Gemeente Amsterdam

Specificatie Veiligheidsfuncties Algemeen

Documentgegevens	
Auteur:	V&OR
Document:	Specificatie Veiligheidsfuncties Algemeen
Revisie:	F2.0
Status:	Definitief
Datum:	21-8-2019

Gemeente Amsterdam

Opsteller				
Bedrijf	**Naam**	**Functie**	**Datum**	**Handtekening**
RHDHV	5.1,2,e	5.1,2,e	01-08-19	
RHDHV	5.1,2,e	5.1,2,e	21-08-19	

Controle				
Bedrijf	**Naam**	**Functie**	**Datum**	**Handtekening**
V&OR	5.1,2,e	5.1,2,e		
V&OR	5.1,2,e	5.1,2,e		

Vrijgave				
Bedrijf	**Naam**	**Functie**	**Datum**	**Handtekening**
V&OR		5.1,2,e		

Revisiebeheer			
Revisie	**Datum**	**Auteur**	**Wijziging**
F1.0	1-8-2019	5.1,2,e (RHDHV)	Alle commentaar van de controleurs is in deze versie verwerkt.
F1.1	8-8-2019	5.1,2,e (RHDHV)	Alle commentaar zoals besproken met 5.1,2,e verwerkt
F2.0	21-8-2019	5.1,2,e (RHDHV)	Laatste commentaar verwerkt

Gemeente Amsterdam

Inhoudsopgave

1 Inleiding

Dit document 'Specificatie Veiligheidsfuncties' maakt deel uit van de Standaard Beweegbare bruggen en Sluizen Gemeente Amsterdam.

1.1 Beschrijving Brug- en sluisstandaard

De standaard beweegbare bruggen en schutsluizen bestaat uit documenten die de inrichting van de werkprocessen en de functionele en technische eisen aan bruggen en sluizen beschrijven, in het licht van de wetgeving, beleidsdoelstellingen en netwerkmanagement van de gemeente Amsterdam. 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 de gemeente Amsterdam.

De 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 van de gemeente Amsterdam.

1.2 Doel

De doelstelling van de gemeente Amsterdam 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 document 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 beweegbare kunstwerken 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 beweegbare kunstwerken 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.

1.3 Scope

De scope van dit document beperkt zich tot de besturingstechnische veiligheidsfuncties die in het bediening- en besturingssysteem gerealiseerd moeten worden, en het proces om deze te realiseren.

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) 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 kunstwerken zich bevinden.
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

beweegbare kunstwerken. De bruikbaarheid van dit document beperkt zich dus tot de projectorganisaties van de processen aanleg en onderhoud.

1.4 Leeswijzer

In dit document worden de algemene veiligheidsrisico's van het brug en sluisproces beschreven (hfst 2), de geclassificeerde veiligheidsfuncties (hfst 3) en de verificatie en validatie van de veiligheidsfuncties (hfst 4).

In de documenten Specificatie Veiligheidsfuncties Beweegbare Brug, Specificatie Veiligheidsfuncties Schutsluis en Specificatie Veiligheidsfunctie brug-sluis combinatie worden de specifieke risico's en veiligheidsfuncties nader beschreven.

2 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 het document Specificatie Veiligheidsfuncties Beweegbare Brug worden de geïdentificeerde risico's gerelateerd aan het brugproces beschreven.

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 het document Specificatie Veiligheidsfuncties Schutsluis worden de geïdentificeerde risico's gerelateerd aan het sluisproces getoond.

De combinatie van een beweegbare brug en schutsluis komt niet heel veel 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 de gemeente Amsterdam 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 de Specificatie Veiligheidsfuncties Beweegbare Brug, Schutsluis en combi brug-sluis zijn niet uitputtend. Daarnaast is er in deze Specificaties 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.

3 Veiligheidsfuncties

3.1 NEN-EN-IEC-62061

De geïdentificeerde risico's in de Specificaties Veiligheidsfuncties Beweegbare Brug, Schutsluis, combi Brug-Sluis 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- en besturingssysteem, 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 de besturingsinstallatie van het object.

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. De gemeente Amsterdam heeft een voorkeur voor de systematiek van de NEN-EN-IEC 62061 omdat deze de volledige levenscyclus beschrijft. De in dit document beschreven systematiek gaat daarom uit van de NEN-EN-IEC 62061, deze norm dient dan ook toegepast te worden.

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

3.2 Classificatie

Voor de classificatie van het SIL-target van de verschillende besturingstechnische veiligheidsfuncties in het brug- en schutsluis proces, is gebruik gemaakt van de risicograaf uit de norm NEN-EN-IEC 62061:

			Zwart = hoog risico													
			Grijs = middelmatig risico													
			Wit = laag risico													
Consequenties		Severity	Class Cl (Fr + Pr + Av)					Frequency and duration Fr				Probability of hazardous event Pr		Avoidance Av	
		Se	3-4	5-7	8-10	11-13	14-15	Duur blootstelling per keer:	D < 10 min.	D ≥ 10 min.					
Onherstelbare verwonding zodanig dat werken na genezing erg moeilijk of zelfs onmogelijk wordt. Bijvoorbeeld dood, verlies van oog, verlies van arm.		4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≥ 1 keer / uur	5	5		Zeer hoog	5		
Normaal gesproken onherstelbare verwonding, werken na genezing wordt bemoeilijkt. Bijvoorbeeld één of meer gebroken ledematen, verlies van één of meer vingers.		3		(OM)	SIL 1	SIL 2	SIL 3	≥ 1 keer/dag - < 1 keer / uur	4	5		Waarschijnlijk	4		
Snijwonden, doorstekingen en kneuzingen (behandeling door arts noodzakelijk).		2			(OM)	SIL 1	SIL 2	≥ 1 keer/2 wkn- < 1 keer / dag	3	4		Mogelijk	3	Onmogelijk	5
Schrammen en lichte kneuzingen (opgelost door eerste hulp).		1				(OM)	SIL 1	≥ 1 keer/ jaar - < 1 keer / 2 wkn	2	3		Zelden	2	Zelden	3
								< 1 jaar	1	2		Verwaarloosbaar	1	Mogelijk	1

De risicograaf laat een viertal parameters zien die leiden tot een SIL:

- Se = Severity; ernst van de verwonding
- Fr = Frequency and duration; frequentie of blootstellingsduur
- Pr = Probablity of hazardous event; kans van optreden van gevaarlijke gebeurtenis
- Av = Avoidance; mogelijkheid om het gevaar te ontwijken cq. Het letsel te beperken

3.2.1 Severity

De ernst van de verwonding (Se = Severity) is opgedeeld in 4 gradaties:

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. amputaties en gebroken botten, etc. werken na genezing weer mogelijk; schade aan object en/of andere eigendommen; schade aan omgeving.	3
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

Het gaat hierbij om het zwaarst voorzienbare letsel dat zou kunnen optreden.

3.2.2 Frequency and duration

De Frequency and Duration (Fr) is de frequentie of blootstelling aan het gevaar en de duur van de blootstelling gedurende de activiteit.

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

Bij het bepalen van de Blootstelling dient onderscheid te worden gemaakt tussen blootstelling van weggebruikers, vaarweggebruikers en bedienaars, deze groep zal alleen blootgesteld wordt tijdens een bediening van een brug en dat zal in de regel korter zijn dan 10 minuten. Onderhoudspersoneel zal daarentegen minder vaak worden blootgesteld omdat een object een aantal malen per jaar onderhoud behoeft maar de duur zal wel langer zijn dan 10 minuten.

3.2.3 Probablity of hazardous event

De Probability of Hazardous Event (Pr) of wel de kans van optreden van de gevaarlijke gebeurtenis (risico).
In de norm is aangeven bij het bepalen van de Pr uitgegaan moet worden van de worst-case scenario. Hierbij dient rekening gehouden te worden met menselijke fouten als gevolg van stres die het werken met of in de buurt van een gevaarlijke machine, maar ook gemakzucht als gevolg dagelijks of regelmatig werken met gevaarlijke machines.
Bij het bepalen van de Pr dient dan ook al snel rekening gehouden te worden met een " erg hoge" kans van optreden (zie hiervoor ook de EN-IEC-62061 A.2.4.2 Probability of occurrence of hazardous event).

Kans van optreden van de gevaarlijke gebeurtenis	Kans (Pr)
Erg hoog	5
Waarschijnlijk	4
Mogelijk	3
Zelden	2
Verwaarloosbaar	1

3.2.4 Avoidance (av)

Avoidance ofwel de mogelijkheid tot het ontwijken van het gevaar of het beperken van het letsel. Hierbij dient met de onderstaande aspecten rekening gehouden te worden:

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

Mogelijkheid om het gevaar te ontwijken of het letsel te beperken (AV)	
Onmogelijk	5
Zelden	3
Mogelijk	1

3.2.5 Classificatie

Onderstaande tabel geeft de methodiek weer om het SIL-target 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 SIL-target. OM staat voor “other measures” en geeft aan dat andere maatregelen toegepast dienen te worden.

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

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.

3.3 Beweegbare brug en schutsluis

In Specificatie Veiligheidsfuncties Beweegbare Brug worden respectievelijk de minimaal noodzakelijke veiligheidsfuncties en de daaraan gestelde eisen waarin deze veiligheidsfuncties actief moeten zijn en het gewenste gedrag van de veiligheidsfuncties beschreven. Dit is ook gedaan voor de schutluis in Specificatie Veiligheidsfuncties Schutsluis en de Specificatie Brug-Sluis Combinatie. De in de Specificatie Veiligheidsfuncties Beweegbare Brug, Schutsluis en Brug-Sluis Combinatie gedefinieerde waarde voor SIL-target zijn minimale waarden. Uit de risicobeoordeling kan blijken dat een hoger veiligheidsniveau (SIL-target) noodzakelijk is. In Specificatie Veiligheidsfuncties Beweegbare Brug, Schutsluis en Brug-Sluis Combinatie zijn voor sommige veiligheidsfuncties criteria aangegeven die het risiconiveau mede bepalen.

3.4 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.

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!

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.

3.5 Documenten eisen en veiligheidssystemen

De Opdrachtnemer is, als fabrikant/leverancier en ontwerper van de veiligheidscircuit, verplicht om het vastleggen en beschikbaar stellen van documentatie. Het gaat hierbij om twee soorten documentatie:

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

3.6 Ontwerp, verificatie en validatie

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.

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 Gemeente Amsterdam worden overgedragen is onderstaande eis gespecificeerd.

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

- 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.

3.7 Functionele veiligheid

3.7.1 Doel

De machinerichtlijn stelt een aantal eisen aan het besturingssysteem van een machine met als uitgangspunt dat er geen gevaarlijke situaties mogen ontstaan door falen van het besturingssysteem.

Een besturingssysteem moet zodanig zijn ontworpen en gebouwd dat:

- zij bestand zijn tegen de normale bedrijfsbelasting en tegen invloeden van buitenaf,
- een storing in de apparatuur of de programmatuur van het besturingssysteem niet tot een gevaarlijke situatie leidt,
- fouten in de besturingslogica niet tot een gevaarlijke situatie leiden,
- redelijkerwijs voorzienbare menselijke fouten gedurende de werking niet tot een gevaarlijke situatie leiden.

Om bovenstaande te voorkomen heeft de gemeente standaard veiligheidsfuncties per type object beschreven in Specificatie Veiligheidsfuncties Beweegbare Brug, Schutsluis en Combinatie Brug-Sluis.

Om de veiligheidsfuncties nader uit te werken en te ontwerpen, testen en te verifiëren en valideren dient een functioneel veiligheidsplan opgesteld te worden.

3.7.2 Functioneel veiligheidsplan

Onderdeel van de uitwerking en het ontwerp van de veiligheidscircuits die het gevolg zijn van de veiligheidsfuncties is een functioneel veiligheidsplan. Dit plan dient onderdeel te zijn van het Technisch Dossier van de Besturingsinstallatie van het object.
Het Functioneel Veiligheidsplan dient opgesteld te worden conform de EN-IEC-61062 en bestaat uit minimaal uit de onderstaande onderdelen en zoals beschreven en vastgelegd in hoofdstuk 4 van de EN-IEC 62061, zie onderstaande tabel.

EN IEC 62051 4.2.1 A functional safety plan shall be drawn up and documented for each SRECS design project, and shall be updated as necessary. The plan shall include procedures for control of the activities specified in Clauses 5 to 9.

NOTE 1 The content of the functional safety plan should depend upon the specific circumstances, which can include:
– size of project;
– degree of complexity;
– degree of novelty of design and technology;
– degree of standardization of design features;
– possible consequence(s) in the event of failure.

In particular the plan shall:
a) identify the relevant activities specified in Clauses 5 to 9.
b) describe the policy and strategy to fulfill the specified functional safety requirements.
c) describe the strategy to achieve functional safety for the application software, development, integration, verification and validation.
d) identify persons, departments or other units and resources that are responsible for carrying out and reviewing each of the activities specified in Clauses 5 to 9.
e) identify or establish the procedures and resources to record and maintain information relevant to the functional safety of a SRECS.

NOTE 2 The following should be considered:
- the results of the hazard identification and risk assessment;
- the equipment used for safety-related functions together with its safety requirements;
- the organization responsible for maintaining functional safety;
- the procedures necessary to achieve and maintain functional safety (including SRECS modifications).

f) describe the strategy for configuration management (see 9.3) taking into account relevant organizational issues, such as authorized persons and internal structures of the organization.
g) establish a verification plan that shall include:
- details of when the verification shall take place;
- details of the persons, departments or units who shall carry out the verification;
- the selection of verification strategies and techniques;
- the selection and utilization of test equipment;
- the selection of verification activities;
- acceptance criteria; and
- the means to be used for the evaluation of verification results.
h) establish a validation plan comprising:
- details of when the validation shall take place;
- Identification of the relevant modes of operation of the machine (e.g. normal operation, setting);
- requirements against which the SRECS is to be validated;
- the technical strategy for validation, for example analytical methods or statistical tests;
- acceptance criteria; and
- actions to be taken in the event of failure to meet the acceptance criteria.

NOTE 3 The validation plan should indicate whether the SRECS and its subsystems are to be subject to routine testing, type testing and/or sample testing.

3.7.2.1 *Identificatie van de veiligheidsfuncties*

Ten behoeve van de gestructureerde ontwerpmethode welke gehanteerd moet worden bij het ontwerpen, testen en realiseren van de veiligheidsfuncties is het belangrijk dat alle veiligheidsfunctie een uniek nummer of een unieke naam hebben. In de risicobeoordeling wordt bij de risico's welke met een veiligheidsfunctie gereduceerd worden, verwezen naar een veiligheidsfunctie middels deze unieke identificatie. In de Specificatie Veiligheidsfuncties Beweegbare Brug, Schutsluis en Combinatie Brug-Sluis hebben alle Standaard veiligheidsfuncties een unieke identificatie. Voor beweegbare bruggen begint deze met VFB met nr, voor schutsluizen is dat VFSL met nr en voor Combinatie Brug-Sluis is dat VFCBS met nr.

3.7.2.2 *Classificatie van de veiligheidsfuncties*

Wanneer veiligheidsfuncties gedefinieerd zijn in de risicobeoordeling, volgt de classificatie van de veiligheidsfuncties. Met classificatie van een veiligheidsfunctie wordt bedoeld het bepalen van het benodigde SIL-niveau van de veiligheidsfunctie. In de Specificatie Veiligheidsfuncties Beweegbare Brug, Schutsluis en Combinatie Brug-Sluis is de minimale SIL classificatie van de Standaard Veiligheidsfuncties van de Gemeente Amsterdam aangegeven. Uit de risicobeoordeling van de aannemer moet blijken of deze classificatie voldoet.

3.7.2.3 *Functionele specificatie van de veiligheidsfuncties (SRS)*

In de Safety Requirement Specification van de standaard veiligheidsfuncties zijn bepaalde aannames gedaan en ontbreken eventuele object specifieke specificaties. Het is essentieel dat de aannemer toets of de specificaties van de veiligheidsfuncties toepasbaar zijn op het specifieke object. Eventuele aanvulling zoals omgevingsomstandigheden of andere uitgangspunten zoals een hydraulische aandrijving in plaats van een elektromechanische aandrijving zullen moeten worden beschouwd en gespecificeerd. Bijlage A bevat een template welke gebruikt kan worden om de functionele specificaties van deze veiligheidsfuncties vast te leggen.

Specificatie van standaard veiligheidsfuncties (SRS)	
Identificeer veiligheidsfuncties (VHF)	Als een veiligheidsfunctie als risico reducerende maatregel wordt toegepast, neem dan de naam en/of het ID-nummer van deze functie op in het risicobeoordeling en –reductiedocument als verwijzing. Tevens wordt onderbouwd dat met de toegepaste veiligheidsfuncties en de overige risico reducerende maatregelen de desbetreffende risico's afdoende zijn gereduceerd. Daarnaast wordt een aantal veiligheidsfuncties gebruikt om economische schade te voorkomen of omdat de norm NEN 6787 dit vereist (zoals retardeerbewaking voorkoming van mechanische schade).
Bepalen vereiste SIL Target-level per VHF	Bepaal, beargumenteer en documenteer het vereiste SIL Target-level Se, Fr, Pr, Av

Opstellen SRS	Controleer of de specificaties van de veiligheidsfuncties uit de standaard SRS toepasbaar zijn op dit object. (Referentie de norm: EN IEC 62061 §5.2)
uitgevoerd dd: Filenaam/namen:	
<u>Aanvulling</u> op de specificatie van veiligheidsfuncties (SRS)	
Aanvulling	Als een brug functionaliteit nodig heeft die niet voorzien is in de Standaard, wordt een aanvulling op de standaard SRS opgesteld. Hanteer hiervoor eenzelfde wijze als de standaard SRS of gebruik de template uit dit bijlage 3.5.1d. (Denk bijvoorbeeld aan veiligheid gerelateerde delen van hydraulische besturingssystemen) Voeg tevens per veiligheidsfunctie eventueel ontbrekende (object specifieke) specificaties toe. Denk hierbij bijvoorbeeld aan: - Per subsysteem (input - logic - output) de te verwachtte omgevingsomstandigheden; - De vereiste totale responsetijd; - De verwachtte aanspraakfrequentie van de veiligheidsfunctie; - Eventuele overbrugbaarheid van de veiligheidsfunctie; - Brug specifieke parameters zoals vertragingstijden e.d. welke van toepassing zijn op de veiligheidsfunctie. Als er geen aanvullingen zijn, wordt het aangeleverde document geaccepteerd en geaccordeerd.
uitgevoerd dd: Filenaam/namen: Gebruikte tools: Onder verantwoordelijkheid van: Team samenstelling:	In te vullen door opdrachtnemer

3.7.2.4 Hardware Ontwerp (HDS)

Het ontwerp (hardware) van de veiligheidsfuncties moet gebaseerd zijn op de SRS. Het Hardware Ontwerp (HDS Hardware Design Specification) dient opgesteld te worden conform de EN-IEC-61062. Bijlage B bevat een template welke gebruikt kan worden om de specificaties van de hardware van deze veiligheidsfuncties vast te leggen.

In onderstaande tabel is weergegeven hoe het hardware ontwerp dient te worden beschreven en vastgelegd.

Specificatie van het hardware-ontwerp (HDS)	
Opstellen functionele architectuur/ Concept ontwerp	Ontwerp een functionele architectuur bij elke veiligheidsfunctie (sensor/ logic/ actuator). (EN IEC 62061 6.6)
Componentkeuze	Kies subsystemen (kant en klaar) of ontwerp subsystemen met geschikte componenten. EN IEC 62061 6.7)
Diagnose per subsysteem	Ontwerp de benodigde diagnosefuncties (EN IEC 62061 6.8) Wordt de diagnose door de subsystemen gedaan? Of voert de logische unit dit uit? Omschrijf terugkoppeling, plausibiliteitcontrole, testpulsen etc.
Systematische fouten	Maak een lijst van maatregelen en technieken die in acht genomen worden om systematische fouten te voorkomen en beheersen. conform EN IEC 62061 6.7.9
uitgevoerd dd: Filenaam/namen:	
<u>Aanvulling</u> op de specificatie van het hardware-ontwerp	
Aanvulling	Als een brug functionaliteit nodig heeft die niet voorzien is in de Standaard van de gemeente Amsterdam wordt een aanvulling opgesteld. Hanteer hiervoor eenzelfde wijze als de standaard SRS of gebruik de template uit dit bijlage B. Als er geen aanvullingen zijn, wordt het aangeleverde document geaccepteerd en geaccordeerd.

uitgevoerd dd: Filenaam/namen: Gebruikte tools: Onder verantwoordelijkheid van: Team samenstelling:	In te vullen door opdrachtnemer

3.7.2.5 Functionele Specification van de Software (SSRS)

Naast de SRS benoemt de SIL-norm ook de Software Safety Requirement Specification. In dit document dient vastgelegd te worden hoe eventuele fail-safe software ontworpen moet worden. Het uitgangspunt van de SSRS is het FSP, de SRS en de bepaalde architectuur (Hardware Fault Tolerance) van de veiligheidsfuncties.
De SSRS wordt net zoals de SRS als directielevering meegeleverd. Wanneer echter aanvullende object specifieke veiligheidsfuncties toegevoegd gaan worden en hiervoor gebruik gemaakt wordt van fail-safe software zal een aanvulling op de SSRS opgesteld moeten worden. Aangezien de inhoud en opzet van de SSRS sterk afhangt van het ontwerp van de specifieke veiligheidsfuncties en toegepaste fail-safe PLC is hier geen algemene template voor beschikbaar. Vandaar dat hieronder de belangrijkste eisen opgesomd zijn waaraan de SSRS moet voldoen:

1. Er moet een duidelijke link zijn naar de veiligheidsfuncties waar de Fail safe software subsystemen deel van uitmaken;
2. De requirements van de Fail safe software subsystemen moet voldoende gedetailleerd gespecificeerd worden zodat het benodigde SIL niveau behaald kan worden;
3. In de specificatie van de requirements van de Fail safe software subsystemen moet dusdanig opgesteld worden zodat deze duidelijk, ondubbelzinnig, verifieerbaar, testbaar en onderhoudbaar is;
4. De specificatie van de requirements van de Fail safe software subsystemen moet alle benodigde informatie bevatten waarmee de juiste keuze van de Fail-safe PLC en de configuratie daarvan bepaald kan worden (als namelijk uit de requirement specificatie blijkt dat floating-point berekeningen noodzakelijk zijn, dan zal de toe te passen Fail safe PLC daarvoor geschikt moeten zijn).
   De eisen welke aan de veiligheidsfuncties gesteld worden welke een Fail safe software subsysteem bevatten, zijn de volgende:
   - een specificatie van de functionaliteit van alle functieblokken welke onderdeel uitmaken van een subsysteem;
   - een specificatie van de in- en outputs van alle toegepaste functie blokken;
   - alle informatie over de formats en bereiken van zowel de input- als de outputdata in relatie tot de functieblokken;
   - wanneer relevant een beschrijving van de grenzen van elk functieblok (hierbij moet gedacht worden aan de maximale responsetijd, grenswaarden enz.);
   - een specificatie van alle diagnose functies van bijvoorbeeld sensors of actuatoren welke in onderdeel uitmaken van de veiligheidsfunctie;

- een specificatie van de functies welke garanderen dat de machine naar een veilige toestand gaat en daar blijft;
- een specificatie van de aanwezige functies welke de foutafhandeling verzorgen binnen de Fail safe software subsystemen;
- een specificatie van de functies welke benodigd zijn om periodiek testen van de veiligheidsfuncties (on- en offline) mogelijk te maken;
- een specificatie van de functies welke voorkomen dat ongeautoriseerde / onbevoegde personen modificaties uit kunnen voeren aan de Fail safe software subsystemen;
- een specificatie van alle benodigde interfaces naar standaard functies (niet veiligheidsgerelateerde besturingsfuncties);
- een specificatie van de prestaties, response tijde en capaciteit van de Fail safe software subsystemen.

5. Het wordt aangeraden om 'semi-formal methods' zoals logic, functieblokken of tijd-weg diagrammen op te nemen in de SSRS wanneer dit relevant is en duidelijkheid schept.

3.7.2.6 Verificatie

In het ontwerptraject van veiligheidsfunctie moeten op verschillende punten in het proces verificatiestappen ingebouwd worden. Het doel van het uitvoeren van een gedegen verificatie van het ontwerpproces om te komen tot 100% foutloos gerealiseerde veiligheidsfuncties. Gaandeweg het proces kunnen eventuele fouten geconstateerd en gecorrigeerd worden.
Dit betekend dat naast de SIL-verificatie waarbij bepaald wordt of het SIL-target met het gekozen ontwerp van een veiligheidsfunctie behaald wordt, ook een aantal procesverificatiestappen noodzakelijk zijn.
Onderstaand

Standaard SIL verificatie	
Bepaal diagnosefuncties	Bepaal DC (eventueel in combinatie met SFF) voor de subsystemen waarvoor dit relevant is.
Bepaal of het ontwerp voldoet aan de architectuureisen (SIL CL)	Gebruik de variabelen DC/SFF en HFT. De gebruikte SIL tool kan bepalen of aan de architectuureisen is voldaan, zorg voor voldoende documentatie in de SIL tool
Bereken of het ontwerp voldoet aan de betrouwbaarheidseisen (SIL calculated, PFHd)	Wordt uitgevoerd door de SIL tool, zorg voor voldoende documentatie. Gebruik waar mogelijk leveranciersbibliotheken voor veiligheid gerelateerde data.
Target SIL bereikt?	Wordt uitgevoerd door de SIL tool. EN IEC 62061 §6.6
uitgevoerd dd: Filenaam/namen:	Altijd documenteren wie verificatie heeft uitgevoerd en wie controle gedaan heeft. Verificatie voor zien van bestandsnaam volgens Standaard Gemeente Amsterdam.

<u>Aanvulling</u> op de SIL verificatie	
Aanvulling	De opdrachtnemer controleert de SIL verificatie die door de gemeente is aangeleverd. Het SIL level van veiligheidsfuncties die aanvullende functionaliteit of afwijkende componenten gebruiken wordt aanvullend aangetoond. Van hydraulische subsystemen kan indien nodig met de norm EN ISO 13849-1 een Performance Level worden bepaald. Als er geen aanvulling is wordt het aangeleverde document geaccepteerd en geaccordeerd.
uitgevoerd dd: Filenaam/namen: Gebruikte tools: Onder verantwoordelijkheid van: Team samenstelling:	In te vullen door opdrachtnemer Software tool voor SIL of PL verificatie

3.7.2.7 SIL verificatie ontwerpfase

In onderstaande tabel is standaard verificatierapport aangegeven die per veiligheidsfunctie dient te worden uitgevoerd.

Verificatierapport 1 na analyse fase, per veiligheidsfunctie			
VHF nummer			
Verificatie door: Naam/datum			
Item	**Omschrijving**	**Documentatie**	**Akkoord**
Check risicoreductie	Wordt in de risicobeoordeling (of elders) verwezen naar deze veiligheidsfunctie?	RB/SRS	

Target SIL gespecificeerd	Zijn de argumenten voor het bepalen van het benodigde SIL level aanwezig.	SRS	
Omgevingsomstandigheden correct in SRS opgenomen	Zijn de heersende omgevingsomstandigheden in de SRS opgenomen	SRS	
SIL CL	Is met de gekozen architectuur het benodigde SIL niveau haalbaar.	SIL tool	
HFT=0 / DC≥90%	Als een subsysteem niet redundant is (HFT0) mag een DC van meer dan 90% gebruikt worden mits er aanvullende maatregelen zijn getroffen. Zijn in dat geval deze maatregelen gedocumenteerd?	SIL tool	
Omgevingsomstandigheden	Controleer (via datasheets van componenten) of het component bestand is tegen de in SRS omschreven omgevingsomstandigheden. Sensor(en): Logic unit: Actuator(en):		
Compatibiliteit	Controleer (via datasheets van componenten) of de subsystemen onderling compatibel zijn		
Target SIL bereikt	Is het benodigde SIL level van deze veiligheidsfunctie behaald?	SIL tool	

3.7.2.8 Testplan en testen van de veiligheidsfuncties

Alle veiligheidsfuncties moeten getest worden conform een op te stellen testplan. Een testplan moet gebaseerd worden op de toegepaste logic unit (s) en de software architectuur. De omvang en

diepgang van het testplan hangt daarom samen met de complexiteit van het project. De software in het fail-safe deel van de PLC moet volledig (100%) getest worden.

In onderstaande tabel is aangegeven welke onderdelen minimaal in het testplan moeten worden opgenomen:

Gemeente Amsterdam

Testplan functionele veiligheid	
Testplan	Stel het testplan op. Een testplan wordt gebaseerd op de toegepaste logic unit (s) en software architectuur. De omvang en diepgang van het testplan hangt af van de complexiteit van het project. Software in het failsafe deel van een veiligheidsPLC moet volledig (100%) getest worden. Elke veiligheidsfunctie moet volledig (100%) getest worden. **Het testplan betreft alleen functionele veiligheid en is onafhankelijk van FAT/SAT/IAT plannen.** **Het testplan wordt vóór de FAT opgesteld en tijdens FAT al gedeeltelijk ingevuld. Het plan kan pas compleet worden ingevuld tijdens SAT/IAT.** Het testplan zou de volgende inhoud kunnen hebben I/O check: Controleer alle I/O van de failsafe PLC, incusief: • Instellingen van de I/O kaarten (redundantie, equivalent, testpulsen, light/dark test, discrepancy time etc.) • Functionele benamingen (ingang brug op wordt actief als de brug op is) Redundantie en diagnose test: Test alle in en uitgangen: • Laat alle ingangen falen (naar 0 en 24V) en controleer diagnose, meldingen en gedrag van het systeem. • Laat alle uitgangen falen (naar 0 en 24V) en controleer diagnose, meldingen en gedrag van het systeem. • Laat alle componenten falen (zoals plakkende relais)) en controleer diagnose, meldingen en gedrag van het systeem. Functionele test: • Controleer of elke veiligheidsfunctie correct wordt uitgevoerd. • Test alle failsafe software, op een manier die past bij de architectuur • Afstelling, schakelmomenten, montage (degelijkheid) van sensoren • Instelling, montage (degelijkheid) van actuatoren Versiebeheer (signature). Omgevingscondities tijdens test. Aandacht voor de aanwezige bedienvormen.
uitgevoerd dd: Filenaam/namen: Gebruikte tools:	In te vullen door opdrachtnemer

Onder verantwoordelijkheid van: Team samenstelling:	

3.7.2.9 Verificatie na realisatie

De laatste stap in het ontwerptraject van de functionele veiligheid, is het aantonen dat alle veiligheidsfuncties 100% foutloos zijn gerealiseerd. Het validatieplan dat is opgenomen in het FSP van bijlage 3.5.1a berust op het principe waarbij gecontroleerd moet worden of alle voorgaande verificatie- en teststappen grondig zijn uitgevoerd en gedocumenteerd. Pas als geconstateerd en vastgelegd is dat alle benodigde stappen uit het FSP.
Voor de validatie dient per veiligheidsfunctie een verificatie rapport opgesteld te worden zoals aangegeven in onderstaande tabel.

Verificatierapport 2 na realisatiefase, per veiligheidsfunctie			
VHF nummer			
Verificatie door: Naam/datum			
Item	**Omschrijving**	**Documentatie**	**Akkoord**
Naam check	Hebben de componenten in alle relevante documenten, software en tekeningen dezelfde naam? Sensor(en): Logic unit: Actuator(en):		

Schema check	Worden de componenten conform de inbouwhandleiding toegepast? (let bijvoorbeeld op zekeringen) Sensor(en): Logic unit: Actuator(en):		
Testplan	Is de veiligheidsfunctie opgenomen in het testplan? Is (deels in de volgende fase) met het testplan de software inclusief functionaliteit en redundantie volledig te testen?		

3.7.2.10 Modificaties

Alle wijzigingen of modificaties die doorgevoerd worden in de hardware en software nadat de finale testen zijn uitgevoerd dienen vastgelegd te worden in een modificatie protocol. In dit protocol is vastgelegd hoe wijzigen bijgehouden dienen te worden.

In onderstaande tabel is aangegeven hoe de wijzigingen vastgelegd dienen te worden.

Modificaties	
Modificatieprotocol	Omschrijf op welke manier een eventueel noodzakelijke modificatie moet worden uitgevoerd. Verificatie, software en hardware signaturen, wat te testen etc. **Zorg ervoor dat na een wijziging (en dus nieuwe signatuur in de software) het nog steeds aantoonbaar is dat alle software is getest.**

De-commissioning	Omschrijf op welke manier de installatie uit bedrijf genomen kan worden en eventueel welke veiligheidsfuncties dan nog operationeel dienen te blijven.
Uitgevoerd dd: Filenaam/namen: Gebruikte tools: Onder verantwoordelijkheid van: Team samenstelling:	In te vullen door opdrachtnemer

4 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.

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.

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) en door voldoende opgeleid personeel.
De Overbrugging dient hetzelfde veiligheidsniveau (SIL) te hebben als de veiligheidsfunctie die overbrugd wordt.

5 Rectificaties

Controleer altijd of er correcties of aanvullingen zijn op de Specificatie bij de Assetmanager of beheerder van de Standaard Beweegbare Kunstwerken van de Gemeente Amsterdam.

De correcties of aanvullingen dienen altijd meegenomen te worden in het Ontwerp en Realisatie van de nieuwe Bediening, Besturing en Bewakingsinstallatie van het object.

Bijlage A: Template Safety requirements specification

Functionele Specificatie van de veiligheidsfunctie (SRS)	
VHF identificatie: *(nummer)*	
Datum laatste wijziging: Auteur: Team samenstelling: Onder verantwoordelijkheid van:	
Omschrijving van de veiligheidsfunctie	
VHF naam:	
VHF type:	(vergrendeling, bewaking, noodstop enz.)
VHF beschrijving:	
VHF veilige toestand:	
Verwijzing naar het risico dat gereduceerd wordt door de VHF:	
Functionele specificatie van de veiligheidsfunctie	
Vereist SIL of PL niveau van de VHF:	
Stopcategorie volgens EN-IEC 60204-1:	
Verwachte aanspraakfrequentie van de VHF:	
Beschrijving van de toestand van de machine waarin de VHF actief is:	
Beschrijving van de toestand van de machine waarin de VHF NIET actief is:	
Beschrijving van de bedrijfsmodus van de machine waarin de VHF actief is:	
Beschrijving van de bedrijfsmodus van de machine waarin de VHF NIET actief is:	
Is de VHF overbrugbaar	
Prioriteit van de VHF boven andere VHF`s die tegelijkertijd actief kunnen zijn:	
Verwachte omgevingscondities per subsysteem:	Input: Logic: Output:
Vereiste totale responstijd van de VHF:	
Overige relevante specificaties:	

Bijlage B: Template hardware ontwerp (HDS)

Template Hardware Ontwerp (HDS)	
Identificatie VHF:	
Subsysteem:	**Input / sensor**
Type sensor	Fabricaat: Type: Contacten: Faalkansgegevens:
Aantal sensoren	
Functionele beschrijving (inclusief HFT)	
Beschrijving van de aansluitmethode	
Response tijd	
Beschrijving van de faalmechanismen	
Beschrijving van de interne diagnose	*Afhankelijk van de sensor. Een inductieve opnemer zal over het algemeen niet beschikken over enige vorm van interne diagnose, een gecodeerde veiligheidsschakelaar bijvoorbeeld wel. Wanneer diagnose is vereist en de sensor niet beschikt over diagnose zal de CPU de diagnose uit moeten voeren (en andersom).*
Beschrijving van de voorgenomen foutreactie	
Beschrijving van de vereiste testen en testinterval	
Beschrijving CCF	
Maximale technische levensduur	

Subsysteem:	Logic
Logic input kaart	
Type	Fabricaat: Type: Faalkansgegevens:
Type ingang (enkelvoudig, redundant - equivalent/ complementair)	
Discrepancy time (ms)	
Mode ingang (standaard, safe, puls test)	
Response tijd	
Beschrijving van de aansluitmethode	
Beschrijving CCF	
Maximale technische levensduur	
Logic CPU	
Type	Fabricaat: Type: Faalkansgegevens:
Diagnose input subsystem	
Diagnose output subsystem	
Beschrijving van de vereiste testen en testinterval	
Response tijd	
Beschrijving van de voorgenomen foutreactie	
Beschrijving van de aansluitmethode	

Beschrijving CCF	
Maximale technische levensduur	
Beschrijving van de resetfunctie, reset volgorde en locatie(s)	
Beschrijving van de vereiste interfacing met de standaard besturing of ander machines/functies	
Beschrijving van eventuele overbrugging	
Logic output kaart	
Type	Fabricaat: Type: Faalkansgegevens:
Type uitgang (enkelvoudig –redundant	
Mode uitgang (standaard- safe – puls test)	
Response tijd	
Beschrijving van de voorgenomen foutreactie	
Beschrijving van de aansluitmethode	
Beschrijving CCF	
Maximale technische levensduur	

Subsysteem:	Output / actuator
Type	Fabricaat: Type: Faalkansgegevens:
Aantal actuatoren	
Functionele beschrijving (inclusief HFT)	
Beschrijving van de aansluitmethode	
Response tijd	
Beschrijving van de faalmechanismen	
Beschrijving van de interne diagnose	
Beschrijving van de voorgenomen foutreactie	
Beschrijving van de vereiste testen en testinterval	
Beschrijving CCF	
Maximale technische levensduur	