zullen van elk object een aantal veiligheidsrisico's worden gevonden die onaanvaardbaar zijn. Deze veiligheidsrisico's dienen gereduceerd te worden met de methode die ook weergegeven is in de

norm NEN-EN-ISO 12100, waarbij het de verplichting is om risico's zoveel mogelijk bij de bron weg te nemen (zie Figuur 2).

VF#001: Voer een risicobeoordeling uit conform de NEN-EN-ISO 12100:2010. Deze risicobeoordeling dient integraal onderdeel te zijn van het gehele ontwerpproces en de gehele machine te beschouwen.

Opmerking: Indien de scope van de werkzaamheden niet de gehele machine bevat dient de risicobeoordeling zich te beperken tot de onderdelen die wel onderdeel van de scope zijn.

VF#002: De risicobeoordeling dient als onderdeel van het Technisch Dossier (TD) aan Rijkswaterstaat overhandigd te worden en tijdens het ontwerpproces ten alle tijden door Rijkswaterstaat ingezien te kunnen worden.

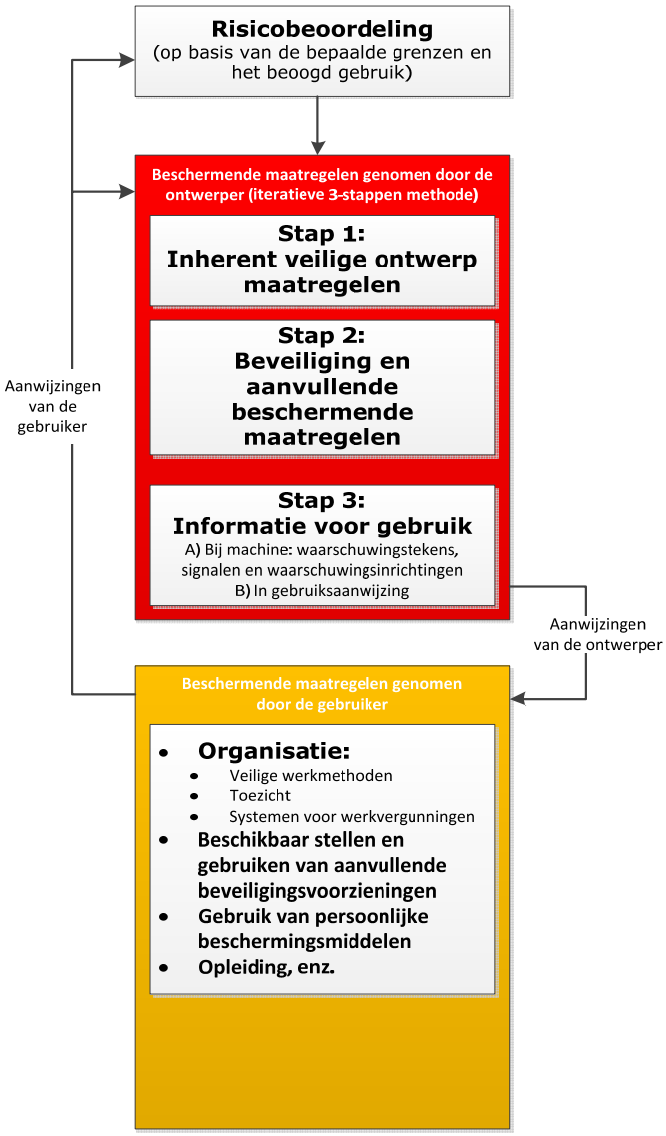
Deze NEN-EN-ISO 12100 en ook de Machinerichtlijn beschrijven beide de volgende verplichte risicoreductie volgorde (zie Figuur 2) die een fabrikant tijdens de ontwerpfase dient aan te houden:

1. Risico's uitsluiten of zoveel mogelijk verminderen door veiligheid in het ontwerp en de bouw van de machine te integreren.
2. De noodzakelijke beveiligingsmaatregelen treffen voor risico's die niet kunnen worden uitgesloten.
3. De gebruikers informeren en waarschuwen over de restrisico's ten gevolge van een tekortkoming van de getroffen beveiligingsmaatregelen, aangeven of een bijzondere opleiding vereist is en vermelden dat persoonlijke beschermingsmiddelen vereist zijn.

VF#003a: De machine dient intrinsiek veilig te zijn door het elektrotechnische deel aantoonbaar te laten voldoen aan de IEC 60204-1.

VF#003b: De machine dient intrinsiek veilig te zijn door het hydraulische deel aantoonbaar te laten voldoen aan de ISO 4413 en de NBD 06000.

Opmerking; Met intrinsiek wordt bedoeld de risico's zoveel mogelijk bij de bron wegnemen.



Figuur 2

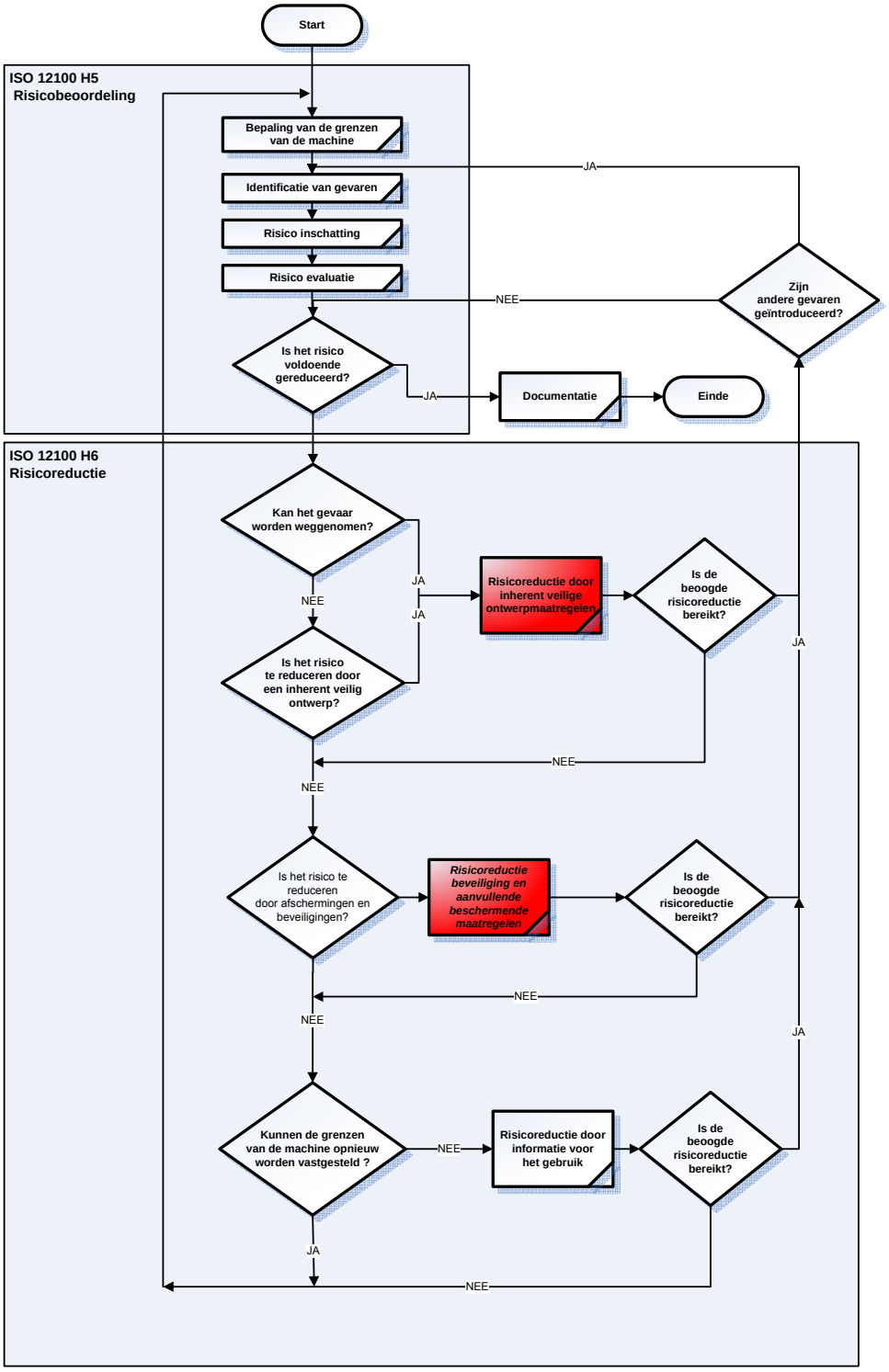
Bij het uitvoeren van de risicobeoordeling is het van groot belang om van te voren vast te stellen wat de grenzen van de machine zijn. Deze grenzen bepalen wat wel en wat niet meegenomen moet worden in de risicobeoordeling. Daarnaast is het belangrijk dat zowel een top-down benadering als een bottom-up benadering wordt toegepast. De top-down benadering richt zich vooral op de risico's vanuit het functionele gebruik. De bottom-up benadering moet in kaart brengen of de bestaande beheersmaatregelen afdoende zijn om de risico's te beheersen (controle of deze beheersmaatregelen voldoen aan de "stand der techniek") en beschouwd risico's die veroorzaakt worden door het falen van componenten en deelsystemen.

Nadat bovenstaande stappen zijn doorlopen moet geïnventariseerd worden of het risico voldoende beheerst is. Met andere woorden is het restrisico acceptabel? Daarnaast moet beoordeeld worden of er door aanbrengen van de beschermende maatregelen geen nieuwe risico's geïntroduceerd zijn.

Het gehele proces van risicobeoordeling en –reductie wordt getoond in Figuur 3. De in hoofdstuk 4 beschreven besturingstechnische veiligheidsfuncties moeten gezien worden als risicoreductie door inherent veilig ontwerpen of het aanbrengen van beveiligingen (de aard van de besturingstechnische veiligheidsfunctie bepaald het type reducerende maatregel), welke in onderdeel zijn van het rood gearceerde blokken.

Onderdeel van de risicobeoordeling moet een FMECA (Failure Modes, Effect and Criticality Analysis) zijn waarin alle faalmodi van ieder component van het systeem beschouwd moeten worden om het veroorzaakte faalgedrag in kaart te brengen. Op deze manier wordt inzicht verkregen in het systeemgedrag van het systeem bij incorrect functioneren van een deel van, of een component in het systeem. Het is hierbij belangrijk om de verschillende toestanden waarin een object zich kan bevinden mee te nemen in de beschouwing. Ook “common cause” falen (CCF) moet beschouwd worden om te voorkomen dat het falen van meerdere componenten tegelijk, veroorzaakt door één oorzaak, leidt tot een onacceptabel risico.

VF#004: Als onderdeel van de risicobeoordeling dient een FMECA (Failure Modes, Effect and Criticality Analysis) tot stand te komen die inzicht geeft in de risico’s op systeemniveau bij het falen van individuele componenten en combinaties van componenten.


Start
ISO 12100 H5
Risicobeoordeling
Bepaling van de grenzen van de machine
Identificatie van gevaren
Risico inschatting
Risico evaluatie
Is het risico voldoende gereduceerd?
JA
Documentatie
Einde
NEE
Zijn andere gevaren geïntroduceerd?
JA
ISO 12100 H6
Risicoreductie
Kan het gevaar worden weggenomen?
NEE
JA
Is het risico te reduceren door een inherent veilig ontwerp?
JA
Risicoreductie door inherent veilige ontwerpmaatregelen
Is de beoogde risicoreductie bereikt?
JA
NEE
NEE
Is het risico te reduceren door afschermingen en beveiligingen?
Risicoreductie beveiliging en aanvullende beschermende maatregelen
Is de beoogde risicoreductie bereikt?
NEE
NEE
JA
Kunnen de grenzen van de machine opnieuw worden vastgesteld ?
NEE
Risicoreductie door informatie voor het gebruik
Is de beoogde risicoreductie bereikt?
JA
NEE

Figuur 3

4 Veiligheidsrisico's brug en sluisproces

De veiligheidsrisico's geïntroduceerd door het gebruik van beweegbare bruggen en schutsluizen zijn afgeleid van de primaire processen die beide objecten vervullen. Voor de beweegbare brug kunnen de volgende primaire functies worden onderscheiden:

- Laten passeren wegverkeer.
- Laten passeren scheepvaart.

De veiligheidsrisico's worden voornamelijk geïntroduceerd door het wisselen tussen deze 2 primaire functies, wat in het vervolg van dit document zal worden betiteld als "het brugproces". Dit brugproces staat dan ook centraal bij het in kaart brengen van de veiligheidsrisico's. In bijlage 1 worden de geïdentificeerde risico's gerelateerd aan een specifieke processtap in het brugproces getoond.

De schutsluis kent generiek de volgende primaire functies:

- Laten passeren van scheepvaart.
- Waterpeil scheiding handhaven.
- Water doorlaten.
- Het scheiden van zoet en zout water.
- Hoog water keren.

In het document worden alleen de risico's meegenomen, die geïntroduceerd worden door de functie laten passeren van scheepvaart omdat. In bijlage 2 worden de geïdentificeerde risico's gerelateerd aan een specifieke processtap in het sluisproces getoond.

De combinatie van een beweegbare brug en schutsluis komt regelmatig voor. Indien deze combinatie invloed heeft op het te volgen proces voor de bedienaar kunnen additionele risico's geïntroduceerd worden. In de risicobeoordeling dient hier rekening mee gehouden te worden en indien noodzakelijk zullen additionele veiligheidsfuncties gerealiseerd moeten worden om deze risico's te beheersen.

De Machinerichtlijn en de bijbehorende geharmoniseerde normen zijn primair bedoeld voor het voorkomen van menselijk letsel. Bij het gebruik van beweegbare bruggen maar vooral schutsluizen dient ook rekening gehouden te worden met mogelijke (milieu) schade aan de omgeving en/of (economische) schade aan het object. Daarnaast zullen calamiteiten met beweegbare bruggen en schutsluizen voor Rijkswaterstaat in ongewenste imagoschade resulteren. Deze aspecten zijn ook meegenomen bij de evaluatie van de geïdentificeerde risico's en het bepalen van de noodzakelijke reducerende maatregelen.

De risico's gedefinieerd in bijlage 1 en 2 zijn niet uitputtend. Daarnaast is er in deze bijlagen rekening gehouden met de meest gebruikte technische oplossingen (elektromechanisch en hydraulisch) voor het aandrijven van een bewegingswerk. Een andere technische oplossing kan nieuwe risico's introduceren die niet in deze lijst voorkomen. Hierdoor is het altijd noodzakelijk om de gehele risicobeoordeling te doorlopen om te bepalen of er additionele risico's van toepassing zijn.

5 Geclassificeerde veiligheidsfuncties

De geïdentificeerde risico's uit bijlagen 1 en 2 resulteren in gevaren met een veiligheidsrisico en/of schade aan het object en/of de omgeving. Vastgesteld is dat deze risico's onacceptabel zijn en daarom dienen deze risico's gereduceerd te worden tot een acceptabel restrisico. Uitgaande van de huidige stand der techniek is het voor deze risico's niet mogelijk om het gevaar bij de bron weg te nemen. Beschermende maatregelen, in de vorm van een veiligheidsfunctie gerealiseerd in het bediening-, besturing- en bewakingssysteem (ook wel 3B genoemd, zie document "Specificatie Technische Installaties 3B Natte Beweegbare Objecten", zijn dus noodzakelijk om de vereiste mate van risicoreductie te realiseren. Veiligheid dient gegarandeerd te zijn door de gehele bedienketen, en is dus niet toe te wijzen aan een specifiek onderdeel van het 3B systeem.

Ontwikkelingen zoals elektronica- en software voor de veiligheidsfuncties in een machinebesturing hebben ertoe geleid dat de norm EN 954-1 uit 1996 niet meer voldoet. Daarom zijn er voor de machinesector twee nieuwe normen opgesteld. De NEN-EN-IEC 62061 en de NEN-EN-ISO 13849-1, die respectievelijk het veiligheidsniveau classificeren in een 'safety integrity level' (SIL) en een 'performance level' (PL).

De normen NEN-EN-ISO 13849-1 en NEN-EN-IEC 62061 (beide geharmoniseerd onder de Machinerichtlijn) geven invulling aan ontwerpeisen voor besturingstechnische veiligheidsfuncties in lijn met de huidige stand der techniek.

Een van deze normen zal dan ook door de ontwerper gebruikt moeten worden om de veiligheidsfuncties te ontwerpen en te integreren. Rijkswaterstaat heeft een voorkeur voor de systematiek van de NEN-EN-IEC 62061 omdat deze de volledige levencyclus beschrijft. De in dit document beschreven systematiek gaat daarom uit van de NEN-EN-IEC 62061, deze norm dient dan ook toegepast te worden.

VF#005: Bij het realiseren van besturingstechnische veiligheidsfuncties dient te worden voldaan aan de eisen uit de NEN-EN-IEC 62061.

Voor de classificatie van het SILtarget van de verschillende besturingstechnische veiligheidsfuncties in het brug- en schutsluis proces, is gebruik gemaakt van de risicograaf uit de norm NEN-EN-IEC 62061. Deze risicograaf kent een viertal parameters, beschreven in Tabel 1 t/m Tabel 4, te weten:

- Se; ernst van de verwonding
- Fr; frequentie of blootstellingsduur
- Pr; kans van optreden van gevaarlijke gebeurtenis
- Av; mogelijkheid om het gevaar te ontwijken cq. Het letsel te beperken

Consequentie	**Severity (Se) of Ernst van het letsel**
Fatale verwonding of zo ernstig dat werken na genezing erg moeilijk wordt; grote schade aan object en/of andere eigendommen; grote schade aan omgeving.	4
Onherstelbare verwonding, b.v.	3

amputaties en gebroken botten, etc. werken na genezing weer mogelijk; schade aan object en/of andere eigendommen; schade aan omgeving.	
ernstige snijwonden, doorstekingen en kneuzingen (behandeling arts noodzakelijk); beperkte schade aan object en/of andere eigendommen; beperkte schade aan omgeving.	2
schrammen en lichte kneuzingen (opgelost door eerste hulp); geen schade aan object en/of andere eigendommen; geen schade aan omgeving.	1

Tabel 1

Tabel 1 beschrijft de ernst van de verwonding (factor Se) en deelt deze op in vier groepen. Het gaat hierbij om het zwaarst voorzienbare letsel dat zou kunnen optreden.

Frequentie	**Blootstellingsduur**	
	≤ 10 min	> 10min
F ≥ 1 keer/uur	5	5
1 keer/dag ≥ F < 1 keer/uur	4	5
1 keer/2 weken ≥ F < 1 keer/dag	3	4
1 keer/jaar ≥ F < 1 keer/2 weken	2	3
F < 1 keer jaar	1	2

Tabel 2

Tabel 2 beschrijft de frequentie van blootstelling van een persoon aan het gevaar en de duur van de blootstelling gedurende de activiteit.

Kans van optreden van de gevaarlijke gebeurtenis	**Kans (Pr)**
Erg hoog	5
waarschijnlijk	4
mogelijk	3
zelden	2
verwaarloosbaar	1

Tabel 3

Tabel 3 beschrijft de kans van optreden van de gevaarlijke gebeurtenis. In de norm is gespecificeerd dat de standaardkeuze hier factor 5 is. Daarvan mag worden afgeweken als er steekhoudende argumenten zijn die van invloed zijn op de kans van optreden.

Mogelijkheid om het gevaar te ontwijken of het letsel te beperken (AV)	
Onmogelijk	5

zelden	3
mogelijk	1

Tabel 4

Tabel 4 beschrijft de mogelijkheid om het letsel veroorzaakt door het gevaar te ontwijken of het letsel te beperken. Hierna volgen voorbeelden van een aantal aspecten die in ogenschouw dienen te worden genomen:

- Plotseling langzaam of snel optreden gevaar.
- Ruimtelijk mogelijkheid ontwijken.
- Scherp, heet, onder spanning.
- Mogelijkheid gevaar te herkennen.

Severity (Se)	**Class (Cl)**				
	3-4	**5-7**	**8-10**	**11-13**	**14-15**
4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3
3		(OM)	SIL 1	SIL 2	SIL 3
2			(OM)	SIL 1	SIL 2
1				(OM)	SIL 1

Tabel 5

Tabel 5 geeft de methodiek weer om het SILtarget van een veiligheidsfunctie te bepalen. Als eerste wordt de juiste rij gekozen op basis van de factor Se. Daarna wordt het getal wat ontstaat door de optelling van de andere drie factoren Fr, Pr en Av. De optelsom wordt Class (Cl) genoemd en daarmee kan de juiste kolom worden gekozen. Het vakje dat het kruispunt vormt tussen de factor Se en Cl bevat het SIL level dat door de veiligheidsfunctie moet worden gerealiseerd, de SILtarget. OM staat voor “other measures” en geeft aan dat andere maatregelen toegepast dienen te worden.

Voor een veiligheidsfunctie kan gelden dat SIL niveau noodzakelijk is vanwege het beperkte risico. In dat geval moet de veiligheidsfunctie geïmplementeerd bestaan uit beproefde veiligheidscomponenten en beproefde veiligheidsprincipes volgens de norm EN-ISO 13849-2, zonder dat kwantitatief aangetoond moet worden dat aan een bepaald SIL niveau voldaan wordt.

VF#006: Vervallen

5.1 Beweegbare brug en schutsluis

In bijlage 3 t/m 5 (voor de beweegbare brug) worden respectievelijk de minimaal noodzakelijke veiligheidsfuncties en de daaraan gestelde eisen, de processtappen waarin deze veiligheidsfuncties actief moeten zijn en het gewenste gedrag van de veiligheidsfuncties beschreven. Dit is ook gedaan voor de schutluis in bijlage 6 t/m 8. De in bijlage 3 en 6 gedefinieerde waarde voor SILtarget zijn minimale waarden. Uit de risicobeoordeling kan blijken dat een hoger veiligheidsniveau (SILtarget) noodzakelijk is. In bijlage 3 en 6 zijn voor sommige veiligheidsfuncties criteria aangegeven die het risiconiveau mede bepalen.

5.2 Beschermende stopfunctie

Op de beweegbare brug en een schutsluis zijn verschillende veiligheidsfuncties actief die werken als een beschermende stopfunctie, die vaak ten onrechte als noodstop wordt aangeduid. Als een brug bij de opwaartse beweging door zijn eindschakelaar loopt, wordt wel eens gezegd: “De brug gaat dan in noodstop”. Dit is niet juist, omdat dergelijke veiligheidsfuncties volgens de huidige normen een “beschermende stop” (Engels: protective stop) functie uitvoeren en geen noodstop uitvoeren.

Naast de noodstop en de beschermende stop wordt in de normen ook gesproken over machine stopfunctie en de stopcategorieën 0, 1 of 2. Deze functies worden uitgelegd in de onderstaande tabel. Voor de noodstop en de machine stop wordt verwezen naar het document “Stop/Noodstop beweegbare bruggen en schutsluizen”.

Naam functie	**Uitleg functies**
Beschermende stopfunctie/ Protective stop function	Veilige stopfunctie als gevolg van aanspreken van een primaire veiligheidsfunctie zoals een retardeerbewaking/eindschakelaar etc. Kan uitgevoerd zijn als stopcategorie 0, 1 of 2. LET OP: stopcategorie 2 is alleen onder bepaalde voorwaarden toegestaan!
Stopcategorie 0	Stop van de bewegingen door directe afschakeling van de aandrijvende delen.
Stopcategorie 1	Vertraagde stop van de bewegingen door eerst afremmen en dan volledige afschakeling van de aandrijvende delen
Stopcategorie 2	Vertraagde stop van de bewegingen zonder afschakeling van de aandrijvende delen. Standaard niet toegestaan voor de noodstopfunctie, maar onder voorwaarden wel voor beschermende stop functies. **LET OP: Voorwaarde is dat de frequentieregelaar (Power Drive System) gecertificeerd is door een Notified body en dient te voldoen aan de norm EN-IEC 61800-5-2!**

Tabel 6

VF#007: De beschermende stopfuncties dienen standaard te worden uitgevoerd volgens stopcategorie 0, tenzij uit de risicobeoordeling blijkt dat een andere stopcategorie leidt tot een groter risicoreductie.

Opmerking; Een van de aspecten die moet worden meegenomen bij bestaande objecten is de toestand waarin het bewegingswerk verkeerd. Stopcategorie 0 kan namelijk in sommige gevallen ernstige schade tot gevolg hebben.

VF#007a: Bij het ingrijpen van een beschermende stopfunctie dienen alle besturingscommando's die voor de aansturing van de bewegende delen zorgen te worden weggenomen.

6 Levenscyclus eisen aan veiligheidsfuncties

In het vorige hoofdstuk zijn een aantal veiligheidsfuncties voor een beweegbare brug en sluis gepresenteerd. Dit hoofdstuk geeft een overzicht van de eisen die gesteld worden veiligheidsfuncties voor alle fasen van de levenscyclus (zie Figuur 5).

De normen die de huidige stand van de techniek op het gebied van besturingstechnische veiligheidsfuncties voor machines weergeven zijn de NEN-EN-ISO 13849-1:2008 en de NEN-EN-NEN-EN-IEC 62061:2005. Het bijzondere aan de norm NEN-EN-IEC 62061 is dat, anders dan in de oude norm EN 954-1:1996 en de ISO 13849-1, eisen en methodieken worden gespecificeerd voor alle fasen van de levenscyclus van een veiligheidsfunctie. Niet alleen het ontwerp, maar ook de inbedrijfstelling, het gebruik, het onderhoud en de modificaties van een veiligheidsfunctie moeten er voor zorgen dat in alle levensfase aan de eisen voldaan wordt.

De eisen die in dit hoofdstuk beschreven zijn gelden voor alle veiligheidsfuncties gespecificeerd in bijlagen 3 en 6, en de besturingstechnische veiligheidsfuncties die volgen uit de reducerende maatregelen die noodzakelijk blijken te zijn uit de risicobeoordeling.

6.1 Willekeurige en systematische fouten

Iedereen heeft wel eens gehoord van de uitspraak: “De keten is zo sterk als de zwakste schakel”. Dit geldt zeker ook voor de besturingstechnische veiligheidsfuncties op een machine, die steeds uitgebreider en complexer worden. Besturingstechnische veiligheidssystemen kunnen falen als gevolg van:

- Willekeurige fouten; spontaan falen van componenten (hardware).
- Systematische fouten; falen door verborgen fouten in hard- en/of software door gemaakte fouten in bijvoorbeeld het ontwerp.
- CCF; het falen van 2 componenten die dezelfde functie uitoefenen door dezelfde faaloorzaak (meestal omgevingsfactoren).

Door toepassing van “functionele veiligheid” kan een veilige situatie worden bereikt en behouden. De veiligheidsfuncties zijn “functioneel veilig” als willekeurige, systematische en CCF, gedurende alle gespecificeerde omstandigheden en binnen het gespecificeerde tijdsbestek, niet kunnen leiden tot het ondeugdelijk functioneren van het systeem en niet resulteren in:

- Verwonding of dood van personen.
- Uitstoot naar het milieu.
- Verlies van apparatuur of productie.

De normen over functionele veiligheid geven aan dat willekeurige fouten op twee manieren benaderd moeten worden. Allereerst worden maatregelen gespecificeerd om willekeurige fouten te beheersen, bijvoorbeeld door toepassing van redundantie of automatische diagnose. En als tweede wordt geëist dat een kwalitatieve en kwantitatieve analyse op de veiligheidsfunctie uitgevoerd wordt.

De systematische fouten dienen op twee manieren benaderd te worden. Ten eerste moeten maatregelen worden gespecificeerd om systematische fouten te voorkomen en moeten beheersende maatregelen worden genomen. Daarnaast moeten fouten zoveel mogelijk gedetecteerd worden en dient het systeem na detectie van een fout zo snel mogelijk een in veilige toestand gebracht te worden. De systematische fouten worden in de nieuwe normen niet meegenomen in de kwantitatieve berekening van de kans op gevaarlijk falen. Voorkomen en beheersen van systematische fouten moet een van de speerpunten zijn van een ontwerper en bouwer van besturingstechnische veiligheidsfuncties.

Daarnaast worden maatregelen gespecificeerd om CCF te beheersen, bijvoorbeeld door de toepassing van diversiteit in het hardware ontwerp en gebruik van 2 verschillende teams die de software schrijven. Het effect van de CCF wordt bovendien meegenomen in de kwantitatieve berekening van de kans op gevaarlijk falen.

In bijlage 10 is een lijst met aandachtspunten opgenomen voor een ontwerper en/of toetser van veiligheidsfuncties of veiligheidsgerelateerde besturingen. Deze lijst bevat voorbeelden van veel gemaakte fouten. Merk op dat deze lijst niet uitputtend is en dus niet als checklist gebruikt kan worden om een veiligheidsfunctie of –besturing te valideren.

6.2 Nieuwe wettelijke eisen logische eenheden voor veiligheidsfuncties

Op 29 juni 2008 is de nieuwe Machinerichtlijn met nummer 2006/42/EG van kracht geworden. Vanaf dat moment dient een fabrikant die een veiligheidsrelais of de veiligheids-PLC afzonderlijk in de handel brengt, deze veiligheidscomponent door een aangemelde instantie (Notified Body of NOBO) te laten controleren. De NOBO dient een zogenaamd EG-type-onderzoek op het veiligheidsrelais of de veiligheids-PLC uit te voeren.

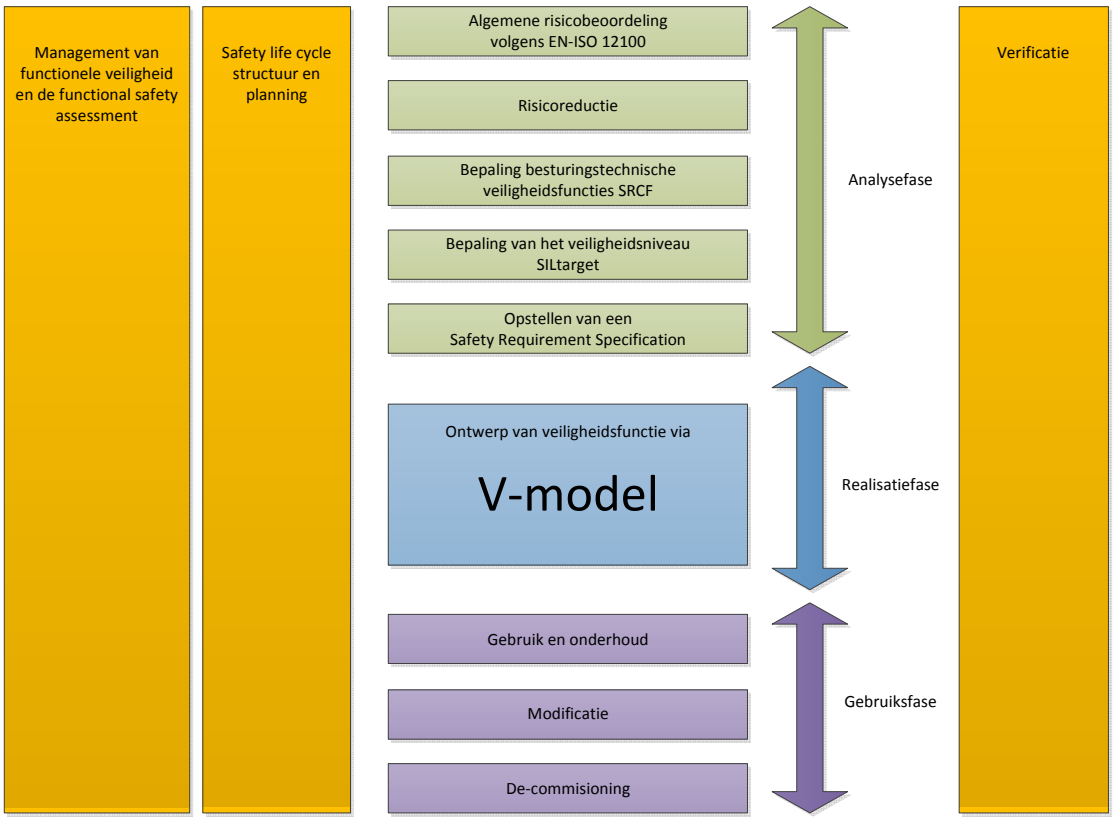
De oude Machinerichtlijn 98/37/EG kende deze eis alleen voor het tweehanden-bedieningsrelais en voor gevoelige elektrische inrichtingen voor de detectie van personen. In de nieuwe Machinerichtlijn (Bijlage IV punt 21) is deze eis uitgebreid naar alle “logische eenheden voor veiligheidsfuncties”. Dit betekent dat naast tweehandenbedieningsrelais onder andere ook noodstop- en hekbewakingsrelais en natuurlijk ook programmeerbare veiligheidscomponenten, zoals veiligheids-PLC’s en veldbussen met een veiligheidsfunctie NOBO-plichtig zijn. Om te voorkomen dat logische eenheden worden toegepast die niet door een Notified Body zijn gecertificeerd is volgende eis van kracht.

VF#008: Indien logische eenheden worden toegepast in een veiligheidsfunctie dienen deze NOBO gecertificeerd te zijn. Dit geldt ook als de logische eenheid alleen wordt ingezet voor diagnosefuncties in een veiligheidsfunctie.

Opmerking: Met logische eenheden worden componenten bedoeld zoals vastgelegd in bijlage V van de Machinerichtlijn.

6.3 Levenscyclus benadering besturingstechnische veiligheidsfuncties

De levenscyclus van een veiligheidstechnische besturingsfunctie bestaat in principe uit drie fases, de analysefase, de realisatiefase en de gebruiksfase. Deze fasen zijn weergegeven in onderstaande figuur.



Figuur 4

De grote oranje balken aan beide zijden van de figuur zijn geven een aantal activiteiten weer, die gedurende de gehele levencyclus van het besturingstechnische veiligheidsfunctie, van belang zijn. Hieronder zullen de verschillende activiteiten uit de verschillende fasen in meer detail worden besproken.

Algemene activiteiten:

1. Management van functionele veiligheid, schrijven functioneel veiligheidsplan en assessment van de functionele veiligheid
2. Opzet van de veiligheids levenscyclus structuur en planning
3. Uitvoeren van verificatie activiteiten gedurende de deelstappen in de verschillende fasen.

<u>Analysefase:</u>

4. Algemene risicobeoordeling van het object volgens de NEN-EN-ISO 12100.

5. Reductie van de geconstateerde risico's.
6. Bepaling van de benodigde besturingstechnische veiligheidsfuncties (in de NEN-EN-IEC 62061 benoemd als SRCF: Safety Related Control Function).
7. Bepaling van het vereiste veiligheidsniveau (SILtarget) van elke veiligheidsfunctie.
8. Opstellen van een Safety Requirement Specification (SRS).

Realisatiefase:

9. Bedenk een functionele architectuur van elke veiligheidsfunctie (meet-evalueer-activeer).
10. Maak een conceptontwerp van elke veiligheidsfunctie (sensor-logic-actuator).
11. Kies de benodigde veiligheidscomponenten in combinatie met standaard componenten; Bouw het geheel samen.
12. Bepaal of het ontwerp kwalitatief voldoet (SIL claim limit).
13. Bepaal of het ontwerp kwantitatief voldoet (SIL calculated) .
14. Voldoet het ontwerp zowel kwalitatief als kwantitatief aan de SRS?
15. Validatie van alle veiligheidsfuncties.

Gebruiksfase:

16. Zorg dat het beheer en onderhoud wordt uitgevoerd volgens de onderhoudshandleiding.
17. Analyse bij modificaties of het veiligheidsniveau van de veiligheidsfuncties behouden blijft.
18. De-commissioning uitvoeren volgens specificatie van leverancier(s).

6.3.1 Beschrijving algemene activiteiten

Hieronder zullen de eerder genoemde stappen en activiteiten in de verschillende fases van de levenscyclus nader worden gespecificeerd. Hierbij wordt specifiek aangegeven welke input voor een activiteit noodzakelijk is, aan welke eisen de specifieke stap moet voldoen en welke output gerealiseerd moet worden en aan RWS ter beschikking worden gesteld.

De eerste drie opgesomde activiteiten zullen gedurende de gehele levenscyclus van het systeem uitgevoerd moeten worden. Omdat deze activiteiten de basis vormen voor de overige activiteiten is het belangrijk om hier al vast te leggen hoe de processen eruit zien die tot goede producten gaan leiden. Om deze reden wil Rijkswaterstaat de uitkomst van deze activiteiten gezamenlijk vastgelegd zien in een plan van aanpak (functioneel veiligheidsplan) dat goedgekeurd moet worden voordat met de overige activiteiten begonnen kan worden.

VF#012: Er dient een functioneel veiligheidsplan opgesteld te worden waarin de resultaten van de eerste drie activiteiten (punt 1 t/m 3) zijn opgenomen. Dit plan dient goedgekeurd te worden door Rijkswaterstaat.

VF#013: Het in punt 4 t/m 16 beschreven proces dient doorlopen te worden volgens het in eis VF#012 opgestelde plan, waarbij de resultaten (output) per stap in de Nederlandse taal gedocumenteerd dienen te worden en worden aangeleverd aan Rijkswaterstaat als onderdeel van het Technisch Dossier (TD).

Opmerking: Van punt 16 dient alleen de input documentatie gerealiseerd te worden, zodat het systeem tijdens gebruik op een goede manier beheerd en onderhouden kan worden.

Punt 1: Management van functionele veiligheid

***Doel*:** Vastleggen van de management en technische activiteiten die nodig zijn om functionele veiligheid van de besturing te realiseren.
Input: Projectspecificatie + organisatie van de Opdrachtnemer
Eisen: NEN-EN-IEC 62061 H4.2.1
Output: Functioneel veiligheidsplan; het Functioneel Veiligheidsplan moet minimaal de volgende onderdelen bevatten:

- Beschrijving van alle relevante activiteiten (opstellen van functionele eisen, ontwerp, verificatie, validatie).
- Beschrijving van de strategie om aan de ontwerpeisen te voldoen.
- Overzicht van de benodigde personen, capaciteit, tools en overige hulpmiddelen.
- Input informatie waarmee het ontwerp proces en de risicobeoordeling kunnen worden gestart.
- Een verificatieplan, zie NEN-EN-IEC 62061 4.2.g. voor informatie over de inhoud.
- Een validatieplan, zie NEN-EN-IEC 62061 4.2.h. voor informatie over de inhoud.

Punt 2: Opzet van een veiligheidslevenscyclus structuur en planning

Doel: Vastleggen van de veiligheidslevenscyclus waarvoor de Opdrachtnemer verantwoordelijk is en de planning van activiteiten die daarbij horen.
Input: Projectspecificatie + organisatie Opdrachtnemer
Eisen: NEN-EN-IEC 62061 H4.2.1
Output: Een eenduidige vastlegging van de veiligheidslevenscyclus met bijbehorende planning.

Punt 3: Uitvoeren van verificatie activiteiten gedurende de deelstappen in de verschillende levenscyclus fasen.

Doel: Uitvoeren van de verificatie activiteiten volgens het opgestelde verificatieplan. Middels een verificatie wordt door middel van testen en inspecties aantoonbaar gemaakt dat de uitkomst van elke activiteit overeenkomt met het vooraf gespecificeerde resultaat.
Input: Verificatieplan (NEN-EN-IEC 62061 H4.2.1.g)
Eisen: Een verificatie wordt uitgevoerd op elke activiteit in de levenscyclus. Dit geldt voor de hardware en de software.
Output: Van elke verificatieactiviteit moet een verificatierapport worden opgesteld waarin de resultaten van de verificatie worden gedocumenteerd.

6.3.2 Beschrijving activiteiten in de analysefase

De activiteiten benoemd in punt 4 t/m 8 hebben als doel om te bepalen welke veiligheidsfuncties noodzakelijk zijn en aan welke eisen deze veiligheidsfuncties dienen te voldoen.

Punt 4: Algemene risicobeoordeling van de machine volgens EN-ISO 12100

Doel: Vastleggen welke gevaren er bij de verschillende delen van het object aanwezig zijn en het schatten van het risico van elk van deze gevaren.

Input: De grenzen van de machine.
Eisen: EN-ISO 12100 H4 en H5. Zie verder hoofdstuk 4 van dit document.
Output: Risico-evaluatie, waarin bepaald of een risicoverlaging is vereist of dat een voldoende veiligheidsniveau is bereikt. Het is de bedoeling dat het restrisico, nadat de benodigde risicoreducerende maatregelen zijn genomen, beneden het acceptabele risico (grensrisico) komt.

Punt 5: Reductie van de geconstateerde risico's

Doel: Vastleggen welke geconstateerde risico's worden gereduceerd en op welke wijze dit plaatsvindt.
Input: Risicobeoordeling en risico-evaluatie.
Eisen: EN-ISO 12100 H6.
Output: Overzicht van de toegepaste risicoreducerende maatregelen en de overblijvende restrisico's.

Punt 6: Bepaling van de benodigde besturingstechnische veiligheidsfuncties

Doel: Vastleggen welke risicoreducerende maatregelen er uitgevoerd worden in de (veiligheids-) besturing van het object.
Input: Risicobeoordeling en –reductie.
Eisen: EN-ISO 12100 H6 en Hoofdstuk 4 van dit document.
Output: Overzichtslijst met de besturingstechnische risicoreducerende maatregelen en hun functionaliteit.

Punt 7: Bepaling van het vereiste veiligheidsniveau (SILtarget)

Doel: Vastleggen van de op basis van het risico vereiste veiligheidsniveau van alle besturingstechnische veiligheidsmaatregelen.
Input: Gegevens uit de risicobeoordeling van het object en hoofdstuk 6 van dit document.
Eisen: NEN-EN-IEC 62061 Bijlage A en hoofdstuk 6 van dit document.
Output: Overzichtslijst van de veiligheidheidsniveaus van de besturingstechnische veiligheidsmaatregelen.

Punt 8: Stel een Safety Requirement Specification (SRS) op

Doel: In detail vastleggen van de functionele eisen en de kwaliteitseisen van elke besturingstechnische veiligheidsfunctie.
Input: Projectspecificatie + informatie uit punt 6 en punt 7.
Eisen: NEN-EN-IEC 62061 H5, bijlage 9 van dit document.
Output: Het SRS document.

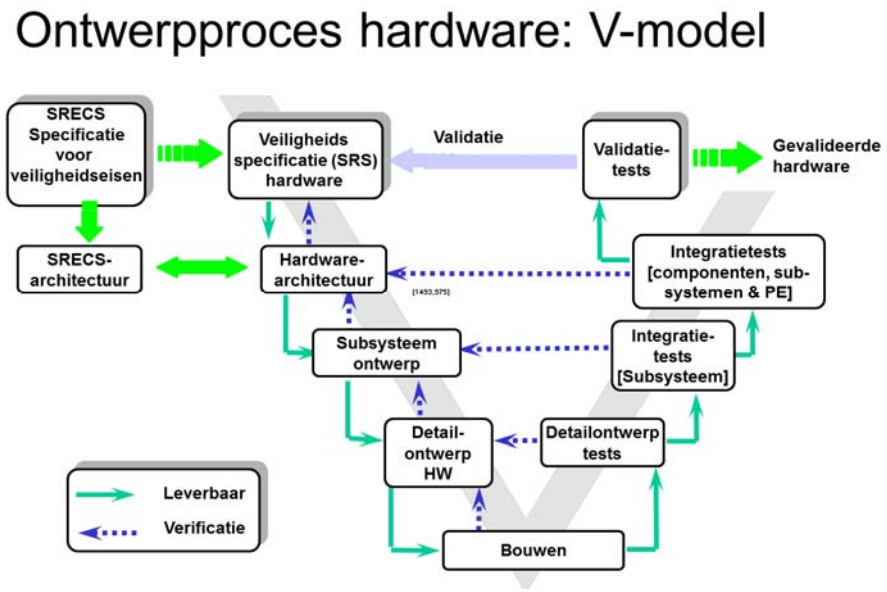
VF#014: Het SRS document bevat minimaal dezelfde onderwerpen en opbouw zoals vastgelegd in Bijlage 9 van dit document.

6.3.3 Beschrijving activiteiten in de realisatiefase

Een model dat in diverse normen voor besturingstechnische veiligheidsfuncties wordt genoemd is het V-model, een voorbeeld wordt getoond in Figuur 5. De linkerarm van het V-model geeft de ontwerpstappen weer. Bij de rechterarm vindt de integratie van de gebouwde ontwerpen plaats. Het aantal lagen in het V-model kan variëren als gevolg van de complexiteit van het ontwerp. Belangrijk is om van te voren vast te leggen welke lagen (ontwerpstappen) bij een specifiek ontwerp worden gerealiseerd. Een dergelijk gestructureerd ontwerp model geeft de mogelijkheid (deel-) ontwerpen op diverse punten te verifiëren. Hiermee wordt voorkomen dat fouten pas worden ontdekt in de gebruiksfase of zelfs nooit worden ontdekt.

VF#015: Voor de realisatie van het systeem waarin de veiligheidsfuncties gerealiseerd worden dient het V-model toegepast te worden.

VF#016: De applicatiesoftware gebruikt voor de veiligheidsfuncties dient ontwikkeld te worden conform paragraaf 6.11 van de NEN-EN-IEC 62061 norm. Hierbij dient het V-model toegepast te worden.



Figuur 5

Punt 9: Bedenk een functionele architectuur (meet-evalueer-activeer)

Doel: Vastleggen van een hardware architectuur voor elke veiligheidsfunctie in functieblokken.
Input: SRS.
Eisen: NEN-EN-IEC 62061 H6.6.2.
Output: Ontwerpspecificatie van de hardware architectuur van elke veiligheidsfunctie in functieblokken.

Punt 10: Maak een conceptontwerp (sensor-logic-actuator)

Doel: Vastleggen van een conceptontwerp van elke veiligheidsfunctie waarmee de verificatie van het vereiste SIL niveau mogelijk is.
Input: Ontwerpspecificatie van de hardware architectuur en de SRS.
Eisen: NEN-EN-IEC 62061 H6.7.
Output: Een conceptontwerp van elke veiligheidsfunctie, waarbij ook een veiligheidsblokschema is gerealiseerd. De veiligheidsfunctie dient in subsystemen te worden weergegeven.

Punt 11: Kies de benodigde veiligheidscomponenten of ontwerp ze zelf (NoBO plichtig); Bouw het geheel samen.

Doel: Keuze van de componenten waarmee de veiligheidsfuncties worden opgebouwd. Vastleggen van de componentgegevens inclusief de veiligheidheidsgegevens voor de berekening van de SIL claim en SIL calculated.
Input: conceptontwerp met veiligheidsblokschema
Eisen: NEN-EN-IEC 62061 H6.7.4.4, bijlage 12 van dit document.
Output: conceptontwerp met alle gegevens van de veiligheidsfunctie, alle subsystemen en componenten vastgelegd in een hardware design specification (HDS), een EG verklaring van overeenstemming, gebruiksaanwijzing en veiligheidsdata.

Van alle parameters moet de herkomst duidelijk en navolgbaar worden vastgelegd. Bij gebruik van bepaalde aannamen zal dit expliciet moeten worden gespecificeerd. Bijlage 12 bevat een voorbeeld van een “hardware design specification (HDS)”, waarin bovenstaande onderwerpen in terug komen.

VF#016a: Het HDS document bevat minimaal dezelfde onderwerpen en opbouw zoals vastgelegd in Bijlage 12 van dit document.

Punt 12: Bepaal of het ontwerp kwalitatief voldoet (SIL claim limit)

Doel: Bepalen (verificatie) of het conceptontwerp voldoet aan de kwalitatieve eisen die voor de veiligheidsfuncties gelden. Dat wil zeggen dat aangetoond wordt dat de “Safe Failure Fraction (SFF)” in combinatie met de “hardware fault tolerance” voldoet aan een SIL niveau dat hoger of gelijk is aan de SILtarget uit de risicobeoordeling.
Input: Veiligheidsblokschema van het conceptontwerp en de Hardware fault tolerance en safe failure fraction gegevens van de componenten.
Eisen: NEN-EN-IEC 62061 H6.7.6.
Output: Een verificatierapport van de beoordeling van de SIL claim (SILCL) van elk subsysteem en de totale veiligheidsfunctie.

Punt 13: Bepaal of het ontwerp kwantitatief voldoet (SIL calculated)

Doel: Bepalen (verificatie) of het conceptontwerp voldoet aan de kwantitatieve eisen die voor de veiligheidsfuncties gelden. Dat wil zeggen dat aangetoond wordt dat de combinatie van subsystemen voldoet aan de kwantitatieve eisen (de som van de PFHd van de subsystemen is kleiner of gelijk aan de gewenste PFHd) welke afhankelijk is van de SILtarget uit de risicobeoordeling.
Input: Veiligheidsblokschema van het conceptontwerp en de faalkansgegevens van de componenten.
Eisen: NEN-EN-IEC 62061 H6.7.8.

Output: Een verificatierapport van de beoordeling van de SIL calculated van elk subsysteem en de totale veiligheidsfunctie.

Punt 14: Voldoet het ontwerp zowel kwalitatief als kwantitatief aan de SRS?

Doel: Vastleggen
Input: De gegevens uit punt 12 en punt 13
Eisen: NEN-EN-IEC 62061 H6.7.6 en H6.7.8.
Output: Beoordeling of zowel de SILCL als de SILcalculated beide groter of gelijk zijn aan het SILtarget uit de risicobeoordeling.

Punt 15: Validatie van alle veiligheidsfuncties

Doel: Controleren dat de veiligheidsfuncties voldoen aan de functionele veiligheidseisen en veiligheids- en kwaliteitseisen (SIL niveau).
Input: Validatieplan en de gerealiseerde veiligheidsfuncties.
Eisen: NEN-EN-IEC 62061 H8.
Output: Validatierapport van alle veiligheidsfuncties.

In het validatierapport dienen voor alle veiligheidsfunctie de volgende gegevens te worden vastgelegd:

- De versie van het validatieplan dat wordt toegepast en de versie van de veiligheidsfuncties die worden getest.
- De veiligheidsfunctie die wordt getest (of geanalyseerd) met een referentie naar de validatie-eisen die zijn vastgelegd in het validatieplan.
- Gebruikte hulpmiddelen en apparatuur, met de hun calibratie gegevens.
- De resultaten van elke test.
- Het verschil tussen de te verwachte uitkomsten en de werkelijke uitkomsten. Bij afwijkingen dient de noodzakelijke aanpassing te worden uitgevoerd en gedocumenteerd en opnieuw getest.

Daarnaast zullen de kwaliteitseisen van de veiligheidsfuncties moeten worden gevalideerd. Zie hiervoor de betreffende paragraaf 8.3.1 van de norm NEN-EN-IEC 62061. Het gaat hierbij om de volgende activiteiten:

- Het functioneel testen tijdens specificatie, ontwerp en integratie fase om fouten in de soft- en hardware van de veiligheidsfuncties te voorkomen.
- Het testen of de veiligheidsfuncties bestand zijn tegen de omstandigheden gespecificeerd in de SRS.
- Het testen of de veiligheidsfuncties zijn bestand tegen elektromagnetische interferentie conform paragraaf 5.2.3 van de norm.
- Testen of de veiligheidsfuncties niet gevaarlijk falen door het moedwillig introduceren van fouten.
- Minimaal 1 of meer additionele test uit paragraaf 8.3.2 van de norm.
- Minimaal 1 of meer additionele test uit paragraaf 8.3.3 van de norm.

De toegepaste technieken en uitkomsten van deze validatie van de systematische kwaliteit dienen te worden gedocumenteerd.

6.3.4 Beschrijving activiteiten in de gebruiks-fase

VF#017: Bij het beheer en onderhoud dienen de eisen uit punt 16 en 17 gehanteerd te worden.

Punt 16. Zorg dat beheer en onderhoud wordt uitgevoerd volgens de gebruikershandleiding

Doel: Er voor zorgen dat de functionele veiligheid gehandhaafd blijft gedurende de fasen gebruik en onderhoud.
Input: Beschrijving van de gebruiks- en onderhoudseisen opgesteld door de fabrikant van de veiligheidsfuncties.
Eisen: NEN-EN-IEC 62061 H7 + SRS H5
Output: Een “functioneel veilig” besturingssysteem door de juiste gebruiks- en onderhoudsprincipes toe te passen.

Minimaal dienen de volgende onderhoudseisen voor de veiligheidsfuncties te worden gespecificeerd:

- Een logboek voor het vastleggen van de onderhoudshistorie van de machine;
- De routine acties die uitgevoerd dienen te worden om het niveau van functionele veiligheid van de veiligheidsfuncties te behouden, inclusief routine vervanging van componenten met een vooraf gedefinieerde levensduur;
- De onderhoudsprocedures die gevolgd moeten worden wanneer er fouten of defecten optreden in de veiligheidsfuncties, inclusief:
  - Procedures voor foutdiagnose en reparatie;
  - procedures waarmee de correcte werking kan worden vastgesteld na uitvoering van een reparatie;
  - Aspecten die bij onderhoud vastgelegd moeten worden.
- De gereedschappen die nodig zijn voor het onderhoud het opnieuw in gebruik nemen, en de procedures voor onderhoud van de gereedschappen en toestellen.
- Een specificatie van de periodieke testen, het preventief onderhoud en correctief onderhoud.

Indien onderhoud gepleegd wordt aan veiligheidsfuncties dient voldaan te worden aan het advies uit bijlage 11. Deze eisen dienen aantoonbaar verwerkt te worden in de werkwijze van de verantwoordelijke Opdrachtnemer en te worden afgestemd met de Opdrachtgever.

Punt 17. Analyseer bij modificaties of het veiligheidsniveau van de veiligheidsfuncties behouden blijft

Doel: Er voor zorgen dat bij de uitvoering van correcties, verbeteringen en aanpassingen aan de veiligheidsfuncties, het vereiste veiligheidsniveau gerealiseerd en/of gehandhaafd blijft.
Input: De aangepaste SRS als gevolg van de modificatie.
Eisen: NEN-EN-IEC 62061 H9
Output: De resultaten van de modificatie van de veiligheidsfuncties.

Het is niet ondenkbaar dat tijdens de levensfase van de veiligheidsfuncties wijzigingen worden aangebracht. Indien dit het geval is gelden de volgende eisen:

- De reden van de wijziging moet gedocumenteerd worden.
- Het effect van de wijziging moet geanalyseerd worden om vast te stellen wat het effect is voor de specifieke veiligheidsfunctie.
- Het effect van de wijziging moet samen met de impact analyse gedocumenteerd worden.
- Alle geaccepteerde wijzigingen die een effect hebben op de veiligheidsfuncties zullen leiden tot een terugkeer naar de geschikte ontwikkel fase (specificatie, ontwerp, validatie, etc.). Alle navolgende fasen moeten worden doorlopen om te waarborgen dat het gewenste veiligheidsniveau behaald wordt en de documentatie bijgewerkt wordt.
- Het configuratie management moet uitgevoerd worden conform paragraaf 9.3 van de norm NEN-EN-IEC 62061.

Punt 18. De-commissioning uitvoeren volgens specificatie van leverancier(s)

Doel: Er voor zorgen dat voorafgaand aan de ontmanteling van een veiligheidsfunctie het object correct uit bedrijf is genomen. Hierbij is van belang om duidelijk vast te leggen welke veiligheidsfuncties tijdens de ontmanteling actief dienen te blijven.
Input: De actuele as-build / as-maintained gegevens van de veiligheidsfuncties en de gegevens van de deelcomponenten.
Eisen: NEN-EN-IEC 62061 H9
Output: Een veilig ontmantelde veiligheidsfunctie.

Voordat de de-commissioning van een veiligheidsfunctie wordt uitgevoerd moet een analyse worden gemaakt van de impact op de functionele veiligheid van het object.
Daarbij moet ook gekeken worden naar de impact op gerelateerde systemen zoals de verkeersregelinstallatie etc. De resultaten van deze impact analyse dienen te worden gebruikt voor het opstellen van heldere verantwoordelijkheden, procedures en een duidelijke werkmethode met een identificatie van de mogelijke gevaren.

6.3.5 Documentatie eisen van veiligheidssystemen

De Opdrachtnemer is, als fabrikant van veiligheidsfuncties, verplicht om het vastleggen en beschikbaar stellen van documentatie. Het gaat hierbij om twee soorten documentatie:

- Ontwerp-, verificatie en validatie documentatie.
- Gebruikers documentatie.

6.3.5.1 Ontwerp-, verificatie en validatie documentatie

Enerzijds dient de ontwerper de ontwerpkeuzes en zijn verificaties en validatie vast te leggen. Hoofdstuk 10 van de SIL norm NEN-EN-IEC 62061 geeft aan welke informatie minimaal door de ontwerper zelf moet worden vastgelegd in het TD van het object. De documentatie zal allereerst:

- nauwkeurig en beknopt zijn;

- gemakkelijk te begrijpen zijn door die personen die er gebruik van moeten maken;
- bij het doel passen waarvoor het bestemd is;
- toegankelijk zijn en onderhoudbaar zijn.
- In de Nederlandse taal geschreven zijn.

De documentatie moet herleidbaar zijn met een naam die het doel van het document weergeeft. Verder moet elk document een revisie index hebben (versie nummer) hebben zodat onderscheid kan worden gemaakt tussen verschillende versies van het document.

Onderstaande tabel kan worden gebruikt als checklist voor de vaststelling of betreffende informatie aanwezig is.

Vereiste informatie	**NEN-EN-IEC 62061 paragraaf**	**Aanwezig J/N Documentnr.**
Functioneel veiligheidsplan	4.2.1	
Specificatie van de veiligheidsfuncties Safety Requirement Specification	5.2	
Functionele specificatie SRCF's	5.2.3	
Safety Integrity specificatie SRCF's	5.3.4	
SRECS ontwerp	6.2.5	
Gestructureerd ontwerpproces	6.6.1.2	
SRECS ontwerpdocumentatie	6.6.1.8	
Structuur van de functieblokken	6.6.2.1.1	
SRECS architectuur	6.6.2.1.5	
Subsysteem SRS	6.6.2.1.7	
Subsysteem architectuur en realisatie	6.7	
Foutuitsluitingen die worden geclaimd	6.7.6 en 6.7.7	
Subsysteem samenbouw	6.7.10	
Software Safety Requirement Specificatie	6.10.1	
Documentatie van het applicatieprogramma	6.11.3.4.5	
Resultaten van de applicatie software module testen	6.11.3.7.4	
Resultaten van de applicatiesoftware integratietesten	6.11.3.8.2	
Documentatie van SRECS integratie testen	6.12.1.3	
Documentatie van SRECS installatie	6.13.2.2	
Documentatie voor installatie, gebruik en onderhoud	7.2	
Documentatie van SRECS validatie testen	8.2.4	
Documentatie van SRECS configuratie management	9.3.1	

Tabel 7

Om de SIL berekening te kunnen uitvoeren dienen van elke in een veiligheidsfunctie toegepaste component de faalkansgegevens te worden bepaald en vastgelegd. De uitgangspunten van de berekening zijn belangrijk bij de verificatie en validatie, maar ook bij de uitvoering van wijzigingen na de ingebruikname. Om te bereiken dat van elke component en veiligheidscomponent de gegevens aan Rijkswaterstaat worden overgedragen is onderstaande eis gespecificeerd.

VF#009: Gebruikte veiligheidscomponenten dienen geleverd te worden met de volgende documenten/gegevens:

1. ***EG Verklaring van overeenstemming (IIA volgens Richtlijn 2006/42/EG) in het Nederlands en de oorspronkelijke taal.***
2. ***Notified Body goedkeurings certificaat (voor Bijlage IV componenten).***
3. ***Notified Body rapport behorend bij het goedkeurings certificaat (voor Bijlage IV componenten).***
4. ***Gebruiksaanwijzing van de veiligheidscomponent in het Nederlands en de oorspronkelijke taal.***
5. ***Applicatie/ montage handleiding van de veiligheidscomponent in het Nederlands en de oorspronkelijke taal.***
6. ***De vereiste veiligheidsgegevens voor de verschillende aansluitmogelijkheden van de veiligheidscomponent zoals beschreven in de gebruiksaanwijzing. Deze gegevens zijn noodzakelijk voor de SIL berekening.***

VF#010: Standaard componenten gebruikt in veiligheidsfuncties dienen geleverd te worden met de volgende documenten/gegevens:

1. ***EG Verklaring van overeenstemming in het Nederlands en de oorspronkelijke taal. Meestal op basis van de EMC-Richtlijn en/of Laagspanningsrichtlijn.***
2. ***Gebruiksaanwijzing van de component in één van de Europese talen, bij voorkeur in het Nederlands en anders in het Engels.***
3. ***Applicatie/ montage handleiding van de component, bij voorkeur in het Nederlands en anders in het Engels.***
4. ***De vereiste veiligheidsgegevens voor de verschillende aansluitmogelijkheden van de component. Deze gegevens zijn noodzakelijk voor de SIL berekening.***

VF#011: De in eisen VF#009 en VF#010 bedoelde componentgegevens dienen digitaal beschikbaar gesteld te worden aan Rijkswaterstaat en integraal onderdeel uit te gaan maken van het op te leveren Technisch Dossier.

6.3.5.2 Gebruikers documentatie

Daarnaast dient de ontwerper bepaalde informatie over te dragen aan de gebruiker.
Hoofdstuk 7 van de SIL norm NEN-EN-IEC 62061 norm geeft aan welke informatie minimaal door de ontwerper overgedragen moet worden aan de gebruiker. Het gaat om informatie voor installatie, gebruik en onderhoud en moet minimaal het volgende bevatten:

- Een uitgebreide beschrijving van de apparatuur, installatie en montage.
- Een beschrijving van het beoogde gebruik van de veiligheidsfuncties en eventuele maatregelen die nodig zijn redelijkerwijs voorzienbaar verkeerd gebruik te voorkomen.
- Informatie van de omgevingscondities (bijv. Verlichting, trillingen, geluidsniveau's, atmosferische verontreinigingen).
- Overzicht blokschema's van de veiligheidsfuncties en de veiligheidsblokschema's van elke veiligheidsfunctie.
- Elektrische, pneumatische en/of hydraulische schema's.
- Proof test interval of levensduur.
- Een beschrijving (met inbegrip van verbindingsschema's) van de interactie tussen de veiligheidsfuncties en de besturingsfuncties van de machine.
- Een beschrijving van de nodige maatregelen om de scheiding tussen de veiligheidsfuncties en de besturingsfuncties van de machine te garanderen.
- Een beschrijving van de beschermende maatregelen en de middelen die de veiligheid handhaven wanneer het nodig is om bepaalde veiligheidsfuncties tijdelijk te overbruggen (bijv. voor handmatige programmering, programma verificatie)
- Programmeer informatie.
- Beschrijving van de onderhoudseisen die voor de veiligheidsfuncties gelden.

7 Overbruggen van veiligheidsfuncties

Zoals in voorgaande hoofdstukken is beschreven zorgen veiligheidsfuncties voor de primaire risicoreductie van gevaren die tot letsel en/of economische schade kunnen leiden. Het is daarom ook niet wenselijk dat een object zijn functie uitvoert zonder dat de veiligheidsfunctie actief is. Desondanks kan er een goede reden (storing, plegen van onderhoud, testen, etc.) zijn om een veiligheidsfunctie tijdelijk buiten gebruik te nemen. Het buiten bedrijf nemen of aanpassen van een veiligheidsfunctie wordt manipulatie genoemd. Bij het tijdelijk buiten bedrijf nemen van een veiligheidsfunctie wordt ook wel gesproken over het “overbruggen van een veiligheidsfunctie”. In dat geval stelt de Machinerichtlijn 2006/42/EG in Bijlage I, hoofdstuk 1, paragraaf 1.2.5 van bijlage I het volgende:

Als de machine voor bepaalde handelingen moet kunnen functioneren met een verplaatste of verwijderde afscherming en/of een uitgeschakelde beveiligingsinrichting, moet de functiekeuzeschakelaar voor de bedienings- of bedrijfsmodus tegelijkertijd:

1. *Alle andere bedienings- of bedrijfsmodi uitschakelen;*
2. *De werking van gevaarlijke functies uitsluitend mogelijk maken door middel van bedieningsorganen die onafgebroken moeten worden bediend;*
3. *De werking van gevaarlijke functies alleen mogelijk maken in omstandigheden met een verminderd risico en daarbij elk gevaar als gevolg van aan elkaar geschakelde regelingen voorkomen;*
4. *De werking van gevaarlijke functies door gewilde of ongewilde invloed op de sensoren van de machine, onmogelijk maken.*

Een veilige overbrugging is mogelijk als tegelijkertijd aan bovenstaande wettelijke eisen wordt voldaan. Voor punt 2 wordt vaak gebruik gemaakt van een tweehandenbediening of een zogenaamde hold-to-run schakelaar. Deze laatste schakelaars zijn speciaal ergonomisch geconstrueerd en hebben 3-standen. In de middenstand kan de machine functioneren en bij doordrukken of loslaten van de knop wordt de overbrugging beëindigd en dienen de gevaarbrengende en bewegende delen zo snel mogelijk veiligheidstechnisch tot stilstand worden gebracht.

Maatregelen die de bij punt 3 genoemde toestand van verminderd risico realiseren zijn bijvoorbeeld: verlaagde snelheid, verlaagd vermogen/kracht, stap-voor-stap bedrijf. Voor enkele speciale machines kunnen andere beschermende maatregelen geschikter zijn.

Verder stelt de Machinerichtlijn dat indien aan deze vier voorwaarden niet gelijktijdig kan worden voldaan, de functiekeuzeschakelaar andere beschermingsvoorzieningen in werking moet stellen, die zijn ontworpen en gebouwd om een veilige werkruimte te garanderen. Kortom weglaten van een van de vier voorwaarden is alleen mogelijk als hiervoor andere maatregelen in de plaats zijn gekomen. Een laatste eis is verder dat de bediener vanaf de bedieningspost het functioneren van de onderdelen waarop hij invloed uitoefent, moet kunnen beheersen.

Het is belangrijk om te vermelden dat de kwaliteit van de toegepaste overbruggingsmaatregelen overeen moet komen met het veiligheidsniveau van de veiligheidsfunctie die is overbrugd. Dus als er een veiligheidsfunctie wordt overbrugd die voldoet aan SIL 2 dienen de technische middelen die voor de overbrugging zijn ingezet minimaal hetzelfde veiligheidsniveau te

realiseren. Daarnaast stelt de machinerichtlijn in paragraaf 1.4.1 van bijlage I dat een beveiligingsinrichting niet eenvoudig buiten werking gesteld mag worden.

VF#018: Overbruggingen dienen alleen geactiveerd kunnen worden door middel van een sleutelschakelaar of het invoeren van een wachtwoord (zie ook paragraaf 9.2.3 van de NEN-EN-IEC 60204-1).

VF#019: De Overbrugging dient hetzelfde veiligheidsniveau (SIL) te hebben als de veiligheidsfunctie die overbrugd wordt.

7.1 Onbedoelde manipulatie

Onbedoelde manipulatie is het aanpassen of buiten bedrijf nemen van een veiligheidsfunctie anders dan de in de vorige paragraaf beschreven overbruggingen. Om onbedoelde manipulatie te voorkomen dient hier tijdens het ontwerp rekening mee gehouden te worden. De ISO 14119 stelt eisen aan het ontwerp om deze vorm van manipulatie te voorkomen. Het toepassen van deze norm kan leiden tot de keuze van andere veiligheidsprincipes en component keuze. Een bekend voorbeeld, welke onbedoelde manipulatie stimuleert, is het toepassen van relais met een testknop.

VF#020: In het ontwerp dient rekening gehouden worden met onbedoelde manipulatie door het toepassen van de eisen uit de ISO 14119.

8 Verificatie en validatie

In de onderstaande tabel staat per eis de fase waarin de eis geverifieerd en gevalideerd moet worden inclusief de bijbehorende verificatiemethode. Hierbij is uitgegaan van de definities in het document “Werkwijzebeschrijving 00044 Verificatie en Validatie”, versie 0.5.

Eis nummer	Levenscyclusfase(n)	Verificatie- en validatiemethode(n)
VF#001	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#002	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#003a	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#003b	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#004	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#005	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#006	Vervallen	
VF#007	Ontwikkelingsfase Realisatiefase	Toets, keuring, FAT, SAT.
VF#007a	Ontwikkelingsfase Realisatiefase	Toets, keuring, FAT, SAT.
VF#008	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#009	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#010	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#011	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#012	Ontwikkelingsfase	Toets.
VF#013	Ontwikkelingsfase Realisatiefase	Toets, keuring, FAT, SAT.
VF#014	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#015	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#016	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#017	Gebruiksfase	Inspectie.
VF#018	Ontwikkelingsfase Realisatiefase	Toets, keuring, FAT, SAT.
VF#019	Ontwikkelingsfase Realisatiefase	Toets, keuring.
VF#020	Ontwikkelingsfase Realisatiefase	Toets, keuring.

Tabel 8

BIJLAGE 1 – Risico's beweegbare brug

Bijlage is ondergebracht in een apart document.

In deze bijlage is per processtap van het brugproces (afgeleid van het document basisbeschrijving werkproces beweegbare brug) aangegeven welke risico's aan een processtap zijn gekoppeld en wat de status (toestand) van een specifieke onderdeel van de beweegbare brug is.

BIJLAGE 2 - Risico's schutsluis

Bijlage is ondergebracht in een apart document.

In deze bijlage is per processtap van het schutproces (afgeleid van het document basisbeschrijving werkproces schutsluis) aangegeven welke risico's aan een processtap zijn gekoppeld en wat de status (toestand) van een specifieke onderdeel van de schutsluis is.

BIJLAGE 3 – Veiligheidsfuncties beweegbare brug

Bijlage is ondergebracht in een apart document.

In deze bijlage zijn de geïdentificeerde risico's uit bijlage 1 gekoppeld aan een maatregel (veiligheidsfunctie). Het SIL niveau van de maatregel is gebaseerd op de geschatte parameters. Daarnaast zijn een aantal eigenschappen (type, stopcategorie, prioriteit) en de bedienvormen waarin ze actief zijn per functie beschreven.

BIJLAGE 4 – Veiligheidsfuncties actief per processtap beweegbare brug

Bijlage is ondergebracht in een apart document.

In deze bijlage zijn de veiligheidsfuncties uit bijlage 3 gekoppeld aan de processtappen uit bijlage 1. Per processtap is aangegeven of de specifieke veiligheidsfunctie actief moet zijn.

BIJLAGE 5 – Functioneel gedrag veiligheidsfuncties beweegbare brug

Bijlage is ondergebracht in een apart document.

In deze bijlage is per processtap uit bijlage 1 aangegeven wat het systeemgedrag van de besturingsinstallatie moet zijn bij de beschreven gebeurtenissen / storingen.

BIJLAGE 6 – Veiligheidsfuncties schutsluis

Bijlage is ondergebracht in een apart document.

In deze bijlage zijn de geïdentificeerde risico's uit bijlage 2 gekoppeld aan een maatregel (veiligheidsfunctie). Het SIL niveau van de maatregel is gebaseerd op de geschatte parameters. Daarnaast zijn een aantal eigenschappen (type, stopcategorie, prioriteit) en de bedienvormen waarin ze actief zijn per functie beschreven.

BIJLAGE 7 – Veiligheidsfuncties actief per processtap schutsluis

Bijlage is ondergebracht in een apart document.

In deze bijlage zijn de veiligheidsfuncties uit bijlage 6 gekoppeld aan de processtappen uit bijlage 2. Per processtap is aangegeven of de specifieke veiligheidsfunctie actief moet zijn.

BIJLAGE 8 - Functioneel gedrag veiligheidsfuncties schutsluis

Bijlage is ondergebracht in een apart document.

In deze bijlage is per processtap uit bijlage 2 aangegeven wat het systeemgedrag van de besturingsinstallatie moet zijn bij de beschreven gebeurtenissen / storingen.

BIJLAGE 9 – Format en voorbeeld Safety Requirements Specification (SRS)

Hieronder is een format van een SRS van een veiligheidsfunctie weergegeven. Dit format beschrijft de informatie die voor iedere individuele veiligheidsfunctie beschikbaar moet zijn. Overkoepelend over alle veiligheidsfuncties heen is het noodzakelijk om een algemene beschrijving van het object te geven. Hierin moet beschreven worden over welke functies het object beschikt, welke functievervullers (bijv. afsluitbomen, seinen, etc.) die relevant zijn voor de veiligheidsfuncties aanwezig zijn, de beschikbare bedienvormen, etc. Ook een overzichtsplaatje met daarin alle functievervullers, die uniek aangeduid zijn, moet toegevoegd worden aan deze algemene beschrijving.

VF nummer	Unieke identificatie van de veiligheidsfunctie, waarbij ook de relatie met de risicobeoordeling wordt gelegd.
VF naam	Naam van de veiligheidsfunctie.
VF type	Type veiligheidsfunctie (bijvoorbeeld vergrendeling, bewaking, beschermende stopfunctie, noodstop, etc.).
VF beschrijving	Beschrijving van de functionaliteit van de veiligheidsfunctie.
VF veilige toestand	Veilige toestand waarheen de veiligheidsfunctie het deel van de machine (beweegbare object) naar toe brengt.

Functionele specificatie VF	
Vereiste SIL niveau	Vereiste SIL niveau waarbij er een relatie gelegd wordt met de risicobeoordeling.
Stopcategorie uit EN-IEC 60204-1	Stopcategorie waaraan de veiligheidsfunctie moet voldoen (indien relevant).
Andere vaste vereisten vanuit wetgeving en normen	Overige eisen waaraan de veiligheidsfunctie moet voldoen. Voorbeelden zijn eisen uit den NEN 6787, eisen met betrekking tot HFT (redundantie), etc.
Verwachte aanspraakfrequentie v.d. VF:	Indicatie van het gebruik van de veiligheidsfunctie (bijvoorbeeld elke brugcyclus).
Besturingsbereik v.d. VF	Op welke onderdelen van de machine heeft deze veiligheidsfunctie invloed op (bijvoorbeeld een opsomming van alle aangesloten aandrijvingen die afgeschakeld worden).

Beschrijving van de bedienvormen van de machine waarin de VF actief is	In welke bedienvormen is de veiligheidsfunctie actief (bijvoorbeeld reguliere, onderhoud en noodbediening-technisch).
Beschrijving van de bedienvormen van de machine waarin de VF NIET actief is	In welke bedienvormen is de veiligheidsfunctie niet actief (bijvoorbeeld noodbediening-hand en bij overbrugging in onderhoudsbediening).
Prioriteit van de VF boven andere VF's die tegelijkertijd actief kunnen zijn.	Is er een overlap of tegenstrijdigheid met een andere veiligheidsfunctie, zo ja, geef aan welke veiligheidsfunctie prioriteit heeft.
Verwachte omgevingscondities per subsysteem	Omgevingscondities per subsysteem (sensor/logic/actuator) opgeven. Voorbeeld: Temperatuurbereik: -20 tot +60 C Luchtvochtigheid: 10 tot 90%; condensvorming mogelijk Luchtdruk: 0,9 en 1,1 bar Stoffen in de lucht: zeewind/zout/zand Chemische substanties: n.v.t. Mechanische trillingen en schokken: xx Brand- en explosierisico: n.v.t. (bijv. Lekkende kegelschepen (LPG)
Beschrijving meldingen operator interface	Korte beschrijving van de gewenste statusmeldingen op het interface van de verschillende bedienvormen.
Vereiste totale responstijd v.d. VF	Geef aan binnen welke tijd moet de totale actie van de veiligheidsfunctie uitgevoerd zijn.

Hieronder is een voorbeeld van een SRS van een veiligheidsfunctie uitgewerkt.

VF nummer	V (bron: bijlage 2 van het document veiligheidsfuncties beweegbare brug en schutsluis), in de risicobeoordeling is dit risico geïdentificeerd als risico x.
VF naam	Neerstand detectie afsluitboom/ ontgrendeling brugdek.
VF type	Vergrendeling.
VF beschrijving	Indien niet alle afsluitbomen gesloten zijn dient het niet mogelijk te zijn om de brug te ontgrendelen. Indien alle afsluitbomen eenmaal gesloten zijn en de brug ontgrendeld is dient de vrijgave gehandhaafd te blijven totdat de brug gesloten is en weer

	vergrendeld.
VF veilige toestand	Brugdek in neerstand en vergrendelt.

Functionele specificatie VF	
Vereiste SIL niveau of PL niveau:	SILtarget = SIL 2 Bron: Risicobeoordelingbrug en bijlage 2 van het document veiligheidsfuncties beweegbare bruggen en schutsluizen.
Stopcategorie uit EN-IEC 60204-1	NVT, er wordt immers geen beweging gestopt. Zo lang niet alle afsluitbomen gesloten zijn dient de hoofdstroom van de grendelinrichting afgeschakeld te zijn.
Andere vaste vereisten vanuit wetgeving en normen	NEN 6787:2012 par. 5.2.6.2; Indien de mechanische vergrendeling(en) ook worden toegepast voor het voorkomen van onbedoelde bewegingen ten gevolge van onverwacht opstarten (niveau E van de besturing volgens NEN-EN 1037:1996+A1:2008) zijn de eisen volgens 6.3.5 uit NEN-EN 1037:1995+A1:2008 van toepassing. Mechanische grendelmechanismen moeten worden voorzien van adequate afschermingen dan wel te worden geplaatst op een locatie die niet toegankelijk is voor onbevoegden.
Verwachte aanspraakfrequentie v.d. VF:	Elke brugcyclus.
Besturingsbereik v.d. VF	De aansturing van grendel 1 (id:uuvv) en grendel 2 (id:xxyy) van het brugdek wordt geblokkeerd.
Beschrijving van de bedienvormen van de machine waarin de VF actief is	Veiligheidsfunctie is actief in de volgende bedienvormen: 1) Reguliere bediening; 2) Onderhoudsbediening; 3) Noodbediening-technisch.
Beschrijving van de bedienvormen van de machine waarin de VF NIET actief is	Veiligheidsfunctie is niet actief in de volgende bedienvormen: 4) Noodbediening-hand. Het is niet mogelijk om deze veiligheidsfunctie te overbruggen.
Prioriteit van de VF boven andere VF's die tegelijkertijd actief kunnen zijn.	Niet van toepassing.
Verwachte	Omgevingscondities slagboom en

omgevingscondities per subsysteem	grendel: Temperatuurbereik: -20 tot +60 C Luchtvochtigheid: 10 tot 90%; condensvorming mogelijk. Luchtdruk: 0,9 en 1,1 bar Stoffen in de lucht: zeewind/zout/zand Chemische substanties: n.v.t. Mechanische trillingen en schokken: xx EMC: licht-industriële omgevingen (IEC 61000-6-3 (emmissie: licht-industrieel) en IEC 61000-6-2 (Immuniteit: industrieel)) Brand- en explosierisico:n.v.t. (bijv. Lekkende kegelschepen (LPG)
Beschrijving meldingen operator interface	Melding 1: Het nummer van de afsluitboom die uit neerstand is tijdens een brugproces moet aan de bedienaar worden gemeld.
Vereiste totale responstijd v.d. VF	Max. 500 ms.

BIJLAGE 10 – Aandachtspunten voor een ontwerper en toetser

Onderstaande lijst bevat aandachtspunten voor een ontwerper en toetser van veiligheidsbesturingen en – functies. Deze aandachtspunten zijn opgesteld naar aanleiding van (recente) ongewenste gebeurtenissen uit de praktijk. In de lijst is een onderscheid gemaakt tussen productrisico's (op systeem niveau, functie niveau en component niveau) en procesrisico's.

Productrisico's

Systeem:

- Een storing in de stuurstroomketen (bijvoorbeeld door een kortsluiting) mag nooit leiden tot het niet aansturen van de voorwaarschuwingseinen, bruglichten, de afsluitboomverlichting en scheepvaartseinen terwijl het brugproces in gang gezet is. Deze dienen dus failsafe aangestuurd worden. Dit geldt ook voor de scheepvaartseinen van de sluis.
- Een storing in de hoofdstroomketen (bijvoorbeeld door een kortsluiting) mag nooit leiden tot gelijktijdige uitval van de bruglichten en afsluitboomverlichting terwijl het brugproces in gang gezet is. Dit geldt ook voor de scheepvaartseinen van de sluis.
- Het uitvallen van het veiligheidsgerelateerde deel van een besturing mag nooit leiden tot het niet aansturen van de voorwaarschuwingseinen, bruglichten, de afsluitboomverlichting en scheepvaartseinen terwijl het brugproces in gang gezet is. Deze dienen dus failsafe aangestuurd worden. Dit geldt ook voor de scheepvaartseinen van de sluis.

Veiligheidsfunctie:

- Het herstellen van een storing / fout in een veiligheid- of besturingsfunctie mag nooit leiden tot het automatisch in gang zetten of voortzetten van een processtap. Dit houdt in dat het functionele deel van de besturing zijn besturingscommando's van bewegende delen moet weghalen zodra een storing / fout gedetecteerd wordt en een veiligheidsfunctie actief wordt (ingrijpt). Zodra de storing in de veiligheidsfunctie hersteld is, en er dus een vrijgave is, zal dit niet leiden tot het automatisch in gang zetten van een processtap.

Component:

- Het toepassen van een relais in een veiligheidsfunctie met een werkende testknop is niet toegestaan. Dit omdat één enkele fout (het per ongeluk indrukken van een testknop) de hele werking van de veiligheidsfunctie ongedaan kan maken.

Procesrisico's

FMECA:

- FMECA is van onvoldoende niveau door incompleetheid (componenten / deelsystemen zijn niet beschouwd) of onvoldoende diepgang (niet alle faalwijzen van een component/ deelsysteem zijn beschouwd).

BIJLAGE 11 – Procedures voor het wijzigen en onderhouden van veiligheidsfuncties

Bijlage is ondergebracht in een apart document.

BIJLAGE 12 – Format van een Hardware Design Specification (HDS)

De Hardware Design Specification (HDS) is een gedetailleerde beschrijving van het ontwerp van de veiligheidsfuncties inclusief de verschillende subsystemen (detectie, logica en actuator) van een veiligheidsfunctie. Hieronder is een format van een HDS van een veiligheidsfunctie weergegeven. Dit format beschrijft de informatie die voor iedere individuele veiligheidsfunctie beschikbaar moet zijn. Overkoepelend over alle veiligheidsfuncties heen is het noodzakelijk om een algemene beschrijving van het object te geven. Hierin moet beschreven worden over welke functies het object beschikt, welke functievervullers (bijv. afsluitbomen, seinen, etc.) die relevant zijn voor de veiligheidsfuncties aanwezig zijn, de beschikbare bedienvormen, etc. Ook een overzichtsplaatje met daarin alle functievervullers, die uniek aangeduid zijn, moet toegevoegd worden aan deze algemene beschrijving.

De HDS is een uitwerking van de eisen uit de SRS. Het is daarom noodzakelijk om de relatie met de SRS te leggen in de HDS.

VF nummer	Unieke identificatie van de veiligheidsfunctie, waarbij ook de relatie met de risicobeoordeling wordt gelegd.
VF naam	Naam van de veiligheidsfunctie.
VF type	Type veiligheidsfunctie (bijvoorbeeld vergrendeling, bewaking, beschermende stopfunctie, noodstop, etc.).
VF beschrijving	Beschrijving van de functionaliteit van de veiligheidsfunctie.
VF veilige toestand	Veilige toestand waarheen de veiligheidsfunctie het deel van de machine (beweegbare object) toe brengt.

Geef daarna kort aan, voordat de subsystemen in detail worden beschreven, uit welke subsystemen de veiligheidsfunctie bestaat en het aantal (per subsysteem: Type component(en) en aantal). Onderbouw dit met een blokschema waarin de relatie tussen de subsystemen duidelijk wordt (denk hierbij aan serie en/of parallelschakeling van subsystemen).

Ieder subsysteem dient daarna in detail beschreven te worden, waarbij minimaal de beschreven informatie vastgelegd dient te worden. Het kan voorkomen dat per subsysteem (detectie, logica, actuator) meerdere type componenten worden toegepast. Deze dienen allemaal afzonderlijk beschreven te worden.

Subsysteem detectie (sensoren)	
Type sensor	Het type sensor dat gebruikt wordt (bijv. mechanisch: normaal contact, mechanisch gedwongen contact, magnetische schakelaar, codering: niet-gecodeerd/gecodeerd, elektronisch: niet-programmeerbaar/

	programmeerbaar, type contact NO/NC).
Aantal sensoren	Het aantal sensoren dat gebruikt wordt in dit subsysteem.
Functionele beschrijving	Beschrijving van de trigger waarop de sensor reageert en wat het gevolg is (relatie input en output) en eventuele tijdsaspecten (vertragingen) die een rol spelen.
Beschrijving aansluitmethodiek	Wat zijn de eisen aan de aansluitmethodiek waaraan voldaan moet worden en die toegepast zijn (bijv. gebruikte contacten/bekabeling/afscherming).
Vereiste responstijd van de sensor(en)	Vereiste responstijd van de sensor.
Beschrijving van de faalmechanismen	Beschrijf hier alle mogelijke faalmechanismen van de sensor.
Beschrijving CCF	Indien gebruik gemaakt wordt van redundantie / diversiteit, beschrijf in dat geval mogelijk common cause falen die beschouwd zijn.
Beschrijving van de toegepaste diagnose functies en testfrequentie	Welke diagnose functies zijn toegepast om falen te detecteren (bijv. testpulsen, terugkoppelloop), leg hierbij de relatie met de geïdentificeerde faalmechanismen. Met welke frequentie worden deze diagnose functies uitgevoerd (continue, voorafgaand aan een processtap, etc.).
Beschrijving van de voorgenomen foutreactiefunctie(s)	Beschrijf de reactie van de functie op systeemniveau als gevolg van het detecteren van een faalmechanisme, zie ook bijlage 5 en 8 van de specificatie veiligheidsfuncties.
Beschrijving van de vereiste testen	Beschrijf de testen die op subsysteem niveau uitgevoerd moeten worden (bijvoorbeeld om het goed functioneren van de diagnose functies te controleren) en de testfrequentie in de beheer & onderhoudsfase.

Subsysteem logica	
Type logica	Het type logica dat gebruikt wordt (bijv. relais, elektronisch, programmeerbaar, netwerk).
Aantal componenten	Het aantal componenten dat gebruikt wordt in dit subsysteem.
Functionele	Beschrijving van de trigger waarop de

beschrijving van de logische functie	sensor reageert en wat het gevolg is (relatie input en output) en eventuele tijdsaspecten (vertragingen) die een rol spelen.
Beschrijving aansluitmethodiek	Wat zijn de eisen aan de aansluitmethodiek waaraan voldaan moet worden en die toegepast zijn (bijv. gebruikte contacten/bekabeling/afscherming).
Vereiste responstijd van de logica	Vereiste responstijd van de logica.
Beschrijving van de faalmechanismen	Beschrijf hier alle mogelijke faalmechanismen van de logica.
Beschrijving CCF	Indien gebruik gemaakt wordt van redundantie / diversiteit, beschrijf in dat geval mogelijk common cause falen die beschouwd zijn.
Beschrijving van de resetfunctie, reset volgorde en locatie(s)	Beschrijf hier (indien van toepassing) hoe de logica gereset wordt, wanneer dit gebeurd en hoe dit eventueel handmatig dient uitgevoerd te worden.
Beschrijving van de toegepaste diagnose functies en testfrequentie	Welke diagnose functies zijn toegepast om falen te detecteren (bijv. geheugen checks, vergelijk PLC outputs, etc.), leg hierbij de relatie met de geïdentificeerde faalmechanismen. Met welke frequentie worden deze diagnose functies uitgevoerd (continue, voorafgaand aan een processtap, etc.).
Beschrijving van de voorgenomen foutreactiefunctie(s)	Beschrijf de reactie van de functie op systeemniveau als gevolg van het detecteren van een faalmechanisme, zie ook bijlage 5 en 8 van de specificatie veiligheidsfuncties.
Beschrijving van de vereiste testen en test interval	Beschrijf de testen die op subsysteem niveau uitgevoerd moeten worden (bijvoorbeeld om het goed functioneren van de diagnose functies te controleren) en de testfrequentie in de beheer & onderhoudsfase.
Beschrijving van de vereiste interfacing met de standaard besturing of andere machines/functies	Beschrijf hier de relatie met de standaard besturing of andere deelsystemen, bijvoorbeeld om fouten te signaleringen op het GUI van gebruikers.
Overbruggingen	Kan deze veiligheidsfunctie overbrugd worden, zo ja, beschrijf op welke wijze dit is uitgevoerd.

Subsysteem actuator	

Type actuator	Het type actuator dat gebruikt wordt (bijv. magneetschakelaar, frequentieomvormer, grendel,etc.).
Aantal actuatoren	Het aantal componenten dat gebruikt wordt in dit subsysteem.
Functionele beschrijving	Beschrijving van de trigger waarop de sensor reageert en wat het gevolg is (relatie input en output) en eventuele tijdsaspecten (vertragingen) die een rol spelen.
Beschrijving van het besturingsbereik	Beschrijving welke functievervullers (seinen, afsluitbomen, etc.) allemaal van status veranderen als deze veiligheidsfunctie aangesproken wordt (zie ook bijlage 5 en 8 van de specificatie veiligheidsfuncties).
Beschrijving aansluitmethodiek	Wat zijn de eisen aan de aansluitmethodiek waaraan voldaan moet worden en die toegepast zijn (bijv. gebruikte contacten/bekabeling/afscherming).
Vereiste responstijd van de actuatoren	Vereiste responstijd van de actuatoren.
Beschrijving van de faalmechanismen	Beschrijf hier alle mogelijke faalmechanismen van de actuatoren.
Beschrijving CCF	Indien gebruik gemaakt wordt van redundantie / diversiteit, beschrijf in dat geval mogelijk common cause falen die beschouwd zijn.
Beschrijving van de toegepaste diagnose functies en testfrequentie	Welke diagnose functies zijn toegepast om falen te detecteren (bijv. testpulsen, terugkoppeling), leg hierbij de relatie met de geïdentificeerde faalmechanismen. Met welke frequentie worden deze diagnose functies uitgevoerd (continue, voorafgaand aan een processtap, etc.).
Beschrijving van de voorgenomen foutreactiefunctie(s)	Beschrijf de reactie van de functie op systeemniveau als gevolg van het detecteren van een faalmechanisme, zie ook bijlage 5 en 8 van de specificatie veiligheidsfuncties.
Beschrijving van de vereiste testen en test interval	Beschrijf de testen die op subsysteem niveau uitgevoerd moeten worden (bijvoorbeeld om het goed functioneren van de diagnose functies te controleren) en de testfrequentie in de beheer & onderhoudsfase.

Een aantal aspecten van de veiligheidsfunctie dient beschreven te worden op het niveau van de veiligheidsfunctie (dus niet op subsysteem niveau).

Functieniveau	

Beschrijving van de faalmechanismen	Beschrijf hier alle mogelijke faalmechanismen op systeemniveau (uitval primaire energie, uitval besturing, uitval bediening).
Beschrijving van de voorgenomen foutreactiefunctie(s)	Beschrijf de foutreactie van de functie als gevolg van het detecteren van een faalmechanisme op systeemniveau, zie ook bijlage 5 en 8 van de specificatie veiligheidsfuncties.
Beschrijving van de vereiste testen en test interval	Beschrijf de testen die uitgevoerd moeten worden om aan te tonen dat de functie correct functioneert, geef per functie aan wat in de beheer & onderhoudfase de testfrequentie is. Minimaal dienen de volgende testen beschreven te worden: - Functionele werking van de veiligheidsfunctie. - Foutreacties van de functie als gevolg van faalmechanismen op subsysteem niveau. - Foutreacties van de functie als gevolg van faalmechanismen op systeemniveau. - Systeemgedrag zoals beschreven in bijlage 5 en 8 van de specificatie veiligheidsfuncties. - Eventuele overbruggingen.

BIJLAGE 13 – Wijzigingen

Versie 1.2

- Expliciete eisen (inclusief verificatie en validatie methode) toegevoegd.
- Risico's nav incidenten (o.a. overtoerenbewaking) toegevoegd.
- Diverse tekstuele wijzigingen.

Versie 1.3

- Diverse verwijzingen naar andere documenten aangepast.
- Diverse tekstuele wijzigingen doorgevoerd (geen aanpassing van eisen en/of verificatie / validatie methoden).

Versie 2.0

- Voorblad n.a.v. vaststelling door de Regiegroep Werkwijzer Aanleg

Versie 2.1

- Diverse verwijzingen naar andere documenten aangepast.
- OP2015 proof gemaakt
- Diverse tekstuele wijzigingen doorgevoerd zoals VHF → VF, Technisch Constructie Dossier → Technisch dossier
- Eis VF#006 vervallen. De ISO 62061 geeft hier voldoende invulling aan.
- Bijlage 9: Format en voorbeeld Safety Requirements Specification (SRS) → EMC is verwijderd bij "Verwachte omgevingscondities per subsysteem" Eisen om te voldoen aan EMC is gespecificeerd in het RWS kader GEEI (techniek) en RWS specificatie proceseisen IA (proces)

BIJLAGE 14 – Begrippen en afkortingen

Hieronder staan de in dit document gebruikte begrippen en afkortingen gedefinieerd. Voor onderstaand overzicht van begrippen en afkortingen is gebruik gemaakt van de in hoofdstuk 2 weergegeven Europese en Nationale normen.

Afscherming (guard) (ISO 12100 par. 3.27)
Fysieke barrière, ontworpen als deel van de machine, om te voorzien in bescherming.

Beschermende stopfunctie (protective stop function) (ISO 10218-1 par 5.5.3)
Veilige stopfunctie als gevolg van aanspreken van een primaire veiligheidsfunctie zoals een retardeerbewaking/eindschakelaar etc.

Beschermende voorziening (protective device) (ISO 12100 par. 3.28)
Beveiligingsvoorziening anders dan een afscherming.

Blokkeervoorziening (interlocking device) (ISO 12100 par. 3.28.1)
Mechanische, elektrische of andersoortige voorziening, waarvan het doel is om de werking van gevaarlijke machinehandelingen onder bepaalde omstandigheden (in het algemeen zo lang een afscherming niet is gesloten) te verhinderen.

Noodstopfunctie (emergency stop function) (ISO 12100 par. 3.40)
Functie die bedoeld is om opkomende of bestaande gevaren voor personen, en opkomende of bestaande schade aan de machine(s) of aan werk in uitvoering af te wenden respectievelijk te verminderen; te worden geactiveerd door één afzonderlijke menselijke actie.

Risicobeoordeling (risk ssessment) (ISO 12100 par. 3.17)
Proces bestaande uit een risicoanalyse en een risico-evaluatie.

Veiligheidsfunctie (safety function) (ISO 12100 par. 3.30)
Functie van een machine waarvan een storing kan leiden tot een onmiddellijke toename van het (de) risico(s).

Hieronder volgt een overzicht van de afkortingen gebruikt in dit document met hun betekenis.

Afkorting	Betekenis
Av	Avoidance: Mogelijkheid om gevaar te ontwijken / beperken
CCF	Common cause failure
DC	Diagnostic coverage
EMC	Electromagnetic compatibility
EN	European Standard
FAT	Factory acceptance test
Fr	Frequency and duration of exposure = Frequentie & blootstellingduur
HDS	Hardware design specification
HFT	Hardware fault tolerance
IEC	International electrotechnical commission
ISO	International standardization organization

MTBF	Mean time between failures
MTTF	Mean time to failure
MTTFd	Mean time to dangerous failure
MTTFoc	Mean time to failure – one channel
MTTR	Mean time to repair (MTTR = MTBF – MTTF)
NEN	Nederlandse norm of Nederlands normalisatie instituut
NO	Normally open
NOBO	Notified body
NPR	Nederlandse praktijkrichtlijn
OM	Other measures
PFD	Probability of (dangerous) failure on demand
PFH	Probability of (dangerous) failure per hour
PL	Performance Level
Pr	Probability of occurance of a hazardous event: Kans op ontstaan van gevaarlijke gebeurtenis
SAT	Site acceptance test
Se	Severity of the possible harm
SFF	Safe failure fraction
SIL	Safety integrity level
SRCF	Safety related control function
SRS	Safety requirement specification
TD	Technisch Dossier voorheen TCD (Technisch Constructie Dossier)