Inhoudsopgave

1. Doel

Het doel van deze instructie is om te beschrijven hoe bij Evonik Antwerpen EMR-beveiligingsinrichtingen tot stand komen, gebouwd en onderhouden worden.

De EMR-beveiligingsinrichtingen die hier besproken worden, zijn een gevolg van procesveiligheidsstudies (PSS) die toegepast worden op Evonik. Aanleunende thema's die reeds geconcludeerd zijn, zullen ook hierin beschreven worden om zo op een ondubbelzinnige wijze steeds dezelfde methode te gebruiken om procesinstallaties te beveiligen met EMR-beveiligingsinrichtingen.

Alle EMR-beveiligingsinrichtingen die gebouwd worden maar die hun oorsprong niet hebben uit een PSS maar uit een andere gehanteerde norm of standaard, regel of wet, dienen gebouwd en behandeld te worden volgens de eisen en voorschriften van dat gehanteerd document.

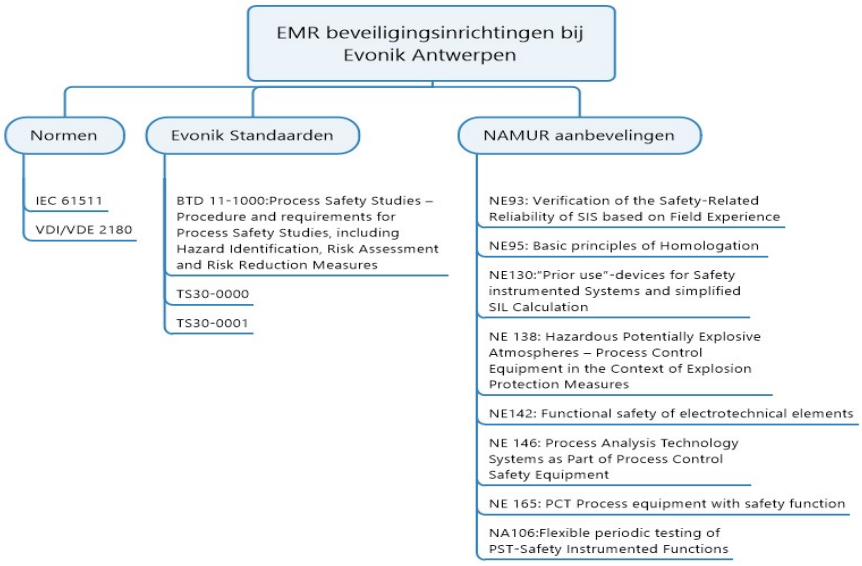
2. Geldingsbereik

Dit document is opgesteld voor de:

- bedrijfsleiding;
- bedrijfsingenieurs;
- EMR-ingenieurs;
- veiligheidsdienst: procesveiligheid;
- projectverantwoordelijken;
- projectmanagers;
- projectingenieurs.

3. Gehanteerde regels, normen en richtlijnen

Er worden verschillende regels, normen en richtlijnen gehanteerd om EMR-inrichtingen correct te gebruiken als onderdeel van de beveiliging van een procesinstallatie. Hieronder worden de voornaamste documenten kort toegelicht.



3.1. IEC 61511

De algemeen gehanteerde standaardnorm voor de functionele veiligheid in de chemische procesindustrie in Europa is IEC 61511. IEC 61511 wordt gebruikt door de eindgebruikers van instrumenten om installaties te beveiligen. De norm IEC 61511 heeft zijn oorsprong uit IEC 61508 “Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE or E/E/PES)”. IEC 61511 is van toepassing op instrumenten en componenten en dus niet gelimiteerd tot E/E/PE.

3.2. VDI/VDE 2180

In de Duitse chemische industrie werd historisch gezien gebruik gemaakt van de norm DIN VDI/VDE 2180. De Duitse norm is geharmoniseerd met de internationale standaard IEC 61511. Het gebruik van beide normen zal tot hetzelfde resultaat leiden.

3.3. Andere normen

In deze geschriften worden links gelegd naar andere normen. Gelieve hier steeds rekening mee te houden.

4. Gehanteerde Evonik-standaarden

4.1. BTD11-1000

De algemeen geldende methode om procesinstallaties te analyseren vanuit het veiligheidsstandpunt wordt bij Evonik uitgevoerd door het volgen van Binding Technical Document BTD11-1000, “Process Safety Studies – Procedure and Requirements for Process Safety Studies, including Hazard Identification, Risk Assessment and Risk Reduction Measures”.

Hieruit volgen categorieën waaraan veiligheidsinrichtingen dienen te voldoen zonder in deze fase al een onderscheid te maken tussen mechanische, elektrische/elektronische of organisatorische maatregelen.

4.2. TS30-0000

Indien er geopteerd wordt voor elektrische/elektronische beveiligingsinrichtingen (EMR-beveiligingsinrichtingen) volgen we de technische standaard TS-30-0000 “Functional Safety by means of PCT”.

4.3. TS30-0001

Bij het bouwen van EMR-beveiligingskringen kan men gebruik maken van gecertificeerde instrumenten of instrumenten waarvan de kwaliteit bewezen is (Prior Use).

Om instrumenten als Prior Use te kwalificeren, dienen deze instrumenten eveneens te voldoen aan verschillende voorwaarden. De weg die afgelegd moet worden om een instrument als bewezen te kunnen beschouwen, staat beschreven in TS30-0001 “Prior Use According to NE130 at Evonik”.

5. Gehanteerde NAMUR-aanbevelingen

Evonik baseert zich vaak op NAMUR-aanbevelingen om praktische omzettingen van normen en wetten te realiseren. Deze zijn ook continu in ontwikkeling.

5.1. NE93: Verification of the Safety-Related Reliability of SIS based on Field Experience

Beschrijft de methodiek om faaldata te verzamelen in actieve installaties en hoe dit invloed heeft op het aantal instrumenten dat noodzakelijk is om een veiligheidskring te bouwen. De verzamelde data zal ons de mogelijkheid geven om de **betrouwbaarheid van instrumenten** te **kwantificeren.**

5.2. NE95: Basic Principles of Homologation

Deze aanbeveling beschrijft de methodiek waarop veldinstrumenten intern onderzocht worden om de kwaliteit te verifiëren.

5.3. NE130: “Prior Use”-Devices for Safety Instrumented Systems and simplified SIL Calculation

Safety Instrumented Systems zouden zo goed als mogelijk vrij moeten zijn van fouten. IEC 61511 vereist de nodige maatregelen tegen systematische, gemeenschappelijke en toevallige fouten. Het gebruik van Prior Use devices is een goede maatregel tegen systematische fouten. Deze aanbeveling beschrijft de methodiek om de **kwaliteit** van **instrumenten** te bepalen.

5.4. NE138: Hazardous Potentially Explosive Atmospheres – Process Control Equipment in the Context of Explosion Protection Measures

Beschrijft de eigenschappen waaraan de EMR-infrastructuur moet voldoen voor beveiligingen m.b.t. explosiebeveiliging.

5.5. NE142: Functional Safety of Electrotechnical Elements

Deze aanbeveling legt uit waarop gelet moet worden bij het gebruik van elektro-componenten in EMR-beveiligingskringen.

5.6. NE146: Process Analysis Technology Systems as Part of Process Control Safety Equipment

Hierin worden de voorwaarden beschreven waaraan analyzers moeten voldoen als ze ingezet worden als een veiligheidsfunctie. Merk op dat de meeste analyzers niet beschikken over faaldata van de instrumenten.

5.7. NE165: PCT Process Equipment with Safety Function

Deze aanbeveling beschrijft de voorwaarden waaraan EMR-infrastructuur moet voldoen als EMR-instrumenten gebruikt worden voor zowel procescontrole als voor procesbeveiliging.

5.8. NA106: Flexible Periodic Testing of PST-Safety Instrumented Functions

Een veiligheidsfunctie gaat niet eeuwig mee in de tijd. De totale faalkans neemt toe in de tijd. Door het uitvoeren van een periodieke test van een veiligheidskring met de juiste kwaliteit, kan de levensduur van een veiligheidsfunctie significant verlengd worden.

Evonik raadpleegt standaard een testfrequentie van iedere 8.760 uren. Bij nood aan afwijking van deze periodiciteit kan NA106 een oplossing bieden.

6. Definities en begrippen

6.1. PSS: Process Safety Studies

PSS staat in dit document voor Process Safety Studies.

6.2. SIL: Safety Integrity Level

Aan EMR-beveiligingsinrichtingen wordt een SIL-cijfer toegekend van 1 t.e.m. 4. Hoe hoger het cijfer, hoe strenger de voorwaarden zullen zijn voor de EMR-beveiligingsinrichtingen. Dit SIL-niveau wordt bepaald in de PSS.

6.3. SIF: Safety Integrity Function

Er worden sensoren en actoren geplaatst om uiteindelijk een actie uit te voeren. Deze actie heeft dan als doel om een bepaald potentieel gevaarlijk scenario af te wenden. Een specifieke actie om een specifiek scenario af te wenden, is een functie.

6.4. SIS: Safety Integrity System

In een installatie zijn verschillende veiligheidsfuncties aanwezig. De meeste functies zijn verbonden met elkaar op een onafhankelijk niveau. Deze onafhankelijke samenhang van SIF's wordt het Safety Integrity System genoemd. Vaak is een centrale Safety Controller de verbindende factor.

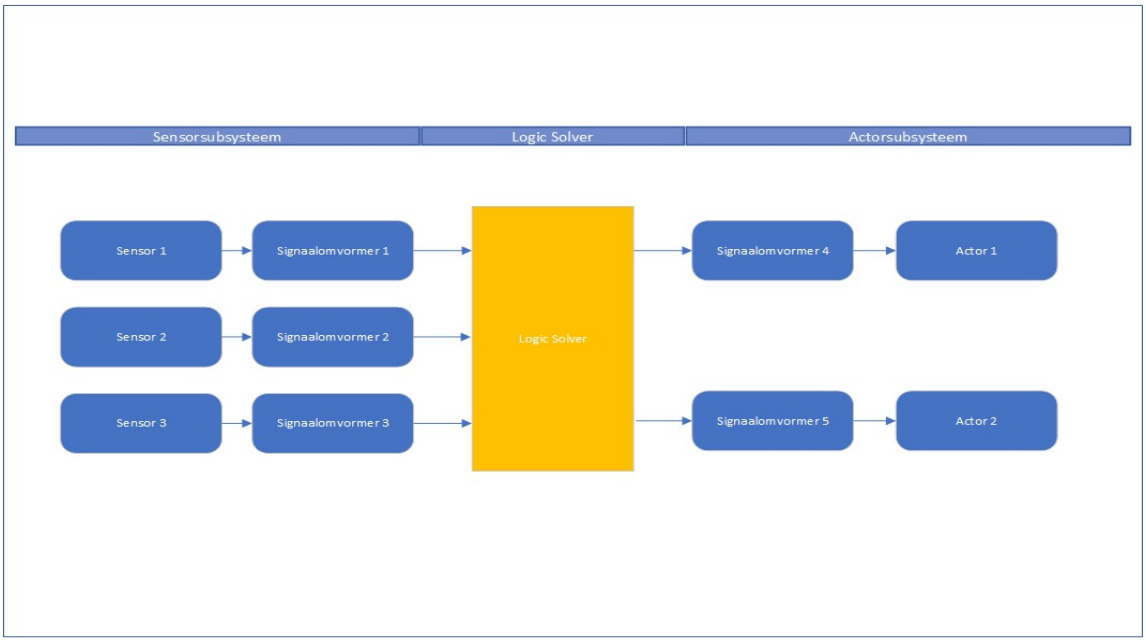
6.5. BPCS: Basic Process Control System

Dit is het DCS of het PLS: het centrale controlesysteem voor het proces. Doordat het SIS gescheiden is van de BPCS zal er een communicatieverbinding opgezet worden tussen deze systemen. Dit heeft als doel om instrumenten van de SIS te kunnen raadplegen op het centrale BPCS; dit om zaken te kunnen opvolgen of om te alarmeren.

6.6. Subsysteem

Een EMR-beveiligingsinrichting bestaat uit subsystemen. Een volledige EMR-beveiligingsinrichting kan je onderverdelen in 3 subsystemen:

- sensorsubsysteem;
- Logic Solver;
- actorsubsysteem.



6.7. HFT: Hardware Fault Tolerance

HFT is een cijfer van 0 t.e.m. 2 dat van belang is bij het ontwerp van de architectuur. Deze ontwerpparameter geeft weer hoeveel toestellen van het subsysteem mogen falen in een onveilige manier, maar dat de goede werking van de veiligheidsfunctie gegarandeerd blijft.

HFT	Betekenis
0	Als er **meer dan 0** instrumenten in een subsysteem onveilig falen, zal de veiligheidsfunctie niet meer werken op het moment van noodzaak.
1	Als er **meer dan 1** instrument in een subsysteem onveilig faalt, zal de veiligheidsfunctie niet meer werken op het moment van noodzaak.
2	Als er **meer dan 2** instrumenten in een subsysteem onveilig falen, zal de veiligheidsfunctie niet meer werken op het moment van noodzaak.

De min. HFT moet voldoen aan tabel 2, 3 van IEC 61508-2 of tabel 6 van IEC 61511.

Zaken die de minimum HFT beïnvloeden, zijn:

- de mode (low/high/continuous) (zie modi van een veiligheidsfunctie);
- het vastgelegde SIL-niveau;
- het gebruik van gecertificeerde instrumenten of Prior Use-instrumenten.

6.8. Modi van een veiligheidsfunctie

De frequentie die men verwacht dat deze functie aanspreekt, heeft invloed op de afwikkeling. Voorafgaande alarmen en schakelpunten hebben een gunstig effect op de Demand Mode.

IEC 61508 definieert 3 modi:

Low Demand Mode	Het afvragen van de veiligheidsfunctie gebeurt ≤1x per jaar.
High Demand Mode	Het afvragen van de veiligheidsfunctie gebeurt >1x per jaar.
Continuous Mode	De veiligheidsfunctie is continu actief om een veilige status te garanderen.

6.8.1. (Low/High) Demand Mode

Dit betekent dat de veiligheidsfunctie geactiveerd wordt bij het onderschrijden/overschrijden van een procesgrootheid. Hierbij is het proces in gevaar als:

- de veiligheidsfunctie gefaald is in een gevaarlijke toestand
- én de veiligheidsfunctie geactiveerd dient te worden.

6.8.2. Continuous Mode

Bij Continuous Mode is het zo dat de veiligheidsfunctie continu actief is om het proces veilig te houden.

Het proces is in gevaar als:

- de veiligheidsfunctie gefaald is in een gevaarlijke toestand.

Denk bijvoorbeeld aan het permanent garanderen van spoelingen of inertisering van een systeem.

6.9. Prior Use-toestellen

Dit is de algemene Engelse benaming voor instrumenten waarvan de kwaliteit bewezen is door het gebruik in procesinstallaties. De typische Duitse benaming is Betriebsbewährte Geräten.

Deze toestellen hebben een hele weg afgelegd om dit label te mogen dragen. Volgens verschillende NAMUR-richtlijnen zijn deze geëvalueerd. Eens deze het label Prior Use meekrijgen, kunnen deze gebruikt worden voor EMR-beveiligingsinrichtingen. Het gebruik van deze Prior Use-toestellen geeft een aantal voordelen. Dit zal verder worden beschreven in deze instructie.

De NAMUR-richtlijnen waaraan de evaluatie van de Prior Use-toestellen voldoet:

- NE93: Verification of the Safety-Related Reliability of SIS based on Field Experience;
- NE95: Basic Principles of Homologation;
- NE130: “Prior Use”-Devices for Safety Instrumented Systems and simplified SIL Calculation.

6.10. PFD: Probability of Failure on Demand

Dit is een gemiddelde waarde die aangeeft wat de kans is dat het toestel of EMR-beveiligingsinrichting faalt op een onveilige manier, op het moment dat het noodzakelijk is. Voor ieder SIL-niveau i.c.m. de Demand Mode zijn er vereisten opgesteld wat de faalkans maximaal mag zijn voor de kring.

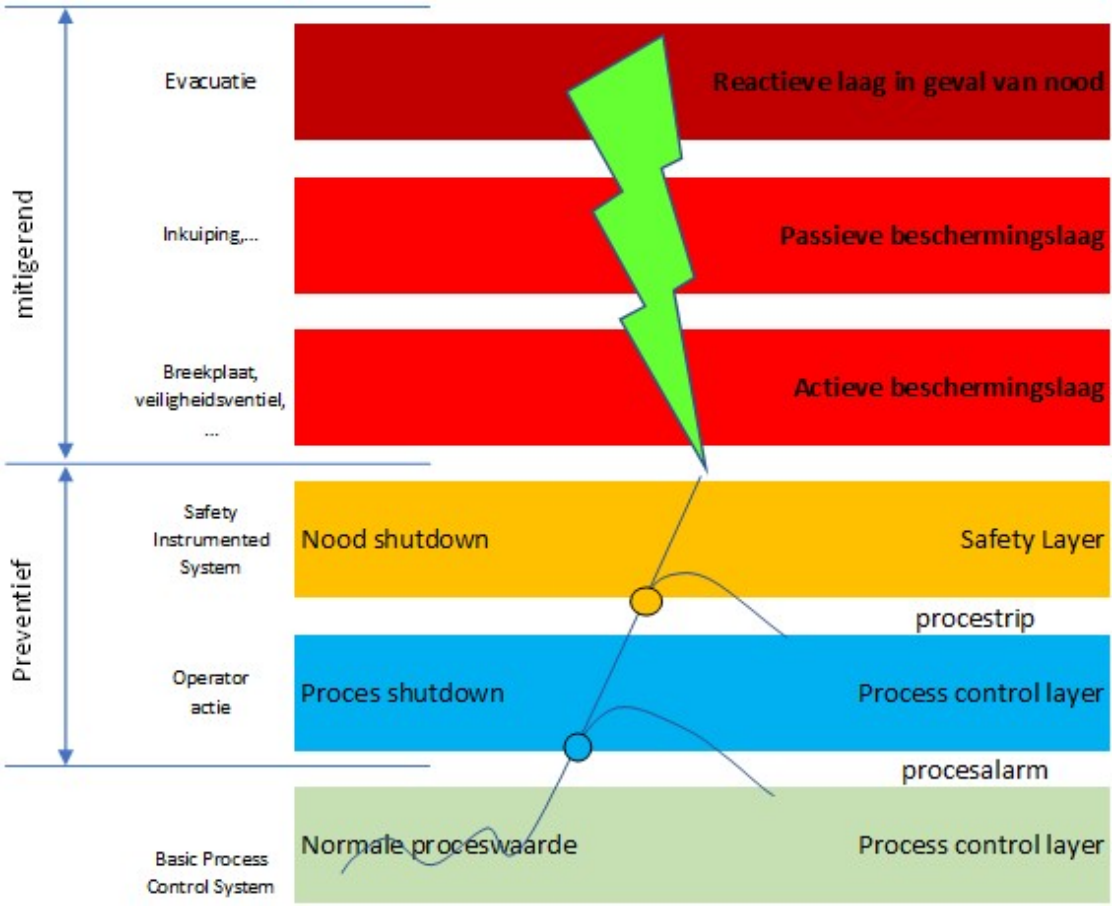
6.11. PTC: Proof Test Coverage

Dit is de kwaliteit van de test met betrekking tot het vinden van alle onveilige falingen van een component.

7. Toepassingsgebied

In hoofdzaak zijn instrumenten voor EMR-beveiligingsinrichtingen ontworpen om te gebruiken in het preventieve bereik. Denk hierbij aan de klassieke niveau-, temperatuurs-, druk- en debietsmetingen samen met de typische afsluiters.

Zij hebben als doel om procesgrootheden waar te nemen en in te grijpen als het proces buiten een normaalbereik komt. Als er op dit punt wordt ingegrepen, zullen de technische grenzen van de installatie niet bereikt worden waardoor er geen gevaarlijke situaties ontstaan.



Tijdens veiligheidsstudies kunnen scenario's naar boven komen waarbij men een beroep wil doen op instrumentele beveiliging maar waar de afdekking in het mitigerende bereik is.

Als men een beroep wil doen op alternatieve meetmethodes of detectie in het mitigerende bereik, kan men ervan uitgaan dat de uitwerking een stuk complexer wordt. Het is eveneens mogelijk dat er geen instrumenten op de markt beschikbaar zijn die voldoen aan alle eigenschappen om deze te mogen gebruiken in een EMR-beveiligingskring volgens de normen die Evonik volgt.

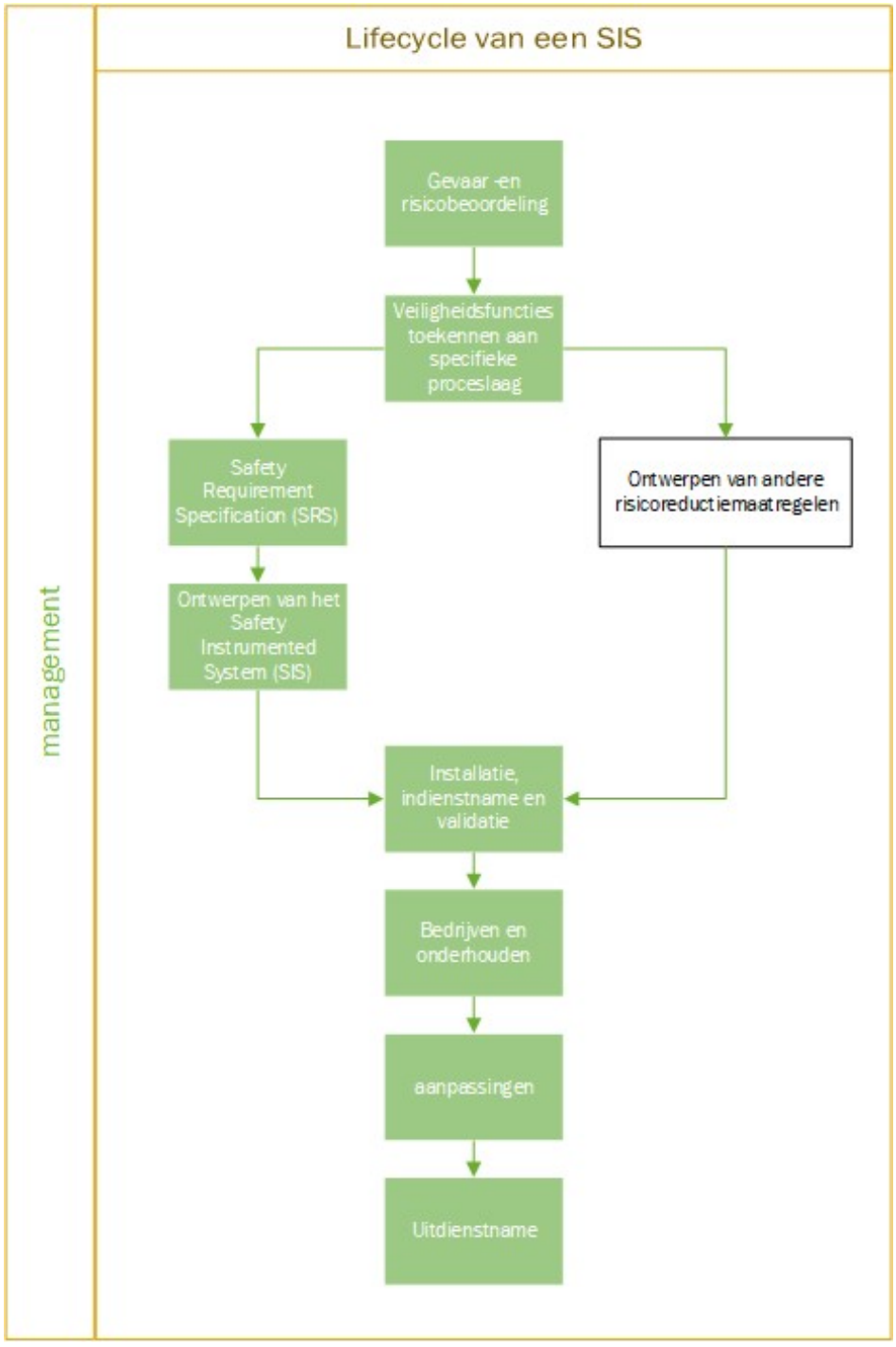
Omwille van deze reden moet men trachten exoten of complexe instrumenten zo weinig mogelijk in te zetten en maximaal gebruik te maken van klassieke detectie in het preventieve bereik. Enkel als er geen alternatief is, kan hiervan afgeweken worden. Dit kan impliceren dat de EMR-ingenieur niet alle noodzakelijke documenten en certificaten kan voorleggen.

Indien de EMR-ingenieur dit vaststelt, dient dit gemeld te worden aan de VOE/PV. De VOE/PV zal de eindbeslissing nemen of men al dan niet met alternatieve instrumenten de procesinstallatie zal beveiligen.

Aanpassingen aan de procesinstallatie zelf dienen ook steeds in overweging genomen te worden. Een inherent veilige installatie is altijd beter dan te meten en te reageren.

Het installeren van EMR-beveiligingsinrichtingen brengt een significante installatie- én onderhoudskost met zich mee.

8. Veiligheidslevenscyclus volgens IEC 61511



Deze levenscyclus is genormeerd en moet volledig doorlopen worden om te kunnen spreken van een volledige EMR-beveiligingsinrichting. Hieronder wordt verder beschreven hoe deze stappen praktisch ingevuld worden om een volledige levenscyclus van de EMR-beveiligingsinrichtingen te doorlopen.

9. Risicobeoordeling

In deze stap worden de gevaren geïdentificeerd en beoordeeld. Bij Evonik wordt de technische standaard BTD11-1000 “Process Safety Studies” (PSS) hiervoor gehanteerd. Het initiatief om deze beoordeling te maken, ligt bij de bedrijfsleiding (VOE) of de projectverantwoordelijke (PV).

9.1. Expertengroep voor PSS

Tijdens de PSS dient een gemengde expertengroep aanwezig te zijn. Een EMR-vertegenwoordiger is hoogst aanbevolen en in de meeste gevallen zelfs vereist om deel te nemen. De aanwezigheid van een EMR-vertegenwoordiger kan in een vroeg stadium reeds technische moeilijkheden voorkomen. Zie BTD11-1000 en de procedure “Risicobeheersing”: VKM / PRO / 016 voor de details over de samenstelling van het expertenteam bij veiligheidsstudies.

9.2. Vastleggen van type beveiliging: EMR-toestellen

Finaal wordt er een risicoklasse bekomen voor elk scenario aangeduid met volgende karakters: A, B, C, D, E1, E2. Van een catastrofaal tot een acceptabel risico.

Deze risicoklasse zegt nog niets over het type van beveiliging maar enkel over de noodzakelijke kwaliteit van de beveiliging.

Op het werkblad van de PSS wordt vervolgens aangegeven welke beveiligingsmaatregelen toegepast zullen worden om het risico af te dekken. Als er gekozen wordt voor instrumentele beveiliging in het bereik van A, B, C of D, dan spreken we over een Z-functie.

Deze keuze resulteert in een SIL-niveau[1]:

Risicoklasse	SIL-niveau
A	SIL 4
B	SIL 3
C	SIL 2
D	SIL 1

9.3. Vastleggen van acties

Tijdens de risicobeoordeling dient per scenario bepaald te worden welke grootheden gemeten dienen te worden en wat de actie dient te zijn om het gevaar af te wenden. Merk op dat een actie zoals “afschakelen installatie” niet voldoende is. Hier moet concreet gerefereerd worden naar leidingen, specifieke plaatsen in het proces of reeds bestaande ventielen.

Houd er rekening mee dat bij het definiëren van meerdere actoren die dienen te schakelen, het moeilijker wordt om het gewenste SIL-niveau te bereiken. Het limiteert eveneens de mogelijkheid om gebruik te maken van vereenvoudigde modellen volgens TS30-0000 en NE93.

[1] Door niet-instrumentele en instrumentele beveiligingen te combineren, kan dit afwijken. Raadpleeg BTD11-1000 voor de exacte classificatie.

Definieer daarom **enkel** de actoren die het scenario afwenden. Bijkomend kunnen er nog andere actoren schakelen, dit buiten beschouwing van de veiligheid maar wel met het oog op productie.

9.4. Vastleggen hulpmiddelen

Vele instrumenten in een procesinstallatie hebben hulpmiddelen nodig om te kunnen functioneren. Om de goede werking van de EMR-beveiligingsinrichting te garanderen, moet het falen van deze hulpmiddelen mee besproken worden. Als het falen van deze hulpmiddelen leidt tot het niet meer functioneren van de EMR-beveiligingsinrichting, dan zal deze hulpinrichting van dezelfde kwaliteit moeten zijn als de EMR-beveiligingsinrichting zelf.

Merk op dat het vaak niet vanzelfsprekend is om deze hulpmiddelen uit te voeren volgens dezelfde SIL-kwaliteit. Tracht daarom hulpmiddelen te vermijden.
Voorbeelden zijn:

- tracing op een drukmeting;
- debietsbewaking naar analyzers;
- stikstofinperreling op niveaumetingen.

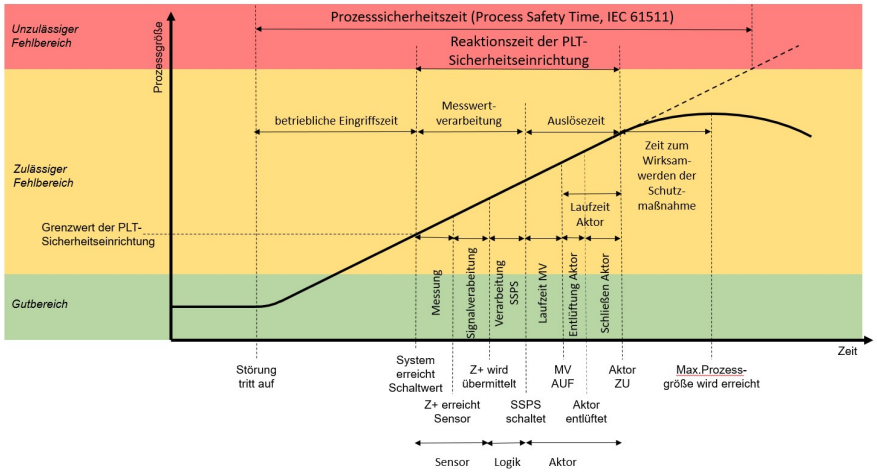
Op de “Fachausschuss EMR Datenbank” is er een werkdocument beschikbaar dat deze discussie kan ondersteunen.

9.5. Reactietijd van een SIF

Alle componenten van EMR-beveiligingsinrichtingen hebben een reactietijd. Bij het aanvangen van een PSS is het belangrijk dat de standaardreactietijden die EMR-E gebruikt, besproken worden. Als er vervolgens geen specifieke wensen aangehaald worden bij de aparte scenario’s, zal EMR-E deze standaardreactietijden hanteren om de EMR-beveiligingsinrichtingen te ontwerpen. Als er wel afwijkende eisen opgegeven worden, dient de EMR-vertegenwoordiger in te schatten of de wens van het bedrijf realistisch is.

9.5.1. Standaardreactietijden

Ideaal zal tussen het bereiken van het ontoelaatbare niveau en het schakelen van de actoren geen tijd zitten. In de realiteit hebben alle onderdelen hun verwerkingstijden waarmee rekening gehouden moet worden.



Standaardreactietijden sensoren

Functie	Reactietijd	Meettolerantie / nauwkeurigheid
F	5 s	3 %
L	5 s	5 %
P	5 s	3 %
T	5 s	3 %

Standaardreactietijd veiligheidssturing

1 s

Standaardreactietijd actoren

DN	Sluitingstijd
15	2 s
25	4 s
40	4 s
50	4 s
65	6 s
80	6 s
100	10 s
125	10 s
150	10 s
200	15 s
250	15 s
300	20 s
350	20 s

Opmerking: Om de totale reactietijd te weten, dienen alle deelreactietijden gecumuleerd te worden. Houd rekening met eventuele tijdsvertragingen. Deze hebben eveneens een nadelig effect op de totale reactietijd.

Indien tijdsvertragende elementen noodzakelijk zijn, dienen deze ook gedefinieerd te zijn.

9.6. Vastleggen Demand Mode

De Demand Mode dient ook bepaald te worden. De PSS is een geschikt moment om dit te doen.

9.7. Overbruggingen

Het implementeren van EMR-beveiligingsinrichtingen kan een significante invloed hebben op de beschikbaarheid van een procesinstallatie. In sommige situaties zal men systematische overbruggingen wensen. Het overbruggen van EMR-beveiligingsinrichtingen zonder gepaste vervangingsmaatregelen is niet toegestaan. Indien men toch systematische overbruggingen wenst, dient men in de PSS de potentiële gevolgen hiervan in kaart te brengen en de nodige acties te definiëren.

Zie ook hoofdstuk Uitdienstneming.

10. Toekenning van de beveiliging aan de juiste beschermingslaag

Volgens de levenscyclus moet in de volgende stap de beveiligingsinrichting toegekend worden aan de juiste beveiligingslaag. Zie toepassingsgebied.

Bij het toepassen van BTD11-1000 zullen de beveiligingsinrichtingen toegekend worden aan de juiste beveiligingslaag en is deze stap afgedekt.

11. Safety Requirement Specification

De EMR-beveiligingsinrichting moet voldoen aan verschillende eisen. Om een goede beveiligingsinrichting te kunnen bouwen, dient er een specificatie opgesteld te worden, zodat de ontwerper van de EMR-veiligheidsinrichting de verwachtingen van de VOE/PV kan invullen.

De SRS dient o.a. informatie te bevatten over:

- het vereiste SIL-niveau;
- de Demand Mode;
- de gewenste architecturen van sensoren en ventielen;
- de maximale responstijd van de veiligheidsfunctie;
- het vastleggen van schakelwaarden;
- speciale overbruggingscondities of opstartvoorwaarden;
- het gewenste testinterval;
- een beknopte maar specifieke beschrijving van de uit te voeren actie.

Evonik maakt de veronderstelling dat deze gegevens besproken worden tijdens de PSS. Indien dit niet gebeurt of onvolledig is, kan de EMR-ingenieur een beroep doen op een SRS-werkblad. Dit werkblad bevat vervolgens alle informatie voor de ontwerper van de EMR-beveiligingsinrichting.

Het wordt sterk aanbevolen om voor iedere nieuwe veiligheidsfunctie een SRS-werkblad in te vullen. Dit zorgt ervoor dat alle noodzakelijke informatie om een correcte veiligheidsfunctie te bouwen, gebundeld is.

12. Ontwerp van de EMR-beveiligingsinrichting

12.1. Inleiding

Nadat de belangrijkste gegevens verzameld zijn, kan er overgegaan worden tot het ontwerpen van de veiligheidsfunctie. Er zijn drie stappen volgens IEC 61511 die overwonnen moeten worden om aan te tonen dat de veiligheidsfunctie aan alle ontwerpcriteria voldoet nl. de architectuur, het valideren van de faalkans en de validatie van de systematische integriteit.

Hieronder wordt verder beschreven welke werkwijze gevolgd kan worden om een volledige EMR-beveiligingsinrichting te bouwen volgens de vooropgestelde normen.

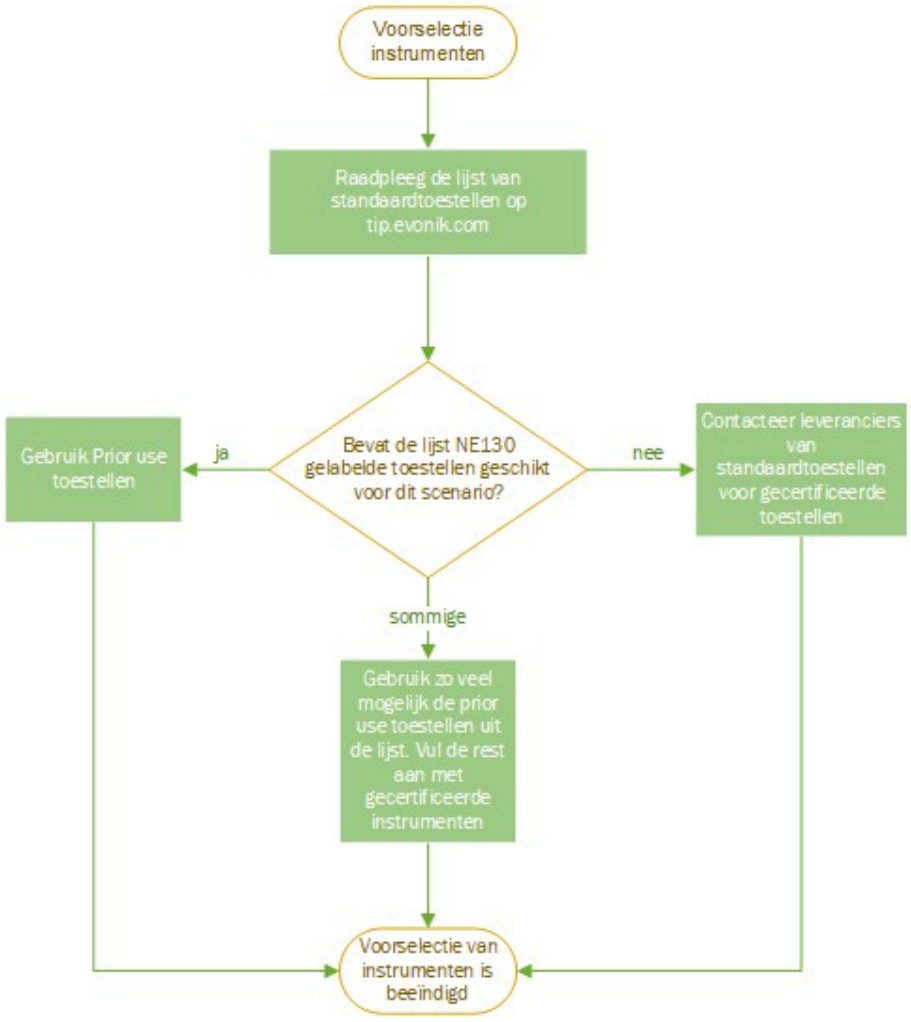
Tijdens het ontwerp moeten ook zaken zoals periodieke testen en overbruggingen uitgewerkt worden.

12.2. Voorselectie instrumenten van subsystemen

12.2.1. Veldinstrumenten en signaalomvormers

Op dit moment kan een eerste keuze gemaakt worden van de gewenste veldinstrumenten en eventuele signaalomvormers waarmee we de sensor- en actorsubsystemen gaan bouwen.

De geprefereerde instrumenten van Evonik zijn opgenomen in de “Standardgeräteliste”. De toestellen die gemarkeerd zijn in de kolom “NE130” zijn “Prior Use”-toestellen en dus de geprefereerde instrumenten om te gebruiken in EMR-beveiligingskringen. Het overzicht is terug te vinden op de centrale databank van Evonik, TIP-Portal https://tip.evonik.com/.



Het gebruik van gecertificeerde instrumenten maakt de verdere afwikkeling van het ontwerp complexer. Tracht kringen volledig met Prior Use-toestellen te ontwerpen.

Na het uitwerken van de volgende stappen zal blijken of de gekozen instrumenten geschikt zijn voor de gedefinieerde specificaties.

12.2.2. Logic Solver

Als er een controller gebruikt wordt voor de logische verwerking, dient deze te voldoen aan de norm IEC 61508.

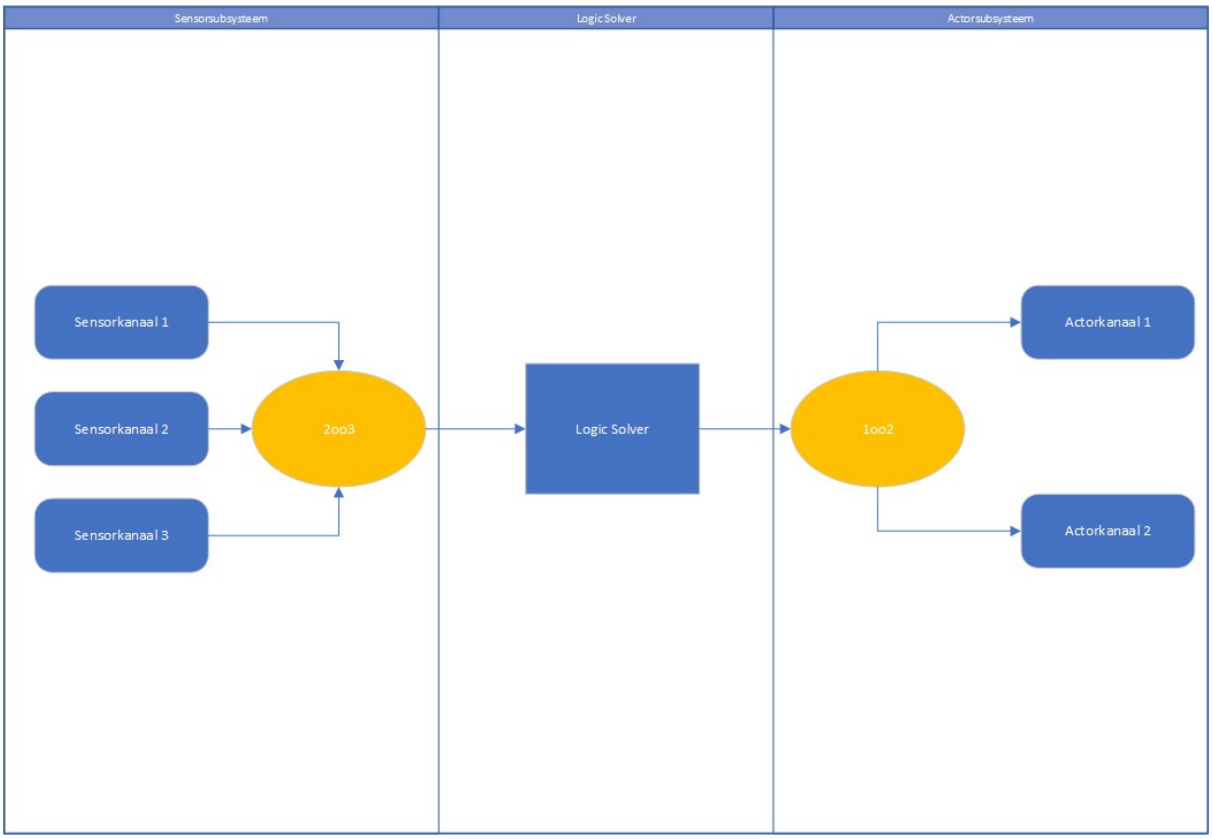
12.3. Architectuur

Een architectuur wordt vastgelegd voor de sensor- en actorsubsystemen van de EMR-beveiligingskring. De architectuur geeft weer hoeveel veldtoestellen geïnstalleerd zijn én welke samenhang deze hebben m.b.t. de veiligheidsfunctie.

Er zijn bepaalde vrijheden maar ook bepaalde vereisten aan een architectuur.

De architectuur van een subsysteem wordt uitgedrukt in MooN (M out of N) waarbij M het minimumaantal elementen aangeeft die de veiligheidsfunctie activeren en N voor het totale aantal elementen staat. In annex 2 is a.d.h.v. voorbeelden het begrip MooN verder uitgelegd.

Een schematische voorstelling van een complete EMR-beveiligingskring met de architectuur voor de sensor- en actorsubsystemen is hieronder afgebeeld.

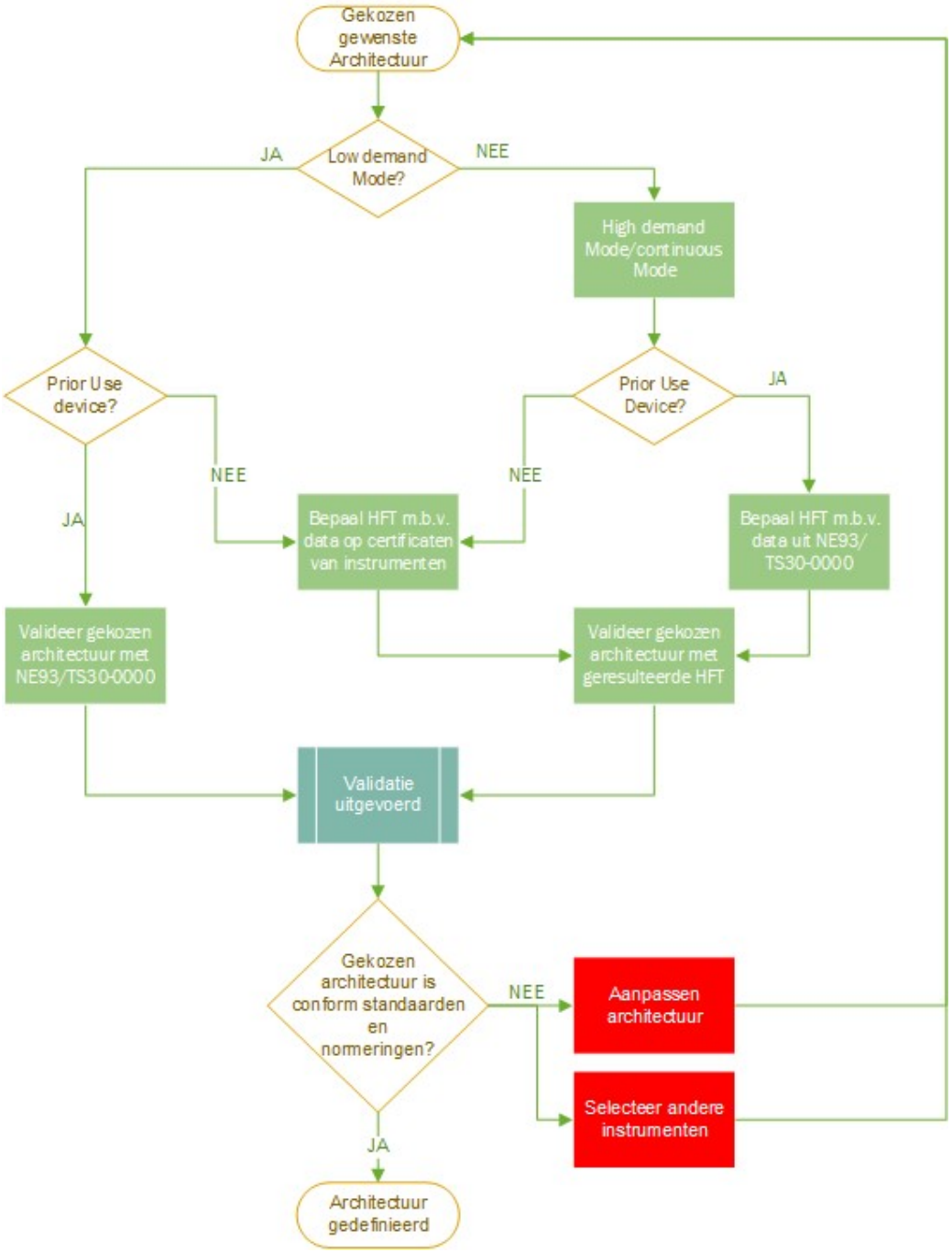


De architecturen moeten een weloverwogen keuze zijn tussen beschikbaarheid en betrouwbaarheid. De wens vanuit productiestandpunt is om een zo hoog mogelijke beschikbaarheid van de installatie te hebben. Dit kan verwezenlijkt worden door parallelle instrumenten te plaatsen. Dit heeft dan weer een nadelige invloed op de betrouwbaarheid van de veiligheidsfunctie.

Volgende factoren hebben een invloed op de toegestane architecturen:

- de Demand Mode;
- het opgegeven SIL-niveau;
- het gebruik van Prior Use of gecertificeerde toestellen.

Hanteer onderstaande flowchart om de architectuur van de SIF vast te leggen.



Merk op dat bij gebruik van Prior Use-toestellen i.c.m. de Low Demand Mode de afloop eenvoudig is.

Bij afwijking hiervan volgt een complexere weg om de architectuur te bepalen. Als men in een situatie komt waar de modus High Demand of Continuous is óf er worden gecertificeerde toestellen gebruikt, dan dient men de ontwerpparameter HFT te bepalen. Het bepalen van de HFT-parameter wordt beschreven in annex 4. Enkele voorbeelden en uitleg van HFT is terug te vinden in annex 5.

12.3.1. Standaardarchitecturen voor Low Demand Mode en Prior Use-toestellen

In het geval van de Low Demand Mode i.c.m. Prior Use-toestellen is het aangewezen om de standaardarchitecturen uit NE93 of TS30-0000 v.a. editie 3 te gebruiken. Dit vereenvoudigt in eerste instantie de verificatie van de architectuur. In tweede instantie zal de latere toetsing van de faalkans van de kring sterk vereenvoudigd worden. Zie hoofdstuk kwantificeren van willekeurige falingen.

In onderstaande tabel is de samenhang van de architectuur en het SIL-niveau volgens NE93 voorgesteld.

Structure		Actuator sub-system	
		1oo1	1oo2
Sensor sub-system	1oo1	SIL 2	SIL 2
	1oo2	SIL 2	SIL 3
	2oo3	SIL 2	SIL 3

Daar de technische standard TS30-0000 v.a. editie 3 een antwoord tracht te bieden op meer combinaties, is het belangrijk om in de verificatiedocumenten aan te geven op welke van de twee opties het ontwerp gebaseerd is.

12.3.2. Architecturen voor High Demand en Continuous

Voor het vastleggen van de architectuur in deze modi dient de factor HFT bepaald te worden. Het vastleggen van de HFT kan eenvoudig zijn in geval van Prior Use devices. Als er gebruik gemaakt wordt van gecertificeerde toestellen is het bepalen van de HFT uitgebreider. Dit is volledig beschreven in annex 4.

12.3.3. Architecturen bij gecombineerd gebruik van Prior Use-toestellen en gecertificeerde toestellen

Er kan geen beroep gedaan worden op de standaardarchitecturen. Voor de bepaling van HFT wordt verwezen naar annex 4.

12.4. Kwantificeren van willekeurige falingen

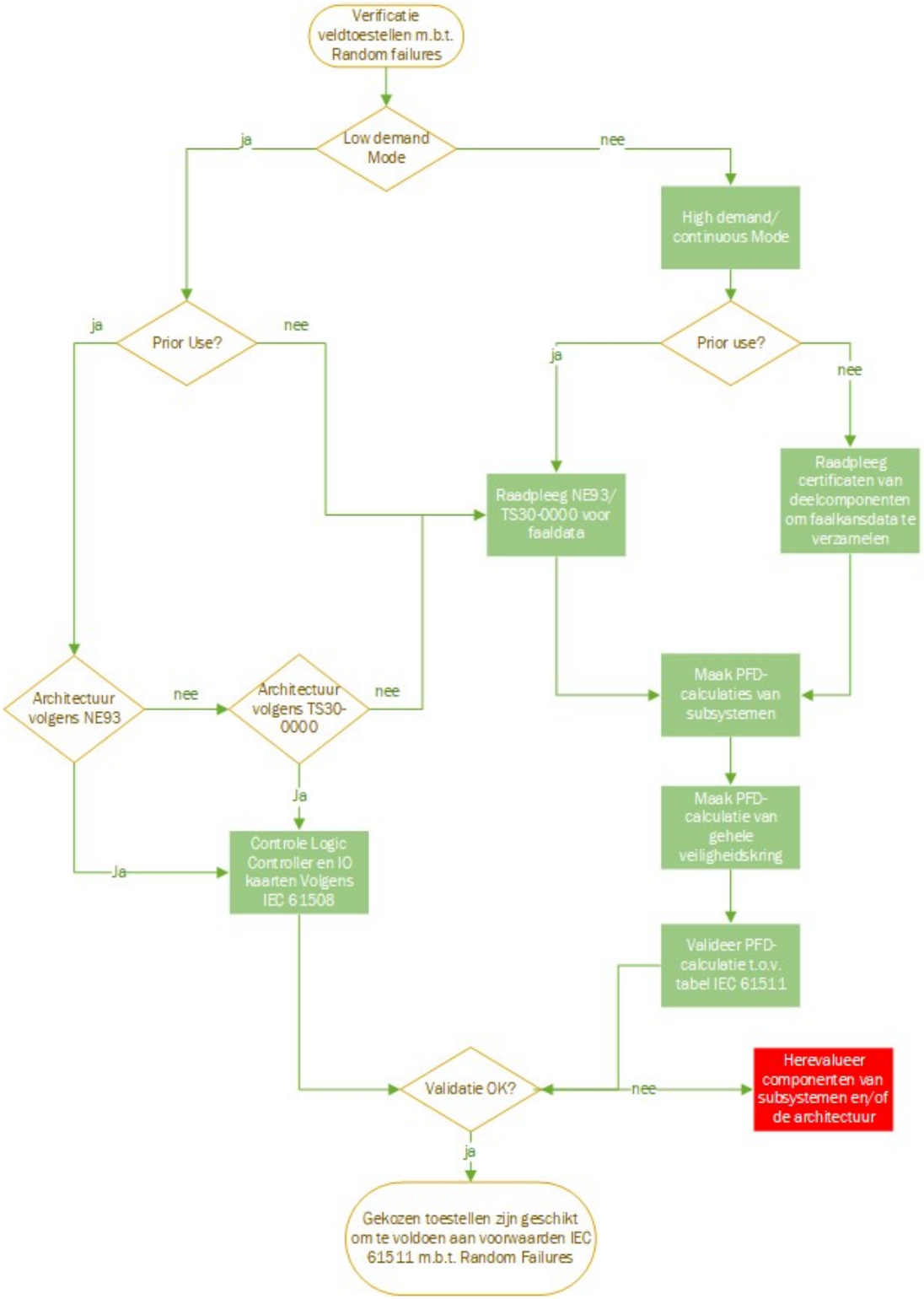
Naast het bepalen van de architectuur moet er afgetoetst worden of de totale faalkans van de EMR-beveiligingsinrichting voldoet aan de eisen van het vooropgestelde SIL-niveau.

Een belangrijke factor bij het bepalen van de vereiste PFD-waarde is wederom de “Demand Mode”. In de meeste gevallen zullen onze veiligheidsfuncties dienen voor “Low Demand Mode”-applicaties. Indien er sprake is van de High Demand of Continuous Mode zullen de faalkansen significant kleiner moeten zijn. Zie onderstaande tabellen.

Low Demand Mode		
SIL-niveau	PFD_{avg}	Vereiste Risicoreductie
4	$\geq 10^{-5}$ tot $\leq 10^{-4}$	>10 000 tot ≤100 000
3	$\geq 10^{-4}$ tot $\leq 10^{-3}$	>1 000 tot ≤10 000
2	$\geq 10^{-3}$ tot $\leq 10^{-2}$	>100 tot ≤1 000
1	$\geq 10^{-2}$ tot $\leq 10^{-1}$	>10 tot ≤100

High Demand Mode – Continuous Mode	
SIL-niveau	PFD_{avg}
4	$\geq 10^{-9}$ tot $\leq 10^{-8}$
3	$\geq 10^{-8}$ tot $\leq 10^{-7}$
2	$\geq 10^{-7}$ tot $\leq 10^{-6}$
1	$\geq 10^{-6}$ tot $\leq 10^{-5}$

Om de juiste werkwijze te bepalen om Random Failures te kwantificeren, kan onderstaande afloop gehanteerd worden.



12.4.1. Kwantificeren van Random Failures bij Low Demand Mode

12.4.1.1. Prior Use-toestellen

Bij het gebruik van Prior Use devices dient er verder geen berekening gemaakt te worden bij de standaard grootheden debiet, niveau, druk en temperatuur als:

- de gebruikte sturing volgens IEC 61508 ontwikkeld is;
- er een standaard architectuur gebruikt wordt volgens NE93 of TS30-0000 ed. 3.

Bij het gebruik van “Prior Use”-toestellen in de “Low Demand Mode” eindigt hier de validatie van de faalkans.

12.4.1.2. Gecertificeerde toestellen

In deze situatie kunnen we geen beroep doen op typicals die uitgewerkt zijn in technische standaards of werkdocumenten. Hier zal de totale faalkans van de EMR-beveiligingskring berekend moeten worden. Raadpleeg annex 3.

12.4.2. Kwantificeren van Random Failures bij High Demand/Continuous Mode

Bij deze modi kunnen we geen beroep doen op typicals die uitgewerkt zijn in technische standaards of werkdocumenten. Hier zal de totale faalkans van de EMR-beveiligingskring berekend moeten worden. Raadpleeg annex 3.

12.4.3. Kwantificeren van Random Failures bij gecombineerd gebruik van Prior Use en gecertificeerde toestellen

Het kan zich voordoen dat een bepaalde toepassing een sensor of actor vereist die niet in de Prior Use-lijst staat. Het is mogelijk om voor deze component de certificaten te hanteren. Als de andere deelcomponenten wel deel uitmaken van de Prior Use-lijst, kunnen de faalkansen volgens NE93 gehanteerd worden.

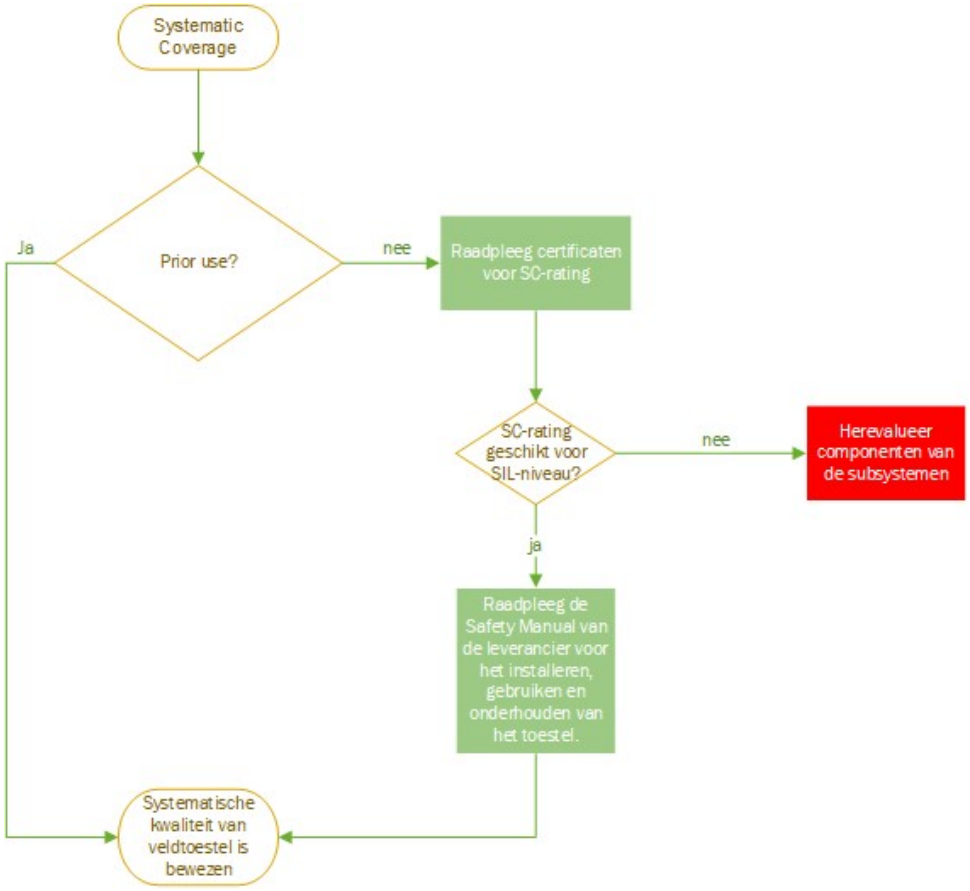
Eveneens zullen we geen beroep kunnen doen op de typicals van technische standaards of werkdocumenten. Hier zal de totale faalkans van de EMR-beveiligingskring berekend moeten worden. Raadpleeg annex 3.

12.5. Afwenden van systematische fouten

Om systematische fouten maximaal te vermijden, zijn er twee zaken die behandeld moeten worden:

a) Good engineering: Systematische fouten zijn vaak gerelateerd aan engineeringsfouten of de mogelijkheid dat men door manuele handelingen de integriteit van een veiligheidsfunctie ondermijnt.
   Zaken die extra aandacht vergen:
   - ingezette materialen voor chemische bestendigheid;
   - inbouwvoorschriften veldtoestellen van de leverancier;
   - gebruik van extra uitrusting bij een veldtoestel. bv. handafsluiters;
   - procedure voor de uitvoering van kalibraties;
   - software-instellingen van veldtoestellen bv. testmode uitgeschakeld.

b) Systematic Coverage volgens IEC 61511: De norm verplicht ons ertoe om aan te tonen dat de instrumenten voldoende geschikt zijn voor de applicatie waarin we ze gaan gebruiken.



12.5.1. Systematische geschiktheid van Prior Use-toestellen

Als de gebruikte veldtoestellen in de Prior Use-lijst staan, is hun systematische geschiktheid bepaald a.d.h.v. NE130 toe te passen.

12.5.2. Systematische geschiktheid bij gecertificeerde toestellen

Op de certificaten zal een SC-rating vermeld staan. SC staat voor Systematic Capability. Het cijfer gekoppeld aan de SC-rating geeft weer voor welk SIL-niveau dit toestel geschikt is als de voorschriften van de veiligheidshandleiding en de installatiehandleiding correct gevolgd worden.

12.6. Opstellen van testplan

Het opstellen van een testplan dient in de ontwerpfase te gebeuren.

EMR-beveiligingsinrichtingen dienen periodiek getest te worden en dit omwille van twee redenen:

- het vaststellen van passieve fouten (λ_{du}) van veldtoestellen;
- de levensduur van een EMR-beveiligingsinrichting te optimaliseren.

12.6.1. Testen van EMR-beveiligingskringen uitsluitend bestaande uit Prior Use-toestellen

Bij het gebruik van Prior Use-toestellen wordt er uitgegaan van een testfrequentie van 1 jaar (8.760 h).

De methode van testen moet zodanig zijn dat de sensor maximaal getest wordt. De berekeningen van NE130 veronderstellen dat na het testen een veldtoestel weer de kwaliteit van een nieuw toestel heeft. Dit is in de praktijk nooit zo!

Om dit te benaderen, dienen de testen maximaal uitgevoerd te worden.

Gebruik voor nieuw te implementeren Z-kringen *EMR / FORM / 0545* als standaard sjabloon voor het opstellen van een procedure voor de periodieke test. Zie bijlage 7.

Bij het opstellen van periodieke testformulieren dien je rekening te houden met volgende zaken:

- 4…20mA-controle is niet toegelaten als periodieke test van een EMR-beveiligingsinrichting. Dit is een looptest.
- Een weerstandsimulator aan een transmitter koppelen om een temperatuurkring te controleren, is onvoldoende. Ook de temperatuursensor zelf dient gecontroleerd te worden.
- Bij het gebruik van testknoppen van een levelswitch controleer je de kwaliteit in de “safety manual” van de fabrikant of leverancier. De PTC van de test moet min. 90 % bedragen.
- Debietsmetingen dienen geverifieerd te worden met referentiemetingen. Raadpleeg eveneens de safety manual van deze instrumenten.
- Afsluiters die als lekdicht gedefinieerd zijn, dienen uitgebouwd te worden en getest op een testbank. Een open/toe-verificatie is onvoldoende.

12.6.2. Testen van EMR-beveiligingskringen gebaseerd op faalkansberekening

Als de stap “kwantificeren van random falingen” gedaan is a.d.h.v. een berekening, is het mogelijk om in diezelfde berekening de factoren “testfrequentie” en “testkwaliteit” op te nemen. Er zijn meer mogelijkheden om af te wijken van de jaarlijkse testfrequentie en testmethode.

Aangezien dit voor extra complexiteit zorgt, mag dit enkel toegepast worden in uitzonderlijke situaties. Bij uitzonderlijke situaties verstaan we dat het jaarlijks testen van deze inrichtingen een zodanige impact heeft op de beschikbaarheid van de installatie (langere stilstand) of extra veiligheidsrisico’s teweegbrengt bv. betreden van gesloten ruimtes, ...

Variabel testen vereist ook extra investeringen in infrastructuur. Vaak zal dit afgedekt worden door elektronische systemen die met behulp van diagnose de kwaliteit van de instrumenten bepalen. Bij afwijking van de jaarlijkse testperiode of maximale testkwaliteit refereren we naar NA106.

In annex 6 wordt er dieper ingegaan op het nut van kwalitatieve en periodieke testen.

12.6.3. Testen van Safety Controllers

De meeste EMR-beveiligingsinrichtingen worden aangesloten op een safety controller. Deze safety controllers dienen onderhouden en getest te worden volgens de voorschriften van de leverancier of fabrikant om te voldoen aan de normen.

12.7. Herstellingen

In het ontwerp dient rekening gehouden te worden met eventuele herstellingen van EMR-beveiligingsinrichtingen.

In de meeste gevallen zal bij detectie van een faling van een toestel de veiligheidsactie meteen geactiveerd worden.

In de modellen van faalkansen wordt de hersteltijd (MTTR) in geval van een defect als zeer kort beschouwd t.o.v. de totale levensduur. Dit geeft de mogelijkheid om technische hulpmiddelen in te schakelen om de procesinstallatie niet te sterk te verstoren in geval van een vastgesteld defect:

- Er dient een diagnosesysteem geactiveerd te worden dat vaststelt dat het toestel defect is.
- Bij het vaststellen van een defect wordt een timer gestart (bv. 8 h).
- Binnen deze vooropgestelde tijd dient de daaropvolgende actie uitgevoerd te zijn, anders zal de veiligheidsactie uitgevoerd worden.

Opmerking: Deze functie mag niet gebruikt worden om EMR-beveiligingsinrichtingen te overbruggen om procesacties uit te voeren. Omgaan met overbruggingen wordt besproken in hoofdstuk Uitdienstneming.

12.8. Programmatie

In de meeste gevallen zal een safety controller via een logische functie in het geheugen de veiligheidsactie uitvoeren. Niet elke programmeerbare logica is geschikt voor EMR-beveiligingsinrichtingen. Deze controllers moeten IEC 61508 gecertificeerd zijn om gebruikt te mogen worden in EMR-beveiligingskringen.
Bij het gebruik van controllers is het belangrijk dat de veiligheidsvoorschriften en voorwaarden van de fabrikant in acht genomen worden.

12.8.1. Overbruggingen

Indien overbruggingen gedefinieerd zijn in de PSS of SRS dienen deze geïmplementeerd te worden in de sturing. Overbruggingen mogen nooit geactiveerd kunnen worden vanuit het BPCS en dienen direct in de veiligheidssturing in te grijpen.

Zie hoofdstuk Uitdienstneming voor meer informatie over tijdelijke uitdienstneming van een EMR-beveiligingsinrichting.

12.8.2. Diagnosesystemen

Als diagnosesystemen verwacht worden om bv. het aantal instrumenten te reduceren of om onmiddellijke plant trips te voorkomen, dan kunnen deze geprogrammeerd worden in de sturing. De voorwaarden van deze systemen zijn terug te vinden in TS30-0000 v.a. editie 3.

12.8.3. Uitwerking programmatie

12.8.3.1. Functieplannen

Voor EMR-beveiligingskringen dienen er functieplannen opgesteld te worden. Deze dienen goedgekeurd te worden door de VOE/PV. Dit is niet anders dan bij gewone EMR-kringen die geprogrammeerd worden.

12.8.3.2. Aanpassingen logica

Merk op dat de aanbevelingen en voorwaarden van de fabrikant in acht genomen worden. Denk hierbij aan het gebruik van gecertificeerde blokken, genereren van logs, genereren van codes, …

12.9. Bedradings- en aansluitschema's

De volgende stap bij het ontwerp is het genereren van de bedradings- en aansluitschema's. Dit is niet anders dan de gewone elektrische schema's die gekend zijn, maar er dienen wel extra punten in acht genomen te worden:

- Beschikbaarheid van hulpenergieën bv. stuurlucht en elektrische energie: zorg dat deze voldoende beschikbaar zijn voor de garantie van de goede werking. Bij het wegvallen van hulpenergie dient de veilige stand gewaarborgd te zijn.
- Direct aansluiten van veldtoestellen op de controller: zet geen scheidingskaarten of signaalontkoppelingen in de kringen als dit niet nodig is. Indien van toepassing dienen deze eveneens te voldoen aan alle eisen van het SIL-niveau.
- Raadpleeg de installatiehandleiding van de fabrikant om te voldoen aan alle voorschriften voor de garantie van een goede werking.

12.10. Montageplan

- Maak een montageplan, zodat de installateur ondubbelzinnig de EMR-instrumenten kan installeren.

13. Installatie van een EMR-beveiligingsinrichting en verificatie

13.1. Montage van instrumenten voor EMR-beveiligingsfuncties en verificatie

Als het montageplan volledig klaar is, kan de mechanische en elektrische installatie van de EMR-beveiligingskring uitgevoerd worden.

Om zeker te stellen dat de minimumvereisten van de montage gewaarborgd zijn, dient voor ieder geïnstalleerd veldtoestel de controlelijst *EMR / FORM / 0548 deel 1* voor montage en configuratie ingevuld te worden. Zie bijlage 2.

13.2. Configuratie van instrumenten voor EMR-beveiligingsinrichtingen en verificatie

De meeste veldtoestellen zijn uitgerust met de nodige elektronica waar verschillende parameters ingesteld kunnen worden. Bij EMR-beveiligingsinrichtingen zijn deze instellingen van groot belang voor de veiligheid.

Ook bij het gebruik van Prior Use-toestellen is het belangrijk om de procesparameters te vergrendelen als deze mogelijkheid bestaat. Vergrendeling gebeurt in de meeste gevallen a.d.h.v. een hardware-switch of een wachtwoordinstelling.

Bij het gebruik van gecertificeerde toestellen dient de safety manual geraadpleegd te worden om de instrumenten te mogen gebruiken in EMR-beveiligingskringen.

Extra aandachtspunt bij veldtoestellen voor Z-functies zijn de reacties in geval van storingen (minimum/maximum uitsturing, veiligheidsstand van afsluiters, …).

Om zeker te stellen dat de minimumvereisten van de configuratie gewaarborgd zijn, dient voor ieder geïnstalleerd veldtoestel de controlelijst *EMR / FORM / 0548 deel 2* voor montage en configuratie ingevuld te worden. Zie bijlage 2.

13.3. Programmatie en verificatie

In de meeste gevallen zal een safety controller ervoor zorgen dat een logische functie uitgevoerd wordt. Het nieuwe programma kan in de veiligheidssturing geladen worden. De logica dient eveneens geverifieerd te worden. Als bij de indienstneming een volledige kop-staarttest uitgevoerd wordt, zal op deze wijze de logische afwikkeling geverifieerd worden.

Wanneer er geen kop-staarttest uitgevoerd wordt tijdens de indienstneming, dient de logica separaat gecontroleerd te worden door een onafhankelijke partij, hetzij een ervaren collega, hetzij de leverancier van de controller, hetzij TAS of andere. In dit geval is er geen standaard Evonik Antwerpen-document beschikbaar en dient de ontwerper van de EMR-beveiligingsinrichting documenten op te stellen om de verificatie uit te voeren. Functieplannen kunnen een goede basis vormen voor de verificatie van de logica.

14. Indienstneming van een EMR-beveiligingsinrichting en verificatie

14.1. Indienstneming

Voor elke nieuwe EMR-beveiligingskring dient een indienstneming te gebeuren. Dit wil zeggen dat de volledige en goede functionaliteit van de kring wordt getest.

Gebruik *EMR / FORM / 0543* (bijlage 5) om de verificatie van de functionaliteit van een EMR-beveiligingsinrichting te registreren. Beschrijf de te volgen procedure om de veiligheidskring te testen.

Indien het praktisch onmogelijk is om een volledige kop-staarttest te doen, dienen de nodige documenten opgesteld te worden om elk subsysteem te testen. Gebruik eveneens *EMR / FORM / 0543* (bijlage 5) om de verificatie van de sensor- en actordeelsystemen te registreren. In dit geval is er nog een bijkomend verificatieverslag van de logica nodig om de volledige verificatie van de indienstneming te documenteren.

15. Bedrijven en onderhouden van EMR-beveiligingsinrichtingen

EMR-beveiligingsinrichtingen zijn onafhankelijke inrichtingen die als primaire functie hebben om de veiligheid van een procesinstallatie te verhogen. Vaak worden deze componenten beschikbaar gesteld om het proces te monitoren. Het gemak van deze instrumenten kan soms leiden tot een verzoek om manipulaties te doen in het voordeel van de productie.

Manipulaties aan deze inrichtingen tijdens actieve productie zijn niet toegelaten zonder bijkomende analyses en maatregelen.

Voor het correct gebruik en onderhoud van componenten dient men ook steeds de gebruikshandleiding van de fabrikant te raadplegen.

15.1. Periodiek testen

De periodieke testen moeten ingepland worden door de verantwoordelijke partijen voor het onderhoud van de procesinstallatie. Zij dienen voldoende tijd te voorzien om kwalitatieve testen uit te kunnen voeren. Het testplan wordt in de ontwerpfase uitgewerkt. Gebruik hiervoor voor nieuw te implementeren Z-kringen document *EMR / FORM / 0545,* zie bijlage 7. Hierin worden de factoren “testmethode” en “frequentie” uitgewerkt.

15.2. Herstellingen

Zorg dat alle veiligheidsmaatregelen gerespecteerd zijn bij het herstellen van EMR-beveiligingsinrichtingen.

16. Aanpassingen

Wijzigingen aan EMR-beveiligingsinrichtingen hebben steeds een grote impact. Wijzigingen mogen slechts uitgevoerd worden als er een veiligheidsstudie aan voorafgegaan is.

Bij wijzigingen dienen alle bestaande documenten gecontroleerd te worden of ze nog actueel zijn. Zo niet, dienen ze vernieuwd te worden.

17. Uitdienstneming

Een uitdienstneming kan van tijdelijke of permanente aard zijn.

17.1. Permanente uitdienstneming

Als een uitdienstneming van een EMR-beveiligingsinrichting van permanente aard is, dient er steeds een veiligheidsstudie aan vooraf te gaan.

17.2. Tijdelijke uitdienstneming

Tijdelijke uitdienstnemingen kunnen zich soms opdringen om bijvoorbeeld een defect toestel te vervangen of om een periodieke reiniging uit te voeren.

Het is niet toegelaten om een EMR-beveiligingsinrichting tijdelijk te overbruggen of de installatie te bedrijven zonder gepaste vervangingsmaatregelen. Deze maatregelen dienen dezelfde kwaliteit te hebben van de desbetreffende EMR-beveiligingsinrichting.

17.2.1. Standaardmethode

Wanneer een EMR-beveiligingsinrichting tijdelijk (gedeeltelijk of volledig) uit dienst genomen moet worden, dient het formulier *EMR / FORM / 0547 “Uit- en herindienstnemingsformulier”* ingevuld te worden. Zie bijlage 9.

Het is belangrijk dat er een vervangingsmaatregel opgegeven wordt die dezelfde betrouwbaarheid heeft dan de EMR-veiligheidsfunctie.

De verantwoordelijkheid om een EMR-beveiligingsinrichting uit dienst te nemen en de installatie verder te bedrijven, ligt bij de VOE/PV.

17.2.2. Alternatieve methode

Als overbruggingen regelmatig uitgevoerd moeten worden, kan het productiebedrijf zelf een procedure opstellen. Er kunnen dan (sleutel)schakelaars geïnstalleerd worden die rechtstreeks op de veiligheidssturing de EMR-beveiligingsinrichting overbruggen. Bij het gebruik van een schakelaar wordt automatisch de bedrijfsprocedure in werking gesteld. Het formulier “Uit- en herindienstnemingsformulier” dient dan niet ingevuld te worden.

Het activeren van een overbrugging met een schakelaar kan dan eventueel in de tijd beperkt worden door gebruik van een timer.

Gebruik bij voorkeur sleutelschakelaars.

18. Documentatie

Iedere stap van de levenscyclus dient gedocumenteerd te worden. Voor het ontwerp, de installatie en de indienstneming wordt er extra aandacht gevestigd op de verificatie en validatie. Verificatie betekent dat iets gecontroleerd wordt op gedefinieerde parameters of specificaties. De validatie is dan de bijkomende controle dat deze verificatie uitgevoerd is.

18.1. Risicobeoordeling en toekenning van beveiliging aan de beschermingslaag

De gevaren- en risicobeoordeling en toekenning worden gedocumenteerd in een documentatiestandaard ter beschikking gesteld door de EANV-veiligheidsdienst of de externe partner.

Voor EMR specifiek kan het document *EMR / FORM / 0540* gebruikt worden om de risicoreductie van de EMR-beveiligingsinrichting te documenteren. Zie bijlage 1.

18.2. Safety Requirements Specification

De safety requirements specification is een aspect dat genormeerd is in IEC 61511. Evonik tracht om deze noodzakelijke specificaties in het PSS-werkdocument mee te verwerken. Indien in de PSS niet alle noodzakelijke details opgenomen zijn, kan er voor iedere nieuwe EMR-beveiligingsinrichting (Z-functie) een werkdocument ingevuld worden. Dit document is beschikbaar op Ennov met referentie *EMR / FORM / 0549*. Zie bijlage 10.

18.3. Ontwerp van de EMR-beveiligingsinrichting

18.3.1. Architectuur

De verificatie van de architectuur gebeurt door de nodige documenten te verzamelen die aantonen dat de gekozen architectuur voldoet aan de opgegeven eisen. Hiervoor is geen standaard werkformulier beschikbaar.
Indien de verificatie van de architectuur toereikend is, kan document *EMR / FORM / 0546 deel 1* ingevuld worden ter validatie. Zie bijlage 8.

18.3.2. Faalkans

De verificatie van de faalkans van de EMR-beveiligingsinrichting gebeurt door de nodige documenten te verzamelen die aantonen dat de totale faalkans voldoet aan de opgegeven eisen.

Indien de verificatie van de faalkans toereikend is, kan document *EMR / FORM / 0546 deel 2* ingevuld worden ter validatie. Zie bijlage 8.

18.3.3. Systematic Coverage

De verificatie van de systematic coverage EMR-beveiligingsinrichting gebeurt door de nodige documenten te verzamelen die aantonen dat de veldtoestellen geschikt zijn voor de opgegeven eisen.

Indien de verificatie van de systematic coverage toereikend is, kan document *EMR / FORM / 0546 deel 3* ingevuld worden ter validatie. Zie bijlage 8.

18.4. Installatie en indienstneming

De installatie bestaat uit drie luiken:

- montage veldinstrumenten;
- configuratie veldinstrumenten;
- functionele afwikkeling (logica).

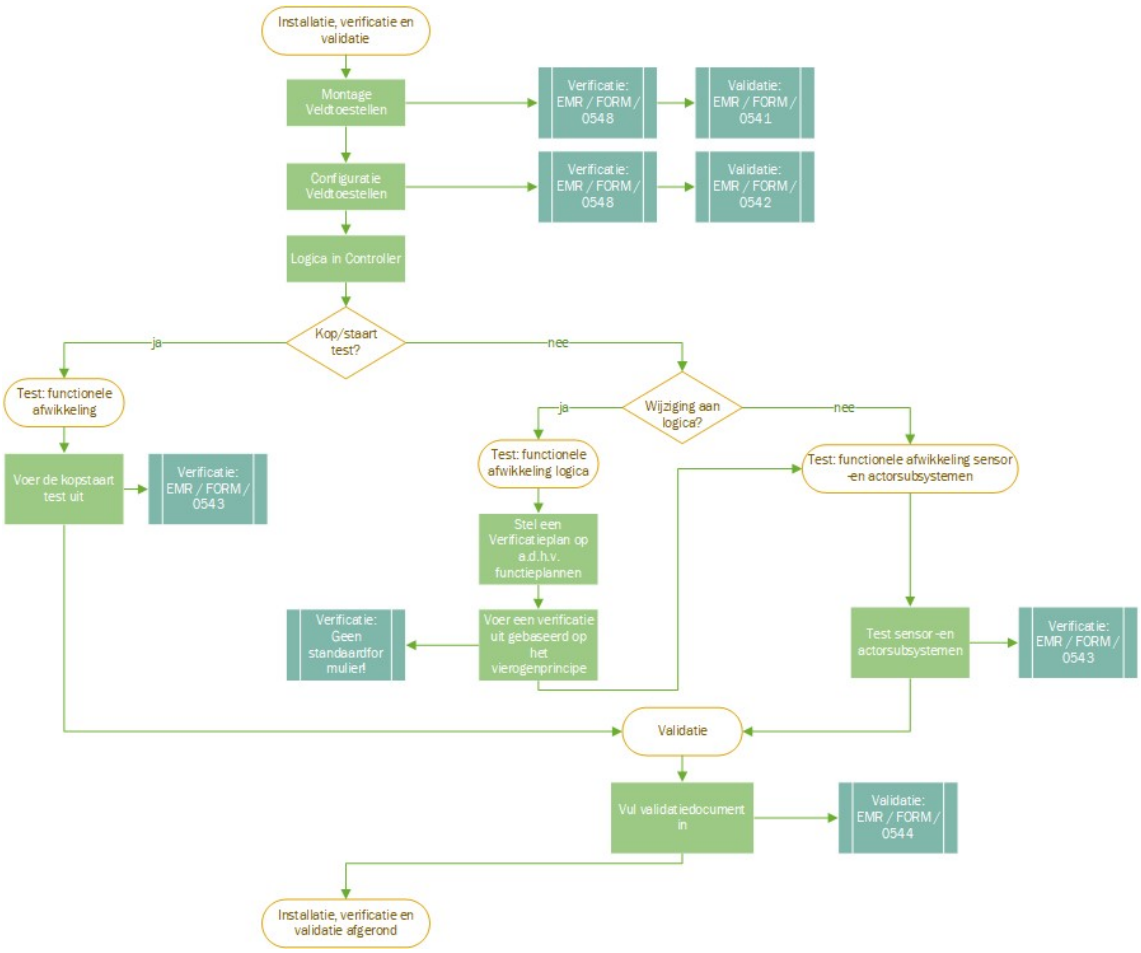
Ook deze drie luiken dienen geverifieerd en gevalideerd te worden. De verificatie van deze drie stappen zijn reeds behandeld bij de hoofdstukken Installatie en Indienstneming.

Wanneer de verificaties toereikend zijn, kunnen volgende documenten ingevuld worden ter validatie:

- montage veldinstrumenten: *EMR / FORM / 0541* - bijlage 3;
- configuratie veldinstrumenten: *EMR / FORM / 0542* - bijlage 4;
- functionele afwikkeling (logica): *EMR / FORM / 0544* - bijlage 6.

De verzameling van de drie validatieformulieren is het bewijs dat het systeem de noodzakelijke stappen heeft doorlopen en dat hierbij de installatie in dienst is genomen.

Voor het installeren met verificatie en validatie kan onderstaande afloop gehanteerd worden.



18.5. Periodiek testen

De periodieke testen dienen gedocumenteerd te worden om aan te tonen dat dit systematisch getest wordt. Dit document dient als bewijs bij audits en dient min. 10 jaar beschikbaar te zijn.

De inschatting van de goede werking van een EMR-beveiligingsinrichting dient te gebeuren door de EMR-bedrijfsopvolger van die specifieke installatie. De EMR-bedrijfsopvolger dient dan aan de bedrijfsverantwoordelijken te rapporteren of alle geplande tests succesvol uitgevoerd zijn.

Gebruik voor nieuw te implementeren Z-kringen *EMR / FORM / 0545* als template voor de periodieke test van een EMR-beveiligingsinrichting. Zie bijlage 7.

18.6. Uitdienstneming

18.6.1. Permanente uitdienstneming

Een permanente uitdienstneming zal voortvloeien uit een PSS of een MoC. Hieraan zal de nodige documentatie gekoppeld worden.

18.6.2. Tijdelijke uitdienstneming

Om een tijdelijke uitdienstneming te documenteren, wordt *EMR / FORM / 0547* gebruikt. Zie bijlage 9. Bij iedere tijdelijke uitdienstneming waarbij het formulier “Uit- en herindienstneming” is ingevuld, kan het document voor een periode bijgehouden worden. Dit kan de traceerbaarheid naar wederkerende problemen verhogen. Dit is echter geen verplichting maar wel aangeraden.

Annex 1. Praktische uitwerkingen en ervaringen

“Mitbenützung” ofwel gebruik van componenten van EMR-beveiligingsinrichtingen voor operationele toepassingen

Bij het installeren van een EMR-beveiligingsinrichting kan het vaak opportuun lijken om deze instrumenten eveneens te gebruiken voor gewone controle-inrichtingen. Denk hierbij bv. aan een drukmeting die hoort bij een Z-functie maar waarvan men deze controller ook wil gebruiken voor een drukregeling.

Aangezien er via de safety controller en het BPCS-systeem digitale communicatiesystemen opgezet zijn, kan deze informatie gebruikt worden op het BPCS-systeem voor controle.

Volgens de norm dienen controle- en beveiligingssystemen van elkaar gescheiden te zijn. Er moet maximaal ingezet worden op het scheiden van controle en safety. In sommige toepassingen of om toch een overmaat van instrumenten te voorkomen, kan “Mitbenützung” toegepast worden als een **faling** van de betrokken component **niet** rechtstreeks kan leiden tot het **gevaarlijke scenario**.

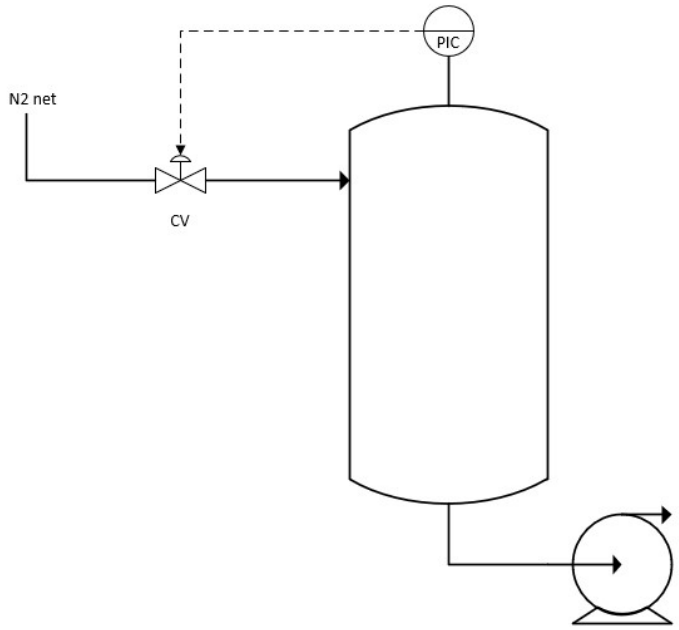
Voorbeeld éénkanalig systeem:

Een tank met een chemische oplossing heeft een permanente stikstofspoeling. Als de chemicaliën vrijkomen, zal dit leiden tot een gevaarlijk scenario.

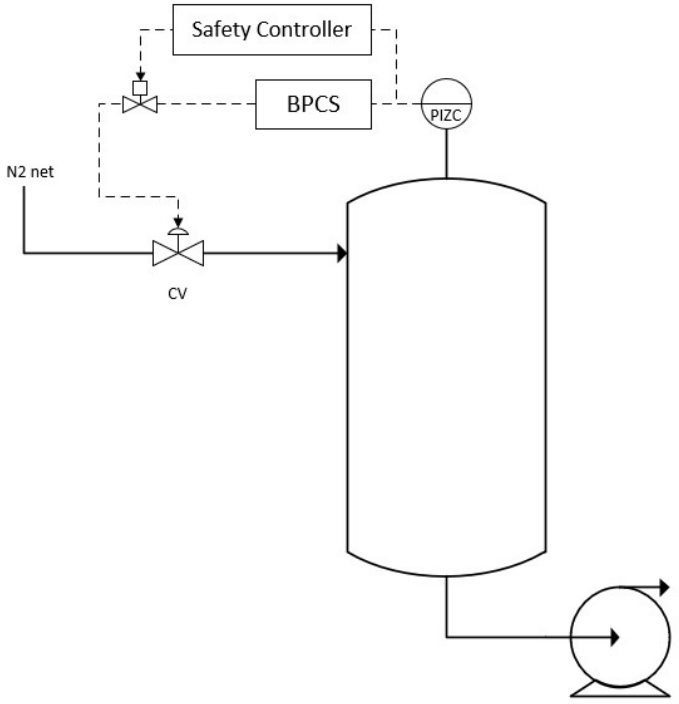
De ontwerpdruk van de tank is lager dan de druk op het stikstofnet.

Het afdekken van het risico zou uitgevoerd kunnen worden met een éénkanalig systeem (1 sensor, 1 actor).

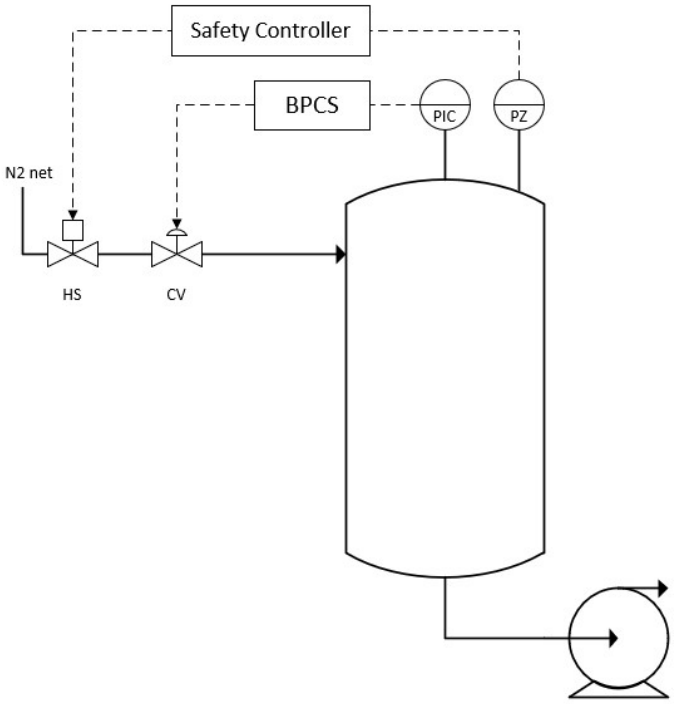
Daar de druk op de tank geregeld moet worden, is er een drukmeting en een regelventiel nodig.



Wens: Drukmeting en regelventiel van PIC gebruiken voor veiligheidsfunctie PICZ.



Aangezien zowel het falen van de sensor als het regelventiel kan leiden tot het onveilige scenario, is bovenstaande opstelling niet toegelaten **voor dit scenario.** Regeling en beveiliging dienen onafhankelijk uitgevoerd te worden.



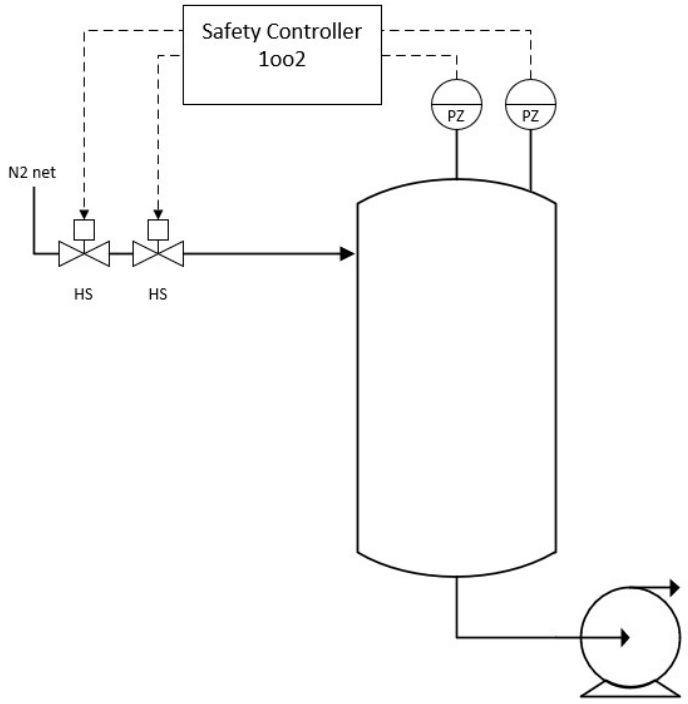
Opmerking: Beschouw in de PSS steeds het falen van sensor en actor apart. Bij falen van een actor kan je volgende vragen stellen: Wat als de veren in een aandrijving breken? Wat als het membraan scheurt? Wat als de kegel/zit loskomt? Wat als de hulpenergie wegvalt? … Als dit kan leiden tot de initiërende activiteit, dan mag deze actor niet gebruikt worden om dit scenario te voorkomen.

Tweekanalig systeem

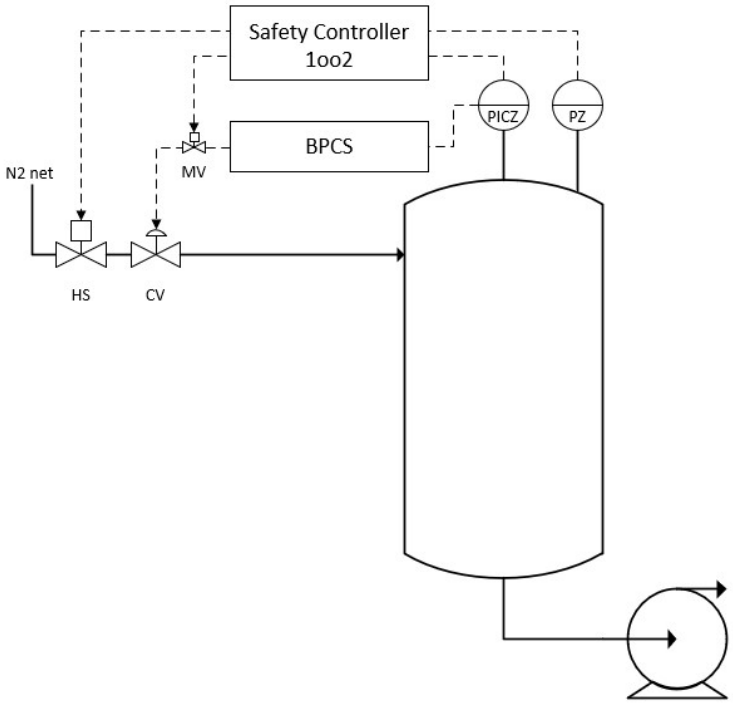
Een tank met een chemische oplossing heeft een permanente stikstofspoeling. Als de chemicaliën vrijkomen, zal dit leiden tot een gevaarlijk scenario.

De ontwerpdruk van de tank is lager dan de druk op het stikstofnet.

Het afdekken van het risico dient uitgevoerd te worden met minimaal een tweekanalig systeem (2 sensoren, 2 actoren). Veronderstel SIL 3.



Wensuitvoering:



Dit is toegelaten als:

- sensoren 1 en 2 een vergelijkingsbewaking hebben in de safety controller (zie TS30-0000 voor de voorwaarden van een vergelijkingsbewaking) en
- de sensoren 1-kanalig SIL 2 zijn en
- de actoren 1-kanalig SIL 2 zijn en
- het optreden van een gefaalde sensor leidt tot de activatie van een timerfunctie van 8 uren. De veiligheidsfunctie mag 8 uren gereduceerd zijn naar het SIL 2-niveau. Als binnen 8 uren de fout niet opgelost is, zal de veiligheidsfunctie geactiveerd worden.
- Het falen van een actor moet gedetecteerd worden. Dit kan door bv. partial stroke-testen, schakelingen of bewegingen van een ventiel a.d.h.v. stellingsmelding, …

Z-alarmen

TS30-0000 bespreekt het gebruik van Z-alarmen. Er wordt vermeld dat deze tot SIL 2 uitgerust kunnen worden. Daar een alarm geen automatische actie is, dient er nog steeds een procedure gevolgd te worden waarin beschreven staat welke handelingen er uitgevoerd moeten worden. Aangezien dit niet in lijn ligt met de fundamenten van functional safety, mag dit enkel ingezet worden indien er geen andere opties mogelijk zijn.

Het gebruik van Z-alarmen heeft ook zijn technische moeilijkheden:

- Beschikbare toestellen zijn buitentoepassingen met een hoog akoestisch geluidssignaal. Niet geschikt voor in controlekamers.
- De afwikkeling van Z-alarmen gebeurt buiten DCS om maar in veiligheidssturing.
- De opbouw is fundamenteel identiek aan een klassieke EMR-beveiligingskring. Het alarmapparaat vervangt hier het actordeelsysteem.
- De spanningsvoorziening moet redundant en gebufferd uitgevoerd zijn.
- De spanningsvoorziening moet bewaakt worden.
- Z-alarmen dienen een aparte, hogere priorisering te krijgen dan gewone procesalarmen.

Gebruik van instrumentele beveiligingen bij equipment voor explosiebeveiliging

Fabrikanten of leveranciers leveren dikwijls equipment die geschikt is voor explosiezones. De fabrikant zal in sommige gevallen voorschrijven om EMR-inrichtingen te installeren als bijkomende beveiliging. De leverancier of fabrikant kent de lokale installatie niet en kan daarom geen aanbeveling maken van de kwaliteit van deze EMR-instrumenten. Hiervoor dient de eindgebruiker steeds een gepaste risicoanalyse te doen. Deze analyse dient gedaan te worden tijdens de PSS.

Opgelet! Hieronder volgt een mogelijke behandelingswijze. Houd rekening met de persoonlijke inschattingen van de ontwerpers van dit document en het is niet bindend maar slechts een hulpmiddel voor de veiligheidsanalyse.

Faalkans van een equipment volgens BTD11-0000

BTD11-1000 laat toe om de frequentie van een explosiescenario te bepalen aan de hand van onderstaande tabel.

Normaal bedrijf	Ontstekingsbronnen te verwachten bij…	F3	F2	F1	F0
Te verwachten falingen		F4	F3	F2	F1
Zeldzame falingen		F5	F4	F3	F2
Zelfs niet bij zeldzame falingen			F5	F4	F3
		Explosiezone			
		nEx	2	1	0

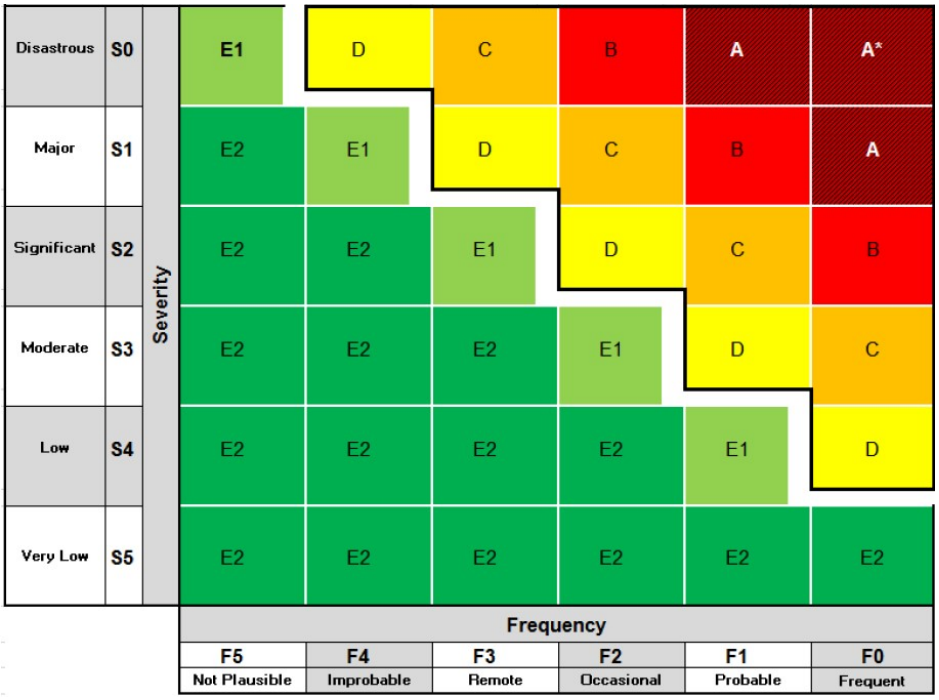
De fabrikant geeft zelf al aan dat zijn toestel in geval van falen een ontstekingsbron kan worden. Daarom beveelt deze aan om extra instrumentele beveiligingen te voorzien. Hiermee wordt vastgesteld dat **F4, F3, F2 en F1** kanshebbers zijn (Te Verwachten Falingen). Het uiteindelijke F-getal is dan afhankelijk van de zone waar dit equipment geplaatst zal worden.

De volgende stap is het inschatten van de gevolgen in geval van een calamiteit. Dit wordt gedaan door tabel 4 van BTD11-0000 toe te passen.

Category	People		Environment
	Employees	Public *)	
S0 *Disastrous*	Large number of fatalities	Multiple fatalities or life-threatening injury or multiple permanent injuries	Large area left uninhabitable
S1 *Major*	Multiple fatalities or life-threatening injury or multiple permanent injuries	Single fatality, permanent or long lasting injury or multiple injuries	Extensive long-term environmental impact, significant cleanup/ remediation necessary, or a very large unconfined release, internal and external report required
S2 *Significant*	Single fatality, permanent or long lasting injury or multiple injuries	Single non-permanent injury requiring medical treatment	Long-term environmental impact, significant cleanup/ remediation necessary, or a large unconfined release, internal and external report required
S3 *Moderate*	Single non-permanent, lost time injury requiring medical treatment	Single minor injury requiring first-aid treatment	Temporary environmental impact with damage to sensitive environment or a minor unconfined release with major mitigation response actions, internal and external report required
S4 *Low*	Single minor injury requiring first-aid treatment (without lost time)	Minimal public impact possible (e.g. odor, noise)	Environmental release with minor impact beyond site boundaries or moderate impact within site boundaries, clean up necessary, internal and external report required
S5 *Very low*	No impact	No impact	Incidental spill, cleaned up by personnel in area within plant boundaries, minor environmental release within site boundaries, internal report required
*) This has to be defined prior to the study according to local requirements.			

In de meest courante gevallen is **S2** “Significant” plausibel. Als een equipment zou exploderen, kan een persoon in de omgeving zeer ernstig gekwetst geraken of dodelijk getroffen worden.

Als dan de risicomatrix van BTD11-1000 toegepast wordt om in te schatten aan welke kwaliteit de EMR-inrichtingen moeten voldoen, krijgen we volgende resultaten:



Zone 0-20	F1	S2	Risicoklasse C
Zone 1-21	F2	S2	Risicoklasse D
Zone 2-22	F3	S2	Risicoklasse E1
nEx	F4	S2	Geen risicoklasse

Als equipment geplaatst wordt in een explosiezone 0-20

Er zijn extra te nemen maatregelen zoals voorzien in tabel 14 risicoklasse C van de BTD 11-1000, bijvoorbeeld het uitvoeren van de beveiligingskring volgens SIL 2 met een jaarlijkse inspectie. Het inzetten van een EMR-beveiligingsinrichting op het SIL 2-niveau brengt het restrisico op E1.

Deze instrumentele beveiliging krijgt een Z-label en dient volgens de volledige levenscyclus van een EMR-beveiligingsinrichting uitgewerkt te zijn.

Vanaf 2025 zal er nog een bijkomende monitoring voorzien moeten worden om de Evonik-doelstelling van E2 voor ieder scenario te bereiken.

Als equipment geplaatst wordt in een explosiezone 1-21

Er zijn extra te nemen maatregelen zoals voorzien in tabel 15 risicoklasse D van de BTD 11-1000, bijvoorbeeld het uitvoeren van de beveiligingskring volgens SIL 2 met een jaarlijkse inspectie. Het inzetten van een EMR-beveiligingsinrichting op het SIL 2-niveau brengt het restrisico op E1.
Deze instrumentele beveiliging krijgt een Z-label en dient volgens de volledige levenscyclus van een EMR-beveiligingsinrichting uitgewerkt te zijn.

Vanaf 2025 zal er nog een bijkomende monitoring voorzien moeten worden om de Evonik-doelstelling van E2 voor ieder scenario te bereiken.

Als equipment geplaatst wordt in een explosiezone 2-22

Er zijn te nemen maatregelen zoals voorzien in risicoklasse E1 van de BTD 11-1000: geen voorwaarden met betrekking tot de gebruikte componenten maar wel het monitoren van de situatie door de geplaatste beveiliging. Het gebruik van deze instrumentele beveiliging zal het risico reduceren tot E2. Deze instrumentele beveiliging krijgt geen Z-label.

Hardverdrade EMR-beveiligingsinrichtingen

In de meeste gevallen worden de EMR-instrumenten verbonden met een safety controller waarbij in het geheugen logica geprogrammeerd is om bepaalde acties uit te voeren. Echter is dit geen noodzaak. Beveiligingskringen kunnen hardverdraad uitgevoerd worden en zelfs in sommige gevallen noodzakelijk.

Sensoren kunnen met behulp van potentiaalvrije contacten rechtstreeks schakelingen uitvoeren die aansluitend actoren doen schakelen.

Er wordt geen andere systematiek gebruikt voor dit soort EMR-beveiligingskringen t.o.v. alle andere. Hier dient ook de volledige levenscyclus afgedekt te worden.

Analyzers gebruiken als instrumentele beveiliging

Bij verschillende scenario's lijken analyzers een passende oplossing te bieden om afwijkingen tijdig te detecteren. Tegenwoordig zijn er voor heel wat toepassingen reeds analyzers met een SIL-certificaat beschikbaar.

Analyzers zullen nagenoeg niet in de Prior Use-lijst opduiken, omdat de populatie van ingezette toestellen zodanig klein is waardoor de afwikkeling van analyzers volgens NE130 moeilijk te realiseren is.

Bij het gebruik van procesanalysetechnieken onderscheiden we twee situaties:

Analyzers met SIL-certificering

Deze kunnen uitgewerkt worden als normale EMR-beveiligingsinrichtingen. Hier dient dan de berekeningsmethode toegepast te worden.

Analyzers zonder SIL-certificering

In dit geval zal de verantwoordelijkheid volledig bij Evonik liggen. Het is belangrijk om te beseffen dat hier erg veel inspanning geleverd zal moeten worden om de kwaliteit van deze instrumenten te bewijzen.

Om een analyzer te kwalificeren als een instrument geschikt voor EMR-beveiligingsinrichtingen dient er een expertenteam opgezet te worden die een volledige studie zal doen naar dit toestel. Aangezien EANV niet over deze experten beschikt, zal dit steeds buitenshuis gebeuren.

NE146 beschrijft de volledige werkwijze om PAT-toestellen te kwalificeren voor EMR-beveiligingsinrichtingen.

Uitschakelen van elektromotoren als deel van een EMR-beveiligingsinrichting

In sommige gevallen zal het uitschakelen van een elektromotor een onderdeel zijn van een EMR-beveiligingsinrichting. In de meeste gevallen zullen contactoren de stroom naar de elektromotor onderbreken. Bij het gebruik van een frequentiedrive is het mogelijk dat een frequentiedrive ingezet wordt die een ingebouwde veiligheidsafschakeling heeft. Er zijn drives op de markt beschikbaar die een SIL 2-beveiliging hebben.

Als men de motor met frequentiedrive wil afschakelen a.d.h.v. contactoren, dan kan men stroomopwaarts van de drive de nodige contactoren zetten om de stroom te onderbreken.

Afloop EMR-beveiligingsinrichting

Indien er gekozen wordt voor een elektromotor als actor dient eveneens de volledige cyclus doorlopen te worden zoals weergegeven in hoofdstuk 8. De drie types falingen dienen ook voor deze subsystemen afgedekt te worden:

- Random Failures;
- Common Cause Failures;
- Systematic Failures.

Om dit te realiseren worden volgende voorschriften gegeven:

Contactor in SIL 1-kring:

- De contactor dient van het type AC3 of AC4 te zijn.
- De faalkans van de EMR-beveiligingskring dient bepaald te worden. Bij de Elektro-ingenieurs zijn er lijsten beschikbaar van “Proven in Use”-contactoren. Bij gebruik van deze “Prior Use”-contactoren volstaat een enkelvoudige uitvoering van het subsysteem.
- Het wordt sterk aanbevolen om de contactor te overdimensioneren. Dit reduceert significant de kans dat de stroomvoerende contacten zouden “vastlassen” door de belasting.

Contactor in SIL 2-kring:

- De contactor dient van het type AC3 of AC4 te zijn.
- De faalkans van de EMR-beveiligingskring dient bepaald te worden. Bij de Elektro-ingenieurs zijn er lijsten beschikbaar van “Proven in Use”-contactoren. Bij gebruik van deze “Prior Use”-contactoren volstaat een enkelvoudige uitvoering van het subsysteem.
- Het is verplicht om de contactor te overdimensioneren om de kans op “vastlassen” van de stroomvoerende contacten significant te reduceren.

Contactor in SIL 3-kring:

- De contactor dient van het type AC3 of AC4 te zijn.
- De faalkans van de EMR-beveiligingskring dient bepaald te worden. Bij de Elektro-ingenieurs zijn er lijsten beschikbaar van “Proven in Use”-contactoren. Deze kunnen gebruikt worden om via de vereenvoudigde weg de faalkans te argumenteren.
- Bij gebruik van deze “Prior Use”-contactoren dient een meerkanaalsuitvoering van het subsysteem toegepast te worden, d.w.z. dat er minstens twee contactoren gebruikt worden die in serie de stroom zullen onderbreken.
- Het is verplicht om de contactor te overdimensioneren om de kans op “vastlassen” van de stroomvoerende contacten significant te reduceren.

Overdimensioneren

Indien overdimensioneren toegepast wordt, zijn volgende criteria te volgen:

- De stroom die gevoerd wordt over de schakelcontacten mag maximaal de helft zijn van de toegelaten stroom volgens de technische specificatiesheet van de component.
- De schakelfrequentie van de componenten mag maximaal de helft zijn van de toegelaten schakelfrequentie volgens de technische specificatiesheet van de component.
- Het totaal aantal schakelingen moet 10x minder zijn dan het vermelde aantal schakelingen volgens de technische specificatiesheet van de component.

Voorbeeld van overdimensioneren

We veronderstellen een contactor met volgende eigenschappen:

- I_n 25A@AC3 (400 V);
- max. aantal schakelingen per uur: 750;
- max. levensduur van de contacten: 1.694.912 schakelingen.
-

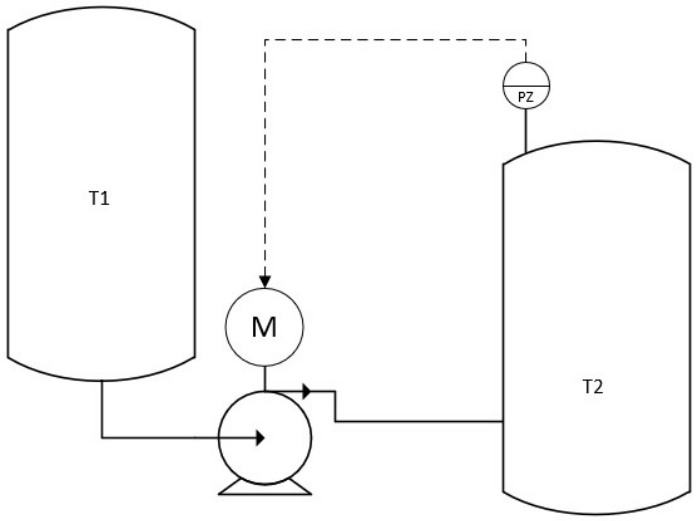
Indien deze contactor gebruikt wordt voor een Z-functie, dan zal men moeten bewaken dat:

- een motor max. I_n 12,5A aangedreven wordt en dus een maximaal vermogen van 5,5 kW heeft;
- deze contactor maximaal 375 schakelingen per uur doet;
- deze contactor maximaal 169.491 schakelingen doet en dan vervangen wordt.

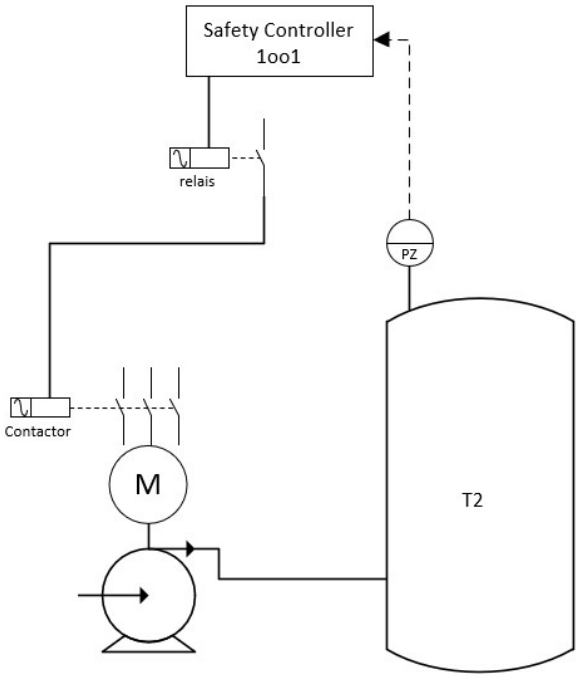
Praktisch voorbeeld

Een pomp verplaatst vloeistof van T1 naar T2. De pomp heeft een capaciteit die T2 over zijn designdruk zou kunnen brengen. Als de tank zou scheuren, spreken we over een scenario dat we dienen af te dekken met een SIL 2 EMR-beveiliging.

Processchema:



Voorstelling elektrische schakeling:



waarbij het relais een veiligheidsrelais is. O.a. HIMA biedt deze aan, beschikbaar met alle noodzakelijke certificaten en documenten.

Annex 2. Voorbeelden en verduidelijking architectuur van subsystemen

Veronderstellingen bij de voorbeelden

Veronderstel dat hier steeds over sensorsubsystemen gesproken wordt. De methodiek voor actoren is identiek.

We gaan uit van een proces waarin de procesgrootheid zal stijgen om in een gevaarlijk gebied te komen.

Redundantie

Redundantie heeft in deze context de betekenis dat twee instrumenten exact hetzelfde doen en dit in functie van de **beschikbaarheid van de installatie**.

1oo1

Er is slechts één sensor geïnstalleerd. Als deze goed functioneert, zal bij het overschrijden van de procesgrootheid de veiligheidsfunctie geactiveerd worden.

Als deze sensor gefaald is naar de onveilige kant, dan zal bij het overschrijden van de procesgrootheid in het proces de veiligheidsfunctie niet geactiveerd worden. De sensor meet de procesgrootheid foutief.

Als deze sensor faalt naar de veilige kant, dan zal de veiligheidsfunctie geactiveerd worden terwijl dit noodzakelijk was. **Er is geen verhoogde betrouwbaarheid van de veiligheidsfunctie.**

Er is geen redundantie.

2oo2

Er zijn twee sensoren geïnstalleerd. Als beide goed functioneren, zullen deze gelijktijdig het overschrijden van de procesgrootheid aanduiden. Beide sensoren dienen deze overschrijding te registreren om de veiligheidsfunctie te activeren.

Als 1 sensor onveilig faalt, dan zal bij het overschrijden van de procesgrootheid de veiligheidsfunctie niet aanspreken. Dit is omdat de gefaalde sensor de overschrijding van deze procesgrootheid niet registreert. Enkel de goed functionerende registreert dit gebeuren. Eén sensor is onvoldoende om de veiligheidsfunctie te activeren.

De veiligheidsfunctie werkt niet wanneer het wel zou moeten, dus hier is sprake van **een verlaagde betrouwbaarheid van de veiligheidsfunctie**.

Als er 1 instrument veilig faalt, zal de veiligheidsfunctie niet geactiveerd worden. **Er is redundantie.**

1oo2

Er zijn twee sensoren geïnstalleerd. Als beide goed functioneren, zullen deze gelijktijdig het overschrijden van de procesgrootheid aanduiden. In dit geval is het toereikend als slechts 1 van de twee sensoren het overschrijden van de procesgrootheid registreert.

Het voordeel van deze opstelling doet zich voornamelijk voor wanneer 1 sensor onveilig gefaald is. Als de procesgrootheid de toegelaten waarde overschrijdt, zal slechts de sensor die nog goed functioneert dit waarnemen. Deze zal de veiligheidsfunctie in dat geval activeren. **Er is een verhoogde betrouwbaarheid van de veiligheidsfunctie.**

Als er 1 instrument veilig faalt, zal de veiligheidsfunctie geactiveerd worden. **Er is geen redundantie.**

2oo3

Er zijn in het totaal 3 instrumenten geïnstalleerd. Als deze drie sensoren goed functioneren, zullen deze gelijktijdig het overschrijden van de procesgrootheid aanduiden. In dit geval zijn er slechts twee sensoren nodig die het overschrijden van de procesgrootheid moeten registreren om de veiligheidsfunctie te activeren.

Als 1 instrument onveilig faalt en dus de overschrijding niet registreert, zullen de andere twee sensoren dit nog wel registreren. **Er is een verhoogde betrouwbaarheid van de veiligheidsfunctie.**

Als 1 instrument veilig faalt en dus onterecht een te hoge procesgrootheid aanduidt, zal deze de veiligheidsfunctie niet activeren, omdat er twee sensoren deze overschrijding dienen te registreren. **Er is redundantie**.

1oo3

Er zijn in het totaal 3 instrumenten geïnstalleerd. Als deze drie sensoren goed functioneren, zullen deze gelijktijdig het overschrijden van de procesgrootheid aanduiden. In dit geval is er slechts één sensor nodig die het overschrijden van de procesgrootheid moet registreren om de veiligheidsfunctie te activeren.

Als 2 instrumenten onveilig falen en dus de overschrijding niet registreren, zal de andere sensor dit nog wel registreren. **Er is een extra verhoogde betrouwbaarheid van de veiligheidsfunctie.**

Als 1 instrument veilig faalt en dus onterecht een te hoge procesgrootheid aanduidt, zal deze de veiligheidsfunctie activeren. **Er is geen redundantie**.

Conclusie: elk type architectuur heeft zijn voor- en nadelen.

Annex 3. Kwantificeren van Random Failures bij gecertificeerde toestellen (geen Prior Use-toestellen)

In deze situatie kunnen we geen beroep doen op typicals die uitgewerkt zijn in standaards. Hier zal het aftoetsen van de faalkansen manueel gedaan moeten worden.

Evonik Antwerpen heeft geen standaard calculatietool. Ieder individu kan zelf aan de slag gaan om berekeningen te maken of een beroep doen op specialisten zoals bij de Technische Anlagesicherheitsafdeling in Marl (TAS) of Vinçotte.

Achterhalen faaldata λdu

Van ieder component van de volledige veiligheidskring dienen de faaldata achterhaald te worden. Deze zijn terug te vinden op de certificaten van de individuele componenten.

Enkele voorbeelden van componenten die in een veiligheidskring aanwezig zijn:

- sensoren: debiet, druk, niveau, temperatuur, …;
- IO-kaarten;
- logic controllers;
- magneetventielen;
- ventielen en kleppen;
- aandrijvingen;
- veiligheidsrelais;
- en andere.

Berekenen faalkans van een subsysteem

Aangezien deelsystemen van sensoren en actoren vaak volgens meerkanalige opstellingen opgebouwd zijn, dienen de faalkansen van alle subsystemen eerst in kaart gebracht te worden. Voor meerkanalige subsystemen dient men een beroep te doen op formules. Hieronder enkele vereenvoudigde formules die toegepast kunnen worden:

$$PFD_{1oo1} \approx \lambda_{du} \times \frac{T_1}{2}$$

$$PFD_{2oo2} \approx \lambda_{du} \times T_1 = 2 \times PFD_{1oo1}$$

$$PFD_{1oo2} \approx \frac{\lambda_{du}^2 \times T_1^2}{3} + \beta \times \lambda_{du} \times \frac{T_1}{2} = 4/3 \times PFD^2_{1oo1} + \beta \times PFD_{1oo1}$$

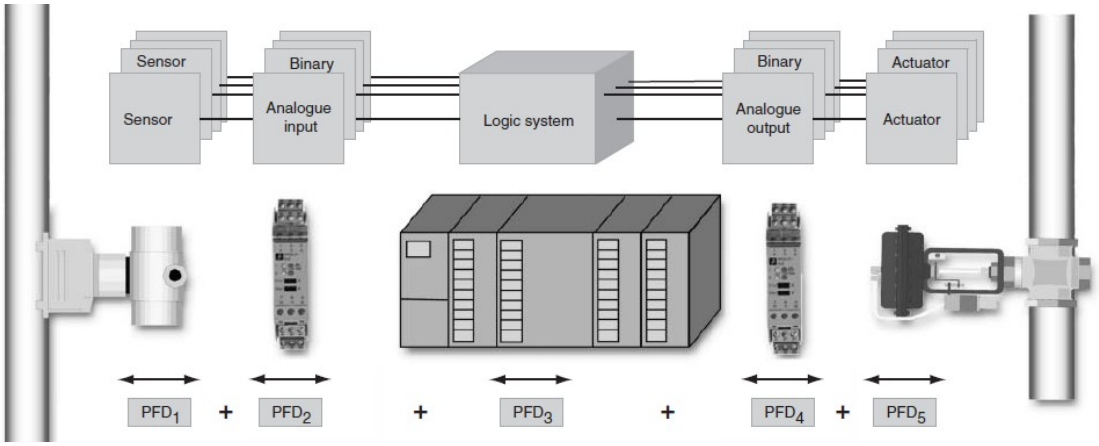
$$PFD_{2oo3} \approx \lambda_{du}^2 \times T_1^2 + \beta \times \lambda_{du} \times \frac{T_1}{2} = 4 \times PFD^2_{1oo1} + \beta \times PFD_{1oo1}$$

$$PFD_{1oo3} \approx \frac{\lambda_{du}^3 \times T_1^3}{4} + \beta \times \lambda_{du} \times \frac{T_1}{2} = 2 \times PFD^3_{1oo1} + \beta \times PFD_{1oo1}$$

$$PFD_{2oo4} \approx \lambda_{du}^3 \times T_1^3 + \beta \times \lambda_{du} \times \frac{T_1}{2} = 8 \times PFD^3_{1oo1} + \beta \times PFD_{1oo1}$$

Faalkans van een volledige veiligheidskring

Wanneer de faalkansen van de deelsystemen bekend zijn, kan de volledige faalkans bepaald worden.



$PFD_{avg\text{-}kring} = PFD_1 + PFD_2 + PFD_3 + PFD_4 + PFD_5$

Combineren van Prior Use-toestellen met gecertificeerde toestellen

Het kan zich voordoen dat een bepaalde toepassing een sensor vereist dat niet in de Prior Use devices-lijst staat. Dan dienen we volgens de afloop van de instrumenten de faalkansen te zoeken. In de meeste gevallen zullen deze terugkomen op de certificaten.

Aangezien we ook voor de mechanische delen van een actor de faalkans dienen te kennen, wordt het een moeilijke opgave. Fabrikanten van ventielen en kleppen staan vaak niet zo ver als fabrikanten van veldtoestellen.

In de lijst van Prior Use devices staan er een aantal actoren opgesomd. Het is mogelijk om de faaldata van de mechanische componenten uit NE93 te hanteren i.c.m. de faaldata op het certificaat van de sensor.

De afloop van de berekening dient gevolgd te worden en de architectuur heeft mogelijk een HFT van +1 (extra veldtoestel), maar er kan op deze manier wel een uitweg gevonden worden om te voldoen aan alle eisen van de norm IEC 61511.

Annex 4. Bepalen van HFT

HFT bepalen bij gebruik van gecertificeerde toestellen

Bij het gebruik van instrumenten gebaseerd op certificaten, dient de gewenste architectuur afgetoetst te worden met de minimum HFT uit onderstaande tabel.

SFF	HFT					
	TYPE B-instrument			TYPE A-instrument		
	0	**1**	**2**	**0**	**1**	**2**
<60 %	Not allowed	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3
60 % - 90 %	SIL 1	SIL 2	SIL 3	SIL 2	SIL 3	SIL 4
90 % - 99 %	SIL 2	SIL 3	SIL 4	SIL 3	SIL 4	SIL 4
>=99 %	SIL 3	SIL 4	SIL 4	SIL 4	SIL 4	SIL 4

De meeste veldinstrumenten zijn type B-componenten. Definitie van type B-componenten kan geraadpleegd worden in de norm IEC 61511.

Met het gebruik van bovenstaande tabel wordt de factor Safe Failure Fraction (SFF) geïntroduceerd. Dit is de verhouding van de kans op veilige en gedetecteerde faaltoestanden van een instrument ten opzichte van de kans op alle faaltoestanden.

$$SFF = \frac{\lambda^{SD} + \lambda^{SU} + \lambda^{DD}}{\lambda^{SD} + \lambda^{SU} + \lambda^{DD} + \lambda^{DU}}$$

Failure rate types

λ^{SD} = Safe Detected fai

Bij gecertificeerde toestellen staat de SFF-waarde vermeld op het certificaat.

Door de SFF van het certificaat te combineren met het te bereiken SIL-niveau, zal een HFT-getal geresulteerd worden.

Dit kan je dan helpen om te controleren of de gewenste architectuur toegestaan is.
Dit doe je door **M** – **N** van je gewenste architectuur te doen.
Doe dit dan voor elk subsysteem, want dit is van toepassing op zowel de sensoren als actoren.

Gecombineerd gebruik van gecertificeerde en Prior Use-toestellen

Van de Prior Use devices mag uitgegaan worden dat ze een SFF van 90-99 % hebben.

HFT bepalen bij Prior Use devices

Dit is enkel noodzakelijk bij het gebruik van Prior Use-toestellen in High Demand of Continuous Mode. Voor Low Demand Mode zijn deze stappen reeds uitgewerkt in NE93 en TS30-0000. Bij gebruik van standaard architecturen dient de HFT niet bepaald te worden.

Table 6 – Minimum HFT requirements according to SIL

SIL	Minimum required HFT
1 (any mode)	0
2 (low demand mode)	0
2 (high demand or continuous mode)	1
3 (any mode)	1
4 (any mode)	2

Typische sensorarchitecturen

1oo1, 1oo2, 1oo3, 2oo3

Typische actorarchitecturen

1oo1, 1oo2, 2oo2

Annex 5. Voorbeelden ter verduidelijking van HFT

De HFT is een getal dat uiteindelijk het minimumaantal geïnstalleerde instrumenten bepaalt. Dit begrip is hieronder uitgelegd a.d.h.v. enkele voorbeelden.

Voorbeelden en verduidelijkingen

Enkele praktische voorbeelden om de betekenis van HFT beter te begrijpen.

HFT = 0

Het minimumaantal geïnstalleerde instrumenten is **1,** maar kan ook bestaan uit meerdere instrumenten.

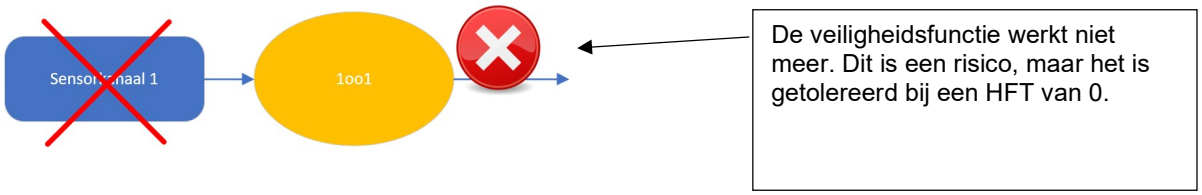
1oo1

Eén veldinstrument is geïnstalleerd voor dit subsysteem. Bv. één sensor.

De gekozen architectuur is 1oo1.

1 – 1 = 0 (HFT)

Eén veldinstrument is voldoende om te voldoen aan een HFT van 0. Het is toegestaan om één toestel in deze kring te hebben dat onveilig gefaald is. De veiligheidsfunctie zal dan niet meer werken, maar het wordt getolereerd volgens de normen om te voldoen aan een HFT van 0.



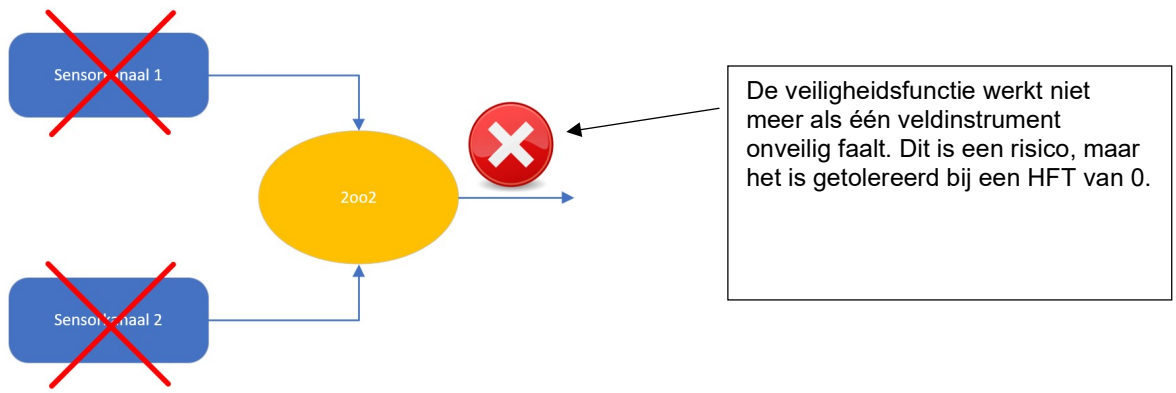
2oo2

Er zijn twee veldinstrumenten geïnstalleerd in dit subsysteem. Bv. 2 sensoren.

De architectuur is 2oo2.

2 – 2 = 0 (HFT)

Bij een 2oo2 zijn er twee parallelle toestellen. Zij doen identiek hetzelfde. De 2oo2 geeft weer dat beide instrumenten correct moeten functioneren om de veiligheidsfunctie te kunnen garanderen. Als één van de twee instrumenten onveilig faalt, zal de veiligheidsfunctie niet meer werken. Dit wordt getolereerd volgens de normen voor een HFT van 0.



HFT = 1

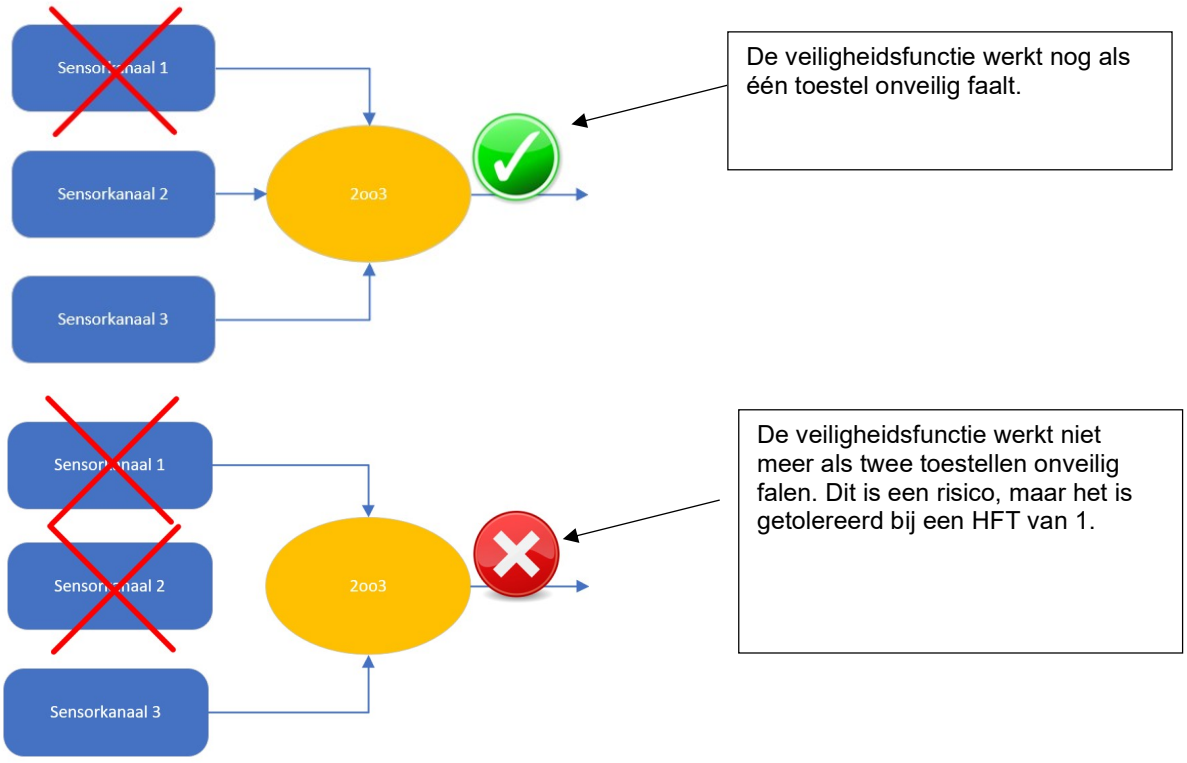
2oo3

Er zijn in dit geval drie instrumenten geïnstalleerd in het subsysteem. Bv. 3 sensoren.

De architectuur is 2oo3.

3 – 2 = 1 (HFT)

Als twee van de instrumenten onveilig falen, zal de veiligheidsfunctie niet meer werken. Bij een HFT van 1 is dit getolereerd volgens de normen. Merk op dat bij het onveilig falen van één instrument de veiligheidsfunctie intact blijft.



HFT = 2

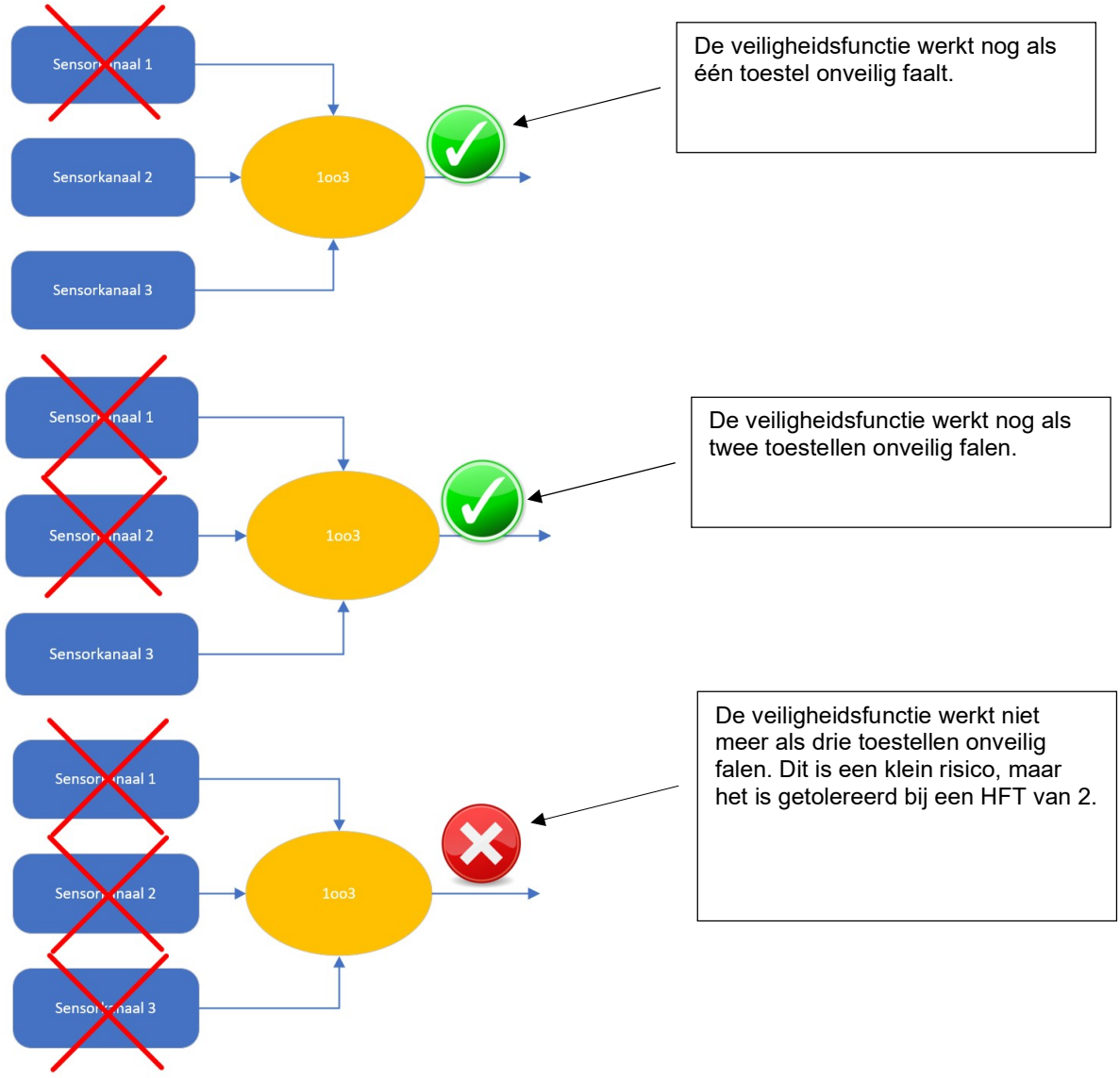
1oo3

Er zijn 3 instrumenten geïnstalleerd in dit subsysteem. Bv. 3 sensoren.

De architectuur is 1oo3.

3 – 1 = 2 (HFT)

Als deze drie instrumenten onveilig falen, zal de veiligheidsfunctie niet meer werken. Merk op dat bij het onveilig falen van één of twee instrumenten de veiligheidsfunctie intact blijft.



Annex 6. Periodiek testen

EMR-beveiligingsinrichtingen dienen periodiek getest te worden. Stel voor iedere EMR-beveiligingsfunctie een testformulier op en geef hier alle noodzakelijke informatie mee om een kwalitatieve test uit te voeren. Gebruik voor nieuw te implementeren Z-kringen *EMR / FORM / 0545*.

Deze periodieke testen dienen om de niet-gedetecteerde onveilige falingen (λ_{du}) van de instrumenten te detecteren. Bij een grote populatie van identieke veldinstrumenten kan men op deze wijze de kwaliteit en betrouwbaarheid in kaart brengen.

Een instrument verliest aan kwaliteit in de tijd. Het periodiek testen heeft ook als doel om de integriteit van de veldinstrumenten te controleren. De frequentie en de manier van testen speelt hier een grote rol.

Frequentie

Om de PFD_{avg} van (sub)systemen te bepalen, wordt het proefinterval in de berekening opgenomen.

Kwaliteit

De manier van testen beïnvloedt de maximale inzetperiode van een EMR-beveiligingsinrichting. Naargelang hoe getest wordt, kan men besluiten dat een veldtoestel nagenoeg dezelfde kwaliteit heeft als een nieuw veldtoestel.

Er zijn testmethodes die ervoor zorgen dat je gemakkelijker kan testen, maar deze hebben niet de kwaliteit van een totale test. Het is belangrijk om het testprogramma bij het ontwerp vast te leggen. Bij de keuze van Prior Use devices ligt het testinterval vast; bij gebruik van gecertificeerde toestellen kan het testinterval en de wijze van testen anders gekozen worden.

Periodiek testen van Prior Use devices

NE93 maakt gebruik van een interval van 8.760 uren om de PFD_{avg}-waarden vast te leggen.

Als er gebruik gemaakt wordt van de Prior Use devices, dan dienen de instrumenten strikt genomen binnen een interval van 8.760 uren gecontroleerd te worden.

Een beperkte afwijking is toegelaten om testen te laten uitkomen met een geplande stilstandstijd. Men moet zich ervan bewust zijn dat uitstel van enkele maanden niet toegelaten is. Deze beperkingen moeten in acht genomen worden bij het inplannen van bedrijfsstilstanden.

Volgens NE93 en TS30-0000 wordt ervan uitgegaan dat na de periodieke test de kwaliteit terug is zoals een nieuw veldtoestel.

De kwaliteit van de periodieke testen dient maximaal te zijn, zodat aangenomen kan worden dat een veldtoestel na een test nagenoeg dezelfde kwaliteit heeft als een nieuw veldtoestel.

Denk aan:

- controle van Pt100's in een gekalibreerde verwarmingskamer;
- flow door een flowmeter met een gekalibreerde referentiemeter;
- opdrukken van drukmetingen met een gekalibreerde drukvoorgever;
- onderdompelen van sondes in een vloeistof/vaste stof.

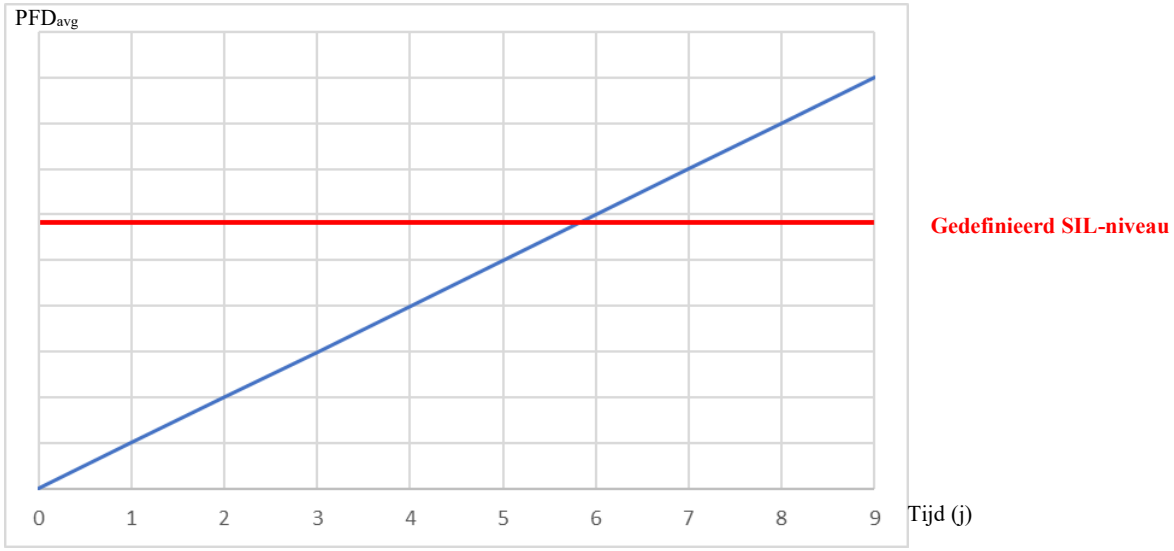
Periodiek testen van gecertificeerde toestellen

Bij het gebruik van gecertificeerde toestellen of de combinatie van gecertificeerde en Prior Use devices, is men vrij om het testinterval te bepalen. De berekening zal dan uitwijzen of dit testinterval acceptabel is.

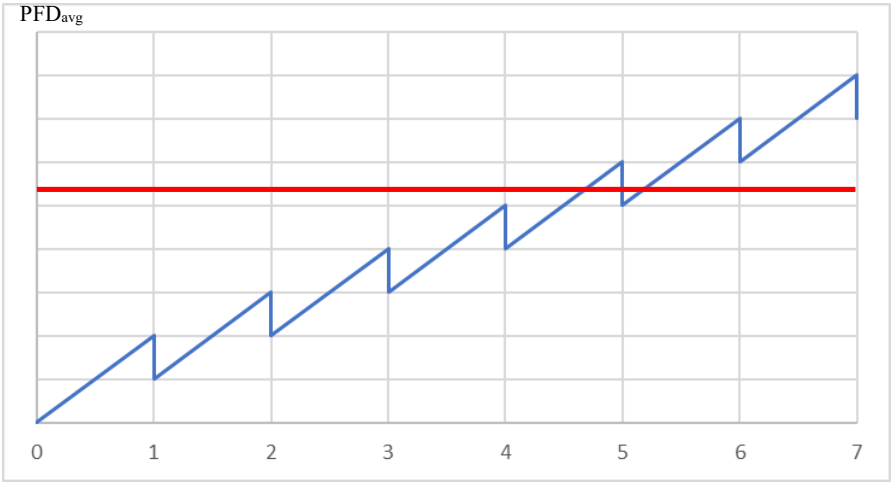
Merk op: bovenstaande tekst zal mogelijk de interesse wekken om meer de berekeningsmethode toe te passen en zo testintervallen uit te stellen. De kans is reëel dat bij het gebruik van berekende kringen er extra veldinstrumenten geïnstalleerd moeten worden door verhoging van de HFT-waarde. Hierdoor zullen er meer veldinstrumenten geïnstalleerd moeten worden om de EMR-beveiligingsinrichtingen te kunnen bouwen conform de gehanteerde normen.

Grafische voorstelling a.d.h.v. voorbeelden van invloed testkwaliteit en frequentie

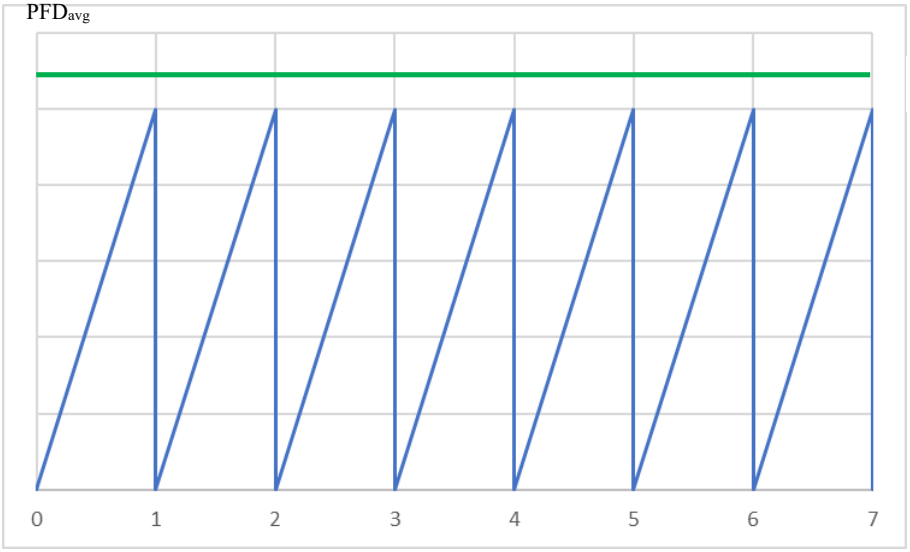
EMR-beveiligingskring wordt niet getest in de tijd.



EMR-beveiligingskring wordt jaarlijks getest maar niet met maximale kwaliteit.



EMR-beveiligingskring wordt jaarlijks getest met een maximale kwaliteit.



Technologische hulpmiddelen voor periodieke testen in geval van berekende methode

Partial Stroke Testing van ventielen

Bij een partial stroke-test zal een klepstandsteller de stand van een ventiel voor een bepaalde slag doen verplaatsen. De bijhorende inspanning van de aandrijving wordt in kaart gebracht om te controleren of dit nog loopt zoals bij indienstneming.

Een partial stroke-test heeft bv. een testkwaliteit (PTC) van 50 %, d.w.z. dat na een bepaald aantal partial stroke-testen toch een volledige test gedaan moet worden van het desbetreffende ventiel. Hiermee kan het uitbouwen van een ventiel uitgesteld worden.

Diagnose en gezondheidschecks

Vele fabrikanten van sensoren zetten in op moderne diagnosemethodes. Veldinstrumenten hebben vaak intern verschillende sensoren die data verzamelen over de toestand van het toestel. Met interfaces kunnen dan rapporten gegenereerd worden die de kwaliteit en de gezondheid van het veldtoestel documenteren. Mogelijke evoluties zijn dat deze rapporten ook geaccepteerd worden om te dienen als een periodiek testrapport.

Indien dit soort technologieën geïmplementeerd worden, dient men steeds op rekenbasis de PTC te verifiëren. Gaandeweg zullen deze technologieën meer plaats gaan vinden in de periodieke testen.

Bijlage 1. Bepaling van de categorie en uitvoeringseisen Risk Matrix

EMR / FORM / 0540: Bepaling van de categorie en de uitvoeringseisen

Pagina 1 van 2 EMR / FORM / 0540 / 000	EMR-beveiligingssysteem Bepaling van de categorie en de uitvoeringseisen	EVONIK Leading Beyond Chemistry

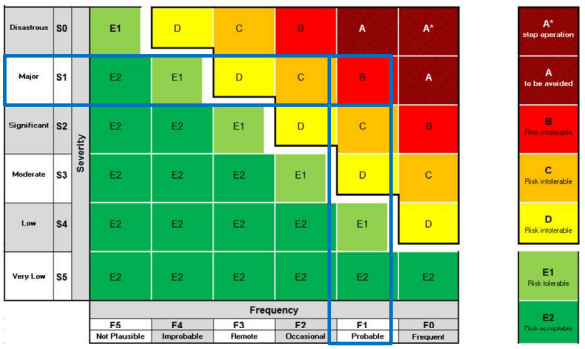
De bepaling van de categorie van een EMR-beveiligingssysteem volgt uit het veiligheidsgesprek.
De resultaten hiervan zijn op de volgende bladzijde verduidelijkt.

Eenheid	Procesdeel	Te beschermen apparaat	Datum
Bv. AC/MC	Bv. Rein AC-destillatie	Bv. 5501	xx/xx/xxxx

Het EMR-beveiligingssysteem beantwoordt aan volgende wetten, eisen en richtlijnen.

BTD 11-1000	Evonik Process Safety Concepts
TS 30-0000	Evonik Technical Standard: Funktionale Sicherheit mit Mitteln der Prozessleittechnik
Instructie Antwerpen: VEI-RB / INS / 535	Beveiliging van installaties d.m.v. EMR-technische maatregelen
DIN EN 61511	Functional Safety for Process Industry
VDI/VDE 2180	Sicherung von Anlagen der Verfahrenstechnik mit Mitteln der Prozessleittechnik

Bepaling van de risicoklasse



Gevolg:	S1
Frequentie:	F1
Risicoklasse:	B

Pagina 2 van 2 EMR / FORM / 0540 / 000	EMR-beveiligingssysteem Bepaling van de categorie en de uitvoeringseisen	EVONIK Leading Beyond Chemistry

Procesparameter	*Pressure*
Type afwijking	*Hoog / Laag / Geen / …*
Oorzaak	*Falen regelkring / Handventiel gesloten / …*
Finale gevolg	*Schade aan tank met vrijzetting toxisch gas / explosie / …*
Zwaarte (S)	*S1*
S-verklaring	*Korte motivering waarop "S" gebaseerd is*
Frequentie (F)	*F1*
F-verklaring	*korte motivering waarop "F" gebaseerd is*
Risicoklasse	*B*

Maatregelen voor risicoreductie

Maatregel nr.:	Graad van maatregel	Uitleg
1	*C*	*SIL2 EMR-beveiliging: drukmeting op tank en sluit toevoerleidingen xxx en yyy*
2	*D*	*Checklijst periodieke controlerondgang*
3	*E1*	*Onafhankelijke drukmeting op de tank met hoog alarm*

Opmerkingen

	Naam	*Handtekening*	*Datum*
Projectverantwoordelijke			
VOE			
Veiligheidsdienst			
Bedrijfsingenieur			
M&R-verantwoordelijke			

Bijlage 2. Verificatie van montage en configuratie

EMR / FORM / 0548: EMR-controleformulier voor montage en configuratie van EMR-instrumenten. Dit document bevat standaardformulieren voor volgende veldinstrumenten: FI, LI, LS, TI, PI, HS en CV.

Pagina 1 van 1 **EMR / FORM / 0548 / 000**			**EMR-installatie controleformulier:** **Montage en configuratie van EMR-instrumenten: FI**		EVONIK Leading Beyond Chemistry
Eenheid			**Deelinstallatie / apparaat**		**Positienummer**
Eerste indienstneming	☐		**Vervanging**	☐	**ATEX** ☐
	Te controleren?	**OK**	**Niet OK**	**Montage**	
1.	☐	☐	☐	Doorstroomrichting correct	
2.	☐	☐	☐	Display van toestel horizontaal afleesbaar	
3.	☐	☐	☐	Display goed bereikbaar, afleesbaar	
4.	☐	☐	☐	Positienummer op toestel en op kabels, decabon (2-zijdig)	
4.	☐	☐	☐	Controle isolatie of tracing procesdelen (bv. waterslot druksensor)	
5.	☐	☐	☐	Alle wartels goed aangedraaid	
6.	☐	☐	☐	Aarding aangesloten aan toestel (van toepassing als externe aardingsklem aanwezig is)	
7.	☐	☐	☐	Kabelbanen geaard	
8.	☐	☐	☐	Labels aangebracht van keuringsplichtig toestel (KMB, CO_2-monitoring, energiemeting, Z, ...)	
	Te controleren?	**OK**	**Niet OK**	**Configuratie**	
9.	☐	☐	☐	Eenheden: uitgang op toestel hetzelfde als ingang van PLS	
10.	☐	☐	☐	Omschakeling totalizer / meetwaarde op display uitgeschakeld op toestel	
11.	☐	☐	☐	Controle van demping (in sec.) ingesteld in toestel	
12.	☐	☐	☐	Controle van waarde-uitsturing bij fout (min./max.)	
13.	☐	☐	☐	Positienummer in software van toestel (HART)	
14.	☐	☐	☐	Meetbereik uitgang op toestel hetzelfde als ingang van sturing	
15.	☐	☐	☐	Meetbereik uitgang op toestel hetzelfde als op PLS-beeld	
16.	☐	☐	☐	Controle debietsonderdrukking juist ingesteld in toestel	
17.	☐	☐	☐	Looptest uitgevoerd, 4-8-12-1-20 mA voorgeven in toestel en controle op PLS	
18.	☐	☐	☐	Juiste gegevens op loopschema, aanpassingen doorgeven aan EMR-Eng.	
19.	☐	☐	☐	Communicatiemethoden ingeschakeld (HART, wifi, bluetooth, ...)	
20.	☐	☐	☐	Vergrendeling parameters actief (bij Z-functies)	
Opmerkingen					

	Naam	*Handtekening*	*Datum*
Uitvoerder controle			
M&R-verantwoordelijke			

Bijlage 3. Validatierapport van de montage

EMR / FORM / 0541: Als de montage van de veldinstrumenten gecontroleerd is, dient het validatierapport ingevuld te worden.

Pagina **1** van **1** EMR / FORM / 0541 / 000	**EMR-beveiligingsinrichting** **Validatierapport: Montage**	EVONIK Leading Beyond Chemistry

Eenheid	**Procesdeel**	**Te beschermen apparaat**	**Datum**

Onderstaande EMR-posities behoren tot deze EMR-beveiligingsinrichting:

EMR-positienummer	**Categorie**	**Opmerking**

1. Montage-afname

_____ Datum

_____ Handtekening Montageverantwoordelijke

_____ Datum

_____ Handtekening Vakafdeling

Opmerking:
Dit document wordt ingevuld per EMR-beveiligingsinrichting. Ieder veldtoestel wordt opgesomd in de beschikbare regels. Dit document wordt enkel goedgekeurd als alle instrumenten aan de voorgeschreven voorwaarden voldoen. Hanteer formulier EMR / FORM / 0548 waar de montagevoorwaarden beschreven staan.

Bijlage 4. Validatierapport van de configuratie

EMR / FORM / 0542: Als de configuratie van de veldinstrumenten gecontroleerd is, dient het validatieformulier ingevuld te worden.

Pagina **1** van **1** EMR / FORM / 0542 / 000	**EMR-beveiligingsinrichting** **Validatierapport: Configuratie**	EVONIK Leading Beyond Chemistry

Eenheid	**Procesdeel**	**Te beschermen apparaat**	**Datum**

Onderstaande EMR-posities behoren tot deze EMR-beveiligingsinrichting:

EMR-positienummer	**Categorie**	**Opmerking**

1. Configuratie-afname

_____ Datum

_____ Handtekening Montageverantwoordelijke

_____ Datum

_____ Handtekening Vakafdeling

Opmerking:
Dit document wordt ingevuld per EMR-beveiligingsinrichting. Ieder veldtoestel wordt opgesomd in de beschikbare regels. Dit document wordt enkel goedgekeurd als alle instrumenten aan de voorgeschreven voorwaarden voldoen. Hanteer formulier EMR / FORM / 0548 waar de configuratievoorwaarden beschreven staan.

Bijlage 5. Verificatie van de functionaliteit

Test van subsystemen

Stel de nodige documenten op die de functionele uitvoering van de EMR-beveiligingsinrichting beschrijven om deze te controleren. EMR-functieplannen kunnen een goede basis vormen voor deze logische test.

Kop-staarttest

EMR / FORM / 0543: Verificatie logische functionaliteit van de EMR-beveiligingsinrichting

Pagina 1 van 1 **EMR / FORM / 0543 / 000**			**EMR-beveiligingssysteem** **Verificatie logische functionaliteit EMR-beveiligingsinrichting**				EVONIK Leading Beyond Chemistry		
Eenheid			**Deelinstallatie**					**R&I-nummer(s):**	
Onderstaande EMR-posities maken deel uit van de EMR-beveiligingsinrichting.									
	Nummer	**Functie**	**Sensor**	**Actor**	**Type actie (sensor)**	**Schakel-punt**	**Veldtoestel**	**Grenssignaalgever**	**Max. reactietijd actor (s)**
1.	**1234.56**	**LICZSA**	☑	☑	ZA+	85%	VEGA: VEGAFLEX 86	P+F: KFD2-STC4-1.2o	-
2.	**6543.21**	**PIC(Z)SA**	☐	☑	-	-	Samson 3241 + Samsomatic 3963	P+F: HID 2037	5
3.			☐	☐					
4.			☐	☐					
5.			☐	☐					
6.			☐	☐					
7.			☐	☐					
8.			☐	☐					
9.			☐	☐					
10.			☐	☐					
11.			☐	☐					
12.			☐	☐					
Signaalverwerking									
Maximale reactietijd SIF (s)			**20 s**						
Beschrijving signaalverwerking									
- Bij het bereiken van LZ+ van 1234.56 zal het ventiel 6543.21 met een tijdsvertraging van 5 s sluiten. - Bijkomend zullen ventielen 3412.56 en 4365.12 sluiten via PLS (niet SIF).									
Bijhorende documenten									
Functie-plannen: PC6543.21, SM_65_1, YS3412.56, TC4365.12									
Andere:									
Test-voorschrift	- Laat het niveau van de tank stijgen tot boven het Z+-schakelpunt. - Controleer het ingangssignaal op HIMA bij bereiken Z+. - Bij het bereiken van het schakelpunt zal er een timer van 5 s starten.						- Na de timer zal het uitgangssignaal van ventiel 6543.21 naar 0 gaan. - Het ventiel zal dichtschakelen. - Laat het niveau zakken onder Z+.		
Opmerkingen									

	Naam	*Handtekening-paraaf*	*Datum*
Uitvoerder controle			
M&R-verantwoordelijke			
VOE / PV			

Bijlage 6. Validatie van de functionaliteit

EMR / FORM / 0544: Validatierapport: SIF

Pagina **1** van **1** EMR / FORM / 0544 / 000	**EMR-beveiligingsinrichting** **Validatierapport: SIF**	EVONIK Leading Beyond Chemistry

Eenheid	**Procesdeel**	**Te beschermen apparaat**	**Datum**

Onderstaande EMR-posities behoren tot deze EMR-beveiligingsinrichting:

EMR-positienummer	**Categorie**	**Opmerking**

1. Functionele afname

_____ Datum

_____ Handtekening Montageverantwoordelijke

_____ Datum

_____ Handtekening Vakafdeling

Opmerking:
Dit document wordt ingevuld per EMR-beveiligingsinrichting. Ieder veldtoestel wordt opgesomd in de beschikbare regels. Dit document wordt enkel goedgekeurd als de volledige EMR-beveiligingsinrichting functioneert zoals beschreven staat in de ontwerpdocumenten. Raadpleeg EMR / FORM / 0543 om de volledige omschrijving van de functietest te raadplegen.

Bijlage 7. Periodiek testen van een SIF

Pagina 1 van 1 **EMR / FORM / 0545 / 000**	**EMR-beveiligingssysteem** **Rapport periodieke controle**	EVONIK Leading Beyond Chemistry

Eenheid		**Deelinstallatie**		**R&I-nummer(s):**	

Onderstaande EMR-posities maken deel uit van de EMR-beveiligingsinrichting.

	Nummer	Functie	Sensor	Actor	Type actie (sensor)	Schakel-punt	Veldtoestel	Grenssignaalgever	Max. reactietijd actor (s)
1.	1234.56	LICZSA	☑	☐	ZA+	85 %	VEGA: VEGAFLEX 86	P&F: KFD2-STC4-1.2o	-
2.	6543.21	PIC(Z)SA	☐	☑	-	-	Samson 3241 + Samsomatic 3963	P&F: HID 2037	5
3.			☐	☐					
4.			☐	☐					
5.			☐	☐					
6.			☐	☐					
7.			☐	☐					
8.			☐	☐					
9.			☐	☐					
10.			☐	☐					
11.			☐	☐					
12.			☐	☐					

Testfrequentie:	**jaarlijks**	**Keuring in stilstand?**	**Ja:** ☐	**Nee:** ☐

Signaalverwerking

Beschrijving signaalverwerking

- Bij het bereiken van LZ+ van 1234.56 zal het ventiel 6543.21 met een tijdsvertraging sluiten.
- Bijkomend zullen ventielen 3412.56 en 4365.12 sluiten via PLS (niet SIF).

Bijhorende documenten

Functie-plannen: PC6543.21, SM_65_1, YS3412.56, TC4365.12

Andere: (Gedetailleerd testprotocol, werkpakket, …)

Test-voorschrift	- Laat het niveau van de tank stijgen tot boven het Z+-schakelpunt. - Controleer het ingangssignaal op HIMA bij bereiken Z+. - Bij het bereiken van het schakelpunt zal er een timer van 5 s starten.	- Na de timer zal het uitgangssignaal van ventiel 6543.21 naar 0 gaan. - Het ventiel zal dichtschakelen. - Laat het niveau zakken onder Z+.

Controle op inbouw door operations na Z-functietest? ☐	**Sensor(en)?** ☐	**Actor(en)?** ☐

Opmerkingen

	Naam	*Handtekening-paraaf*	*Datum*
Uitvoerder operations check			
Uitvoerder periodieke test			
M&R-verantwoordelijke			

Bijzonderheden:

- Het veld “andere” kan gebruikt worden om extra referenties of documenten te koppelen. Voor complexe EMR-beveiligingskringen zal dit document onvoldoende zijn om een volledig en kwalitatief testvoorschrift te noteren. Hiervoor kan dan een bijkomend document opgesteld worden, specifiek om deze EMR-beveiligingsinrichting te controleren. De naam van dit bijkomend document kan dan vermeld worden in dit vrij veld.

- **Controle door operations**: op het testformulier **kan** gemarkeerd worden of de EMR-instrumenten een visuele controle nodig hebben na het uitvoeren van de test. Dit kan zinvol zijn als de instrumenten gemonteerd worden van de procesinstallatie voor de periodieke test. Operations dient dan te controleren dat de instrumenten terug ingebouwd zijn. Indien dit veld **JA** wordt gemarkeerd, dient er ook een naam en handtekening van iemand van operations geplaatst te worden. Indien **NEE**, dan blijft dit veld open.
- De uitvoerder van de periodieke test (EMR) ondertekent het document niet vooraleer operations de controle gedaan heeft.

Bijlage 8. Validatie van architectuur – faalkans– systematic coverage

Pagina 1 van 1 **EMR / FORM / 0546 / 000**	**EMR-beveiligingssysteem** **Validatie architectuur - faalkans - systematic coverage**			EVONIK Leading Beyond Chemistry
Eenheid		**Deelinstallatie**		**R&I-nummer(s):**
Beschrijving veiligheidsfunctie				
	1. Architectuur			
	SIL-level		**Demand Mode**	
	Sensorsubsysteem volgens norm of standaard			
	Actorsubsysteem volgens norm of standaard			
	Naam	*Handtekening-paraaf*	*Datum*	
Ontwerper				
M&R-verantwoordelijke				
	2. Faalkans			
	SIL-level		**Demand Mode**	
	Faalkansberekening gebaseerd op norm of standaard			
	Faalkans sensorsubsysteem			
	Controller incl. IO-kaarten			
	Faalkans actorsubsysteem			
	Totale faalkans			
	Naam	*Handtekening-paraaf*	*Datum*	
Ontwerper				
M&R-verantwoordelijke				
	3. Systematic coverage			
	SIL-level			
	Systematic Coverage gebaseerd op norm of standaard			
	Naam	*Handtekening-paraaf*	*Datum*	
Ontwerper				
M&R-verantwoordelijke				

Bijlage 9. Uit- en herindienstnemingsformulier

Pagina **1** van **1** EMR / FORM / 0547 / 000	**EMR-beveiligingssysteem (Z-functie)** **Rapport: Uitdienst- en herindienstneming**	EVONIK Leading Beyond Chemistry

Eenheid: **Procesdeel:**	**Ordernr.:** **Overbruggingsformulier: nr.**	**EMR-pos.nr.:**

Bevestiging van de opdracht tot uitdienstneming:
(De opdracht moet door de eenheid schriftelijk op dit formulier bevestigd worden met opgave van de reden en de genomen vervangingsmaatregel.)

Reden uitdienstneming: ……..

Vervangingsmaatregel: ……

……

……

_____ Datum _____ Tijd _____ Naam + Handtekening Bedrijfsverantwoordelijke

Uitdienstneming beveiliging:

A. ☐ Meetwaarde vastzetten / schakelwaarde verzetten in niet-Hima (bv. Mutec, via Hart, …)

B. ☐ Meting / ventiel afkoppelen (uitbouw)

C. ☐ Analysemeting in spoeling

D. ☐ Meetwaarde vastzetten in SSPS (Hima, Siemens, PCS, …)

E. ☐ (Magneet)ventiel afkoppelen (ventiel blijft ingebouwd)

→ zie ook steeds maatregelen standaard brugformulier EMR

Opmerkingen: ……..

……

_____ Datum _____ Tijd _____ Naam + Handtekening uitvoerder EMR

Herindienstneming beveiliging:

A / B / C → **Functionele controle** volgens controlevoorschrift is **noodzakelijk.**

☐ Overbrugging weggenomen en functionele controle met controlevoorschrift uitgevoerd
→ Functionele controle is geprotocolleerd via het gebruikelijke document.

☐ Overbrugging weggenomen zonder functionele controle volgens controlevoorschrift
→ **Functionele controle is nog uit te voeren!**

D / E → Functionele controle is niet vereist.

☐ Overbrugging weggenomen

_____ Datum _____ Tijd _____ Naam + Handtekening uitvoerder EMR

_____ Datum _____ Tijd _____ Naam + Handtekening Bedrijfsverantwoordelijke

Bijlage 10. Safety Requirement Specification

Bedrijf	Plaats	PSS	Datum	SIF-Nr.
Evonik	Antwerpen	PSS ACMC	09/02/21	**SIF0001**

Installatie	Deelinst./appar.	Gevolgen	Frequentie	Risicoklasse	SIL	Demand-Mode	Maatregelnr.
ACMC	5101	S1	F1	B	SIL3	LOW	1.43.1.1.1.1

Afte venden scenario

Barsten van de reactor wegens te hoge druk

Uitwerking van veiligheidsfunctie

Sluiten van stoom en reactiegas bij hoge druk

Verwijzing naar externe documenten

Procesbeschrijving	Procesbeschrijving nr.5110
procedure	Procedure ACMC/INS/123
Vervangingsmaatregelen	Geen vervangingsmaatregelen

Sensorarchitectuur	actuarchitectuur	testinterval
1oo2 (1oo2)	3oo3 (1oo2)	jaarlijks

overbruggingen	opstart	afstellen	testen	andere
	nein	ja	ja	ja

Beschrijving van het overbruggingsconcept

F-Meting bij afstellen

Afwijking bij de reactietijd van de EMR-beveiligingsinrichting?	nein
Gemiddelde reactietijd van de EMR-beveiligingsinrichting (in s)?	21

Sensor	nummer	functie	type	grenswaarde	meettolerantie	reactietijd	demping	tijdsvertraging	faalsignaal
A	5101.01	PIZSA	ZA+	5 bar	3%	5	0	0	21 mA
B	5101.02	PIZSA	ZA+	5 bar	3%	5	0	0	21 mA
C	5101.03	FIZA	ZA-	100L/h	3%	5	0	0	3,2 mA
D	5101.04	FIZA	ZA-	100L/h	3%	5	0	0	3,2 mA
E	5101.05	FIZA	ZA-	100L/h	3%	5	0	0	3,2 mA
F	5101.06	FIZA	ZA-	100L/h	3%	5	0	0	3,2 mA
G									
H									
I									
J									

bijzonderheden bij Sensoren

Drukmeting sensor A moet N2 gespoeld worden om polymeeraanlading tegen te gaan (sensor C en D). Drukmeting sensor B moet met N2 gespoeld worden om polymeeraanlading tegen te gaan (sensor E en F)

MTTR	Aktie bij sensorfalen (<3,6 mA)	Aktie bij sensorfalen (>21mA)
8h	activering SIF	Overbrugging van 8h

Concept / vervangmaatregelen bij MTTR

MTTR-concept

Afwijking van het (standaard) manuele ontregelconcept?

afwijkend ontregelconcept

Actor	nummer	functie	veiligheidsst.	DN	min. schakeltijd	max. schakeltijd	lekdichtheid is relevant	dichtheidsklasse	freq. dichtheidstest
A	5110.01	YZ	ZU	25	0	4	neen	IV	
B	5110.02	YZ	ZU	50	0	4	neen	IV	
C	5111.01	YZ	ZU	80	0	6	neen	IV	
D	5111.02	YZ	ZU	100	0	10	neen	IV	
E	5112.01	YZ	ZU	150	0	10	neen	IV	
F	5112.02	YZ	ZU	200	0	15	neen	IV	
G									
H									
I									
J									

Bijzonderheden bij actoren

xx

Naam	Functie	Datum	Handtekening
Peter Vogel	PV	1/01/2000	
Maximilian Mustermann	Moderator	1/01/2000	
Paul Mustermann	PM	1/01/2000	
Maximilian Mustermann	PI	1/01/2000	
Peter Ludwig Testmann	PLT	1/01/2000	
Weitere Teilnehmer	?	1/01/2000	