HOGESCHOOL UTRECHT

ACTEMIUM

Afstudeerverslag

Actemium, Veghel

Veiligheidssysteem EduLab ProcessCell

Auteur:	M.Leijten
Studentnr:	1604084
Datum:	15-dec-14
Cursuscode:	TEET-AGBACHEX-14

Afstudeerverslag

Veiligheidssysteem EduLab ProcessCell

Auteur: M.Leijten
Studentnr: 1604084

Revisienr: V1.0
Datum: 15-dec-14
Plaats: Veghel
Cursus: Afstuderen
Cursuscode: TEET-AGBACHEX-14

Bedrijfsbegeleider: Bart Verburg
Schoolbegeleider: Albert Moes

De ingeleverde hardcopy van dit verslag met revisienummer V1.0 is gelijk aan de met voldoende beoordeelde digitale versie met revisienummer V1.0.

Revisiebeheer en goedkeuring

Versie	Datum	Aanpassingen	Naam
V0.0	03-10-2014	Afstudeerverslag opstellen	M.Leijten
V1.0	08-12-2014	Aanpassen concept na opmerkingen Albert Moes	M.Leijten

Tabel 0-1: Revisiebeheer

Actemium	Naam	Functie	Handtekening / Datum
Opgesteld door	Maartje Leijten	Stagiair	19-08-2014
Goedgekeurd door			

Tabel 0-2: Goedkeuring bedrijf

Opdrachtgever	Naam	Functie	Handtekening / Datum
Goedgekeurd door			
Goedgekeurd door			
Geautoriseerd door			

Tabel 0-3: Goedkeuring opdrachtgever

Algemene gegevens

Afstudeerster / auteur	:	Maartje Leijten
Adres	:	Gitaarstraat 12
Postcode en plaats	:	5702 SW Helmond
Land	:	Nederland
Telefoonnummer	:	0652689069
Studentnummer	:	1604084
E-mail adres	:	Maartje.leijten@student.hu.nl
Cursus	:	Afstuderen
Cursuscode	:	TEET-AGBACHEX-14
Opleiding	:	Industriële Automatisering
Stageperiode	:	18-08-2014 t/m 23-01-2015

Stage bedrijf	:	Actemium
Adres	:	Costerweg 5
Postcode en plaats	:	5466 AM Veghel
Land	:	Nederland
Telefoonnummer	:	041349999
Bedrijfsbegeleider	:	Bart Verburg
E-mail adres	:	Bart.verburg@actemium.nl
Telefoonnummer	:	01413349833
Bedrijfsondersteuning	:	Johan van Lent
E-mail adres	:	Johan.vlent@actemium.nl
Telefoonnummer	:	01413349828

Opleidingsinstituut	:	Hogeschool Utrecht
Adres	:	Oudenoord 700
Postcode en plaats	:	3513 EX Utrecht
Land	:	Nederland
Telefoonnummer	:	0884818283
1e examinator	:	Erwin van akkeren
E-mail adres	:	Erwin.vanakkeren@hu.nl
Telefoonnummer	:	0884818179
2e examinator / schoolbegeleider	:	Albert Moes
E-mail adres	:	Albert.moes@hu.nl
Telefoonnummer	:	0884818643

Samenvatting

De opdracht waarvoor dit verslag is geschreven, is het toevoegen van een veiligheidssysteem aan een procesinstallatie binnen Actemium. Daarnaast moeten er standaard documenten gemaakt worden die helpen bij het ontwerpen van een veiligheidssysteem. Het veiligheidssysteem moet namelijk voldoen aan de IEC61511 norm. In die norm is een stappenplan weergegeven voor het engineeren van een veiligheidssysteem. Omdat Actemium dit soort projecten steeds vaker van klanten krijgt, worden de standaarddocumenten afgestemd op de eisen van de norm, maar ook aan de eisen en wensen van Actemium, zodat zij die documenten kan gebruiken in haar toekomstige projecten.

Het stappenplan uit de IEC61511 norm is gecombineerd met de methode uit projectmanagement van Roel Grit, waardoor er een gefaseerd stappenplan is ontstaan. De analyse betreft het onderzoeken van de norm en de installatie. Het ontwerp betreft het maken van de standaarddocumentatie van de risicoanalyse, de allocatie van veiligheidsfuncties, het eisenpakket van het veiligheidssysteem en de validatie documenten (FAT / SAT). Daarna worden deze documenten gebruikt bij het ontwerpen van het veiligheidssysteem, waarbij naast het invullen van deze documenten ook de tekeningen en berekeningen worden gemaakt die van belang zijn.

Het veiligheidssysteem dat wordt toegevoegd is bedoeld om de volgende drie risico's te reduceren:

1. Het te snel oplopen van de temperatuur bij een exotherme reactie in een reactortank;
2. Het te hoog worden van de druk in een reactortank;
3. Het te hoog worden van het niveau in een watertank.

Voor deze risico's worden er drie veiligheidsfuncties toegevoegd die bestaan uit een druk-, temperatuur- of niveausensor, een veiligheidsPLC en in totaal acht veiligheidsventielen die ervoor moeten zorgen dat bepaalde leidingen afgesloten worden in geval van gevaar.

Actemium is aanbevolen om in ieder geval de norm te blijven volgen en de standaard documenten aan te passen bij een uitgave van de nieuwe norm. Daarnaast zijn er bepaalde methodieken gekozen waarop de standaarddocumenten zijn gebaseerd. Het kan goed zijn om ook standaarddocumenten te maken van andere methodieken zodat zowel Actemium als hun klanten de keuze hebben in de verschillende methodieken. Ten aanzien van het veiligheidssysteem geldt dat deze na toevoeging (maar) drie risico's reduceert, terwijl er veel meer te reduceren zijn in de installatie. Het kan dus verstandig zijn om ook de andere risico's te onderzoeken en te reduceren met de documentatie die gemaakt is in dit project.

Voorwoord

Mijn naam is Maartje Leijten uit Helmond en ik ben op dit moment bezig met de afstudeerfase van de opleiding Industriële automatisering te Utrecht. Voor deze afstudeerfase is het de bedoeling dat ik een HBO-waardige en geschikte opdracht bij een bedrijf ga uitvoeren om hiermee aan te tonen dat ik het niveau van een HBO ingenieur heb. De opdracht die mij is aangeboden door Actemium is het toevoegen van een veiligheidssysteem aan een procesinstallatie binnen Actemium. Een veiligheidssysteem zou ervoor moeten zorgen dat de installatie naar een veilige toestand gebracht wordt als de besturing niet meer werkt zoals het hoort. Deze opdracht vind ik interessant en uitdagend genoeg om als afstudeeropdracht te gebruiken, vooral omdat mijn interesse al bij de procesautomatisering lag en ik al vaker met veiligheid te maken heb gehad binnen projecten. Vandaar dat ik deze opdracht heb aangenomen om voor mijn afstudeerstage te gebruiken.

Hierbij wil ik graag de gelegenheid nemen om Actemium te bedanken voor de mooie en uitdagende opdracht die ze mij gegeven hebben. Ook wil ik Bart Verburg bedanken voor de begeleiding vanuit Actemium, Johan van Lent voor de ondersteuning bij de normen en Hans van Wijk voor de ondersteuning bij de installatie. Ook wil ik graag de Hogeschool Utrecht en vooral Albert Moes en Erwin van Akkeren bedanken voor de begeleiding vanuit de Hogeschool Utrecht.

Maartje Leijten
Veghel, december 2014

Inhoudsopgave

Inleiding

Voor u ligt het afstudeerverslag dat is gemaakt naar aanleiding van het afstudeertraject van de opleiding industriële automatisering, Hogeschool Utrecht. Dit verslag geeft inzicht in het onderzoek, het ontwerpproces en de realisatie van het project veiligheidssysteem Edulab ProcessCell. Het afstudeertraject is uitgevoerd bij Actemium in Veghel.

De opdracht van dit project is het engineeren van een veiligheidssysteem dat voldoet aan de geldende normen. Daarnaast moeten er standaarddocumenten gemaakt worden die gebruikt kunnen worden bij het ontwerpen van een veiligheidssysteem. Voor deze afstudeeropdracht zullen de volgende stappen doorlopen moeten worden: onderzoek naar de geldende normen, de bestaande installatie en besturing; ontwerpen van standaarddocumenten; ontwerpen van het veiligheidssysteem met behulp van die standaarddocumenten; implementeren van het veiligheidssysteem; testen en valideren van de resultaten; vastleggen van alle benodigde documentatie.

In het afstudeerverslag zal allereerst kennis gemaakt worden met het bedrijf, de organisatie in het project en de projectopdracht. Daarna worden er een aantal onderzoeken beschreven en het ontwerp met de gemaakte ontwerpkeuzes weergegeven. Vervolgens wordt weergegeven hoe de realisatie van het volledige project verlopen is. Tot slot wordt het resultaat beschreven en wordt het project geëvalueerd met aansluitend de conclusies en aanbevelingen.

Vanuit de tekst zal verwezen worden naar bijlagen die in een apart document bijgevoegd zullen worden. Deze zijn voornamelijk bedoeld als aanvullende informatie of om beter inzicht in het project te krijgen. Daarnaast wordt er vanuit de tekst ook verwezen naar de gebruikte bronnen die van belang zijn geweest in dit project.

1 Het afstudeerbedrijf: Actemium

In dit hoofdstuk wordt ter kennismaking een korte beschrijving gegeven van VINCI (het moederbedrijf van Actemium), Actemium en het EduLab (fysieke leeromgeving binnen Actemium).

Vinci

Actemium is een onderdeel van het Franse bedrijf VINCI. VINCI is actief in verschillende markten, waaronder Motorways, Constructions en Energies. De markt Energies is onderverdeeld in Industry, Infrastructures, Telecommunications en de Service sector. Actemium is een van de zogenaamde 'brand names' (merknaam of handelsnaam) binnen de sector Industry (zie Afbeelding 1-1 en Afbeelding 1-2). De naam Actemium wordt gebruikt voor alle business units die zich met industriële processen bezighouden.

Afbeelding 1-1: VINCI indeling
("Actemium", Algemene presentatie Actemium nl - 2014 (intern document), 2014)

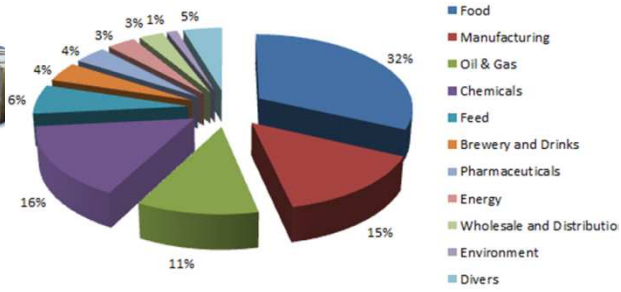
Afbeelding 1-2: VINCI Energies indeling
("Actemium", Algemene presentatie Actemium nl - 2014 (intern document), 2014)

Actemium

Actemium heeft wereldwijd ongeveer 300 business units verspreid over 35 landen, waaronder 21 in Nederland. De locaties van de vestigingen in Nederland zijn (onder andere): Assen, Amersfoort, Dieren, Dordrecht, Eindhoven, Goes, Veendam, Veghel, Zevenaar en Zwolle. Binnen Actemium wereldwijd werken ongeveer 19000 ingenieurs en technici waarvan 850 in Nederland. Actemium levert verschillende diensten aan klanten waaronder automatisering, engineering, onderhoud en installatie (zie Afbeelding 1-3). Daarnaast is Actemium actief in vele verschillende marktsegmenten waaronder food, manufacturing, oil & gas en chemicals (zie Afbeelding 1-4). De locatie in Veghel op de Costerweg 5 huisvest business units die onder andere de markten food, chemicals en pharmaceuticals bedienen.

De missie van Actemium is het helpen van haar klanten bij het behalen van concurrentievoordeel en het verbeteren van industriële prestaties. Hiervoor doet Actemium projecten van begin tot eind, dus vanaf de advisering en engineering tot aan de realisatie, inbedrijfstelling en het onderhoud. Het doel is dan ook om op maat gemaakte voorstellen te leveren aan de klant die uiteindelijk een langdurige samenwerking kunnen opleveren. ("Actemium", Over Actemium, 2014)

Afbeelding 1-3: Diensten Actemium
("Actemium", Algemene presentatie Actemium nl - 2014 (intern document), 2014)



Afbeelding 1-4: Marktsegmenten Actemium
("Actemium", Algemene presentatie Actemium nl - 2014 (intern document), 2014)

Het EduLab

Binnen het gebouw van Actemium in Veghel staat het EduLab. Dit lab is in 2001 opgezet met als doel om de techniek van vandaag ter beschikking te stellen aan studenten. De bedoeling was ook om echte installaties in het EduLab te zetten en geen modellen. Hiervoor is samenwerking gezocht met klanten, leveranciers en scholen om dit te voltooien. Hiervoor heeft Vanderlande Industries als eerste een sorteermachine geleverd (zie Afbeelding 1-5) en waren er grote plannen voor een machine uit de procesautomatisering. Die is vijf jaar later gebouwd (zie Afbeelding 1-6) waardoor studenten nu aan twee redelijk grote installaties kunnen werken om kennis te maken met en te oefenen in het vakgebied industriële automatisering. Er worden bijvoorbeeld cursussen gegeven voor Avans Hogeschool en er zijn speciale kijk- / kennismaakdagen voor leerlingen van het VMBO, de Havo en het VWO om ze nieuwsgierig te maken naar techniek. Ook kunnen ze op deze manier stagiairs en afstudeerders interessante opdrachten geven waarbij uiteindelijk iets fysiek opgeleverd wordt. De studenten zien dus wat ze automatiseren. (Achatot, EduLab, 2012)

Afbeelding 1-5: Edulab Xorter
(Achatot, EduLabXorter, 2012)

Afbeelding 1-6: EduLab ProcessCell
(Achatot, EduLabProcess, 2012)

2 Organisatie en werkwijze

Voordat op de inhoud van de opdracht wordt ingegaan (hoofdstuk 3), wordt in dit hoofdstuk de organisatie van het project weergegeven. Hier wordt beschreven hoe de communicatie, de goedkeuringen en de archivering geregeld worden binnen dit project.

2.1 Organisatie

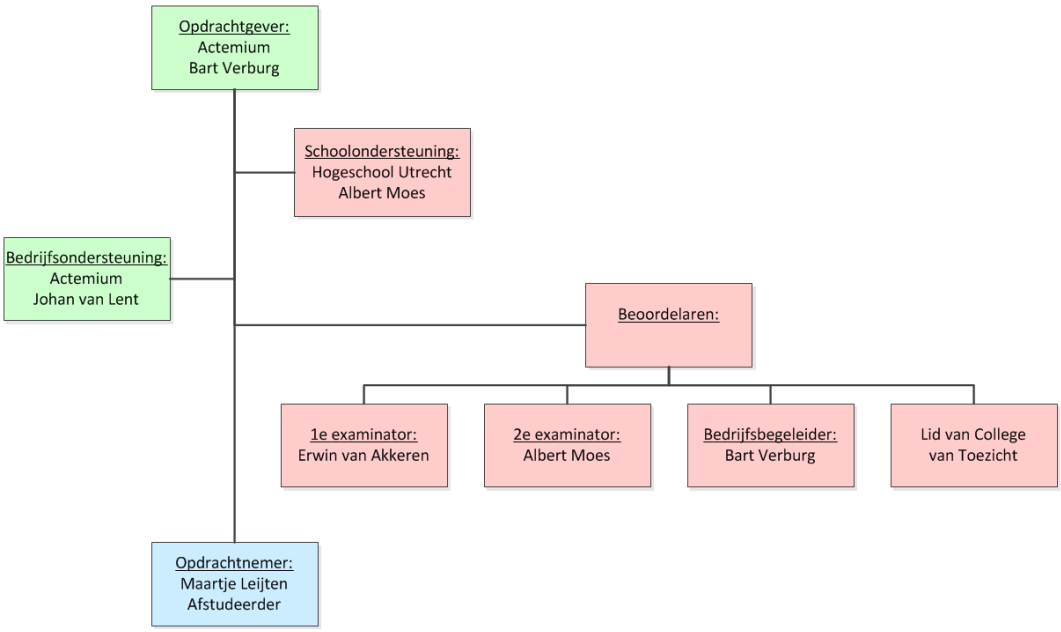
In Afbeelding 2-1 is te zien hoe de verdeling tussen de opdrachtgevers, de begeleiders en de opdrachtnemers is vormgegeven.

- De opdrachtgever is Bart Verburg, hij is tevens de bedrijfsbegeleider.
- Johan van Lent is een expert op het gebied van de IEC normen die horen bij de opdracht dus hij zal de afstudeerster ondersteunen tijdens het project.

Vanuit school is er een 1e examinator, een 2e examinator en een begeleider toegewezen.

- De 1e examinator is Erwin van Akkeren. Hij zal alleen betrokken zijn bij de beoordeling van verslagen, de presentatie en de verdediging.
- De 2e examinator en tevens begeleider is Albert Moes. Hij zal vanuit school ondersteunen tijdens het project. Ook hij is betrokken bij de beoordeling van verslagen, de presentatie en de verdediging.
- Het lid van College van Toezicht is nu nog niet bekend, maar deze zal te zijner tijd bekend gemaakt worden als de zitting ingepland is.

Alle rollen van dit project worden door de afstudeerster uitgevoerd. Dit betekent dat de afstudeerster zowel projectleider als uitvoerder is. Ook bij besprekingen en vergaderingen zal de afstudeerster zelf de notulen maken, de planning maken, de kostenprijsberekening uitvoeren, enzovoorts.



Afbeelding 2-1: Organisatie binnen de opdracht

2.2 Werkwijze

Communicatie

De wijze van communiceren tussen partijen die betrokken zijn in dit project zal afhangen van de betreffende partij. Tussen de afstudeerster en Hogeschool Utrecht zal de communicatie voornamelijk bestaan uit e-mail contact. Er is een aantal momenten waarop de schoolbegeleider uitgenodigd zal worden voor een bezoek aan Actemium om belangrijke zaken door te spreken. Tussen de afstudeerster en Actemium zal de communicatie voornamelijk mondeling zijn in de vorm van vergaderingen of korte vraagmomenten. Via e-mail is het mogelijk om een afspraak te maken voor de vergaderingen en die zullen voornamelijk gebruikt worden voor de oplevering van documenten of voor beslismomenten waarbij de opdrachtgever medebeslisser is in bepaalde zaken. Deze momenten, in totaal 15, worden als mijlpalen weergegeven in de planning (hoofdstuk 8).

Afspraken

Volgens de bedrijfsstandaard zal er eens per week een gesprek zijn over de voortgang van de stagiair. Dit wordt samen met alle andere stagiairs die in het bedrijf aanwezig zijn gedaan. Met de schoolbegeleider is de afspraak gemaakt dat er wekelijks een e-mail gestuurd wordt met daarin de voortgang en eventuele vragen. Verder geldt er een aanwezigheidsplicht van 40 uur per week tenzij er andere verplichtingen zijn, zoals afspraken met school of persoonlijke afspraken. Deze afspraken moeten ruim op tijd doorgegeven worden aan de begeleider. Werktijden zijn niet vooraf vastgelegd dus er is de mogelijkheid om in de ochtend tussen zeven uur en negen uur te beginnen. Wel is er vanuit Actemium aangegeven dat ze het liefst hebben dat stagiairs tot minimaal vier uur aanwezig zijn.

Revisiebeheer, goedkeuring en archivering

In het hoofdstuk Revisiebeheer en goedkeuring is Tabel 0-1 van dit document te zien. Hierin wordt bijgehouden wanneer er aanpassingen zijn gedaan, door wie die aanpassingen zijn gedaan en wat die aanpassingen inhouden. Omdat er een aantal momenten is waarop de bedrijfsbegeleider en de schoolbegeleider het document inzien, kan het voor komen dat daar een aantal aanpassingen uitkomt. Die zullen dan uiteindelijk terug te vinden zijn in het revisiebeheer. Wanneer het volledige document goedgekeurd is door (in dit geval) de begeleiders in plaats van de opdrachtgevers kunnen in Tabel 0-2 en Tabel 0-3 de naam, functie en datum ingevuld worden ter goedkeuring van het verslag. Het hoofdstuk Revisiebeheer en goedkeuring zal in elk document toegevoegd worden om het revisiebeheer bij te houden.

In het computernetwerk van Actemium is een aantal mappen aangemaakt waar alle documenten opgeslagen kunnen worden. Alle documenten die te maken hebben met school zullen in een map geplaatst worden die voor stagiairs is. Zo worden deze documenten bewaard voor andere stagiairs als voorbeeld wanneer de afstudeerstage klaar is. Alle documenten die gemaakt zijn voor het ontwerp van de opdracht zullen worden opgeslagen in een map met de naam ‘interne projecten’. Voor de archivering wordt er een map aangemaakt waar alle voorgaande documenten in geplaatst zullen worden. Zo blijven in ieder geval alle revisies bewaard.

3 De opdracht

In dit hoofdstuk wordt uiteengezet wat het probleem is waardoor deze opdracht is ontstaan, wat de doelen van Actemium zijn bij deze opdracht, wat de opdracht vanuit de opdrachtgever is, wat de eisen en randvoorwaarden van de opdracht zijn en wat er in dit project uiteindelijk opgeleverd gaat worden.

3.1 Het probleem

De laatste jaren is de wet- en regelgeving en de controle daarop in de chemische sector een stuk strenger geworden. De reden voor deze strengere wet- en regelgeving en de controle daarop is gelegen in een aantal rampen en ongelukken die de laatste jaren voorgekomen zijn bij bedrijven die met chemische producten te maken hebben (OSP, 2014). Daarom zijn veel bedrijven in de chemische sector verplicht om onder andere de installaties en productstromen te herzien en vast te stellen of extra beveiligingsmaatregelen nodig zijn. Voor bedrijven in de procesindustrie betekent dit vaak dat complete installaties opnieuw bekeken moeten worden zodat rampen en grote ongelukken niet meer voorkomen. Helaas zijn de risico's nooit volledig uit te sluiten. Ze kunnen echter wel sterk verminderd worden met een aantal passende maatregelen, waaronder de toevoeging van een veiligheidssysteem. Omdat bedrijven echter zelf veelal niet de kennis en kunde in huis hebben om daadwerkelijk te beoordelen of de installatie veilig is of niet, wordt dit vaak uitbesteed aan bedrijven als Actemium. Actemium heeft een aantal specialisten in huis die dergelijke projecten, die te maken hebben met die veiligheid, kunnen uitvoeren. Dit zijn er echter nog niet heel veel en zij kunnen bij nieuwe klanten ook nog geen voorbeelden laten zien van een veiligheidssysteem. Het laten zien van een veiligheidssysteem van een mogelijke concurrent is geen oplossing.

3.2 Het doel van Actemium

Actemium heeft voor zowel klanten als voor leerlingen, studenten en eigen personeel een aantal modellen in het EduLab staan. Om nu voor deze klanten, leerlingen, studenten en eigen personeel ook een voorbeeld te hebben van een veiligheidssysteem, is er besloten om de huidige procesinstallatie uit te voeren met een veiligheidssysteem. Op deze manier kan Actemium laten zien dat ze niet alleen een veiligheidssysteem kunnen implementeren maar dat ze dit veiligheidssysteem ook zelf kunnen ontwerpen en implementeren volgens de geldende wet- en regelgeving met de daarbij horende normen. Daarnaast is het zeer belangrijk om bij nieuwe klanten voor het engineeren van veiligheidssystemen eigen documentatie te kunnen gebruiken, in de huisstijl van Actemium.

3.3 De opdracht

Om het probleem van Actemium te ondervangen moet er een veiligheidssysteem toegevoegd worden aan de Edulab installatie. Daarnaast moeten er standaarddocumenten gemaakt worden die de ingenieur van een veiligheidssysteem kan gebruiken als leidraad voor het volgen van de juiste norm. Door de opdrachtgever is in de originele opdracht (zie bijlage I) aangegeven dat er gewerkt zal worden met de IEC61508 norm. Er is echter een afgeleide norm beschikbaar die specifiek bedoeld is voor de procesindustrie. Dit betreft de IEC61511 norm. In overleg met de opdrachtgever is besloten om voornamelijk gebruik te maken van de IEC61511, met daarbij de IEC61508 te ondersteuning.

Door middel van het volgen en toepassen van de IEC61511 norm kan er een veiligheidssysteem toegevoegd worden aan de procesinstallatie in het EduLab (zie bijlage II voor de P&ID). Normaal gesproken wordt er in de installatie alleen gewerkt met water, maar voor deze opdracht is besloten dat de installatie geschikt gemaakt moet worden voor natronloog. Daarmee worden de risico's wat realistischer (groter) gemaakt ten opzichte van de situatie waarin water wordt gebruikt.

Omdat er een sponsor is voor het leveren van een veiligheidsPLC, is reeds bekend met welk merk PLC er gewerkt gaat worden, namelijk HIMA. Binnen een aantal weken na de start van het project is er ook de mogelijkheid geboden om een tweedaagse cursus te volgen om te leren een HIMA PLC te programmeren.

Omdat bij het volgen van de IEC61511 norm een groot aantal risico's vastgesteld kan worden die waarschijnlijk niet allemaal te reduceren zijn binnen de stagetijd, is er door de opdrachtgever besloten om vooraf drie risico's vast te stellen die gereduceerd moeten worden. De drie vastgestelde risico's die aanvaardbaar gemaakt moeten worden zijn de volgende:

1. Het te snel oplopen van de temperatuur bij een exotherme reactie in een reactortank;
2. Het te hoog worden van de druk in een reactortank;
3. Het te hoog worden van het niveau in een watertank.

De doelstelling wordt dus:
Ontwerp en implementeer een veiligheidssysteem met een HIMA PLC, door middel van het toepassen van de IEC61511 norm op drie vooraf vastgestelde risico's in de huidige procesinstallatie in het EduLab, om deze geschikt te maken voor het gebruik van natronloog.

De acties die nodig zijn om deze opdracht te voltooien zijn onder andere:

- Het onderzoeken van de huidige installatie en besturingen.
- Het onderzoeken van de IEC61508 en IEC61511, onder meer om het stappenplan te begrijpen.
- (Stap 1) Het maken van een risico analyse.
- (Stap 2) Het toewijzen van de risico's in een beschermlaag.
- (Stap 3) Het opstellen van de Safety Requirements Specifications (SRS).
- (Stap 4) Het ontwerpen van een Safety Instrumented System (SIS).
- (Stap 5) Het installeren, inbedrijfstellen en valideren van het systeem (FAT/SAT).
- Het maken van alle documenten die nodig zijn voor het toepassen van de norm, in Actemium huisstijl.

3.4 Eisen en randvoorwaarden

Om de eisen en wensen van de opdrachtgever weer te geven is de MoSCoW methode gebruikt ("Wikipedia.nl", Moscow methode, 2014). Op deze manier wordt snel duidelijk wat echt in het project meegenomen moet worden en wat bijvoorbeeld alleen bij voldoende tijd meegenomen wordt. Zie Tabel 3-1.

MoSCoW methode	
Must have (Verplicht)	- Er moeten standaard documenten in Actemium huisstijl komen voor alle stappen waar documenten benodigd zijn. - Het veiligheidssysteem moet ontworpen worden volgens de IEC61511. - Het veiligheidssysteem moet gebruik maken van een HIMA HIMatrix veiligheid PLC. - Het veiligheidssysteem zal de drie risico's aanvaardbaar maken. - Het veiligheidssysteem moet volledig onafhankelijk van de besturingssystemen zijn.
Should have (Het liefst wel)	- Het veiligheidssysteem moet toegevoegd worden aan de huidige installatie. - Het veiligheidssysteem moet bij een van de drie bestaande SCADA applicaties een melding geven als het ingegrepen heeft.
Could have (Zou leuk zijn)	- Het veiligheidssysteem moet bij alle drie de bestaande SCADA applicaties een melding geven als het ingegrepen heeft.

Would have (Zou leuk zijn maar is voor de volgende stagiair)	- Het veiligheidssysteem zal alle risico's in de installatie aanvaardbaar maken.

Tabel 3-1: MoSCoW methode

3.5 Eindproducten

De volgende eindproducten dienen te worden opgeleverd:

- Standaard documenten in Actemium huisstijl voor het toepassen van de IEC61511.
- Een ontwerp van een veiligheidssysteem voor de EduLab ProcessCell.
- Het veiligheidssysteem bij de EduLab ProcessCell gebouwd, inbedrijfgesteld, getest en gevalideerd.
- De meldingen in de bestaande SCADA systemen wanneer het veiligheidssysteem ingegrepen heeft.
- De bijbehorende documentatie inclusief de uitgevoerde FAT en/of SAT.

4 Onderzoek algemeen

Om vast te stellen wat er precies onderzocht moet gaan worden, zijn er in het PID (Bijlage III) een hoofdvraag en een aantal deelvragen vastgesteld. Door deze vragen te beantwoorden zal duidelijk worden waar in het project aan voldaan moet worden (normen) en welke belangrijke informatie meegenomen moet worden in het ontwerpen van het veiligheidssysteem. De komende drie hoofdstukken bevatten de beantwoording van de deelvragen die betrekking hebben op de normen (hoofdstuk 5), de installatie (hoofdstuk 6) en de besturing (hoofdstuk 7). In dit hoofdstuk zal echter eerst worden weergegeven wat de hoofd- en deelvragen zijn, en wordt de algemene deelvraag over natronloog onderzocht.

4.1 De hoofd- en deelvragen

De hoofd- en deelvragen die in het PID zijn vastgesteld zijn de volgende:

Hoofdvraag:

Hoe kan bij het gebruik van natronloog in de EduLab procesinstallatie, de procesinstallatie en de besturing daarvan veiliger worden gemaakt, door het toepassen van de IEC61511 en IEC61508 norm op de installatie en het toevoegen van een onafhankelijk veiligheidssysteem dat voldoet aan de IEC61511 en IEC61508 norm?

Deelvragen:

Algemeen:

1. Welke eigenschappen van natronloog zijn er bekend, die van belang zijn bij het ontwerpen van een veiligheidssysteem bij de procesinstallatie?

Normen:

1. Hoe kan de IEC61508 norm gebruikt worden om de procesinstallatie veiliger te maken en te laten voldoen aan de machinerichtlijn?
2. Hoe kan de IEC61511 norm gebruikt worden om de procesinstallatie veiliger te maken en te laten voldoen aan de machinerichtlijn?
3. Wat is de relatie tussen de IEC61508 en de IEC61511 norm, die beide van toepassing zijn bij het laten voldoen van een procesinstallatie aan de machinerichtlijn?
4. Wanneer is een geconstateerd risico in de procesinstallatie zodanig gereduceerd met gebruik van de geldende normen dat het risico aanvaardbaar is?

Installatie:

1. Wat is de functie van de procesinstallatie bij het gebruik van natronloog?
2. Welke risico's doen zich voor bij het gebruik van natronloog in de procesinstallatie?
3. Hoe kan een veiligheidssysteem dat voldoet aan de machinerichtlijn en dat onafhankelijk is van de normale besturing, toegevoegd worden aan de procesinstallatie?

Besturingen:

1. Wat is de functie van een veiligheidssysteem bij een procesinstallatie in de chemische industrie?
2. Wat kan een veiligheidsPLC meer of beter dan een gewone PLC bij het besturen van een veiligheidssysteem in de procesinstallatie dat moet voldoen aan de IEC61511 norm?
3. Hoe kan er in de huidige SCADA systemen een melding getoond worden aan de operator van de procesinstallatie wanneer het veiligheidssysteem ingegrepen heeft op de normale besturing?

4.2 Algemene deelvraag 1: natronloog

In deze paragraaf wordt ingegaan op de gevaren die de verwerking van natronloog met zich mee brengt. Allereerst wordt weergegeven wat natronloog is en waarvoor het gebruikt wordt. Daarna zal verder ingegaan worden op de belangrijke informatie met betrekking tot opslag, behandeling en eerste hulp maatregelen.

Welke eigenschappen van natronloog zijn er bekend, die van belang zijn bij het ontwerpen van een veiligheidssysteem bij de procesinstallatie?

NaOH

Natronloog is een vloeibare stof die gemaakt kan worden van natriumhydroxide gemengd met water, ook wel bekend als NaOH. Het is een sterke base met een pH waarde van 14. Wanneer natriumhydroxide samengevoegd wordt met water ontstaat er een exotherme reactie. Dat wil zeggen dat de stoffen energie aan de omgeving afgeven in de vorm van warmte. Natronloog wordt in verschillende varianten verkocht waarbij vaak het percentage natriumhydroxide wordt aangegeven. Veel voorkomende vormen zijn 100% (natriumhydroxide in vaste vorm) 50% (vloeibare vorm met 50% natriumhydroxide) en 33% (vloeibare vorm met 33% natriumhydroxide). Veel voorkomend gebruik van natriumhydroxide en natronloog is als gootsteenontstopper of voor het maken van zeep.

De stof is corrosief en moet dus met voorzichtigheid behandeld worden. Aanraking met ogen, huid of inslikken / inhaleren is zeer gevaarlijk omdat het kan leiden tot weefselbeschadiging, roodheid, jeuk en brandwonden. Om te weten wat te doen bij ongelukken met natriumhydroxide of natronloog, of hoe de producten te behandelen (opslag, brand) zijn er Material Safety Data Sheets (MSDS) gemaakt. Deze moeten volgens de wet en regelgeving door een leverancier of producent gemaakt worden om de afnemer te informeren over de gevaren van het product. Daarin is alle benodigde informatie terug te vinden betreffende het handelen bij ongelukken met natriumhydroxide of natronloog, de opslag en verwerking van Natronloog, enz. De MSDS is te zien in Bijlage IV MSDS NaOH 50-100%. ("Wikipedia.nl", Natriumhydroxide, 2014)

Belangrijke informatie

("Sigma-aldrich.com", 2014)

Labelaanduiding:  gevaar / bijtend

Beschermingsmiddelen:

- Gelaatsmasker voor ogen en gezicht
- Handschoenen voor de handen
- Pak of schort (afhankelijk van de concentratie) voor het lichaam
- Ademhalingsmasker voor longen en luchtwegen (waar ademhaling risico's zich voordoen)

Mogelijke gezondheidsaandoeningen:

Inademing: Het weefsel van de slijmvliezen en bovenste ademhalingswegen kunnen ernstig beschadigen
Inname: Het kan inwendig in de mond en slokdarm brandwonden veroorzaken.
Huid: Het kan brandwonden veroorzaken waar er contact is of is geweest met de huid
Ogen: Het kan brandwonden en verminderd zicht of blindheid veroorzaken

Eerste hulp maatregelen:

Bij inademing:	Slachtoffer naar de frisse lucht brengen. Als het slachtoffer niet meer ademt, kunstmatig beademen. Let op: bij mond op mond beademing dat er kans is dat sporen van natronloog op of rondom lippen zitten. Een arts raadplegen.
Bij inname:	Mond spoelen met water, niet laten braken en niets laten drinken of eten als het slachtoffer bewusteloos is. Een arts raadplegen
Bij aanraking met de huid:	Getroffen kleding en schoenen direct uittrekken, huid wassen met zeep en veel water. Een arts raadplegen.
Bij aanraking met de ogen:	Ogen 15 minuten grondig en met veel water spoelen. Een arts raadplegen.

Hantering en opslag:

- Voorkom inademing van de damp of nevel
- Opslaan op een koele droge plaats met voldoende ventilatie
- Geopende containers zorgvuldig afsluiten en rechtop bewaren om lekken te voorkomen

Maatregelen voor het onbedoeld vrijkomen van de stof:

- Persoonlijke beschermingsmiddelen gebruiken, adem damp of nevel niet in, zorg voor voldoende ventilatie en evacueer overig personeel
- Zorg dat het lekken of morsen stopt bij de bron als dit veilig kan en voorkom dat het product in de riolering terecht komt
- Stof opnemen met een inert absorberend materiaal, in gesloten en geschikte containers bewaren en afvoeren als gevaarlijk afval
- Restanten en onherbruikbare stoffen laten verwijderen door een vergunninghoudend verwijderingsbedrijf

Maatregelen bij brand:

- Geschikte blusmiddelen zijn: waternevel, alcoholbestendig schuim, droogpoeder of kooldioxide
- Indien nodig persluchtmasker dragen

4.3 Deelconclusie onderzoek algemeen

Door een antwoord te zoeken op de gestelde hoofd- en deelvragen, zal voldoende informatie beschikbaar komen om een veiligheidssysteem te kunnen ontwerpen. Daarnaast kan dezelfde informatie gebruikt worden voor het maken van de standaarddocumenten die Actemium graag wil.

Bij de beantwoording van de algemene deelvraag zijn de belangrijkste eigenschappen van natronloog naar voren gekomen, namelijk: het is bijtend / corrosief en de nevel / damp ervan is gevaarlijk voor de gezondheid. Omdat natronloog een pH heeft van 14 zal het in water schadelijk zijn voor het leven dat er in dat water zit. Dat wil dus zeggen dat lekken of verbranden zoveel mogelijk voorkomen moet worden ten behoeve van de bescherming van personen en milieu.

5 Onderzoek normen

In dit hoofdstuk worden, aan de hand van de gestelde deelvragen, de normen die van toepassing zijn op het veiligheidssysteem onderzocht. Allereerst worden de IEC61508 en de IEC61511 toegelicht (paragrafen 5.1 en 5.2). Daarna zal de relatie tussen die twee normen bekeken worden (paragraaf 5.3). Tot slot wordt onderzocht wanneer een risico acceptabel is volgens de normen (paragraaf 5.4). Het is bekend dat de normen nogal moeilijk leesbare stof is met veel technische termen. Het onderwerp is echter een heel belangrijk onderdeel van dit project, dus is het wel belangrijk dat het goed onderzocht wordt. Daarom is dit hoofdstuk toch toegevoegd ondanks dat het de leesbaarheid van het verslag verminderd.

5.1 Normen deelvraag 1: IEC61508

In deze paragraaf wordt in vier subparagrafen ingegaan op de relevante delen van de IEC61508 norm. Allereerst worden de drie belangrijkste, normatieve delen toegelicht. Deze delen bevatten alle algemene eisen, de hardware eisen en de software eisen. Daarna worden heel kort de laatste vier, minder belangrijke en informatieve delen toegelicht. Deze delen bevatten onder andere de afkortingen, begrippen en toepassingen van de eerste drie delen uit de norm.

Hoe kan de IEC61508 norm gebruikt worden om de procesinstallatie veiliger te maken en te laten voldoen aan de machinerichtlijn?

De IEC61508 is een norm voor functionele veiligheid voor elektrische (E) / elektronische (E) / programmeerbare elektronische (PE) systemen (kortweg E/E/PE). Deze norm fungeert als aanpak bij het ontwerpen, implementeren en alle andere safety lifecycle activiteiten van systemen die bestaan uit E en/of E en/of PE elementen die een veiligheidsfunctie moeten uitvoeren. Hoewel deze norm voornamelijk bedoeld is voor het gebruik in E/E/PE systemen, kan hij ook gebruikt worden voor veiligheidssystemen die gebaseerd zijn op ander technologieën zoals mechanische, hydraulische en pneumatische systemen.

5.1.1 Algemene eisen

(IEC, NEN-EN-IEC61508-1:2010 en, 2014)

De inhoud van deel 1 bestaat voornamelijk uit de algemene eisen die van toepassing zijn bij het gebruik van de IEC61508 norm. De clausules die van belang zijn in dit document zijn clausule 5, 6, 7 en 8. De overige clausules zijn clausules die standaard toegevoegd worden aan elk deel met bijvoorbeeld het bereik van de norm, de normatieve verwijzing, een verwijzing naar de definities en afkortingen, bronnen en bijlagen.

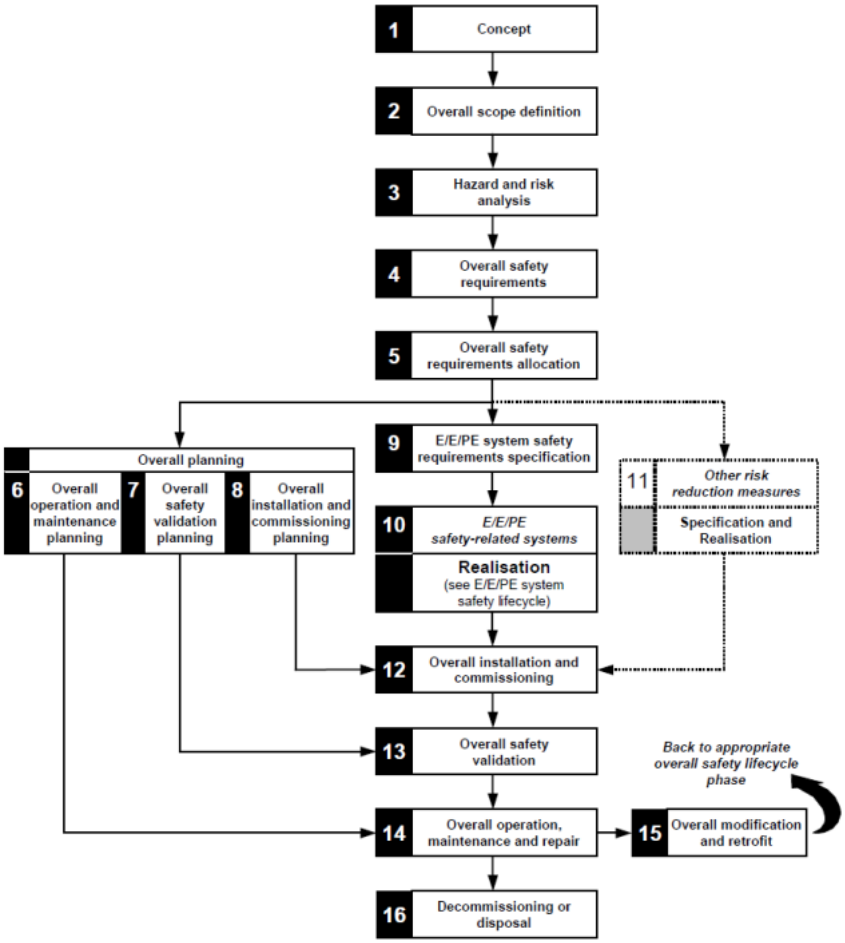
In clausule 5 zijn de doelstelling en de eisen voor de documentatie vastgelegd. Hierin staat onder meer dat er voldoende informatie over elke fase van de safety lifecycle vastgelegd moet zijn en dat er een inhoudsopgave aanwezig moet zijn bij de documenten die gemaakt worden.

In clausule 6 zijn de doelstellingen en eisen van het beheer van de functionele veiligheid vastgelegd. Hierin staat onder meer dat er procedures gemaakt moeten worden ter bepaling van de informatie die tussen relevante partijen moet worden uitgewisseld en de wijze waarop deze informatie moet worden uitgewisseld.

In clausule 7 zijn de doelstellingen en eisen van de algemene safety lifecycle uitgelegd (zie Afbeelding 5-1). In de safety lifecycle zijn alle fasen, van opbouw tot afbreken van een installatie, waarbij veiligheidsfuncties van belang zijn weergegeven. Tevens is hier weergegeven op welke wijze deze fasen kunnen worden doorlopen. Omdat het doel van de fasen uit de bewoording in de afbeelding niet duidelijk wordt is Tabel 5-1 toegevoegd. In deze tabel wordt op elke fase een korte toelichting gegeven.

In clausule 8 zijn de doelstelling en de eisen weergegeven van een functionele veiligheidsbeoordeling. Hierin staat onder meer dat een aangewezen persoon een functionele veiligheidsbeoordeling mag uitvoeren na elke

fase van de safety lifecycle of na een aantal fasen om overlap te voorkomen. Ook staat hierin wat er gedocumenteerd moet worden als bewijs dat de functionele veiligheidsbeoordeling is uitgevoerd. Aan het einde van deze clausule staat hoe bepaald kan worden wie gekwalificeerd is voor het uitvoeren van een functionele beoordeling. Dit wordt bepaald door gebruik te maken van consequenties die kunnen voorkomen door de vastgestelde risico's, of door gebruik te maken van het vastgestelde veiligheidsniveau (SIL). Uit dat SIL niveau zal blijken of de uitvoering van de functionele veiligheidsbeoordeling door een onafhankelijk persoon, een onafhankelijke afdeling of een onafhankelijk organisatie moet worden verricht.



Afbeelding 5-1: Algemene safety lifecycle IEC61508

Nr.	Fasenaam	Doel van de fase
1	Concept	◊ Het ontwikkelen van een voldoende niveau van begrip van de apparatuur of het systeem en de omgeving (fysiek, wetgeving, enz.) zodat het mogelijk is de andere safety lifecycle activiteiten naar tevredenheid uit te voeren.
2	Overall scope definition	◊ Het vaststellen van de grenzen van de apparatuur of het systeem. ◊ Het specificeren van de omvang van de gevaren- en risicoanalyse (bijvoorbeeld proces gevaren, gevaren voor het milieu enz.).
3	Hazard and risk analysis	◊ Het bepalen van de gevaren, gevaarlijke gebeurtenissen en gevaarlijke situaties die gerelateerd zijn aan de apparatuur of het systeem (in alle toestanden) voor alle redelijkerwijs te verwachten situaties, inclusief storingen en redelijkerwijs te verwachten onjuist gebruik. ◊ Het vastleggen van de apparatuur of systeem risico's die worden geassocieerd met de gevaarlijke situatie.

4	Overall safety requirements	◊ Het specificeren van de algemene veiligheidseisen, in termen van veiligheidsfunctie eisen en veiligheid integriteitseisen, te ontwikkelen voor het E/E/PE systeem, en andere risico reducerende maatregelen om zo het vereiste functionele veiligheid te behalen.
5	Overall safety requirements allocation	◊ Het toewijzen van de veiligheidsfuncties die gespecificeerd staan in de overall safety requirements, aan het aangewezen E/E/PE systeem of andere risico reducerende maatregelen. ◊ Een veiligheidsniveau (SIL) toewijzen aan elke veiligheidsfunctie (SIF) die uitgevoerd wordt door een E/E/PE systeem.
6	Overall operation and maintenance planning	◊ Het ontwikkelen van een plan voor normaal bedrijf en onderhoud van het E/E/PE systeem, om ervoor te zorgen dat de vereiste functionele veiligheid gehandhaafd wordt gedurende de normale bedrijfsvoering en onderhoud.
7	Overall safety validation planning	◊ Het ontwikkelen van een plan voor de algemene veiligheidsvalidatie voor het E/E/PE systeem.
8	Overall installation and commissioning planning	◊ Het ontwikkelen van een plan voor het op een gecontroleerde manier installeren van het E/E/PE systeem waardoor de vereiste functionele veiligheid gehandhaafd wordt. ◊ Het ontwikkelen van een plan voor het op een gecontroleerde manier inbedrijfstellen van het E/E/PE systeem, waardoor de vereiste functionele veiligheid gehandhaafd wordt.
9	E/E/PE safety requirements specification	◊ Het definiëren van de E/E/PE systeem veiligheidseisen, in termen van E/E/PE systeem veiligheidsfunctie eisen en E/E/PE systeem veiligheid integriteitseisen, om de vereiste functionele veiligheid te handhaven.
10	E/E/PE safety-related systems realisation	◊ Het creëren van het E/E/PE systeem conform de E/E/PE systeem veiligheidseisen (bestaande uit E/E/PE systeem veiligheidsfunctie eisen en E/E/PE systeem veiligheid integriteitseisen).
11	Other risk reduction measures (specification and realisation)	◊ Het creëren van andere risico reducerende maatregelen om te voldoen aan de veiligheidsfunctie eisen en veiligheid integriteitseisen gespecificeerd voor dergelijke systemen (buiten het toepassingsgebied van deze norm om).
12	Overall installation and commissioning	◊ Het installeren van het E/E/PE systeem. ◊ Het inbedrijfstellen van het E/E/PE systeem.
13	Overall safety validation	◊ Het valideren dat het E/E/PE systeem voldoet aan de specificatie voor de algemene veiligheidseisen in de termen van de algemene veiligheidsfunctie eisen en de algemene veiligheid integriteitseisen, met inachtneming van de veiligheidseisen toewijzing volgens fase 5.
14	Overall operation, maintenance and repair	◊ Het waarborgen dat de functionele veiligheid van het E/E/PE systeem gehandhaafd wordt op het gespecificeerde niveau. ◊ Het waarborgen dat de technische vereisten, nodig voor het normaal bedrijf, onderhoud en reparatie van het E/E/PE systeem zijn gespecificeerd en verstrekt aan de personen die verantwoordelijk zijn voor het toekomstige normaal bedrijf en onderhoud van het E/E/PE systeem.
15	Overall modification and retrofit	◊ Het definiëren van de procedures die nodig zijn om te waarborgen dat de functionele veiligheid voor het E/E/PE systeem passend is, zowel gedurende als na aanpassingen en toevoegen van onderdelen.

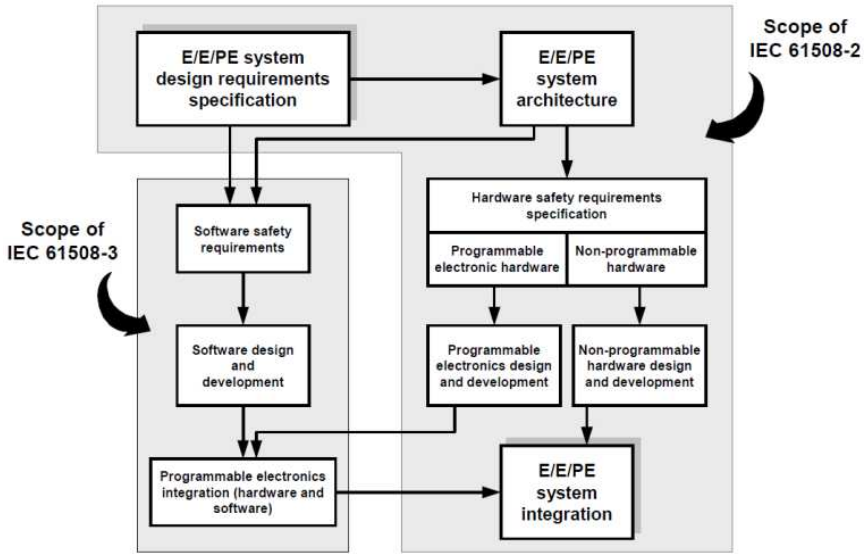
16	Decommissioning or disposal	◊ Het definiëren van de procedures die nodig zijn om ervoor te zorgen dat de functionele veiligheid voor het E/E/PE systeem passend is in de gegeven omstandigheden tijdens en na het ontmantelen of verwijderen van de apparatuur of het systeem.

Tabel 5-1: Fasen safety lifecycle met uitleg

5.1.2 Richtlijnen voor E/E/PE systemen.

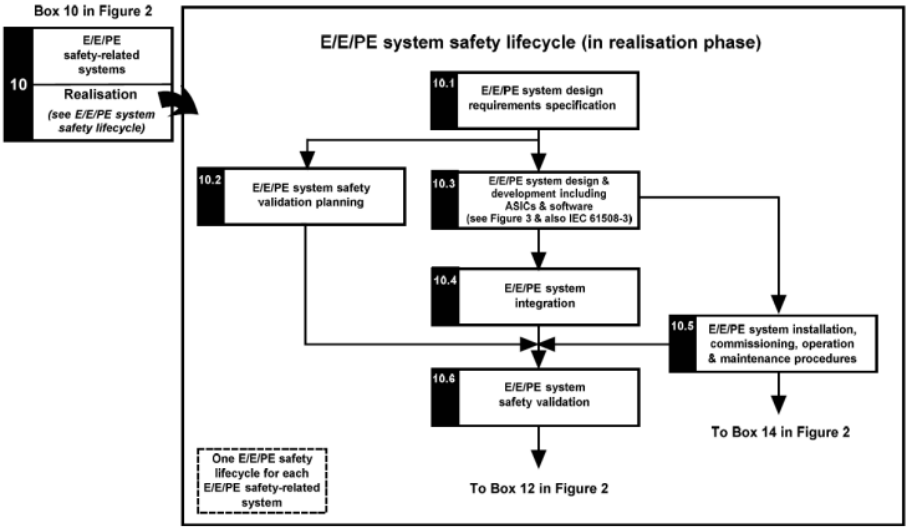
(IEC, NEN-EN-IEC61508-2:2010 en, 2014)

Ook deel 2 is relevant voor het ontwerpen van een veiligheidssysteem. Deel 2 bestaat voornamelijk uit de eisen waaraan de activiteiten die tijdens het ontwerpen en realiseren van het E/E/PE systeem uitgevoerd worden moeten voldoen. Het gaat hier dus vooral over fase 10 in de safety lifecycle. Hierbij wordt vooral gekeken naar de hardware in het E/E/PE systeem. De software zal behandeld worden in IEC61508-3 (zie Afbeelding 5-2).



Afbeelding 5-2: Relatie tussen IEC61508-2 en IEC61508-3

De clausule die van belang is in dit document is clausule 7. Hierin zijn de doelstellingen en eisen van de safety lifecycle in de realisatiefase uitgelegd (zie Afbeelding 5-3). In de safety lifecycle worden alle fasen weergegeven die plaatsvinden in de realisatiefase van het hardware deel van het E/E/PE systeem.

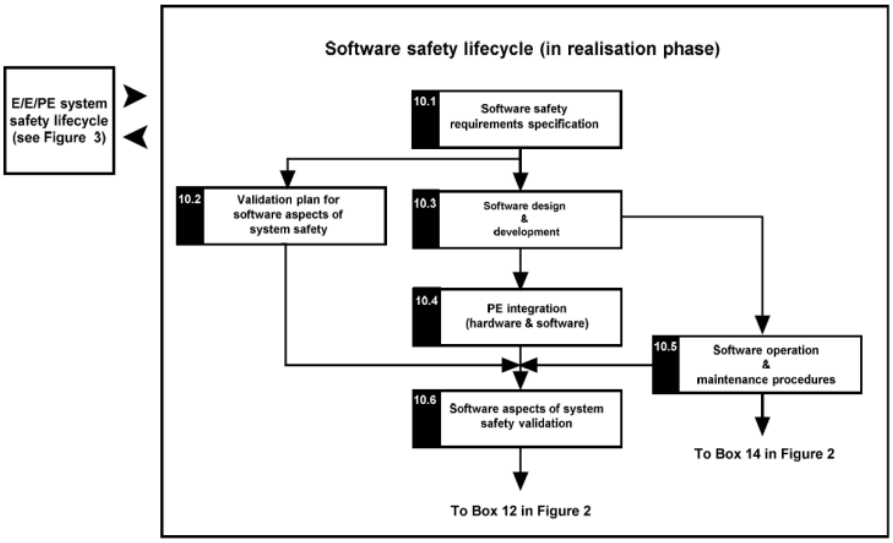


Afbeelding 5-3: Realisatiefase IEC61508-2

5.1.3 Eisen voor programmatuur

(IEC, NEN-EN-IEC61508-3:2010 en, 2014)

De inhoud van het volgende relevante deel, namelijk deel 3, bestaat voornamelijk uit de eisen voor de activiteiten, die tijdens het ontwerpen en realiseren van het E/E/PE systeem uitgevoerd worden. Het gaat hier dus vooral over fase 10 in de safety lifecycle. (zie Afbeelding 5-1). Hierbij wordt vooral gekeken naar de software in het E/E/PE systeem. De clausule die van belang is in dit document is clausule 7.Hierin zijn de doelstellingen en eisen van de safety lifecycle in de realisatiefase uitgelegd (zie Afbeelding 5-4). In de safety lifecycle staan alle fasen weergegeven die plaatsvinden in de realisatiefase voor het softwaredeel van het E/E/PE systeem.



Afbeelding 5-4: Realisatiefase IEC61508-3

5.1.4 Definities, afkortingen en informatieve delen

Deel 4 (Definities en afkortingen) bestaat voornamelijk uit de definities en afkortingen die in deel 1 tot en met 7 gebruikt worden. De afkortingen worden in tabelvorm gegeven met daarbij het uitgeschreven woord. Daarna worden de definities van woorden gegeven met daarbij een uitgebreide uitleg, soms voorzien van voorbeelden en afbeeldingen. (IEC, NEN-EN-IEC61508-4:2010 en, 2014)

In deel 5 (Voorbeelden van methodes voor het vaststellen van veiligheidsniveaus) worden voorbeelden gegeven van hoe een veiligheidsniveau bepaald kan worden. Voornamelijk in de bijlagen staan de voorbeelden die gebruikt kunnen worden voor het bepalen van het veiligheidsniveau van apparatuur of een systeem (IEC, NEN-EN-IEC61508-5:2010 en, 2014).

In deel 6 (Richtlijnen voor de toepassing van IEC61508-2 en IEC61508-3) wordt aangegeven hoe de IEC61508-2 en IEC61508-3 toegepast kunnen worden. Voornamelijk in de bijlagen worden de voorbeelden en methoden weergegeven voor het toepassen van de IEC61508-2 en IEC61508-3 (IEC, NEN-EN-IEC61508-6:2010 en, 2014).

In deel 7 (Overzicht van voorzieningen en technieken) wordt een overzicht van voorzieningen en technieken voor het gebruik van alle delen uit de IEC61508 norm gegeven. Voornamelijk in de bijlagen worden overzichten van technieken en voorzieningen weergegeven die gebruikt kunnen worden voor alle delen in deze norm (IEC, NEN-EN-IEC61508-7:2010 en, 2014).

5.1.5 Tussenconclusie IEC61508

De IEC61508 norm is een overkoepelende norm die gebruikt kan worden voor het verbeteren en behouden van functionele veiligheid in de automatisering. Omdat deze norm globale eisen en voorbeelden geeft, is het wat lastiger om dit te koppelen aan veiligheidssystemen in de procesautomatisering. Hoewel bij het ontwerpen van een veiligheidssysteem gebruik gemaakt kan worden van de IEC61508 norm (die ook zeker van toepassing is), gaat de voorkeur uit naar de meer gespecificeerde norm als de IEC61511. Desalniettemin is van belang dat er wel kennis is van de IEC61508 norm en dat deze norm beschikbaar is bij het ontwerpen van een veiligheidssysteem in de procesautomatisering, omdat deze norm een basis geeft die bekend moet zijn of waarnaar verwezen kan worden vanuit de IEC61511.

5.2 Normen deelvraag 2: IEC61511

In deze paragraaf wordt ingegaan op de indeling van de IEC61511 norm in elf stappen. Allereerst worden deze elf stappen kort toegelicht (subparagraaf 5.2.1). Daarna zal verder ingegaan worden op de voor het project relevante stappen, te weten stap 1 tot en met 5 (subparagrafen 5.2.2 tot en met 5.2.6). Er wordt afgesloten met een tussenconclusie (subparagraaf 5.2.7).

Hoe kan de IEC61511 norm gebruikt worden om de procesinstallatie veiliger te maken en te laten voldoen aan de machinerichtlijn?

5.2.1 Algemene indeling IEC61511 norm

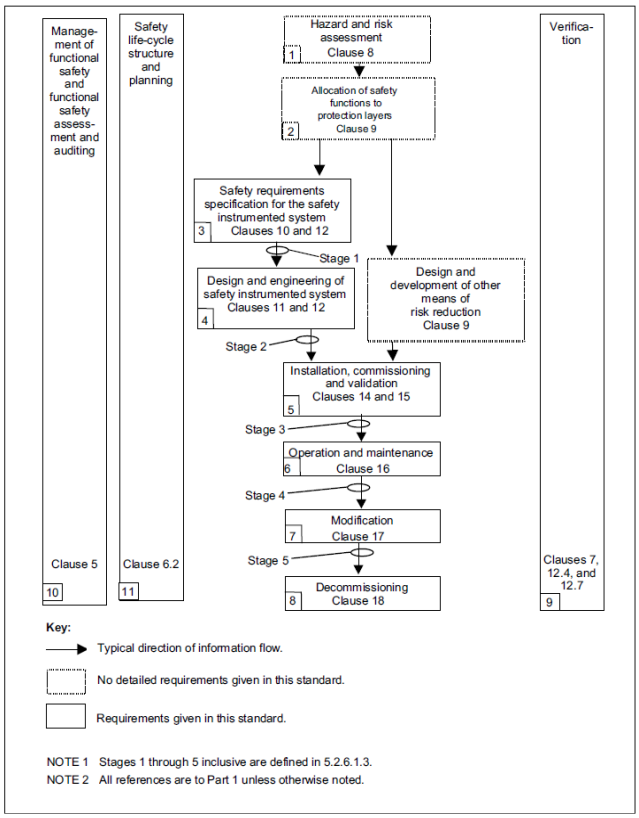
(IEC, NEN-EN-IEC61511-1:2005 en, 2014)

De IEC61511 is een norm die staat voor functionele veiligheid, specifiek voor geïnstrumenteerde veiligheidssystemen voor de procesindustrie. Deze norm is bedoeld om als aanpak te gebruiken bij het ontwerpen, implementeren en alle andere safety lifecycle activiteiten van geïnstrumenteerde veiligheidssystemen in de procesindustrie. Deze norm kan dus toegepast worden op alle onderdelen van geïnstrumenteerde veiligheidssystemen: van input (sensor) tot output (eindelement / actuator). De norm is opgebouwd uit een aantal delen. Deel 1 is het normatieve deel van deze norm. Hierin staan de eisen die gelden in deze norm. Deel 2 en 3 zijn informatief en bevatten vooral methodes en voorbeelden om de eisen van deel 1 te kunnen toepassen.

Deel 1: Raamwerk, definities, systeem, hardware en software eisen

(IEC, NEN-EN-IEC61511-1:2005 en, 2014)

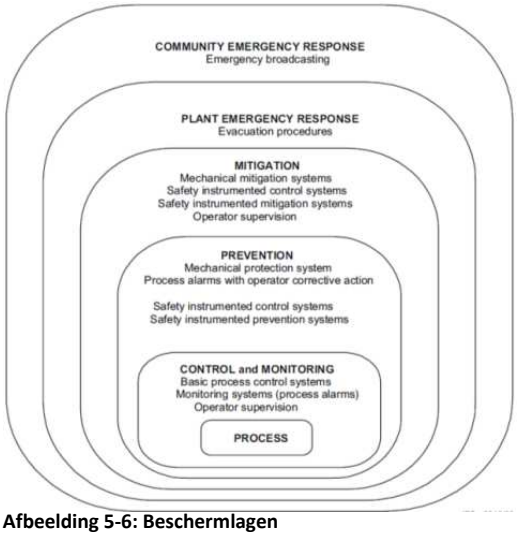
De clausules die van belang zijn in dit document zijn clausule 5 tot en met 18. De overige clausules zijn clausules die standaard toegevoegd worden aan elk deel met bijvoorbeeld het bereik van de norm, de normatieve verwijzing, een verwijzing naar de definities en afkortingen, bronnen en bijlagen. De clausules zijn ingedeeld in het stappenplan van de norm (zie Afbeelding 5-5). Vandaar dat hier per stap de gerelateerde clausules genoemd zullen worden en kort wordt verteld wat er in die clausules staat.



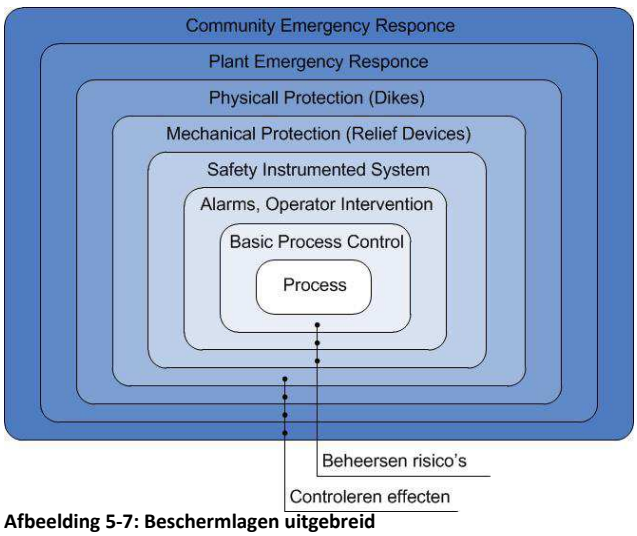
Afbeelding 5-5: Geïnstrumenteerd veiligheidssysteem lifecycle IEC61511

Bij stap 1 is clausule 8 van toepassing. In clausule 8 zijn de doelstellingen en eisen van de procesgevaren en risico-evaluatie vastgelegd. Hierin staat onder andere dat elke gevaarlijke gebeurtenis en risico, de gevolgen en de kans van voorkomen en de toewijzing van deze gevaarlijke gebeurtenissen en risico's aan de beschermlagen beschreven moeten worden.

Bij stap 2 is clausule 9 van toepassing. In clausule 9 zijn de doelstellingen en eisen van de toewijzingen van veiligheidsfuncties aan beschermlagen (zie Afbeelding 5-6 en Afbeelding 5-7) vastgelegd. Hierin staat onder andere dat het toewijzen van veiligheidsfuncties aan beschermlagen voor het doel van preventie, voorkomen of beperken van de gevaren in het proces en het toewijzen van risicobeperkingsdoelstellingen aan veiligheidsfuncties gedaan moet worden in deze fase.



Afbeelding 5-6: Beschermlagen



Afbeelding 5-7: Beschermlagen uitgebreid

Bij stap 3 zijn clausule 10 en 12 van toepassing. In clausule 10 en 12 zijn de doelstellingen en eisen voor het Safety Instrumented System (SIS) veiligheidseisen specificatie vastgelegd. Hierin staat onder andere dat er een beschrijving van alle veiligheidsfuncties, van de veilige toestand, de responsie tijd die nodig is om het systeem in een veilige toestand te brengen, de eisen voor handmatige shutdown en eisen voor het resetten van het systeem na een shutdown in de veiligheidseisen specificatie moet worden opgenomen.

Bij stap 4 zijn clausule 11 en 12 van toepassing. In clausule 11 en 12 zijn de doelstellingen en eisen voor het ontwerpen en engineeren van het SIS vastgelegd. Hierin staat onder andere dat het ontwerp moet voldoen aan de veiligheidseisen specificatie en aan de eisen die in de norm zijn vastgelegd, dat er rekening gehouden moet worden met menselijke vaardigheden en beperkingen bij het ontwerp van het systeem, en dat er bewijsmateriaal aanwezig moet zijn om aan te tonen dat de gebruikte componenten en subsystemen geschikt zijn voor gebruik in een veiligheidssysteem.

Bij stap 5 zijn clausule 13, 14 en 15 van toepassing. In clausule 13, 14 en 15 zijn de doelstellingen, eisen en aanbevelingen voor installatie, commisioning en validatie vastgelegd. Hierbij moeten alle activiteiten vastgelegd zijn in een planning, moet alles geïnstalleerd worden volgens het SRS en moet er een inbedrijfstelling en een validatie gedaan worden. Clausule 13 geeft aanbevelingen voor een FAT, maar aangezien een FAT niet verplicht is, zijn deze aanbevelingen ook niet verplicht.

Bij stap 6 is clausule 16 van toepassing. In clausule 16 zijn de doelstellingen en eisen voor de bediening en onderhoud van de SIS vastgelegd. Hierin staat onder andere dat de operators en onderhoudspersoneel moeten worden getraind, tegenstrijdigheden in wat verwacht is en het werkelijke gedrag moet worden geanalyseerd en dat periodieke beproevingen volgens een geschreven procedure zullen moeten worden uitgevoerd. Elke SIS moet periodiek visueel geïnspecteerd worden en de gebruiker moet documentatie bijhouden om te laten zien dat de inspecties en periodieke beproevingen uitgevoerd zijn zoals geëist wordt.

Bij stap 7 is clausule 17 van toepassing. In clausule 17 zijn de doelstellingen en eisen voor het aanpassen van de SIS vastgelegd. Hierin staat dat procedures voor de controle en de autorisatie op zijn plaats zijn, voordat er iets aangepast mag worden aan de SIS. Deze procedures moeten een duidelijke methode van identificeren en aanvragen van het werk wat gedaan moet worden en de gevaren die daarbij beïnvloed worden bevatten.

In stap 8 is clausule 18 van toepassing. In clausule 18 zijn de doelstellingen en eisen voor het ontmantelen van de SIS vastgelegd. Hierin staat dat procedures voor de controle en de autorisatie op zijn plaats zijn, voordat er iets ontmanteld mag worden aan de SIS. Deze procedures moeten een duidelijke methode bevatten voor het identificeren en aanvragen van het werk dat gedaan moet worden en de gevaren die daarbij worden beïnvloed.

Bij stap 9 zijn clausule 7, 12.4 en 12.7 van toepassing. In clausule 7, 12.4 en 12.7 zijn de doelstellingen en eisen van de verificatie vastgelegd. Hierin staat onder andere dat er vastgelegd moet worden wat de verificatie activiteiten zijn, welke procedures gebruikt worden voor de verificaties, hoe de planning van de verificaties eruit ziet en de personen of afdelingen die de verificaties gaan uitvoeren inclusief de onafhankelijkheid van die personen of afdelingen.

Bij stap 10 is clausule 5 van toepassing. In clausule 5 staan onder andere de regels voor organisatie en middelen, risico evaluatie en risico beheer, planning, implementatie en bewaking, evaluatie, controle en revisies en het geïnstrumenteerde veiligheidssysteem configuratiemanagement. Zo staat er bijvoorbeeld bij evaluatie, controle en revisies dat er procedures gemaakt moeten worden voor de beoordeling van de functionele veiligheid.

Bij stap 11 is clausule 6 van toepassing. In clausule 6 zijn de doelstellingen en eisen van de safety lifecycle vastgelegd. Hierin staat dat alle stappen in de safety lifecycle gepland moeten worden. Daarnaast moeten alle stappen geverifieerd worden. De safety lifecycle is zichtbaar in Afbeelding 5-5.

Deel 2 en 3

Deel 2: Richtlijnen voor de toepassing van de IEC61511-1 (IEC, NEN-EN-IEC61511-2:2005 en, 2014)
In deel twee van de norm staan alle richtlijnen voor de toepassing van de IEC61511-1 weergegeven. De indeling in clausules is dan ook exact gelijk aan die van deel 1. Bij de sub clausules staat de toepassing van de overeenkomstige sub clausule in deel 1 weergegeven, tenzij hier geen extra begeleiding voor is. De sub clausules waar geen extra begeleiding voor is, staan wel genummerd maar daar staat dan bij “geen verdere begeleiding geboden”.

Deel 3: Begeleiding voor het bepalen van de vereiste veiligheidsniveaus (SIL) (IEC, NEN-EN-IEC61511-3:2005 en, 2014)
In deel 3 van de norm staat uitgelegd wat een SIL niveau of SIL classificatie is en hoe dit toe te passen is op een proces. Voornamelijk in de bijlagen worden methodieken en voorbeelden weergegeven die gebruikt kunnen worden om een SIL classificatie aan een systeem of component toe te wijzen.

5.2.2 Invulling stap 1 de risicoanalyse.

Bij stap 1 in de IEC61511 wordt gesproken over het uitvoeren van een risico analyse. Doelen hiervan zijn om te bekijken welke risico’s er voor komen in de betreffende installatie bij alle mogelijke operatie modi (opstarten, uitschakelen, normaal bedrijf, onderhoud enz.). Om deze analyse te doen zijn er een aantal methoden mogelijk die genoemd worden in de IEC norm (IEC, NEN-EN-IEC61511-3:2005 en, 2014):
Veiligheidsbeoordelingen (safety review) wordt gebruikt in een zeer vroeg stadium in het project. Deze methode wordt gebruikt om in de conceptfase al de grootste risico’s te vinden om deze al bij het ontwerp mee te nemen.
Checklist is een methode waarbij vooraf een lijst opgesteld van mogelijke risico’s in een installatie. Deze moet dan punt voor punt gecontroleerd worden in de installatie of dit daadwerkelijk een risico kan opleveren.
What if analyse is een methode waarbij de vraag “wat als?” centraal staat. Deze vraag wordt in elk deel van de installatie gebruikt om te bekijken of er risico’s voorkomen als er ongewone situaties voor zouden komen.
HAZOP (HAZard and OPerability study) is een methode waarbij gebruik gemaakt wordt van een combinatie twee van woorden (gidswoord + element). Deze twee woorden geven een afwijking en een mogelijk risico in de installatie.
Storingscondities en effecten analyse (failure mode and effect analysis ofwel FMEA) is een methode waarbij de functies in een installatie ingedeeld wordt in een blokdiagram. Dit blokdiagram wordt dan uitgebreid geanalyseerd en er moet dan per blok, alle storingscondities en de bijbehorende effecten beschreven worden.
Oorzaak en gevolg analyse (cause-consequence analysis ofwel CCA) is een methode die veel gebruik maakt van een grafische weergave van oorzaken en gevolgen. Hierbij wordt er vooral gefocust op het vinden van de basis oorzaken die verantwoordelijk zijn voor een risico.

De bovenstaande methoden zijn uitgebreider onderzocht dan hier weergegeven staat. Het uitgebreide onderzoek is te vinden in bijlage V. Daarnaast zijn er nog veel meer manieren om de risico’s in een installatie te bepalen, maar aangezien de bovenstaande manieren in de norm genoemd worden zullen deze veel onderdelen bevatten die vereist worden bij een risicoanalyse volgens de IEC61511 norm.
Actemium heeft vooraf al de voorkeur gegeven aan de HAZOP methode omdat dit voor Actemium een bekende methode is. Gezien ervaring bij elke methode belangrijk is, is het begrijpelijk dat Actemium een standaard document wil hebben van de HAZOP methode (zie Tabel 5-2).

Voor de risicoanalyse van de ProcessCell zijn bij alle methoden nadelen te vinden waardoor die methoden niet geschikt zijn voor de ProcessCell. Voornamelijk (een gebrek aan) kennis en ervaring met de installatie en de methode zijn vaak de nadelen waardoor bepaalde methoden niet geschikt zijn. De What if analyse en FMEA methode zouden ook geschikt kunnen zijn voor de risicoanalyse van de ProcessCell, omdat het om een kleinere installatie gaat. Omdat er voor Actemium echter al een standaarddocument gemaakt gaat worden van de HAZOP methode, zal dit document ook gebruikt gaan worden voor de risicoanalyse van de ProcessCell.

Kenmerken van een HAZOP analyse (Gould, 2000)(IEC, NEN-EN-IEC61511-3:2005 en, 2014)("PQRI", 2014)(Pietersen C. , 2014)(IEC, NEN-IEC61882, 2014)	
Groeps-samenstelling	De groep die de risicoanalyse uitvoert, zal onder leiding staan van een voorzitter die ervaring heeft met de HAZOP methode. Er wordt een secretaris aangesteld die alles notuleert en documenteert. De overige groepsleden bestaan uit mensen die specifieke kennis hebben van het proces, het ontwerp of veiligheid.
Uitvoering	Bij het uitvoeren van een HAZOP wordt er gebruik gemaakt van gidswoorden als: geen, meer, minder, evenals, gedeeltelijk, omgekeerd en anders dan. Daarnaast worden er elementen gebruikt als: druk, flow, temperatuur, niveau, reactie, tijd, concentratie, snelheid enz. Door deze woorden te combineren en per onderdeel in een installatie af te werken zal er een lijst van afwijkingen uitkomen, die voor kunnen komen als andere beveiligingen of het BPCS falen. In Afbeelding 5-8, staat een voorbeeld van de documentatie bij een HAZOP die in de IEC61511 gebruikt wordt (IEC, NEN-EN-IEC61511-3:2005 en, 2014).
Documentatie	- Een nummering en een referentie naar de onderdelen die het betreft; - De afwijking (gidswoord en element); - Oorzaken en gevolgen; - Reeds aanwezige beveiligingen (breekplaten, overdrukventielen en/of het BPCS); - De vervolgacties. Daarnaast wordt na het opnemen van de HAZOP de documentatie uitgebreid. De uitbreiding moet bevatten: - Aanbevolen acties; - Prioriteit of risico klasse; - Verantwoordelijke voor de acties; - Status en commentaren.
Voordelen van deze methode	- Het is een systematische en uitgebreide techniek. Alle leidingen en tanks worden uitgebreid behandeld bij het gebruik van de gidswoorden en elementen. - Omdat de gevolgen ook onderzocht worden kan er sneller bepaald worden wat voor vervolgacties een risico moet krijgen om het risico te reduceren.
Nadelen van deze methode	- Omdat alles gedetailleerd bekeken wordt met behulp van de gidswoorden en elementen is het proces tijdrovend en duur. Daarnaast kunnen er afwijkingen uitkomen die geen vervolgacties nodig hebben omdat het risico aanvaardbaar is. - De tekeningen die gebruikt worden moeten zeer gedetailleerd zijn en moeten alle leidingen, onderdelen en bijbehorende bedrijfsomstandigheden en instrumentatie bevatten. - De gidswoorden die gebruikt worden zijn beperkt en zijn niet geschikt voor ongewone gevaren. Er moeten dan extra woorden toegevoegd worden om deze gevaren te kunnen beschrijven. - De teamleden moeten ervaren zijn om alle gevaren, de bijbehorende oorzaken en gevolgen en de realistische vervolgacties te kunnen bepalen. - Met de gidswoorden komen alleen de enkele oorzaken aan het licht en zullen twee of meer oorzaken niet behandeld worden.

Tabel 5-2: HAZOP kenmerken

Item	Deviation	Causes	Consequences	Safeguards	Action
Vessel	High level	Failure of BPCS	High pressure	Operator	
	High pressure	1) High level, 2) External fire	Release to environment	1) Alarm, operator, protection layer 2) Deluge system	Evaluate conditions for release to environment
	Low/no flow	Failure of BPCS	No consequence of interest		
	Reverse flow		No consequence of interest		

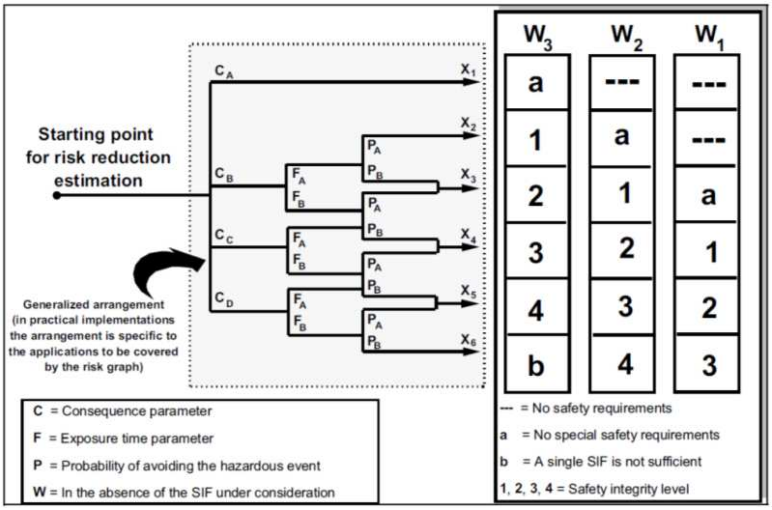
Afbeelding 5-8: Voorbeeld HAZOP uitkomst

5.2.3 Invulling stap 2 De allocatie van veiligheidsfuncties

Om te bepalen of de risico's van stap 1 gereduceerd moeten worden, wordt er in stap 2 een allocatieblad opgesteld waarin onder andere het veiligheidsniveau van alle mogelijke veiligheidsfuncties bepaald wordt. Doelen van deze stap in de IEC61511 zijn het toewijzen van de veiligheidsfuncties aan beschermlagen, het bepalen van de veiligheidsfunctie en het bepalen van het veiligheidsniveau (SIL) van elke veiligheidsfunctie. In het allocatieblad wordt dus een deel van het bepaalde risico uit de risicoanalyse overgenomen. Dit wordt dan aangevuld met de bepaling van het veiligheidsniveau waaraan de veiligheidsfunctie moet voldoen en worden er aanbevelingen gedaan hoe het risico te verlagen met een SIF. Om het veiligheidsniveau te bepalen zijn meerdere methoden mogelijk die kwantitatief, kwalitatief of een combinatie van kwantitatief en kwalitatief zijn. Mogelijke methoden van het bepalen van het veiligheidsniveau zijn:

ALARP principe (As Low As Reasonably Practicable) is een indeling van risico's in drie klassen, waarvan risico's in de hoogste klasse onaanvaardbaar zijn, de risico's in de middelste klasse nog gereduceerd moeten worden om aanvaardbaar te worden en de risico's in de onderste klasse te verwaarlozen zijn. Het idee is dat alle risico's uiteindelijk in de laatste klasse vallen zodat geen verdere reductie nodig is. De indeling is nogal ruw geschat en daarom is deze methode niet geschikt om alleen te gebruiken voor het bepalen van het veiligheidsniveau.
Semi-kwantitatieve methode is een methode die gebruik maakt van een stappenplan waarvan de risicoanalyse een van de stappen is. Daarnaast moeten de risico's uit de risicoanalyse toegewezen worden aan beschermlagen. In de laatste stappen moet er bepaald worden of er een veiligheidsfunctie nodig is die het risico reduceert en wat het veiligheidsniveau dan is.
Beschermlagen matrix methode is een methode waarbij in het ontwerpen van de installatie al rekening gehouden wordt met de voorkomende risico's. Daarna wordt er van de overige risico's bepaald wat de waarschijnlijkheid van voorkomen is en wat de ernst van het gevaar zou zijn. Op basis daarvan wordt door middel van tabellen uit de norm een veiligheidsniveau vastgesteld.
Semi-kwalitatieve methode: de gekalibreerde risicograaf is een zeer bekende methode die veel gebruikt wordt in de wereld van de functionele veiligheid. Er wordt hier gekeken naar de consequenties, de frequentie, de mogelijkheid van ontwijken en de waarschijnlijkheid van voorkomen van een gevaar. Vooraf worden echter wel de criteria in de risicograaf vastgelegd volgens de eisen van het betreffende bedrijf. Door middel van het bepalen van de parameters kan in de risicograaf het veiligheidsniveau afgelezen worden.
Kwalitatieve methode: de risicograaf is een methode die bijna hetzelfde is als de gekalibreerde risicograaf, alleen zijn hier de criteria al vastgelegd vanuit de norm. Ook hier kunnen de parameters bepaald worden om daarna het veiligheidsniveau te kunnen aflezen.
Lagen van bescherming analyse (LOPA) is een vrij uitgebreide methode die in sommige gevallen lastig is om te gebruiken. Er wordt hier gebruik gemaakt van faalcijfers van de bestaande installatie om te bekijken hoe vaak een installatie kan falen per jaar. Op basis daarvan moet er een veiligheidsfunctie toegevoegd worden die dat aantal reduceert naar een acceptabel aantal. Het voordeel van deze methode is dat er zeer nauwkeurig bepaald kan worden binnen welke SIL klasse de risico's vallen. Het nadeel is dat er veel gegevens bekend moeten zijn van de installatie, wat niet altijd het geval is. (IEC, NEN-EN-IEC61511-3:2005 en, 2014)

De voorgaande methoden zijn uitgebreider onderzocht dan hier weergegeven staat. Het uitgebreide onderzoek is te vinden in bijlage VI.
De voorkeur van Actemium gaat uit naar het gebruik van de gekalibreerde risicograaf (zie Afbeelding 5-9). Dit is de meest bekende methode voor Actemium en is ook een veelgebruikte methode bij klanten van Actemium. Wanneer echter van de bestaande installatie voldoende bekend is, is de LOPA methode ook heel geschikt.
Voor de bepaling van het SIL niveau van de ProcessCell is toch gebruik gemaakt van de gekalibreerde risicograaf. Niet alleen omdat daarvoor een standaarddocument gemaakt is voor Actemium, maar ook omdat voor de LOPA methode niet voldoende bekend is bij de ProcessCell.



Afbeelding 5-9: Gekalibreerde risicograaf

De eisen uit de norm
(IEC, NEN-EN-IEC61511-1:2005 en, 2014)
Naast het gebruik van een van de bovenstaande methoden zal het gemaakte allocatieblad nog moeten voldoen aan de eisen die weergegeven zijn in de norm onder clausule 9. Hieronder staan de belangrijkste eisen:

1. Het allocatie proces zal resulteren in:
    a. De allocatie van veiligheidsfuncties in specifieke beschermlagen met het doel van voorkomen, controleren of verzachten van gevaren uit het proces en de geassocieerde apparatuur.
    b. De allocatie van risicoreductie doelen in SIF's.
2. Het vereiste veiligheidsniveau van een SIF zal worden afgeleid.
3. Het BPCS mag geïdentificeerd worden als een beschermlaag zoals te zien in Afbeelding 5-6.
4. De risicoreductie factor voor een BPCS (die niet voldoet aan IEC61511 of IEC61508) die gebruikt wordt als een beschermlaag zal onder de 10 zijn.
5. Als een risicoreductie factor groter dan 10 wordt geclaimd voor het BPCS, dan zal het ontworpen moeten worden volgens de eisen in deze norm.

5.2.4 Invulling stap 3 De veiligheidseisen specificatie

Voor het opstellen van de veiligheidseisen specificatie, ofwel de Safety Requirements Specification (SRS), zijn in de norm geen voorbeelden of methodes gegeven, maar alleen de eisen die de norm stelt (clausule 10 en 12.2). Het document zelf kan dus per bedrijf heel verschillend zijn, maar zal wel veel dezelfde onderdelen bevatten vanuit de regelgeving in de norm. Hieronder staat een selectie van die eisen die belangrijk zijn in het SRS:

1. Een beschrijving van alle SIF's die nodig zijn om de vereiste functionele veiligheid te behalen.
2. Eisen om common cause failures te identificeren en daarmee rekening te houden.
3. Een definitie van de veilige toestand van het proces voor elke geïdentificeerde SIF.
4. Eisen voor de proof test intervallen en de maximaal toelaatbare spurious trip rate.
5. Reageer tijd eisen voor de SIS om het proces naar een veilige toestand te brengen.

6. Het SIL niveau en de modus van operatie (on demand / continuous) voor elke SIF.
7. Een beschrijving van de SIS proces metingen en de trip punten.
8. Eisen gerelateerd aan energize to trip of de-energize to trip.
9. Een applicatiesoftware SRS zal worden ontwikkeld worden en deze zal bekeken worden door de ontwikkelaar om zeker te zijn dat de eisen ondubbelzinnig, consistent en begrijpelijk zijn.

Bovenstaande eisen zijn er slechts een aantal van het totaal aantal die weergegeven worden in de IEC61511, maar deze geven al een aardige indicatie van waarop gelet moet worden in een SRS.

5.2.5 Invulling stap 4 Ontwerpen en engineeren

Voor het ontwerp van de SIS zijn in de norm geen methodes weergegeven maar alleen de eisen die de norm stelt onder clausule 11 en 12.4. Hieronder is een selectie van die eisen weergegeven die belangrijk zijn in het ontwerpproces:

1. Het ontwerp van de SIS zal overeenkomen met de SIS safety requirements specificatie, rekening houdend met alle eisen in clausule 11.
2. De SIS zal zo ontworpen worden dat wanneer hij het proces naar een veilige staat heeft gebracht, hij zal zorgen dat het proces in een veilige staat blijft totdat er een reset is gegeven, tenzij anders gespecificeerd in het SRS.
3. De detectie van een gevaarlijke fout (door diagnostische tests, proof tests of op elke andere manier) in elk subsysteem die een enkele hardware fout kan tolereren zal resulteren in een van onderstaande mogelijkheden:
    a. Een specifieke actie om een veilige staat te behouden of te bereiken;
    b. Continu veilige werking van het proces terwijl het foutieve onderdeel wordt gerepareerd.
4. Componenten en subsystemen die geselecteerd zijn als onderdeel van een SIS, zullen voldoen aan de IEC61508-2 en IEC61508-3 of zullen voldoen aan 11.4 en 11.5.3 tot 11.5.6. Hiervoor moet voldoende bewijs beschikbaar zijn.
5. Smart sensoren moeten beschermd worden tegen schrijven vanaf een remote locatie, tenzij een safety review het schrijven en lezen op een remote locatie toestaat. De safety review moet rekening houden met menselijke factoren als het niet volgen van procedures.
6. Bypass knoppen moeten beschermd worden door sleutelsloten of wachtwoorden om onbevoegd gebruik te voorkomen.
7. Het ontwerp van de SIS communicatie interface moet garanderen dat enig falen van de communicatie interface, het vermogen van de SIS om het proces naar een veilige staat te brengen niet beïnvloedt.
8. De PFD van elke SIF zal gelijk zijn of minder dan de vastgestelde PFD in het SRS. Dit moet geverifieerd worden door berekeningen

Aan in ieder geval bovenstaande eisen moet voldaan worden om het ontwerp aan de IEC61511 te laten voldoen.

5.2.6 Invulling stap 5 Installatie, inbedrijfstellen en validatie

Voor de installatie, de inbedrijfname en de validatie zijn geen voorbeelden of methoden weergegeven maar staan in clausule 14 en 15 de eisen die gelden vanuit de norm. Hieronder is een selectie van eisen weergegeven die belangrijk zijn voor deze stap:

1. Alle SIF componenten zullen correct geïnstalleerd worden volgens het ontwerp en installatieplan.
2. De SIS zal inbedrijfgesteld worden volgens de planning als voorbereiding op de laatste systeemvalidatie. In bedrijfstelling activiteiten zijn inclusief maar niet gelimiteerd tot bevestiging van het volgende:
    - Aarding is goed aangesloten;
    - Energiebronnen zijn goed aangesloten en operationeel;
    - Transportatiestoppen en verpakkingsmaterialen zijn verwijderd;
    - Er is geen fysieke schade aanwezig;

- Alle instrumenten zijn correct gekalibreerd en operationeel;
- Logic solver en inputs/outputs zijn operationeel;
- De interfaces naar andere systemen en randapparatuur zijn operationeel.

3. Correcte documentatie van de inbedrijfstelling van de SIS zal worden geproduceerd, met vermelding van de behaalde test resultaten en of de doelen en criteria, die geïdentificeerd zijn gedurende de ontwerpfase. Als er iets niet voldoet, zal de reden van dat falen gedocumenteerd worden.
4. De validatie van de SIS en de geassocieerde SIF's zal uitgevoerd worden volgens de SIS validatie planning. De validatie activiteiten zullen de volgende onderdelen bevatten (maar niet beperkt zijn tot):
   - Dat de SIS presteert onder normale en abnormale condities (bijvoorbeeld opstarten, shutdown) zoals gespecificeerd in het SRS.
   - Dat de SIS documentatie overeenkomt met het geïnstalleerde systeem.
   - Bevestiging dat de SIF's als gespecificeerd reageren op foutieve proces variabelen (bijvoorbeeld out of range).
   - Dat de SIS zorgt voor de juiste aankondigingen en het juiste operatie display.
   - Dat de SIS reset functie werkt als gedefinieerd in het SRS.
   - Dat bypass functies, opstart overrides, handmatige shutdown systemen en diagnostische alarm functies correct werken.
   - Bevestiging dat de SIS correct werkt bij het verliezen van utiliteiten (bijvoorbeeld elektriciteit of lucht) en bevestiging dat wanneer dit hersteld is, de SIS teruggaat naar de gewenste staat.
5. De software validatie zal laten zien dat alle gespecificeerde software SRS correct zijn uitgevoerd en dat de software de safety requirements niet in gevaar brengt, als de SIS in fout condities en storingsbedrijven werkt, door het uitvoeren van software functionaliteiten die niet gespecificeerd zijn.
6. Wanneer tegenstrijdigheden voorkomen tussen actuele resultaten en verwachte resultaten dan moeten de analyse en beslissingen die gemaakt worden, of er doorgegaan wordt met de validatie of teruggekeerd wordt naar een eerdere stap in de lifecycle, beschikbaar zijn als een deel van de resultaten van de veiligheidsvalidatie.
7. Na de SIS validatie en voor de geïdentificeerde gevaren aanwezig zijn, moeten de volgende activiteiten uitgevoerd worden:
   - Alle bypass functies (bijvoorbeeld PE logic solver en PE sensor forceringen, uitgeschakelde alarmen) moeten teruggezet worden naar hun normale positie.
   - Alle proces isolatie afsluiters moeten goed gezet worden volgens de opstarteisen en procedures.
   - Alle testmaterialen (bijvoorbeeld vloeistoffen) moeten verwijderd worden.
   - Alle forceringen moeten verwijderd worden, en wanneer van toepassing moeten alle machtigingen om te kunnen forceren verwijderd worden.

5.2.7 Tussenconclusie IEC61511

De IEC61511 is een norm die specifiek bedoeld is voor procesautomatisering maar zal soms verwijzingen maken naar de IEC61508. Om een procesinstallatie te laten voldoen aan de IEC61511 is het daarom verstandig om ook de IEC61508 ter beschikking te hebben. Het stappenplan dat weergegeven is in de IEC61511 is voor de procesautomatisering een leidraad om het veiligheidssysteem te kunnen ontwerpen. In stap 1 en stap 2 zijn de methodieken HAZOP en gekalibreerde risicograaf gekozen. Voor stap 3, 4 en 5 is het vrij in te vullen hoe deze documentatie opgezet gaat worden, zolang er maar rekening gehouden wordt met de regels die daarvoor gelden. Door deze stappen uit te voeren zal een deel van de lifecycle uit de IEC61511 gevolgd worden en daarmee zal de installatie die ontworpen gaat worden, voldoen aan de eisen van deze norm en daarmee ook de machinerichtlijn.

5.3 Normen deelvraag 3: IEC61508 versus IEC61511

In deze paragraaf zal aangetoond worden wat de relatie is tussen de twee genoemde normen. Allereerst zal er beschreven worden welke normen er beschikbaar zijn voor functionele veiligheid en hoe die zich verhouden tot elkaar. Daarnaast zal worden aangetoond wat de verschillen zijn en welke norm het beste voor welke toepassing gebruikt kan worden.

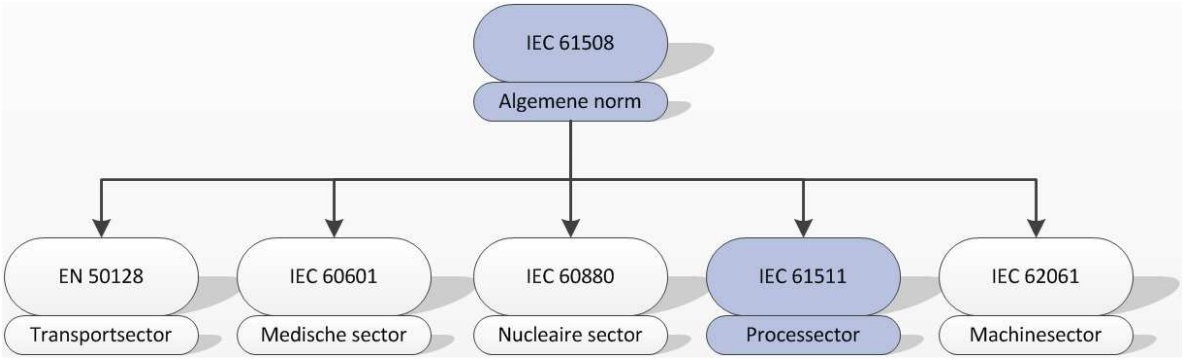
Wat is de relatie tussen de IEC61508 en de IEC61511 norm, die beide van toepassing zijn bij het laten voldoen van een procesinstallatie aan de machinerichtlijn?

Normen voor functionele veiligheid

Om de functionele veiligheid van installaties te kunnen bepalen en garanderen is in het jaar 2000 een aantal normen ontwikkeld. De ontwikkelaar van die normen is de International Electrotechnical Commission (IEC). De normen zijn bedoeld om te gebruiken bij het voldoen aan de wet- en regelgeving, zoals de machinerichtlijnen. Als algemene norm die gebruikt kan worden voor het ontwikkelen en toepassen van alle elektrische-, elektronische- en programmeerbare elektronische systemen die een veiligheidsfunctie uitvoeren is de IEC61508 in het leven geroepen. Omdat deze norm nogal een groot gebied beslaat in verschillende sectoren en bij ontwikkeling van veiligheidssystemen en veiligheidssoftware, zijn er een aantal afgeleide normen gemaakt die wat specifieker op een sector in gaan (zie Afbeelding 5-10). Dit kunnen zowel IEC (internationale) normen zijn als EN (Europese) normen. Omdat deze afgeleide normen specifieker zijn voor een bepaalde sector, zijn ze ook wat beter hanteerbaar omdat er ook voorbeelden gegeven kunnen worden die sector gerelateerd zijn en dus beter te begrijpen zijn. Zie Tabel 5-3. (Lent, Safety Requirement Specifications (intern document), 2011)

Afgeleide norm	Toelichting	Sector
EN 50128 (Spoorwegen en soortgelijk geleid vervoer).	Specifiek bedoeld voor het ontwerpen van veiligheidssystemen voor spoorwegen en soortgelijk geleid vervoer.	Transportsector.
IEC 60601 (Medische elektrische toestellen).	Specifiek bedoeld voor het ontwerpen van veiligheidssystemen voor medische installaties.	Medische sector.
IEC 60880 (Nuclear power plant).	Specifiek bedoeld voor het ontwerpen van veiligheidssystemen voor nucleaire installaties.	Nucleaire sector.
IEC61511 (Veiligheidssystemen voor de procesindustrie).	Specifiek bedoeld voor het ontwerpen van veiligheidssystemen voor procesinstallaties.	Processector.
IEC 62061 (Veiligheid van machines).	Specifiek bedoeld voor het ontwerpen van veiligheidssystemen voor machines.	Machinesector.

Tabel 5-3: Afgeleide normen, toelichting en sectoren

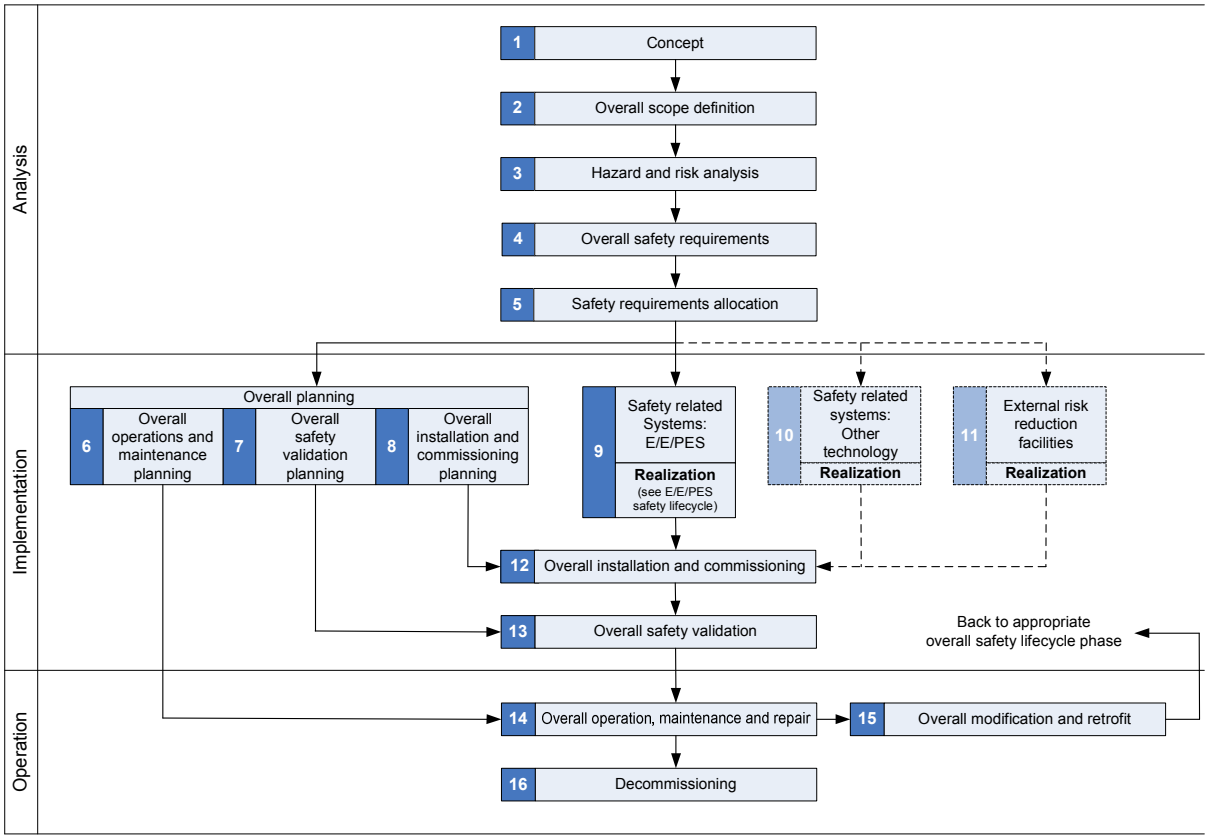


Afbeelding 5-10: Relatie IEC61508 en IEC61511

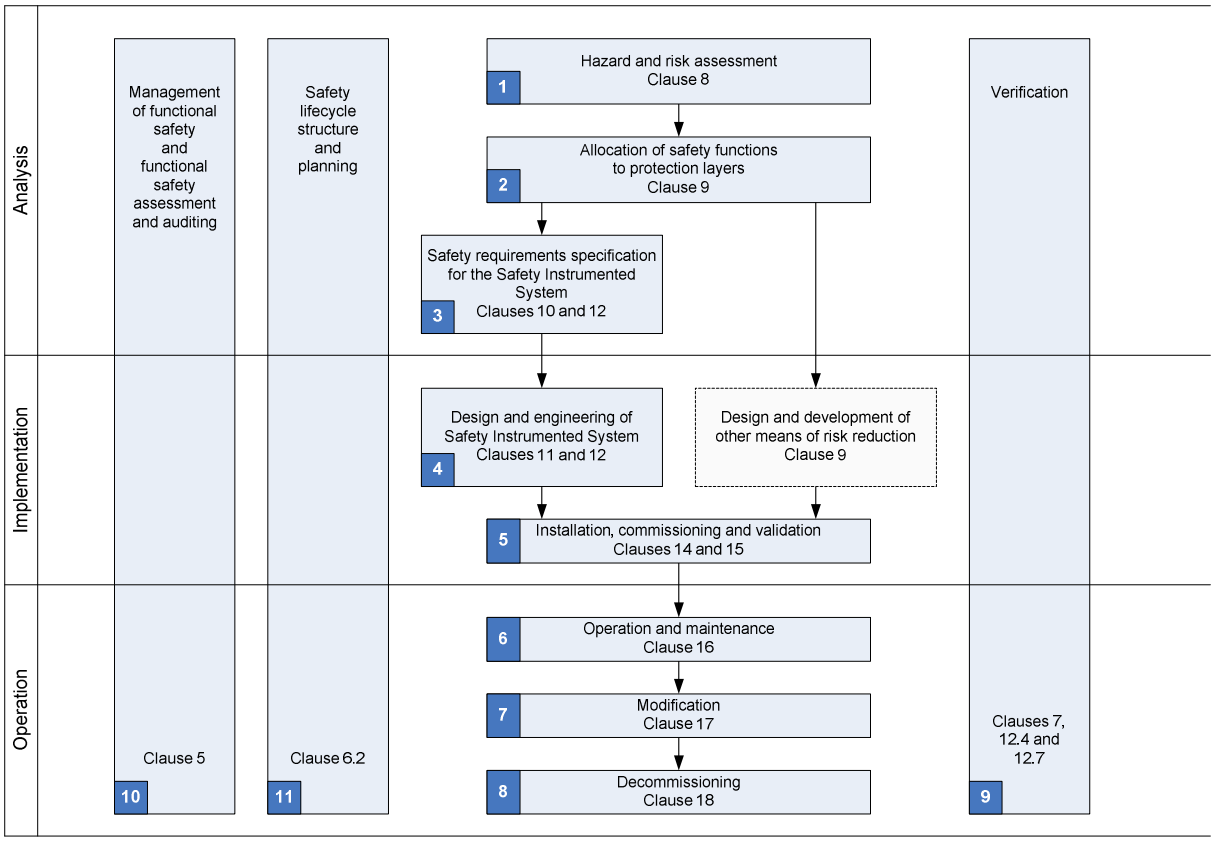
IEC61508 en IEC61511

(IEC, NEN-EN-IEC61511-1:2005 en, 2014)

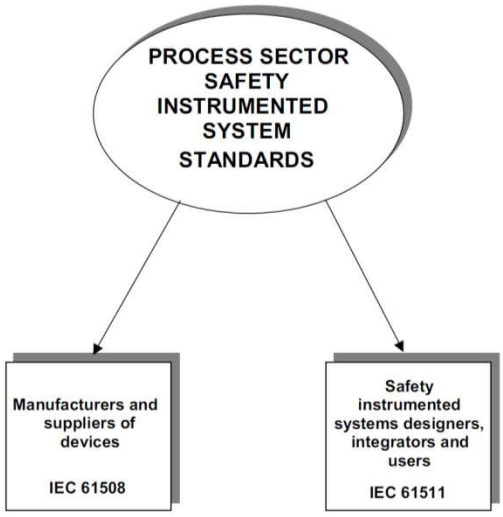
Wanneer er in de procesindustrie een veiligheidssysteem ontworpen gaat worden bij een nieuwe of bestaande installatie, kan er gebruik gemaakt worden van zowel de IEC61508 als de IEC61511. De stappenplannen die in beide normen gebruikt worden komen voor een groot gedeelte overeen met elkaar (zie Afbeelding 5-11 en Afbeelding 5-12). Ze bestaan beide uit drie verschillende fasen namelijk de analysefase, de implementatiefase en de operationele fase. De IEC61511 is echter beter te begrijpen omdat deze gerelateerd is aan de juiste sector en omdat daar voorbeelden in gegeven worden die gerelateerd zijn aan die sector. Gaat het echter over het ontwerpen van SIL waardige componenten die gebruikt worden voor een veiligheidssysteem, dan moet er gebruik gemaakt worden van de IEC61508. Wanneer er gebruik gemaakt wordt van welke norm wordt verduidelijkt in Afbeelding 5-13 en Afbeelding 5-14.



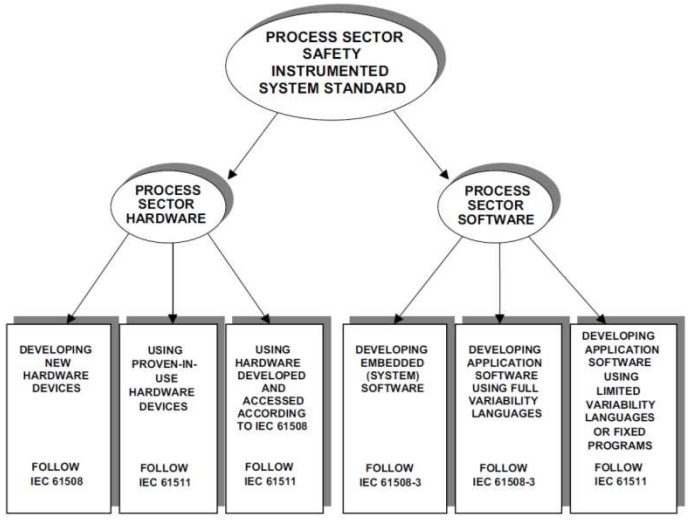
Afbeelding 5-11: Stappenplan IEC61508



Afbeelding 5-12: Stappenplan IEC61511



Afbeelding 5-13: Gebruik normen



Afbeelding 5-14: Gebruik normen met onderscheid hardware / software

5.4 Normen deelvraag 4: risico reductie

In deze paragraaf wordt onderzocht wanneer een risico aanvaardbaar is. Allereerst wordt gekeken wat de definitie van aanvaardbaar is in verschillende omgevingen. Daarna wordt gekeken hoe een ingenieur de grenzen van aanvaardbaar en niet aanvaardbaar kan vastleggen.

<u>Wanneer is een geconstateerd risico in de procesinstallatie zodanig gereduceerd met gebruik van de geldende normen dat het risico aanvaardbaar is?</u>
(IEC, NEN-EN-IEC61511-1:2005 en, 2014)

Wat is aanvaardbaar

Een risico kan voor ieder persoon anders zijn. De een vindt bijvoorbeeld een pannetje melk verwarmen risicovol terwijl een ander dit niet ziet als een risico. Om deze reden is het moeilijk om te bepalen welke risico's aanvaardbaar zijn en welke niet. In de industriële automatisering is dit niet anders. Waar bijvoorbeeld in Nederland 1 dode op een boorplatform in 10 jaar tijd aanvaardbaar is, kan dit in Mexico 1 dode per 4 jaar zijn. Hoe aanvaardbaar een risico is kan dus van veel verschillende factoren afhangen, waaronder de werkzaamheden (olieplatform of limonadefabriek), grootte van een fabriek (oppervlakte van de installatie), hoeveelheid personeel (werken er maar 10 of werken er 10.000 mensen), locatie (staat het in een dichtbevolkt gebied of in de woestijn) en zelfs werelddeel (staat de fabriek in Nederland of in India). De overheid en de normen geven echter geen definitie, hoeveel doden per jaar aanvaardbaar zijn.

Hoe bepaalt een ingenieur dan wat aanvaardbaar is?

Het beste zou zijn om alle risico's te reduceren tot nul, maar dat is niet reëel. Er zal bijvoorbeeld altijd olie gepompt moeten worden op een olieplatform zolang daar vraag naar is in de maatschappij. In de norm wordt aangegeven dat elk risico zo laag mogelijk moet worden, volgens het ALARP principe (As Low As Reasonably Practicable). Bij deze methode wordt niet alleen gekeken naar het aanvaardbaar maken van een risico, maar wordt dit ook afgewogen tegen de benodigde kosten. Bij het kijken naar aanpassingen in een installatie, kan het zo zijn dat de kosten van de aanpassingen hoger zijn dan wat de opdrachtgever een leven waard vindt (gebaseerd op de schadevergoeding aan nabestaanden of medische kosten enz.). De opdrachtgever zal dus uiteindelijk bepalen welke risico's aanvaardbaar zijn en welke niet, door daar waarden aan te geven.

De definitie van een aanvaardbaar risico is dan ook als volgt: het verlies of het risico van dat verlies, dat autoriteiten of bedrijven willen dragen, omdat zij niet bereid zijn om de financiële of materiële middelen op te brengen voor het reduceren van het risico. ("SWC", 2014)

5.5 Deelconclusie normen

De IEC61511 is een afgeleide norm van de overkoepelende norm IEC61508. Waar de IEC61508 gebruikt kan worden voor functionele veiligheid bij alle elektrische, elektronische en programmeerbare elektronische systemen, kan de IEC61511 alleen voor functionele veiligheid binnen de procesautomatisering. Er staan specifiekere eisen en voorbeelden in die gebruikt kunnen worden. Het is echter wel wenselijk om de IEC61508 ook ter beschikking te hebben, gezien deze uitgebreider de methodieken en dergelijke behandeld.

De opbouw van de stappenplannen van beide normen komt veel overeen. Ze bestaan beide uit drie fasen, te weten de analysefase, de implementatiefase en de operatiefase. Voor dit project worden een aantal stappen, uit de analysefase en de implementatiefase, van de IEC61511 gevolgd om het veiligheidssysteem te engineeren. Daarbij wordt voor stap 1 de HAZOP methode gebruikt en voor stap 2 de gekalibreerde risicograaf. Voor de overige stappen moet de regelgeving uit de norm toegepast worden. Daarnaast zullen voor stap 1, 2 en 3 zullen standaarddocumenten gemaakt worden.

Voor het bepalen wanneer een risico aanvaardbaar is, zal de ingenieur moeten overleggen met de klant. De ingenieur kan een voorstel doen waarin er naar een zo laag mogelijk risico wordt toegewerkt. De klant heeft echter altijd het laatste woord in het accepteren of afwijzen van de voorstellen.

6 Onderzoek installatie

Omdat het nieuwe veiligheidssysteem toegevoegd moet worden aan een bestaande installatie, is het belangrijk om deze installatie te onderzoeken. Allereerst wordt onderzocht wat de functie is van de huidige installatie. Daarna wordt er bekeken wat de vooraf gedefinieerde risico's inhouden. Tot slot wordt er onderzocht of er ruimte is om een veiligheidssysteem toe te voegen.

6.1 Installatie deelvraag 1: Functie ProcessCell

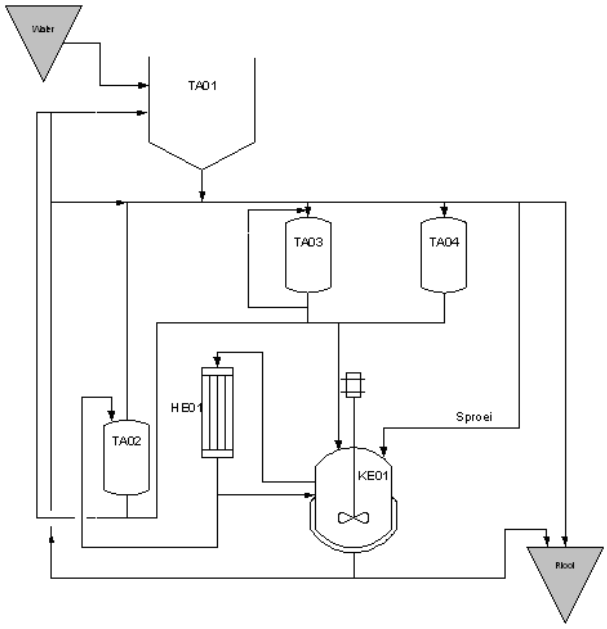
Gezien een veiligheidssysteem moet ingrijpen op de normale werking van het proces, is het nuttig om te weten wat dat normale proces precies doet. In deze paragraaf wordt daarom de functie van het proces onderzocht. Daarnaast wordt er niet alleen gekeken naar de huidige functie, maar ook naar eventuele nieuwe functies bij gebruik van natronloog.

Wat is de functie van de procesinstallatie bij het gebruik van natronloog?

Het doel van deze opdracht is het toevoegen van een veiligheidssysteem aan de EduLab procesinstallatie en om de standaard documenten te maken voor het toepassen van de IEC61511 norm. Omdat het hier gaat om een demo model en geen echte procesinstallatie heeft de procesinstallatie geen specifieke functie behalve voor educatief gebruik.

De afzonderlijke functies

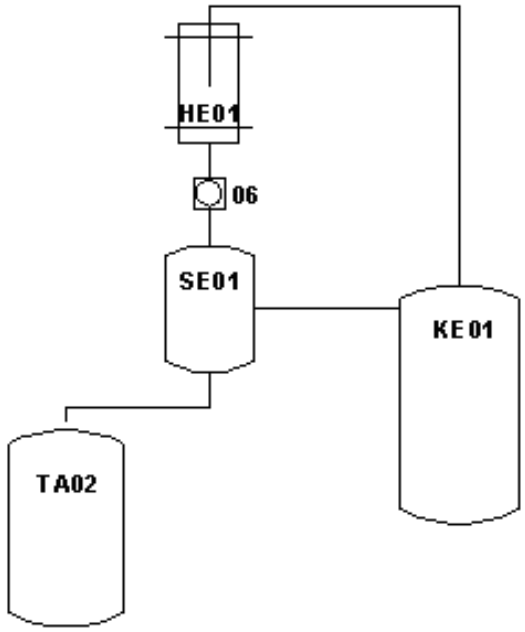
De installatie zelf heeft geen specifieke functie maar de losse onderdelen als de tanks, de reactor en de condensor hebben wel een of meerdere functies die zij kunnen vervullen. In Afbeelding 6-1 zijn de tanks en andere onderdelen te zien die in de EduLab ProcessCell zitten. In bijlage I is de P&ID van de installatie toegevoegd. Hieronder wordt beschreven wat de onderdelen allemaal voor functie hebben en in Afbeelding 6-4 wordt dit visueel weergegeven. (Laar, 2011)



Afbeelding 6-1: Vereenvoudigde weergave EduLab ProcessCell

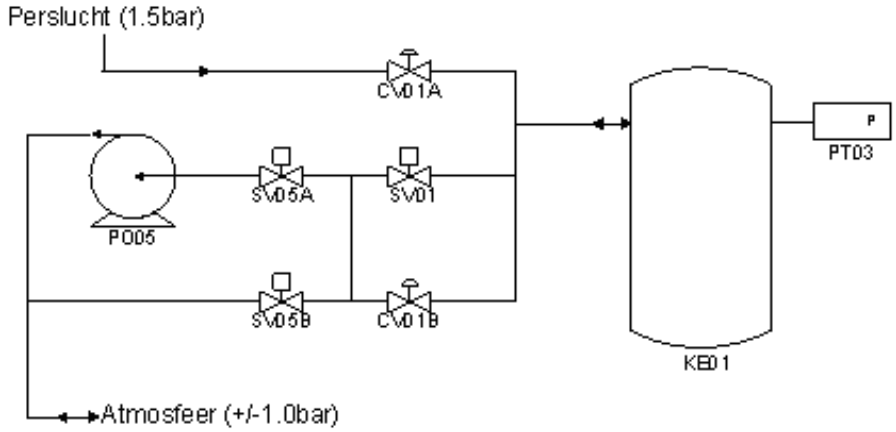
Reactor (KE01) is het belangrijkste deel van de installatie. In deze tank kunnen grondstoffen toegevoegd worden, dit kan gemengd worden met een mixer, de inhoud kan rondgepompt worden, de inhoud kan verwarmd worden en kan op druk gebracht worden. Daarnaast kan het eindproduct gedestilleerd worden of kan door het veranderen van de druk het kookpunt van de inhoud verhoogd of verlaagd worden.

Condensor (HE01) is apart weergegeven in Afbeelding 6-2. Als de vloeistof in de reactor gekookt wordt, stijgt het gas naar de condensor, waar condensatie plaatsvindt. Het condenseren kan versneld worden door de condensor te koelen met leidingwater. Het extra koelen kan geregeld worden met een temperatuurregeling en een flowregeling. Het condensaat zal via SE01 afgevoerd worden naar KE01 of naar TA02. Als het condensaat naar KE01 geleid wordt is er sprake van reflux, dat wil zeggen dat de inhoud van de reactor kan blijven koken zonder dat er massa verloren gaat.



Afbeelding 6-2: Condensaat systeem

Vacuüm/druksysteem is apart weergegeven in Afbeelding 6-3. De reactor kan onder druk gebracht worden door middel van perslucht en de regelafsluiter CV01A. Het vacuüm trekken van de tank gebeurt door de pomp PO05 en de kleppen SV05A en SV01 of CV01B. Voor de gasafvoer worden CV01B en SV05B of SV05A gebruikt.



Afbeelding 6-3: Vacuüm- / druksysteem

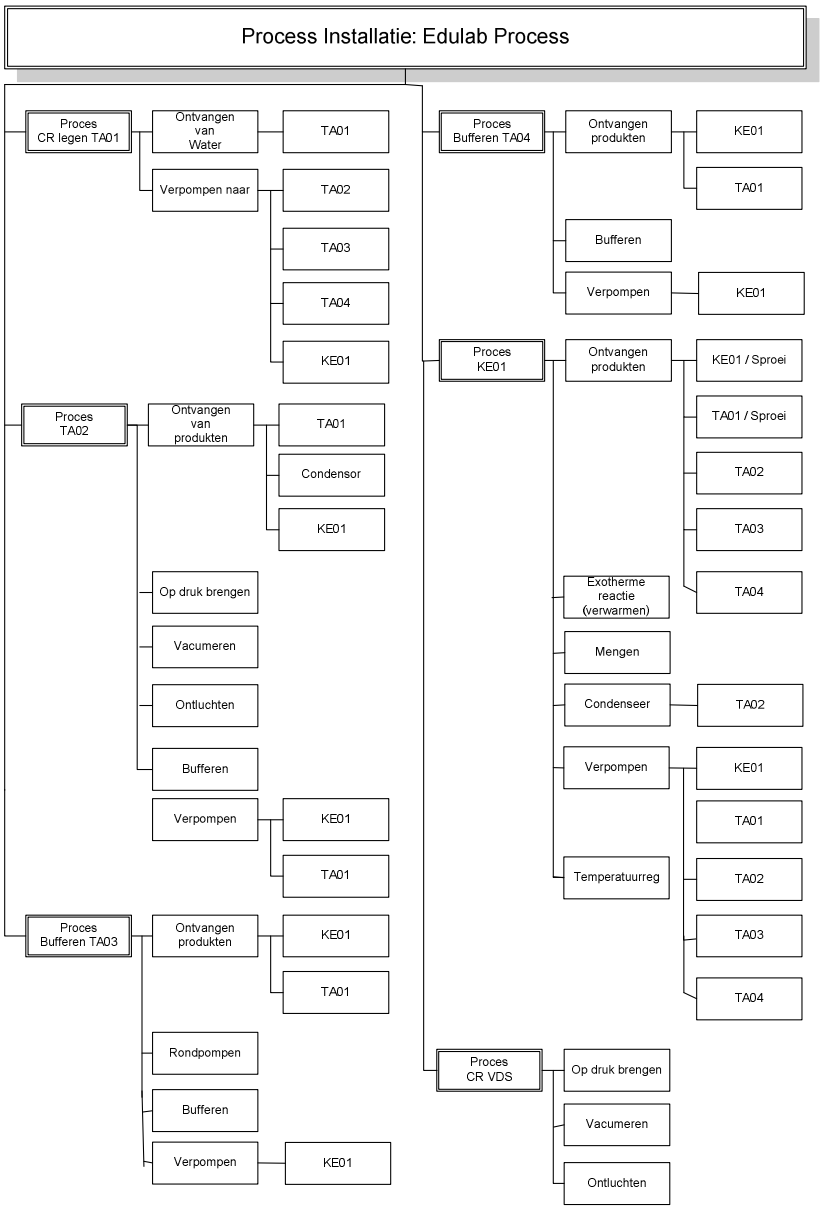
De procesthermostaat kan de temperatuur in de reactor regelen tussen de -25°C en 130°C. Vanwege veiligheidsredenen wordt de temperatuur echter maar tussen de 5°C en 80°C geregeld. Omdat de reactor vacuüm getrokken kan worden waardoor het kookpunt verlaagd kan worden tot 60°C, kan energie bespaard worden en is de installatie milieuvriendelijker.

In buffertanks TA02, TA03 en TA04 kunnen andere stoffen opgeslagen worden om te mengen in de reactor. Met TA03 kan ook nog voorgemengd worden door de inhoud rond te pompen in de installatie.

Heater (HE02) bevat water wat verwarmd of gekoeld wordt, afhankelijk van de gewenste temperatuur. Dat gekoelde of verwarmde water kan dan door de mantel, die om de reactor heen zit, gepompt worden waardoor de inhoud van de reactor gekoeld of verwarmd wordt.

Exotherme reactie (HE03) is een heater die water in korte tijd flink kan verwarmen. Door dit water in de tank toe te voegen kan een exotherme reactie in de reactor gesimuleerd worden. Zo hoeven er geen andere stoffen in de installatie gebruikt te worden behalve water.

Afvoer- / aanvoertank (TA01) zit rechtstreeks aan het stadswater en aan het riool verbonden. Via deze tank kan dus product afgevoerd worden, gespoeld worden en rondgepompt worden met de mogelijkheid van mengen met vers water.



Afbeelding 6-4: Functies EduLab ProcessCell

(Smits, 2009)

Mogelijke functies

In het PID is aangegeven dat de procesinstallatie geschikt moet zijn voor het gebruik van natronloog. Omdat het een demomodel is zal er waarschijnlijk geen natronloog gebruikt worden in de installatie. Maar om de risico's wat reëler te maken wordt natronloog als de verwerkte stof gebruikt. Omdat deze stof gekozen is om te verwerken in de procesinstallaties kunnen dus wel een aantal functies bedacht worden die de procesinstallatie zou kunnen hebben.

Functie 1: Het maken van natronloog.
Door natriumhydroxide te mengen met water in de reactor vindt er een exotherme reactie plaats waarbij natronloog ontstaat. De exotherme reactie kan in de reactor onder controle gehouden worden door het BPCS en door de veiligheidsbesturing.

Functie 2: Het reinigen van de reactor door het uitvoeren van een CIP met natronloog.
Cleaning In Place (CIP) is een veel voorkomende reiniging in procesinstallaties. Het is een reiniging die gedaan wordt door het BPCS, zonder dat daarvoor onderdelen gedemonteerd worden of personen aan te pas komen. Een dergelijke reiniging kan bestaan uit verschillende stadia, maar de meest simpele en veel voorkomende stadia zijn voorspoelen met water, reinigen met natronloog en naspoelen met water.

6.2 Installatie deelvraag 2: de risico's

In deze paragraaf wordt onderzocht wat voor gevaren het gebruik van natronloog met zich meebrengt. De vooraf gedefinieerde risico's worden hier toegelicht en er wordt gekeken naar de gevolgen van die risico's.

Welke risico's doen zich voor bij het gebruik van natronloog in de procesinstallatie?

De risico's die vooraf al vastgesteld zijn waarop het veiligheidssysteem gebaseerd wordt zijn (Lent, Lead engineer hardware, 2014)(Verburg, 2014):

1. Het te snel oplopen van de temperatuur bij een exotherme reactie in een reactortank;
2. Het te hoog worden van de druk in een reactortank;
3. Het te hoog worden van het niveau in een watertank.

Een te hoge temperatuur in de reactor:
De reactor is een gesloten vat waarin vloeistoffen gemengd kunnen worden en waar exotherme reacties in plaats kunnen vinden. Wanneer deze exotherme reactie uit de hand zou lopen, zou daardoor de druk in het reactorvat kunnen oplopen. Als deze te hoog wordt kan het reactorvat scheuren. Dit resulteert in het vrijkomen van schadelijke en hete gasssen, en het vrijkomen van hete vloeistof. Naast de beschadiging aan het reactorvat kan er schade zijn aan andere materialen, aan operators van de installatie of aan het milieu. Om te weten of een exotherme reactie uit de hand zou lopen, moet er gekeken worden naar de temperatuursstijging per tijdseenheid.

Een te hoge druk in de reactor:
Een te hoge druk in de reactor zou wederom resulteren in het scheuren van het reactorvat. Daardoor zou natronloog uit het reactorvat kunnen stromen en schade aanrichten aan materialen, aan operators van de installatie of aan het milieu.

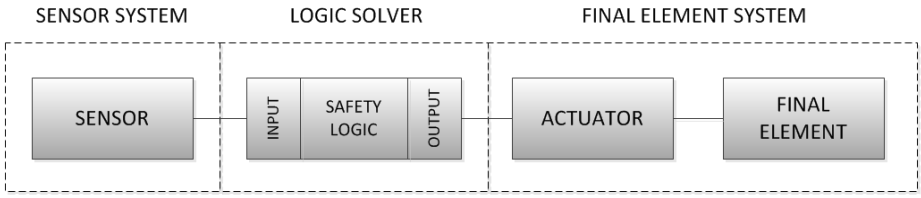
Het overvullen van tank TA01:
Tank TA01 is een tank waar in het demo model zowel vloeistof uitgehaald kan worden voor het vullen van de buffertanks of het vullen van de reactor, als vloeistof in afgevoerd kan worden vanuit de reactor of vanuit tank TA02. Daarnaast kan er vers water uit de stadswaterleidingen toegevoegd worden om de tank te vullen. Wanneer deze tank zou overlopen en de tank zou een bepaalde hoeveelheid natronloog bevatten, dan zou dit schade kunnen veroorzaken aan andere materialen, aan operators van de installatie of aan het milieu.

6.3 Installatie deelvraag 3: veiligheidssysteem toevoegen

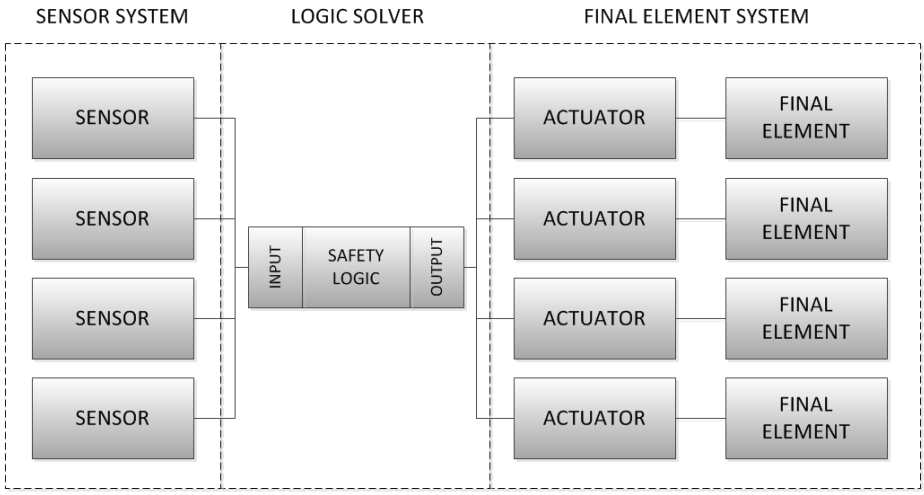
Omdat het veiligheidssysteem toegevoegd moet worden aan een bestaande installatie, moet er bekeken worden of er ruimte is voor de onderdelen. In deze paragraaf wordt onderzocht uit welke onderdelen een veiligheidssysteem bestaat. Daarnaast wordt gekeken naar de mogelijke ruimte om de onderdelen in te kunnen bouwen.

Hoe kan een veiligheidssysteem, dat voldoet aan de machinerichtlijn en dat onafhankelijk is van de normale besturing, toegevoegd worden aan de procesinstallatie?

Bij het ontwerpen van een veiligheidssysteem kan het voorkomen dat er meerdere veiligheidsfuncties toegevoegd moeten worden. Een veiligheidsfunctie bestaat meestal uit een logic solver, een sensor, een actuator en een eindelement zoals te zien in Afbeelding 6-5. Deze veiligheidsfuncties gezamenlijk, met meerdere sensoren en eindelement systemen, vormen het veiligheidssysteem zoals te zien in Afbeelding 6-6. Na het vastleggen van de eisen van het veiligheidssysteem zal bekend zijn hoeveel sensoren, logic solvers, actuatoren en eindelementen er toegevoegd moeten worden bij de huidige installatie.



Afbeelding 6-5: Opbouw SIF



Afbeelding 6-6: Opbouw SIS

De logic solver

De logic solver, ofwel in dit geval de veiligheidsPLC die gesponsord wordt door de leverancier HIMA, zal in een van de kasten naast de installatie toegevoegd moeten worden. In Afbeelding 6-7, Afbeelding 6-8, Afbeelding 6-9 en Afbeelding 6-10 is te zien dat in ieder geval in kast 3 en kast 4 nog voldoende ruimte is om een veiligheidsPLC bij te bouwen.

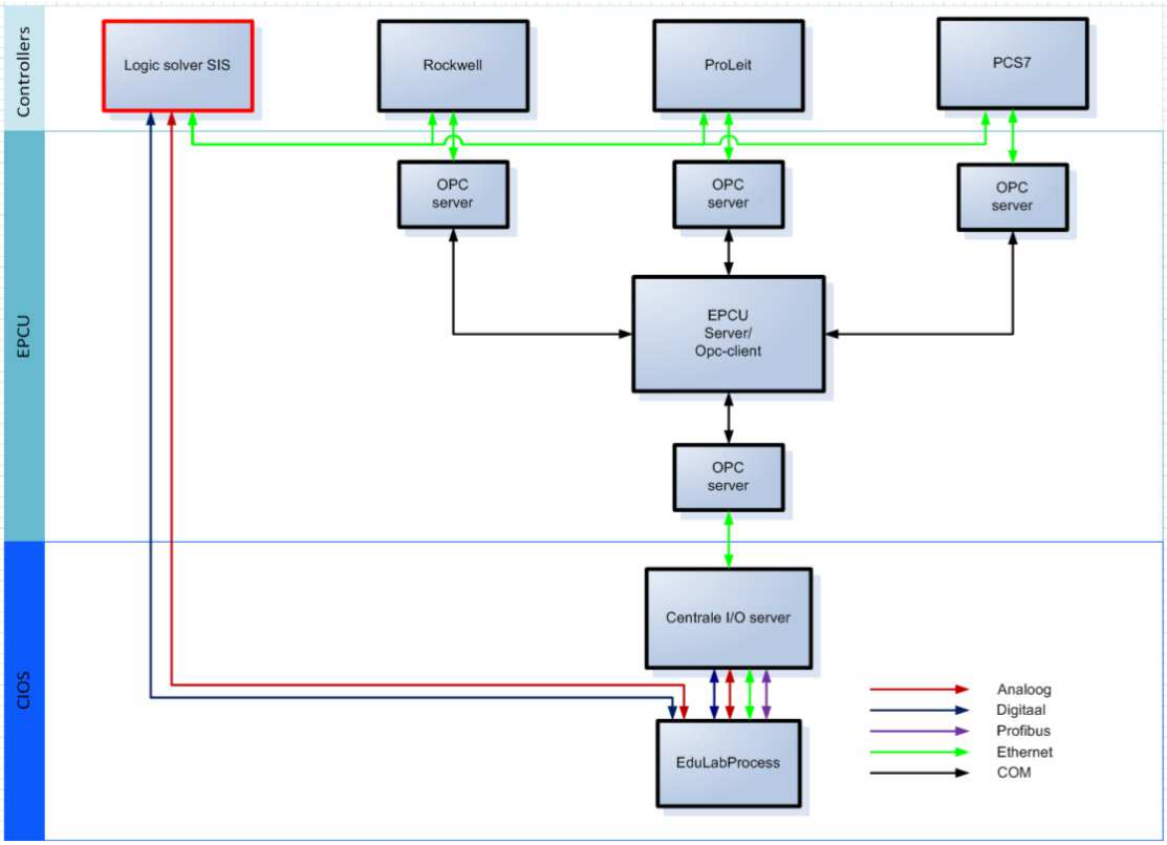

Afbeelding 6-7: Kast 1


Afbeelding 6-8: Kast 2

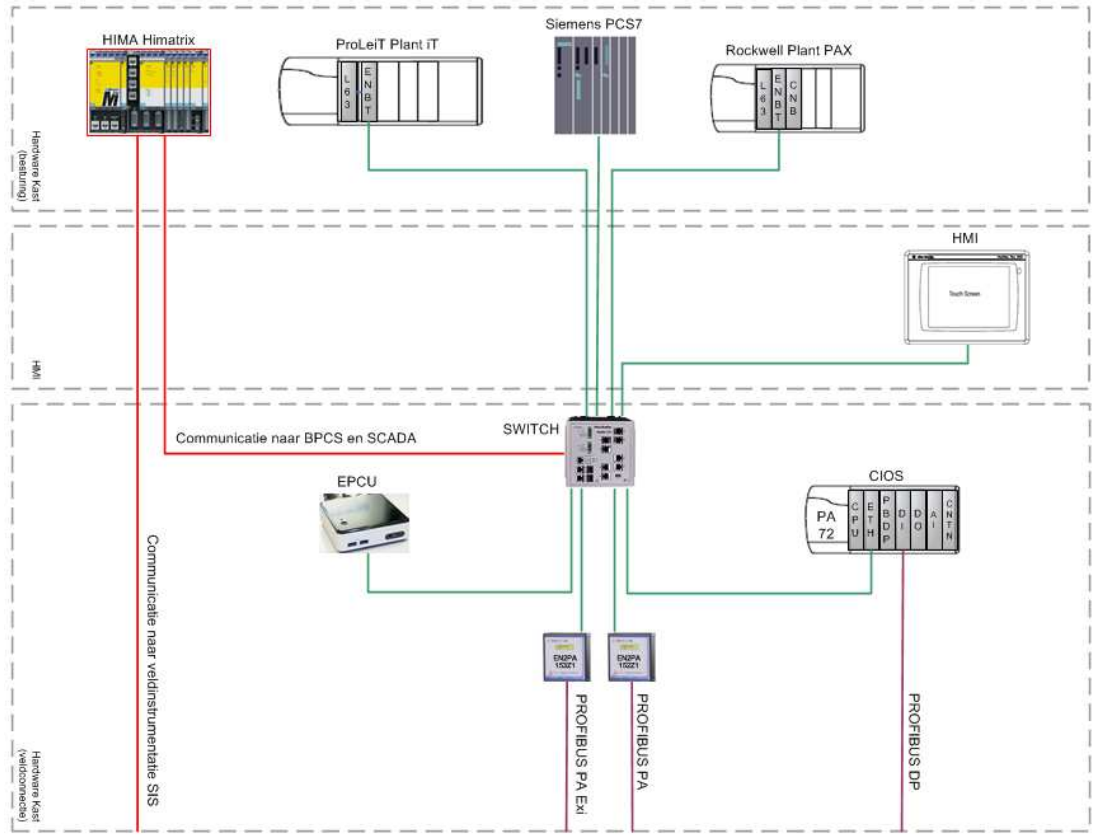

Afbeelding 6-9: Kast 3


Afbeelding 6-10: Kast 4

Hoe de gegevensstromen gaan lopen is te zien in Afbeelding 6-11. Daarin is te zien dat de nieuwe PLC die toegevoegd gaat worden, directe communicatie met de veldinstrumentatie heeft in de vorm van digitale en analoge signalen en communicatie met de besturingssystemen in de vorm van ethernet. De connecties met de veldinstrumentatie zijn te zien in Afbeelding 6-12. (Peters, 2014)



Afbeelding 6-11: Overzicht gegevensstromen

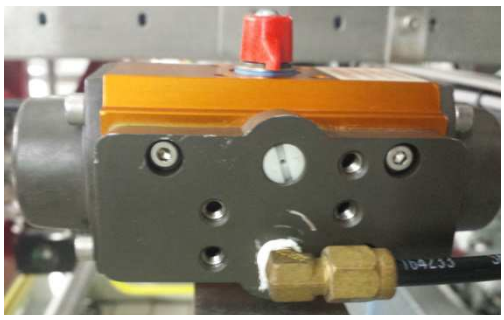


Afbeelding 6-12: Gedeeltelijk overzicht veld

Actuatoren

Voor de actuatoren als solenoïds, veiligheidsventielen en dergelijke moet er gekeken worden naar de huidige opbouw. De huidige kasten die bij de installatie aan de muur hangen zijn vrij vol, maar naast deze kasten is nog voldoende ruimte om een kast bij te bouwen. (zie Afbeelding 6-13). Een andere optie is om de ventielen rechtstreeks op de kleppen te monteren. De kleppen hebben namelijk allemaal een mechanische NAMUR aansluiting (zie Afbeelding 6-14). Dit is een bepaald gatenpatroon dat overeenkomt met het gatenpatroon op een ventiel met een NAMUR aansluiting.

Afbeelding 6-13: Muur met ventielkasten



Afbeelding 6-14: Mechanische NAMUR aansluiting

Sensoren en final elementen

Voor de sensoren en eindelementen die in de installatie zelf ingebouwd moeten worden, zal gekeken moeten worden naar de ruimte op de betreffende tanks / reactor en naar de leidingen waar de componenten ingebouwd moeten worden (zie Afbeelding 6-15). Omdat er al sensoren op de reactortank geïnstalleerd zijn die druk en temperatuur kunnen meten zullen deze gebruikt worden voor het veiligheidssysteem. Er is dus op de reactortank geen extra inbouwruimte nodig voor nieuwe sensoren. Voor de controle van het waterniveau in tank TA01 is bovenop voldoende ruimte om een sensor te plaatsen. Omdat kleppen in de leidingen bijplaatsen te duur zou worden is er vanuit Actemium besloten om geen nieuwe kleppen bij te plaatsen. In plaats daarvan worden er alleen de nieuwe ventielen toegevoegd die dan de oude kleppen aansturen.

Afbeelding 6-15: Procesinstallatie

6.4 Deelconclusie installatie

De installatie is een demo model en vervuld geen specifieke functie. Omdat dit voor de opdracht geen toegevoegde waarde heeft, zal er ook geen fictieve functie bedacht worden. Er zal rekening gehouden worden met de afzonderlijke functies van elke tank, reactor enz. Daarnaast zal er rekening gehouden worden met het gegeven dat natronloog in elk deel van de installatie kan voorkomen.

Bij het uitvoeren van de risicoanalyse zoals beschreven in het stappenplan uit de IEC61511 norm zullen meerdere risico's van de installatie gedocumenteerd worden. Enkel de drie vooraf gedefinieerde risico's zullen echter ook uitgewerkt worden bij de vervolgstappen van het stappenplan uit de IEC61511. Deze risico's zijn vooraf gekozen omdat deze zonder al te veel aanpassingen aan de installatie gereduceerd kunnen worden.

Voor de plaatsing van de logic solver componenten wordt kast 3 gekozen om alles in te bouwen. Voor de ventielen wordt geen extra kast geplaatst, maar wordt gebruik gemaakt van de NAMUR aansluiting. Voor de sensoren is alle ruimte beschikbaar die nodig is of worden er sensoren gebruikt die al in de installatie zitten. Er worden geen nieuwe kleppen geplaatst, dus daar is ook geen ruimte voor nodig in het veld.

7 Onderzoek besturing

In dit hoofdstuk zal onderzoek gedaan worden naar de besturing in een veiligheidssysteem. Allereerst zal onderzocht worden wat de functie van een veiligheidssysteem is (paragraaf 7.1). Daarna zal gekeken worden waarom een veiligheidsPLC beter is dan een gewone PLC (paragraaf 7.2). Tot slot wordt er bekeken hoe er in de huidige installatie een melding naar de SCADA schermen gestuurd kan worden (paragraaf 7.3).

7.1 Besturing deelvraag 1: functie veiligheidssysteem

In deze paragraaf wordt onderzocht waar een veiligheidssysteem voor dient in een installatie, wanneer er al een gewone besturing aanwezig is.

Wat is de functie van een veiligheidssysteem bij een procesinstallatie in de chemische industrie?

(Assmann & Kroonen, 2009)(Pietersen I. C., 2008)(Pranger, 2008)

Veiligheid binnen industriële bedrijven is vaak op te delen in procesveiligheid en arbeidsveiligheid. Het verschil tussen deze twee vormen van veiligheid is dat arbeidsveiligheid gericht is op kleinere bedrijfsongevallen als vallen, struikelen, snijden enz. Procesveiligheid is meer gericht op grotere ongevallen waarbij bijvoorbeeld apparatuur hapert en dat ernstige gevolgen, als meerdere gewonden of doden, als resultaat heeft. Vooral in de chemische industrie, wanneer er chemische stoffen vrijkomen die bijtend, giftig of brandbaar zijn, kan dit grote gevolgen hebben. Het doel van procesveiligheid is dan ook het verwijderen of reduceren van gevaren in plaats van te beschermen tegen die gevaren. Een mogelijkheid om dat te doen is bijvoorbeeld om een veiligheidssysteem toe te voegen aan een procesinstallatie.

De functie

Een veiligheidssysteem of een safety instrumented system (SIS) is bedoeld om de installatie naar een veilige toestand te sturen wanneer er abnormale procescondities voorkomen in de installatie. Veiligheidssystemen moeten beschikbaar en betrouwbaar zijn om ervoor te zorgen dat er zo min mogelijk productieverlies voorkomt. Veiligheidssystemen werken gescheiden en onafhankelijk van het BPCS maar kunnen wel bestaan uit vergelijkbare elementen, namelijk een sensor, een logic solver en een eindelement. De sensor zal de abnormale procesconditie waarnemen, de logic solver zal een signaal van de sensor ontvangen en op basis van deze signalen een beslissing nemen om het eindelement aan te sturen zodat het proces een veilige staat bereikt.

Wanneer alle beveiligingen in het BPCS uitvallen, blijft er een restrisico over. Dat restrisico is het risico wat het veiligheidssysteem moet opvangen. De Safety Integrity Level (SIL) classificatie is een maat voor het restrisico en kan geclassificeerd worden met SIL 1 tot en met SIL 4. Deze klasse bepaalt hoe betrouwbaar en beschikbaar het veiligheidssysteem moet zijn. Wanneer gekeken wordt naar een SIF is het ook zo dat de SIL klasse van de SIF gelijk ligt aan de laagste SIL klasse van de individuele componenten. Een ketting is nou eenmaal zo sterk als de zwakste schakel. Het komt ooit voor dat sommige sensoren of eindelementen niet verkrijgbaar zijn met een SIL klasse hoger dan SIL 2. Wanneer een veiligheidssysteem dus moet functioneren op SIL 3 niveau, zullen er maatregelen getroffen moeten worden als het dubbel (redundant) uitvoeren van sensoren en / of eindelementen om toch de gevraagde klasse te behalen.

7.2 Besturing deelvraag 2: veiligheidsPLC versus gewone PLC

In deze paragraaf wordt onderzocht waarom voor een veiligheidssysteem geen gewone PLC gebruikt kan worden.

Wat kan een veiligheidsPLC meer of beter dan een gewone PLC bij het besturen van een veiligheidssysteem in de procesinstallatie die moet voldoen aan de IEC61511 norm?

Zoals in voorgaande paragraaf al aangegeven, is de functie van een veiligheidssysteem het opvangen van het restrisico wat niet opgevangen kan worden door het normale besturingssysteem. Vanuit de norm wordt ook aangegeven dat het veiligheidssysteem in een andere beschermlaag zit dan het normale besturingssysteem. Dat wil dus zeggen dat de BPCS PLC niet gebruikt mag worden voor de veiligheidsfuncties, maar dat hiervoor een andere PLC gebruikt moet worden die moet voldoen aan de IEC61508. Het gebruik van een gewone PLC voor het uitvoeren van veiligheidsfuncties kan dus wel, maar moet op meerdere manieren gevalideerd worden. Een van deze manieren is het berekenen van de faalkansen van de PLC waar deze bij een gecertificeerde veiligheidsPLC al bekend zijn. Vanuit de norm wordt er dus geadviseerd om een veiligheidsPLC te gebruiken die gecertificeerd is omdat dit een hoop kosten en tijd bespaart bij de validatie van het project.

VeiligheidsPLC versus gewone PLC

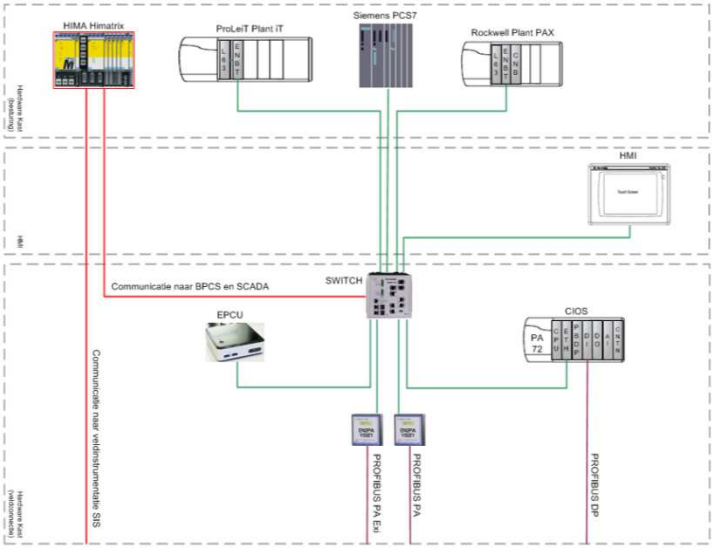
(With, PMA 1-2-2012 pag. 4-7, 2012)(With, PMA 5-2012 pag.4-6, 2012)("Rockwell.Automation", 2002)
Wanneer er vergeleken wordt wat een veiligheidsPLC nu meer of beter kan dan een gewone PLC, komt het vooral neer op de faalkansen van een veiligheidsPLC die hem beter maakt. Zoals bekend wordt een veiligheidsPLC gemaakt en getest volgens de norm. Daarbij worden veel PLC's gecertificeerd met een compatibiliteit voor een bepaald SIL niveau. Deze compatibiliteit wil zeggen dat de PLC zelf niet SIL gecertificeerd is, maar dat deze in combinatie met de geschikte sensoren, actuatoren en eindelementen het betreffende SIL niveau kan behalen. Het SIL niveau wat aan de PLC gekoppeld wordt hoort bij een PFD (Probability of Failure on Demand) die aangeeft hoe vaak de PLC kan falen wanneer deze aangeroepen wordt. Om deze PLC's een goede waarde van PFD te kunnen geven, worden er in de PLC maatregelen getroffen zodat de PLC weinig kan falen. Er zitten bijvoorbeeld meerdere CPU's in die elkaar controleren, de uitgangen worden in drievoud aangestuurd (intern) en gecontroleerd op verschillende manieren. Ook wordt er tijdens gebruik getest of de uitgangen nog goed zijn door het heel kort uitschakelen van deze uitgangen. Wanneer deze uit en weer aangeschakeld worden zal getest worden of deze nog werken, wanneer hiervoor een aanvraag is. En de tijd dat de uitgangen uitgeschakeld zijn, zijn zo kort dat het proces hier niets van merkt. De PLC doet dus aan zelfdiagnose en zal ook delen uitschakelen wanneer er een interne fout geconstateerd wordt. Al deze functies bij elkaar maakt de veiligheidsPLC betrouwbaarder dan een gewone PLC die deze functies niet heeft.

7.3 Besturing deelvraag 3: meldingen naar SCADA

Een veiligheidssysteem dient niet enkel te worden toegevoegd, maar dient ook in het huidige systeem te worden geïntegreerd. Om die reden moet onderzocht worden hoe deze twee systemen kunnen samenwerken. Het is prettig voor de operator om ook te weten dat een veiligheidssysteem ingegrepen heeft bij het falen van het BPCS.

Hoe kan er in de huidige SCADA systemen een melding getoond worden aan de operator van de procesinstallatie wanneer het veiligheidssysteem ingegrepen heeft op de normale besturing?

Om te zorgen dat de operator weet wanneer het veiligheidssysteem heeft ingegrepen en om ondersteunende functies vanuit het BPCS te laten uitvoeren, zal er communicatie nodig zijn vanuit de SIS naar het BPCS en de bijbehorende SCADA. In paragraaf 6.3 is te zien hoe de SIS bij het huidige systeem bijgebouwd kan worden (zie Afbeelding 7-1). De switch in Afbeelding 7-2 is erin gebouwd omdat deze kan zorgen dat de EPCU, en alle signalen uit het veld aankomen bij de drie besturingssystemen. De switch heeft ook connectie met het netwerk in het EduLab zodat de PLC kan communiceren met de SCADA systemen in de operator ruimte. Via de switch kan de SIS dus communiceren met zowel de SCADA systemen, als met de BPCSen, zodat de operator kan zien dat het veiligheidssysteem heeft ingegrepen en dat het BPCS ondersteunende functies kan uitvoeren als het veiligheidssysteem hier om vraagt.



Afbeelding 7-1: Communicatie naar BPCS en SCADA

Afbeelding 7-2: Switch

7.4 Deelconclusie besturing

De functie van een veiligheidssysteem bij een procesinstallatie in de chemische industrie is het opvangen van het restrisico wat het BPCS niet kan opvangen, en daarmee het reduceren of verwijderen van de gevaren.

De zelfdiagnose en de intern redundante uitvoeringen van bepaalde onderdelen maakt een veiligheidsPLC betrouwbaarder voor het uitvoeren van een veiligheidsfunctie dan een gewone PLC. Door deze functies zal de veiligheidsPLC minder snel falen in vergelijking met een gewone PLC.

Via de switch kan de SIS communiceren met het BPCS en de SCADA systemen om te waarschuwen als het veiligheidssysteem ingegrepen heeft. Op Afbeelding 7-2 is te zien dat poort 8 nog vrij is dus daar kan de SIS op aangesloten worden.

8 Ontwerp

Zoals hiervoor in de analyse is weergegeven, wordt bij het gebruik van de normen het stappenplan uit de IEC61511 gebruikt (zie Afbeelding 5-5). Door het volgen van dit stappenplan zal er uiteindelijk een ontwerp gemaakt worden dat gebruikt kan worden voor het veiligheidssysteem. Voordat het zover is zijn er echter een aantal documenten nodig om aan te tonen dat er onderzoek is gedaan naar de eisen van het veiligheidssysteem. In dit hoofdstuk wordt weergegeven welke documenten gemaakt zijn die Actemium in de toekomst voor klanten kan gebruiken en hoe die documenten voor het project zijn gebruikt om het stappenplan te volgen. Omdat Actemium ook veel met klanten uit het buitenland werkt zijn de standaarddocumenten zowel in het Nederlands als in het Engels geschreven. In dit verslag worden alleen de Nederlandse documenten besproken.

8.1 Stap 1: De risicoanalyse

Voor de risicoanalyse moet een standaarddocument gemaakt worden met behulp van de in de analyse gekozen HAZOP methode. Vanuit de norm voor HAZard and OPerability studies (de IEC 61882) en Actemium, zijn een aantal eisen naar voren gekomen waaraan het standaard formulier moet voldoen. In Tabel 8-1 is te zien dat het document bestaat uit minimaal vier pagina's. Een van die pagina's is het werkblad, dat gebruikt wordt voor de HAZOP zelf. De overige pagina's zijn informatief en kunnen buiten de uitvoering van de risicoanalyse ingevuld worden. De informatie die aanwezig moet zijn op elke pagina is:

1 Voorblad:	3 Werkblad HAZOP:
Naam van de opdrachtgever;	Referentienummer;
Opdrachtnummer van de opdrachtgever;	Item;
Project of projectdeel;	Gidswoord;
P&ID referenties;	Element;
Eventueel andere referenties;	Afwijking;
Namen, bedrijf, functie en datum van de personen die meewerken aan de HAZOP;	Oorzaak;
	Gevolg;
Namen van de auteurs;	Voorzorgmaatregelen;
Revisienummer en datum van het document;	Opmerkingen;
Projectnummer van de opdrachtnemer;	Benodigde acties;
Naam van goedkeurder;	Naam voor het uitvoeren van die acties.
Datum van goedkeuring;	
Handtekening ter goedkeuring.	
2 Revisiebeheer:	4 Actielijst:
Revisienummer;	Referentienummer;
Datum;	Beschrijving van het risico;
Aanpassingen;	Benodigde acties;
Naam van de aanpasser.	Naam voor het uitvoeren van die acties;
	De status van de actie.

Tabel 8-1: Eisen risicoanalyse

Het standaarddocument van de risicoanalyse is te vinden in bijlage VII. Omdat de gidswoorden op het werkblad en de status op de actielijst een beperkt aantal mogelijkheden hebben, is van die twee onderdelen een pull down menu gemaakt.

Het uitvoeren van de risicoanalyse

Het standaarddocument is uiteindelijk ingevuld voor de risicoanalyse van de ProcessCell. Het uitvoeren van een risicoanalyse was voor deze opdracht overbodig, gezien de drie risico's vooraf al bekend waren. Toch is er een risicoanalyse ingepland en uitgevoerd met een selecte groep medewerkers om te ervaren hoe dit in zijn werk gaat. Hiervoor is een team samengesteld, bestaande uit de beheerder van het Edulab als proceskenner, de veiligheidscoördinator als veiligheidsexpert, een stagiair als operator en de afstudeerster als projectleider. Bij het uitvoeren van de risicoanalyse is gebruik gemaakt van de P&ID, de functiebeschrijving van de ProcessCell en het standaarddocument als leidraad. Voor de risicoanalyse was 2 uur ingepland, maar dit bleek veel te weinig te zijn. Het team had te weinig ervaring met de HAZOP methode en te weinig kennis van de ProcessCell en zijn werking. Ondanks dat het een kleine installatie is, moeten er veel onderdelen bekeken worden en zou meer tijd, zelfs met een ervaren team, wenselijk zijn. Het ingevulde HAZOP formulier is te vinden in bijlage VIII.

8.2 Stap 2: De allocatie van veiligheidsfuncties

Voor de allocatie van de veiligheidsfuncties moet een standaarddocument gemaakt worden met behulp van de in de analyse gekozen gekalibreerde risicograaf. Vanuit de norm IEC61511 in samenwerking met Actemium zijn een aantal eisen naar voren gekomen waaraan het standaardformulier moet voldoen. In Tabel 8-2 is te zien dat het allocatieblad moet bestaan uit 4 pagina's. Op een van die pagina's wordt het SIL niveau voor veiligheid, milieu en economische schade bepaald. Omdat er maar één risico per allocatieblad gebruikt kan worden, moeten er in totaal drie allocatiebladen ingevuld worden. De informatie die aanwezig moet zijn op elke pagina is:

<table>
<tr><th>1 Algemene informatie:</th><th>3 De uitleg van de keuzen voor het selecteren van het SIL niveau:</th></tr>
<tr><td>Referentienummers van de HAZOP en de P&ID;</td><td rowspan="6">Voor elke selectiemogelijkheid een stuk waarin beschreven kan worden waarom de keuzen gemaakt zijn bij het selecteren van het SIL niveau.</td></tr>
<tr><td>Revisienummer en datum;</td></tr>
<tr><td>Naam van de auteur;</td></tr>
<tr><td>Informatie van de opdrachtgever;</td></tr>
<tr><td>Goedkeuringen;</td></tr>
<tr><td>Het scenario met de titel, de beschrijving, de oorzaken en de effecten en gevolgen.</td></tr>
<tr><th>2 De selectie van het SIL niveau:</th><th>4 De voorgestelde allocatie:</th></tr>
<tr><td rowspan="2">De mogelijkheid om het SIL niveau te selecteren voor safety, milieu en economie;</td><td>De bestaande veiligheidsvoorzieningen;</td></tr>
<tr><td>De voorgestelde veiligheidsvoorzieningen:</td></tr>
<tr><td rowspan="2">De criteria waarmee het SIL niveau geselecteerd moet worden;</td><td>Beschrijving van de SIF;</td></tr>
<tr><td>Ondersteunende functies vanuit het BPCS;</td></tr>
<tr><td rowspan="3">De afbeelding van de risicograaf.</td><td>De proces veiligheidsstaat;</td></tr>
<tr><td>De proces veiligheidstijd;</td></tr>
<tr><td>De overige ondersteunende functies.</td></tr>
</table>

Tabel 8-2: Eisen allocatieblad

Op basis van deze eisen is een standaardformulier gemaakt waarbij het SIL niveau door pull down menu's bepaald kan worden en waar alle eisen in verwerkt zijn. Dit standaardformulier is te zien in bijlage IX.

Het alloceren van de veiligheidsfuncties

Omdat er voor het project drie risico's gereduceerd moeten worden zijn er dus ook drie allocatiebladen ingevuld. Op de gegevens van het risico na, zijn alle drie de bladen tot en met de bepaling en onderbouwing van het SIL niveau bijna hetzelfde ingevuld. Voor alle drie de risico's is een SIL niveau geselecteerd van SIL 1 op basis van milieu en economie. Bij het vrijkomen van vloeistof met natronloog zullen de schade in het milieu en

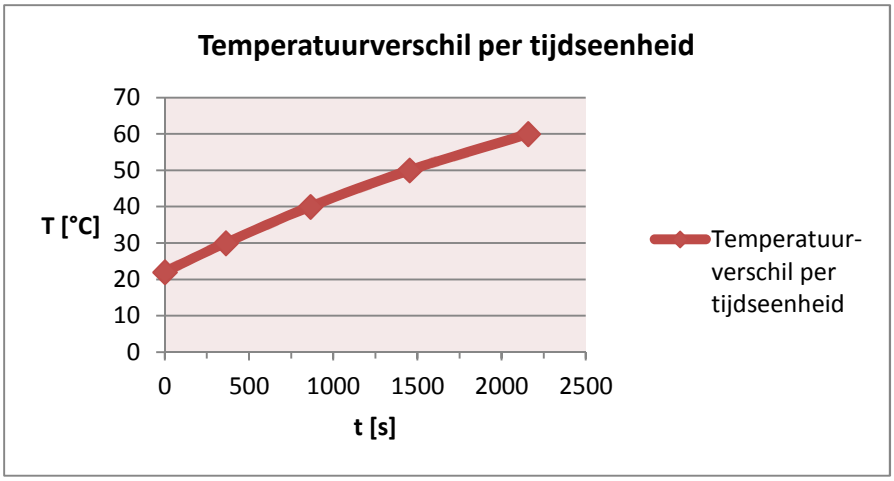
de schade aan de installatie groter zijn dan de gevaren voor de operator, omdat die in een afgeschermde ruimte zit.
Op het laatste blad van de allocatiebladen wordt de voorgestelde allocatie ingevuld. Hiervoor moet vooral gekeken worden naar de voorgestelde allocatie, de proces veiligheidsstaat en de proces veiligheidstijd. De proces veiligheidstijd is de tijd die nodig is om van het kritieke punt tot de gevaarlijke situatie te komen. Als de SIF bijvoorbeeld bij een overvulbeveiliging moet ingrijpen bij 1100 liter en de totale tankinhoud is 1250 liter, dan is de proces veiligheidstijd de tijd die nodig is om van 1100 liter naar 1250 liter te komen. De reactietijd van de SIF en het proces moet kleiner zijn dan de proces veiligheiddstijd om te zorgen dat het proces naar een veilige toestand gebracht kan worden voordat de gevaarlijke situatie plaatsvindt. Voor twee van de drie risico's zijn testen uitgevoerd om de proces veiligheidstijd te bepalen.

Risico 1: een uit de hand lopende exotherme reactie
De voorgestelde allocatie is het toevoegen van een SIL 1 waardige temperatuurtransmitter, een SIL 1 waardige logic solver, een SIL 1 waardige actuator en een SIL 1 waardige klep in de toevoerleiding van heet water dat van de exotherme reactor komt. Bij een te hoge temperatuurstijging moet de klep gesloten worden zodat de toevoer van heet water stopt.
De proces veiligheidsstaat is: geen toevoer meer vanuit de exotherme reactor.
De proces veiligheidstijd is bepaald door een test uit te voeren waarmee de maximum temperatuurstijging per tijdseenheid bepaald wordt.

Testprocedure exotherme reactie:
De tank heeft minimaal 100 liter water nodig om de temperatuur te kunnen meten.

1. *Vul de tank met 100 liter water.*
2. *Start de mixer in de tank en meet de starttemperatuur.*
3. *Start de exotherme reactie op vol vermogen en met 100% (1900l/h) debiet.*
4. *Meet de tijd tot de temperatuur 60 graden bereikt.*
5. *Het temperatuurverschil gedeeld door de tijd geeft de maximale temperatuursverandering per tijdseenheid aan in °C/s.*

Temperatuur [°c]	*Tijd [s]*	*Tempverschil/tijd [°C/s]*
Tstart = 22	*0*	
30	*362*	$\frac{\Delta T}{\Delta t} 22°C\ tot\ 30°C = \frac{(30°C - 22°C)}{(362s - 0s)} = 0{,}022 \frac{°C}{s} = 1{,}33 \frac{°C}{min}$
40	*864*	$\frac{\Delta T}{\Delta t} 30°C\ tot\ 40°C = \frac{(40°C - 30°C)}{(864s - 362s)} = 0{,}020 \frac{°C}{s} = 1{,}20 \frac{°C}{min}$
50	*1452*	$\frac{\Delta T}{\Delta t} 40°C\ tot\ 50°C = \frac{(50°C - 40°C)}{(1452s - 864s)} = 0{,}017 \frac{°C}{s} = 1{,}02 \frac{°C}{min}$
60	*2156*	$\frac{\Delta T}{\Delta t} 50°C\ tot\ 60°C = \frac{(60°C - 50°C)}{(2156s - 1452s)} = 0{,}014 \frac{°C}{s} = 0{,}85 \frac{°C}{min}$



Afbeelding 8-1: Temperatuur verschil per seconde

Uit de grafiek in Afbeelding 8-1 *en de bovenstaande berekeningen is te zien dat het grootste temperatuurverschil per tijdseenheid tussen de 22°C en 30°C zit. Om nu te bepalen wat de veiligheidstijd is wordt een maximale temperatuurstijging van 0,017°C/s of 1°C/min gebruikt. Dit moet pas gemeten worden vanaf 40°C en er wordt dan gekeken hoe binnen welke tijd de 50°C bereikt wordt.*

$$De\ procesveiligheidstijd = \frac{(40°C - 50°C)}{1\frac{°C}{min}} = 10min$$

Risico 2: een te hoge druk in de reactor

De voorgestelde allocatie is het toevoegen van een SIL 1 waardige druktransmitter, een SIL 1 waardige logic solver, vijf SIL 1 waardige actuatoren en vijf SIL 1 waardige kleppen in de toevoerleiding naar de reactor vanuit de vier tanks en vanuit de perslucht aanvoer. Bij een te hoge druk moeten de kleppen gesloten worden zodat alle toevoeren naar de reactor stoppen.
De proces veiligheidsstaat is: geen toevoer vanuit de vier tanks en vanuit de persluchtleiding naar de reactor.
De proces veiligheidstijd is bij dit risico niet te bepalen omdat er veel onbekende gegevens zijn. Van de persluchtleidingen zijn de leidinglengte en de leidingdikte niet bekend. Daarnaast is de totale inhoud van de tank niet bekend, waardoor niet te berekenen is wat de proces veiligheidstijd is. Daarom is in dit geval in overleg met Actemium een aanname gedaan dat de proces veiligheidstijd 5 seconden is.

Risico 3: een te hoog niveau in tank TA01

De voorgestelde allocatie is het toevoegen van een SIL 1 waardige levelswitch, een SIL 1 waardig logic solver, drie SIL 1 waardige actuatoren en drie SIL 1 waardige kleppen in de toevoerleiding naar de tank TA01. Bij een te hoog niveau moeten de kleppen gesloten worden zodat alle toevoeren naar de tank stoppen.
De proces veiligheidsstaat is: geen toevoer vanuit buffertank TA03, het reactorvat en de stadswaterleiding naar tank TA01.
De proces veiligheidstijd is bepaald door te testen wat het volumedebiet van de stadswaterleiding is en daarmee te berekenen hoelang het duurt van het kritieke punt totdat de tank over zou lopen.

Testprocedure vulsnelheid:
De tank zit nu vol met 1100 liter water.

1. *Verwijder 300 liter water via het afvoerputje.*
2. *Vul de tank met water uit de waterleiding tot 1100.*
3. *Meet de tijd die nodig is om van 800 naar 1100 liter te komen.*
4. *Het aantal liter gedeeld door de vultijd geeft het debiet (ϕ) weer in l/s.*

Hoeveelheid [l]	*Tijd [s]*
900	*120*
1000	*250*
1100	*375*

$$\phi = \frac{\Delta I}{\Delta t} = \frac{(1100l - 900l)}{(375s - 0s)} = 0{,}8\frac{l}{s}$$

$$De\ procesveiligheidstijd = \frac{(1250l - 1100l)}{0{,}8\frac{l}{s}} = 187s = 3min7s$$

In bijlage X, bijlage XI en bijlage XII zijn de drie ingevulde allocatiebladen te zien.

8.3 Stap 3: De veiligheidseisen specificatie (SRS)

In de derde stap van de norm worden de veiligheidseisen waaraan het veiligheidssysteem moet voldoen vastgelegd. Deze veiligheidseisen worden bepaald vanuit de uitkomsten van de HAZOP en vanuit de uitkomsten van de allocatiebladen. Voor het maken van de veiligheidseisen specificatie zijn geen specifieke methoden beschikbaar. In de norm zijn enkel een aantal eisen bekend waaraan voldaan moet worden.

Het standaardformulier

Vanuit de norm IEC61511 in samenwerking met Actemium zijn er een aantal eisen naar voren gekomen waaraan het standaardformulier moet voldoen. De opzet van het document is als volgt:

1. Een voorpagina in de standaard lay-out van Actemium documenten.
2. Pagina met algemene gegevens als auteur, opdrachtgever en revisiebeheer.
3. Een inhoudsopgave.
4. Het algemene deel van de SIF.
5. Ruimte voor het SIF schema en het functioneel logisch diagram.
6. De sensorgroepen.
7. De logic solver groepen
8. De eindelement groepen

Omdat er meerdere SIF's toegevoegd kunnen worden bij een installatie zullen punt 4 tot en met punt 8 voor elke nieuwe SIF ingevuld moeten worden. In bijlage XIII is het standaarddocument van het SRS te zien. Bij de onderdelen waar vaste keuzen bij te maken zijn, is gekozen om een pull down menu te maken. Daardoor is het makkelijker voor de ingenieur om het document in te vullen.

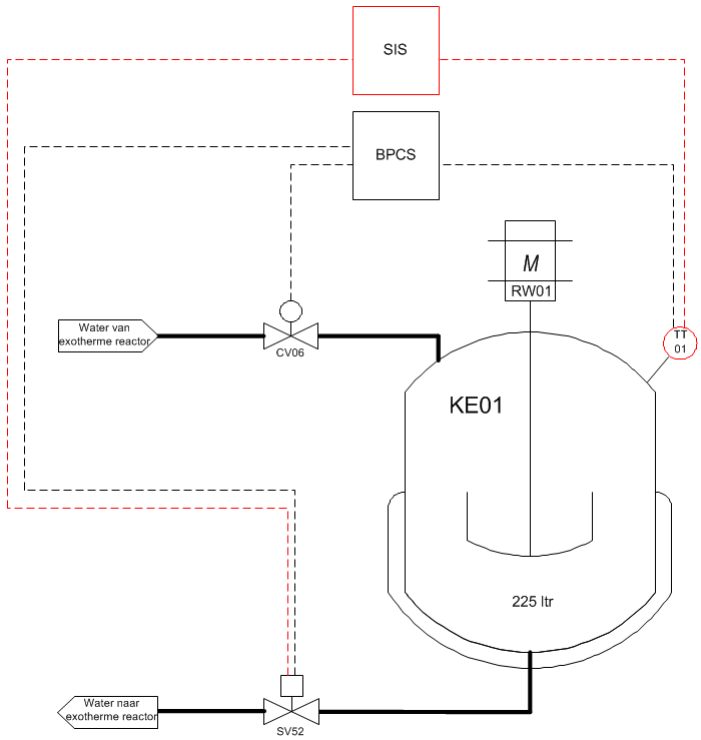
De safety requirements specificatie

Bij het invullen van het standaarddocument van de SRS worden een aantal onderdelen overgenomen vanuit de HAZOP en de allocatiebladen. Daarnaast zijn een aantal eisen voor elke SIF hetzelfde. Dit komt onder andere omdat er dezelfde onderdelen als de logic solver en de eindelementen gebruikt worden. Onderstaand is te zien welke eisen voor alle SIF's hetzelfde zijn. In bijlage XIV is de volledig ingevulde SRS te zien.

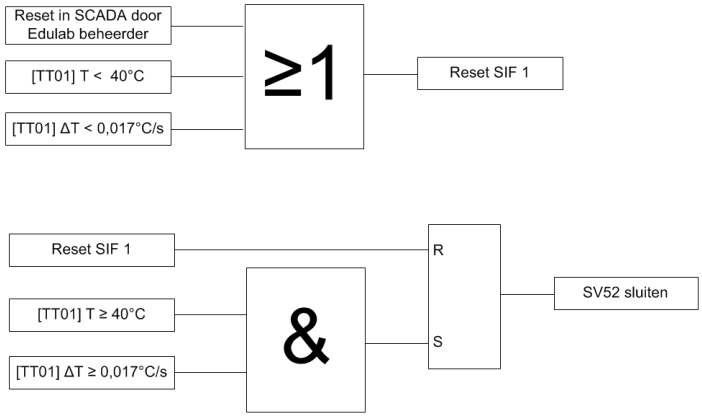
Overeenkomende eisen voor elke SIF	
Demand rate:	Laag aantal aanvragen ≤1/jaar
Marge responsetijd SIF + proces:	25% (de reactietijd van de SIF en het proces mag maar 25% van de veiligheidstijd zijn)
Maximale spurious trip rate:	Minder dan eens per 10 jaar (de installatie mag maar eens per tien jaar naar een veilige staat gaan terwijl er geen gevaar dreigt)
Protectie methode:	De-energize to trip (veilige staat is geen energie)

Trip reset:	De Edulab beheerder moet inloggen als supervisor om de SIF te kunnen resetten met de resetknop op het SCADA scherm
Missie tijd:	De installatie moet in ieder geval 10 jaar meegaan
Voting	1oo1 (geen redundantie dus ook geen voting)
Common cause bronnen en bèta factor	Niet van toepassing (geen voting)
MTTR	72 uur (geteld vanaf de tijd van ontdekken tot het gerepareerd is)
Proof test interval	12 maanden / 60 maanden voor de PLC (alles moet dus 1 keer per jaar getest worden behalve de PLC, die hoeft maar 1 keer per 5 jaar getest te worden)
Logic solver van elke SIF's:	
Proof test coverage:	>90% <100% na een restart (als de PLC uitgeschakeld wordt en opnieuw opgestart komen de meeste fouten naar boven als die er zijn)
Eindelementen groep van elke SIF's	
Aktie:	Sluiten
Proof test coverage:	>97% ≤99% van alle fouten moet met de proof test gevonden worden
Diagnostiek:	Geen
Proces connectie:	Geen (Wanneer de klep zo min mogelijk mag lekken na het sluiten moet hier de selectie tight shut-off leak class geselecteerd worden. Als de vloeistofstroom moet helpen bij het sluiten van de klep in plaats van tegenwerken kan dit ook hier geselecteerd worden)
Interface:	Solenoid valve, omdat in dit geval de klep niet vervangen of nieuw bijgebouwd gaat worden, zal het ventiel dat gebruikt gaat worden wel SIL waardig zijn. De gegevens van de MTTR, de proof test interval en de proof test coverage zijn dan ook voor de solenoid valve
Andere speciale eisen:	Een mechanische NAMUR aansluiting

SIF 1 exotherme reactie KE01	
Algemene deel van de SIF	
SIF identiteit:	TZ-01.06, opbouw van de identiteit: T = temperatuur, Z = beveiligingsactie, 01.06 is het HAZOP referentienummer
Het SIF schema: Het SIF functioneel logisch diagram:	Zijn te zien in Afbeelding 8-2 en Afbeelding 8-3.
Proces override POS:	De SIF mag pas ingrijpen als de temperatuur boven de 40°C is
Overige specifieke eisen:	De mixer moet altijd aanstaan als de temperatuur gemeten moet worden
De eisen voor de sensorgroep:	
Actie:	High trip
Proof test coverage:	>60% ≤90% van alle fouten moet met de proof test gevonden worden
Kabel diagnostiek:	NAMUR (dit betekent dat gedetecteerd kan worden of de sensor buiten het bereik valt of dat er kabelbreuk of kortsluiting is) ("Vierpool", 2014)
Proces connectie:	RTD
Interface:	Signal convertor, deze zorgt ervoor dat het signaal gesplitst wordt zodat het voor zowel het BPCS als de SIS gebruikt kan worden

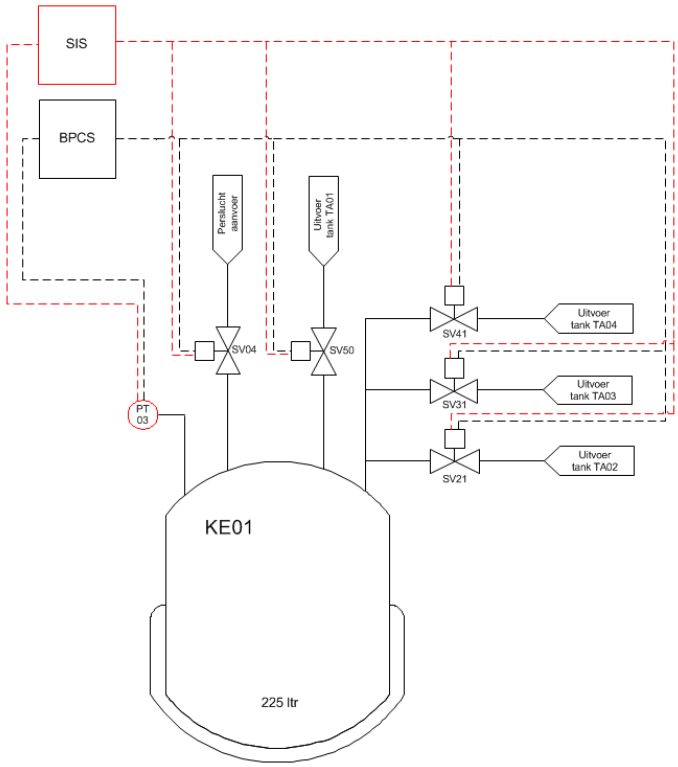


Afbeelding 8-2: SIF 1 schema

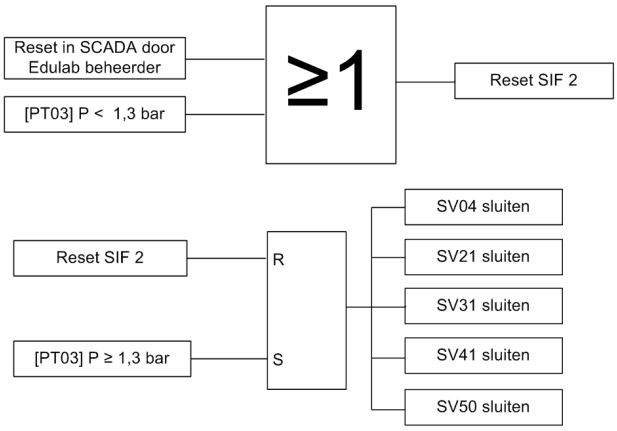


Afbeelding 8-3: SIF 1 functioneel logisch diagram

SIF 2 druk KE01	
Algemene deel van de SIF	
SIF identiteit:	PZ-01.06, opbouw van de identiteit: P = druk (Pressure), Z = beveiligingsactie, 01.07 is het HAZOP referentienummer
Het SIF schema: Het SIF functioneel logisch diagram:	Zijn te zien in Afbeelding 8-4 en Afbeelding 8-5.
De eisen voor de sensorgroep	
Actie:	High trip
Proof test coverage:	>97% ≤99% van alle fouten moet met de proof test gevonden worden
Kabel diagnostiek:	NAMUR (dit betekent dat gedetecteerd kan worden of de sensor buiten het bereik valt of dat er kabelbreuk of kortsluiting is) ("Vierpool", 2014)
Proces connectie:	Schroefdraad ANSI MNPT 1/2
Interface:	Signal convertor, deze zorgt ervoor dat het signaal gesplitst wordt zodat het voor zowel het BPCS als de SIS gebruikt kan worden

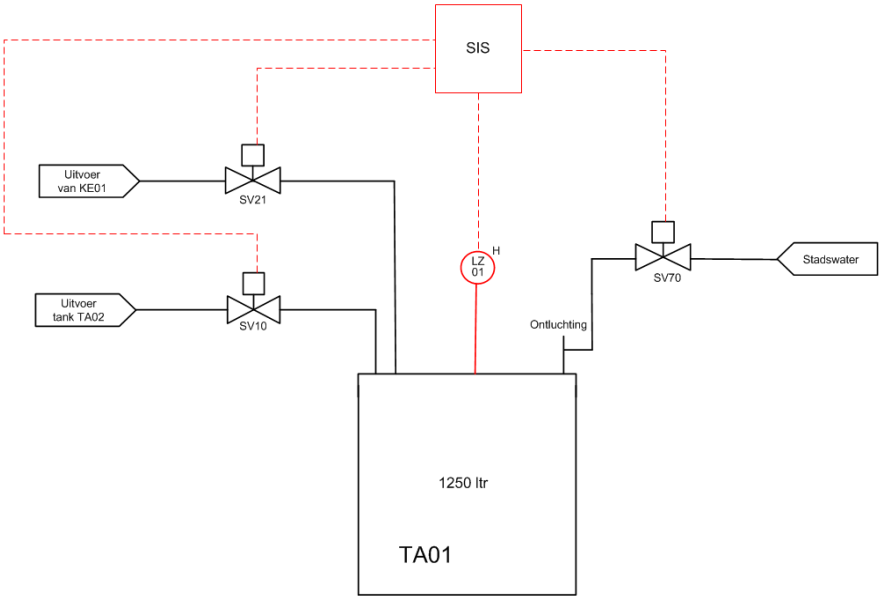


Afbeelding 8-4: SIF 2 schema

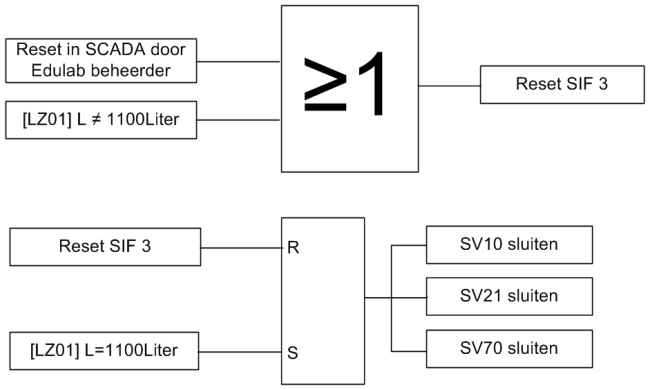


Afbeelding 8-5: SIF 2 functioneel logisch diagram

SIF 3 niveau TA01	
Algemene deel van de SIF	
SIF identiteit:	LZ-01.10, opbouw van de identiteit: L = Niveau (Limit), Z = beveiligingsactie, 01.10 is het HAZOP referentienummer
Het SIF schema: Het SIF functioneel logisch diagram:	Zijn te zien in Afbeelding 8-6 en Afbeelding 8-7.
De eisen voor de sensorgroep	
Actie:	High trip
Proof test coverage:	>90% ≤97% van de fouten moet gevonden kunnen worden met de proof test.
Proces connectie:	Flens
Interface:	Schakelversterker



Afbeelding 8-6: SIF 3 schema



Afbeelding 8-7: SIF 3 functioneel logische diagram

8.4 Stap 4: Ontwerpen en engineeren

Nu alle eisen voor het ontwerp bekend zijn kan het ontwerp gemaakt worden. Daarvoor moeten een aantal taken uitgevoerd worden, namelijk: het kiezen van de onderdelen, bekijken waar en hoe alles ingebouwd gaat worden en alle tekeningen maken / aanpassen.

8.4.1 Onderdeelkeuze

Zoals al eerder aangegeven worden er geen kleppen vervangen of bijgeplaatst. De reden daarvoor is dat het project dan te duur wordt. Het moet fungeren als een demo model maar hoeft dus niet volledig aan de richtlijnen te voldoen. Daarom is er voor gekozen om een extra ventiel tussen het bestaande ventiel en de klep te zetten die altijd open staat, behalve als een SIF moet ingrijpen. Dan zal dat ventiel gesloten worden. Omdat twee SIF's beide de uitvoer van tank TA03 moeten kunnen sluiten kan daar hetzelfde ventiel voor gebruikt worden.

De druktransmitter en de temperatuurtransmitter moeten beide vervangen worden omdat deze met Profibus werken. Met dat signaal kan de SIS niet werken dus moeten beide sensoren vervangen worden door een sensor met een analoog 4-20mA signaal. Daarnaast moet dat signaal gesplitst worden zodat het zowel op de BPCS als op de SIS aangesloten kan worden. Omdat de huidige aansluiting Profibus is en geen 4-20mA signaal, moeten er bovendien twee analoge aansluitingen toegevoegd worden. De benodigde onderdelen die uitgezocht moeten worden zijn te zien in Tabel 8-3.

Aantal	Component
1	Temperatuurtransmitter
1	Druktransmitter
1	Levelswitch
1	Signaalversterker
1	Logic solver
1	Remote I/O
2	Shunt
2	Splitters
2	Analoge inputs
8	Ventielen

Tabel 8-3: Benodigde onderdelen

De temperatuurtransmitter

De temperatuurtransmitter die er nu op zit bestaat uit de meetpen die in de reactor steekt en een kop met Profibus aansluiting. Voor de nieuwe temperatuurtransmitter hoeft dus alleen maar gekeken te worden naar een nieuwe kop met 4-20mA signaal en minimaal een SIL 1 certificaat. De huidige transmitter is een SensyTemp WT R van ABB en is een dubbele Pt 100 en een RTD 3-draads aansluiting. Op basis van deze gegevens zijn er drie temperatuurtransmitters uitgezocht bij verschillende leveranciers die geschikt kunnen zijn voor dit project:

- de TTH300 van ABB;
- de Rosemount 644 van Emerson;
- de TMT82 van Endress + Hauser.

Na het bekijken van de bovenstaande opties is gekozen voor de TMT82 van Endress + Hauser. Dit omdat de TTH300 van ABB wel een safety manual had maar het SIL certificaat niet terug te vinden is. Daarnaast staat er in het safety manual dat de sensor getest is maar er is niets terug te vinden van de testen voor de software in de transmitter. Wanneer deze gegevens niet bekend zijn mag de transmitter niet gebruikt worden voor een SIL geclassificeerd systeem. Van de Rosemount 644 van Emerson is wel een certificaat en een safety manual gevonden, maar ook hier is geen software test gedaan. Van de TMT82 van Endress + Hauser is een certificaat en een safety manual beschikbaar met daarin de classificatie voor zowel de hardware als de software. Deze is dus geschikt om te gebruiken in het project. Het SIL certificaat is te zien in bijlage XV.

De druktransmitter

De druktransmitter die er nu op zit moet volledig vervangen worden door een nieuwe SIL waardige transmitter. De huidige transmitter die op de installatie zit is van ABB en heeft typenummer: 266ASHLKTNB2 E1L1. Op basis van deze gegevens zijn drie druktransmitters uitgezocht van verschillende leveranciers die geschikt kunnen zijn voor dit project:

- de 2600T van ABB;
- de Rosemount 2051 van Emerson;
- de PMC71 van Endress + Hauser.

Na het bekijken van de bovenstaande opties is gekozen voor de PMC71 van Endress + Hauser. Dit omdat de 2600T van ABB wel een safety manual en een SIL certificaat had, maar er is geen test gedaan op de software van de transmitter. Van de Rosemount 2051 van Emerson is ook een certificaat en een safety manual gevonden, maar ook hier is geen test gedaan op de software. Van de PMC71 van Endress + Hauser is een certificaat en een safety manual beschikbaar met daarin de classificatie voor zowel de hardware als de software. Deze is dus geschikt om te gebruiken in het project. Het SIL certificaat is te zien in bijlage XVI.

De levelswitch & signaalversterker

Omdat de levelswitch een nieuwe transmitter is, zijn daar nog helemaal geen gegevens van bekend. De voorkeur vanuit Actemium was om gebruik te maken van een switch die werkt met trillingen (trilvork). Daarnaast moest gekeken worden voor een sensor waarvan de lengte gekozen kan worden omdat de standaard maat vaak niet geschikt is. Op basis van deze gegevens zijn drie switches uitgekozen van verschillende leveranciers die geschikt kunnen zijn voor dit project:

- de Rosemount 2120 van Emerson;
- de Vegaswing 63 van Vega;
- de FTL51 van Endress + Hauser.

Na het bekijken van de bovenstaande opties is gekozen voor de FTL51 van Endress + Hauser. Dit omdat de Rosemount 2120 van Emerson wel een safety manual en een SIL certificaat had, maar er is geen test gedaan op de software van de transmitter. Van de Vegaswing 63 van Vega is wel een safety manual maar geen certificaat te vinden. Van de FTL51 van Endress + Hauser is een certificaat en een safety manual beschikbaar, maar deze is alleen geldig als de switch gebruikt wordt in combinatie met de versterker FTL325P van Endress + Hauser. Van die twee componenten is zowel de safety manual als het SIL certificaat beschikbaar met daarin de classificatie voor hardware en software. Deze is dus geschikt om te gebruiken in het project. Het SIL certificaat is te zien in bijlage XVII.

De logic solver, remote I/O en shunt

De logic solver en de remote I/O zijn beiden gesponsord door HIMA. Dit is een fabrikant van veiligheidsPLC's en de bijbehorende remote I/O. Van deze fabrikant wordt veel gebruikt binnen Actemium. De PLC en remote I/O die gesponsord zijn, zijn de HIMatrix F35 03 met SILworX en de HIMatrix F3 DIO 20/8 02. Van beide componenten zijn zowel de safety manuals als de SIL certificaten beschikbaar met daarin de classificatie voor hardware en software. Deze zijn dus geschikt om te gebruiken in het project. Naast de PLC en de remote I/O moet voor het aansluiten van analoge sensoren een shunt gebruikt worden. Een shunt is een weerstand die fungeert als omvormer van stroom naar spanning. De werking is als volgt: de sensor kan een signaal sturen tussen de 4 en 20 mA. Bij het gebruiken van een shunt zal deze stroom door de weerstand lopen waardoor er een spanning over de weerstand komt te staan. Deze spanning zal variëren aan de hand van de stroomvariatie. Die spanning kan gemeten worden door de PLC. De PLC kan deze spanning dan omzetten in een waarde die gekoppeld is aan het meetprincipe, dus druk, niveau of temperatuur. De shunts zijn verkrijgbaar als connector die rechtstreeks op de PLC passen en worden geleverd per connector met twee shunts. Hiervan hoeft er dus maar één besteld te worden. Het SIL certificaat is te zien in bijlage XVIII.

De splitters

Omdat alles in een SIL waardige loop een certificaat moet hebben, moet ook een onderdeel als een splitter een SIL certificaat hebben. Het enige probleem bij deze onderdelen is dat er niet veel beschikbaar zijn met een SIL classificatie. Van alle leveranciers van splitters is alleen Pepperl en Fuchs een leverancier van SIL waardige splitters. Bij Pepperl en Fuchs zijn uiteindelijk twee types gevonden die geschikt zijn:

- KCD2-STC-Ex1.2O
- KFD2-CR4-1.2O

Van beide types is echter geen certificaat te vinden. Van de KFD2-CR4-1.2O is echter wel een safety manual en een FMEDA gevonden op de website van Pepperl en Fuchs. Een FMEDA is een testrapport om faalcijfers te achterhalen van een component, en mag dus niet gebruikt worden als een certificaat. Uit ervaring van de Lead Hardware ingenieur Johan van Lent geeft Pepperl en Fuchs deze SIL certificaten alleen maar vrij als deze aangevraagd worden. Na het aanvragen werd vanuit Pepperl en Fuchs verwezen naar het FMEDA op hun website, maar niet naar een daadwerkelijk certificaat. Daarom is een tweede keer contact opgenomen met Pepperl en Fuchs met de vraag voor het SIL certificaat, maar daar is helaas niet meer op gereageerd vanuit Pepperl en Fuchs. Er kan dus vanuit gegaan worden dat deze splitters niet SIL gecertificeerd zijn en dus ook niet geschikt voor dit project. Bij gebrek aan andere keuzemogelijkheden is toch gekozen om de KFD2-CR4-1.2O te gebruiken in het project.

De ventielen

Voor de ventielen is gekozen om gebruik te maken van de NAMUR aansluitingen zodat er geen extra kast geplaatst hoeft te worden. De voorkeur van Actemium gaat uit naar ventielen van het merk ASCO. Daarnaast moeten de ventielen met een zo laag mogelijk vermogen gekozen worden omdat hoge vermogens niet nodig zijn. Op basis van deze gegevens zijn een aantal mogelijkheden gevonden bij ASCO.

- de 327 serie;
- de 551, 552, 553 serie.

Van beide series zijn de safety manuals en de SIL certificaten beschikbaar dus de keuze was vrij om een van de twee series te kiezen. Na overleg met Actemium is de 327 serie gekozen met een elektromagnetische aansluiting (solenoid). Het SIL certificaat is te zien in bijlage XIX.

De analoge inputs

Op dit moment zit er al een remote I/O blok in de kast die 4-20mA signalen omzet naar Profibus. Op dat blok zijn geen analoge inputs meer vrij dus moeten er twee bijgebouwd worden. De bekende gegevens van die blokken zijn: de leverancier Phoenix contact, de serie “Inline”, voor 4-draads sensoren (actieve sensoren) en een interbus snelheid 500kBit/s. Het kopstation wat gebruikt wordt kan beide snelheden aan maar past zich aan, aan de snelheid van de eerste aangesloten input of output. Uiteindelijk is er maar een geschikt type uitgekomen en dat is de IB IL AI 4/EF-PAC. Dit is een blok met 4 analoge inputs dus er hoeft maar een blok besteld te worden. Omdat dit aangesloten wordt op de BPCS hoeft hier geen safety manual of SIL certificaat van te zijn.

Gekozen onderdelen

Na het selecteren van de onderdelen zijn de bestelnummers bepaald in samenwerking met Johan van Lent. Het overzicht van deze onderdelen, de leveranciers en de bestelnummers zijn te zien in Tabel 8-4. Naast de SIL certificaten zijn de safety manuals ook zeer belangrijk. Gezien deze erg groot zijn om allemaal toe te voegen, en gezien deze voornamelijk dezelfde informatie bevatten, is er een safety manual van de ventielen toegevoegd als voorbeeld in bijlage XX.

Aantal	Onderdeel	Leverancier	Bestelnummer
1	Temperatuurtransmitter	Endress + Hauser	TMT82-AA-A-2-A-B1-A1-AA-A1-LA
1	Druktransmitter	Endress + Hauser	PMC71-A-B-A-2E-1-RA-A-E-U
1	Levelswitch	Endress + Hauser	FTL51-A-BA2-BB-7-G4-A
1	Levelswitch versterker	Endress + Hauser	FTL325P-G-1-E-1
1	Shunt 500Ω	HIMA	982220067
2	Splitters	Pepperl + Fuchs	KFD2-CR4-1.2O
1	Analoge inputs	Phoenix contact	IB IL AI 4/EF-PAC - 2878447
8	Valve	Asco	SC-G-327B103-24V/DC

Tabel 8-4: Overzicht gekozen onderdelen

8.4.2 Het toevoegen en tekenen

Om te bepalen of alle onderdelen zowel in het veld als in de kast erbij geplaatst kunnen worden, moeten een aantal dingen gecontroleerd worden. Er moet gekeken worden naar een spanningsbron die de componenten kan voeden, er moet gekeken worden naar de warmteontwikkeling in de kast, er moet gekeken worden naar de ruimte die nodig is in de kast en er moet gekeken worden naar de ruimte die nodig is in het veld. In de analyse, paragraaf 4.7.2, is aangetoond dat er twee kasten zijn die nog voldoende ruimte hebben om de onderdelen in te plaatsten. De kast die het meest geschikt is, is kast 3 omdat daarin de meeste ruimte beschikbaar is.

De voeding in de kast

Omdat er een aantal apparaten toegevoegd gaan worden, moet er gecontroleerd worden of de huidige voeding voldoende is om ook de nieuwe apparatuur te kunnen voeden. De voeding die nu in de kast zit is een voeding van 24V / 10A. In Tabel 8-5 is te zien welke apparaten er nu al op de voeding aangesloten zijn.

Onderdeel	nummer	leverancier	Typenummer	stroom[A]
Switch stratix 800	91Z1	Allan Bradley	1783-MS10T	2,00
HMI	102A1	Allan Bradley	2711P-T10C4D6	2,90
PA module	152Z1	Allan Bradley	1788HP-EN2PA	0,68
PA module	153Z1	Allan Bradley	1788HP-EN2PA	0,68

Tabel 8-5: Apparaten op de voeding

Naast de apparaten in de kast komen er dus nog een aantal apparaten bij. Deze zijn te zien in Tabel 8-6.

aantal	Onderdeel	leverancier	typenummer	stroom[A]	Stroom totaal [A]
1	PLC	HIMA	HIMatrix F35 03	0,5	0,5
1	Remote I/O	HIMA	F3 DIO 20/8 02	0,4	0,4
1	Druktransmitter	E + H	PMC71	0,02	0,02
1	Versterker levelswitch	E + H	FTL325P	0,075	0,075
2	Splitter	P + F	KFD2-CR4-1,20	0,1	0,2
1	Temperatuurtransmitter	E + H	TMT82	0,0225	0,0225
8	Ventielen	Asco	SC G 327B103 24VDC	0,154	1,232

Tabel 8-6: Nieuwe apparaten op de voeding

Totaalstroom bestaande apparaten: $Atot_{bestaand} = 2{,}00A + 2{,}90A + 0{,}68A + 0{,}68A = 6{,}26A$
Totaalstroom nieuwe apparaten: $Atot_{nieuw} = 0{,}50A + 0{,}40A + 0{,}02A + 0{,}075A + 0{,}20A + 0{,}023A + 1{,}232 = 2{,}45A$
De apparaten die toegevoegd zullen worden moet nog een extra marge van 25% bijgeteld worden zodat het zeker gevoed kan worden door de huidige voeding. $Atot_{nieuw+25\%} = 2{,}45A + 0{,}25 + 2{,}45A = 3{,}06A$

Totaalstroom bestaand + nieuw: $Atot = 6{,}26A + 3{,}06A = 9{,}32A$
Hieruit blijkt dat de huidige voeding voldoende is om ook de nieuwe apparaten te voeden.

De warmte ontwikkeling in de kast

Voor het toevoegen van de PLC, remote I/O en overige apparatuur in de elektrakast moet bekeken worden of deze kast extra koeling nodig heeft om de temperatuur in de kast te handhaven. Om deze berekening te kunnen maken staat er in de systeemhandleiding van HIMA een formule met uitleg en een voorbeeld hoe een dergelijke berekening gedaan kan worden. Daarnaast heeft de leverancier Rittal een programma dat, nadat de gevonden waarden zijn ingevuld, berekend of al dan niet extra koeling nodig is. De berekening is als volgt:

$$\Delta T_{max} = \frac{P_v}{k * A}$$

$[\Delta T_{max}] = ℃/K \qquad [P_v] = W \qquad [k] = \frac{W}{m^2 * K} \qquad [A] = m^2$

In de manual staat aangegeven dat voor $k = 5{,}5 \frac{W}{m^2 * K}$ aangenomen kan worden. De oppervlakte A is de hitte afdragende oppervlakte die berekend moet worden met een formule die afhankelijk is van de plaatsing van de kast. Bij een kast die tussen twee andere kasten staat en met zijn achterkant tegen de muur geld de volgende formule: $A = 1{,}4 * b * (h + d) + h * d$

De vermogens dissipatie Pv, kan berekend worden door van alle onderdelen die al in de kast zitten en alle onderdelen die er nog bij komen, de gedissipeerde vermogens op te tellen. Hier wordt wel rekening gehouden met de outputs en de vermogensdissipatie die daarvoor geldt, maar worden de inputs verwaarloosd.

Gegevens: $h = 2{,}0m$ $b = 0{,}8m$ $d = 0{,}5m$

Aantal	Onderdeel	Max. temp[°C]	Spanning[V]	Stroom [A]	Vermogen[W]
1	Voeding 24V	70	24	10	240
1	NUC	50			65
1	Switch	60	-	-	15,7
2	PA box	niet bekend	24	0,18	8,64
2	PA box output	niet bekend	24	0,5	24
1	PLC	60	24	0,5	12
4	PLC output	60	2	0,5	4
1	Remote I/O	60	24	0,4	9,6
4	Remote I/O output	60	2	0,5	4
2	Splitter	60	-	-	4,8
1	Versterker niveauswitch	60	24	0,075	1,8

Tabel 8-7: Gegevens onderdelen in de kast

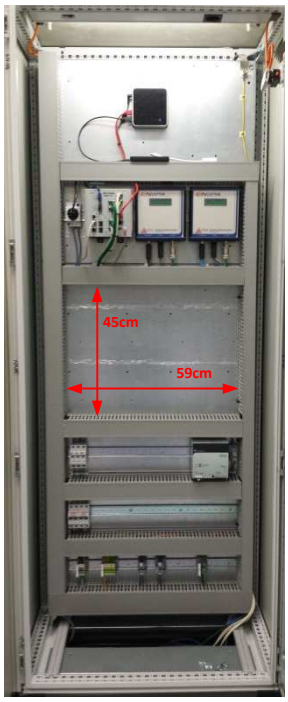
$$\Delta T_{max} = \frac{(240W + 65W + 15{,}7W + 8{,}64W + 24W + 12W + 4W + 9{,}6W + 4W + 4{,}8W + 1{,}8W)}{5{,}5\frac{W}{m^2 * K} * (1{,}4 * 0{,}8 * (2{,}0 + 0{,}5) + 2{,}0 * 0{,}5)}$$
$$= 18{,}64℃$$

Uitgaande van een omgevingstemperatuur van ongeveer 25°C wordt de maximale eindtemperatuur:
$T_{max} = 25℃ + 18{,}64℃ = 43{,}64℃$
In Tabel 8-7 is te zien dat de maximale temperatuur 50°C dus er is geen extra koeling nodig in de kast.

Ter controle worden de gegevens nog een keer ingevoerd in het automatische berekeningsprogramma en daar komt 44°C uit als maximum temperatuur (zie bijlage XXI). De berekening volgens het programma komt op dezelfde temperatuur als de berekening met de formule uit de HIMA datasheet. Er is dus geen extra koeling nodig in de kast.

De ruimte in de kast

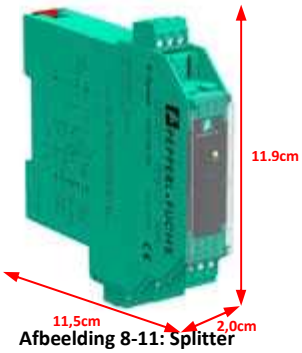
In Afbeelding 8-8 is te zien dat de ruimte die gebruikt kan worden voor het inbouwen van de onderdelen 59cm bij 45cm is. De afmetingen van alle apparatuur die op die plaats gemonteerd moet worden is te zien in Afbeelding 8-9, Afbeelding 8-10, Afbeelding 8-11 en Afbeelding 8-12.



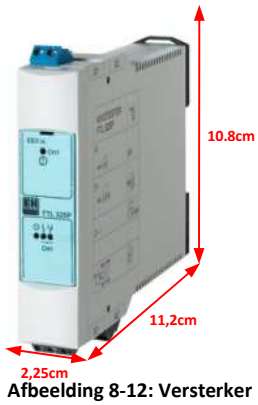
Afbeelding 8-8: Kast 3

Afbeelding 8-9: HIMA HIMatrix F35 3

Afbeelding 8-10: HIMA HIMatrix F3 DIO 20/8 02



Afbeelding 8-11: Splitter



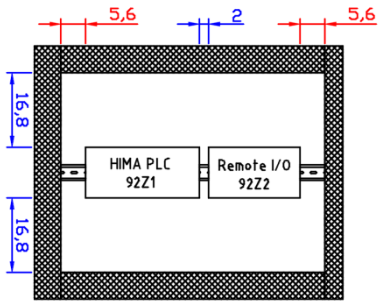
Afbeelding 8-12: Versterker

Naast deze maten is het belangrijk om rekening te houden met de inbouwspecificaties die bij sommige onderdelen gegeven worden.

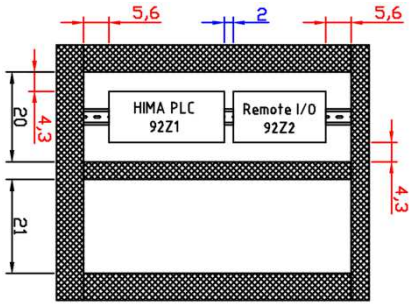
De PLC en remote I/O:

- Moeten 8cm vanaf een kabelgoot geplaatst worden. Indien dat niet mogelijk is, moet de DIN rail naar voren gehaald worden door middel van afstandbussen;
- Moeten onderling horizontaal 2cm van elkaar af geplaatst worden;
- Moeten onderling verticaal 10cm van elkaar af geplaatst worden.

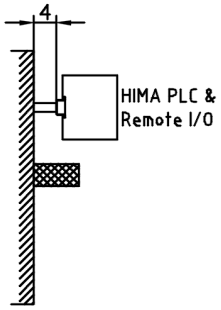
In Afbeelding 8-13 en in Afbeelding 8-14 zijn twee mogelijkheden gegeven voor het inbouwen van de PLC en de remote I/O. De blauwe maten geven aan dat die aan de gegeven eisen voldoen, de rode maten voldoen niet aan de eisen. Zoals te zien is het niet mogelijk om de onderdelen in te bouwen zonder ergens een aanpassing te maken. In de eisen van de PLC en remote I/O staat dat wanneer de 8cm naar de kabelgoot niet haalbaar is dat dan de DIN rail verhoogd kan worden zoals te zien is in Afbeelding 8-15.



Afbeelding 8-13: Kastopstelling 1



Afbeelding 8-14: Kastopstelling 2



Afbeelding 8-15: Verhoogde opstelling

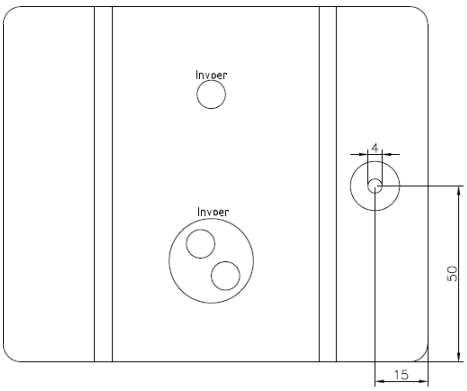
Omdat beide opstellingen mogelijk zijn is er een keuze gemaakt om kastopstelling 2 te realiseren. Zo wordt er rekening gehouden met eventuele uitbreidingen in de toekomst door nog een vak open te laten. Wel moet er gebruik gemaakt worden van de verhoogde opstelling. Omdat de splitters en versterker verder geen inbouw eisen hebben, kunnen die in een vak onder de PLC op een bestaande rail geplaatst worden.

De ruimte in het veld

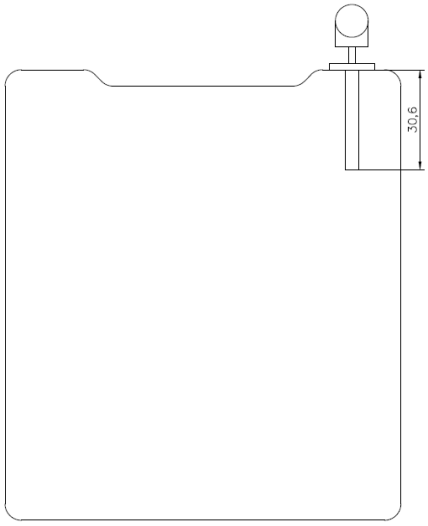
Zoals al beschreven zullen alle ventielen die in het veld moeten komen op de kleppen gebouwd worden. De ruimte op die kleppen is voldoende om de ventielen op te plaatsen en aan te sluiten. De druktransmitter en de temperatuurtransmitter zullen de oude onderdelen vervangen dus daarvoor is al ruimte gereserveerd. De niveauswitch zal wel nieuw ingebouwd moeten worden. Bij het inbouwen van deze switch gelden een aantal eisen waarmee rekening gehouden moet worden:

- De vork moet zo ver als mogelijk van de wand af gemonteerd worden zodat aankoeken van vuil niet zoveel effect heeft.
- De vork moet zo ver als mogelijk van de invoer af gemonteerd worden omdat daar het niveau nogal wild kan schommelen.

In Afbeelding 8-16 en in Afbeelding 8-17 is te zien waar op de tank de sensor moet worden geplaatst.



Afbeelding 8-16: TA01 bovenaanzicht



Afbeelding 8-17: TA01 vooraanzicht

De tekeningen

De tekeningen die voor de installatie aangepast of nog volledig gemaakt moeten worden zijn:

De P&ID is snel aan te passen gezien daarin maar weinig aangepast hoeft te worden. Deze is te zien in bijlage XXII.

De indeling in de kast is in de vorige paragraaf al laten zien. Er moet alleen een net kader om de definitieve opstelling geplaatst worden. Daarnaast moet er een tekening komen van de volledige kast waar ook de toegevoegde splitters en versterker ingedeeld zijn. Deze tekeningen zijn te zien in bijlage XXIII.

De plaatsing van de levelswitch is ook in de vorige paragraaf al laten zien, maar ook daar moet nog een net kader om. De tekening van de levelswitch plaatsing is te zien in bijlage XXIV.
De elektrische tekeningen die bij de installatie horen in het EduLab zijn op dit moment niet up to date. Er circuleren op dit moment drie verschillende pakketten die gemaakt zijn in een oude versie van E-plan. Omdat deze versie bij Actemium niet meer gebruikt wordt, moeten alle tekeningen dus opnieuw getekend worden in de laatste versie van E-plan. Actemium heeft de taak, om het volledige pakket up to date te maken, gegeven aan een andere stagiair binnen Actemium. Er is daarvoor een E-plan licentie aanwezig in het EduLab maar die wordt dus op dit moment gebruikt door die stagiair. Daarnaast is het zoveel wat nog gecontroleerd moet worden dat deze stagiair dit waarschijnlijk niet binnen zijn stageperiode gaat halen. Daarom is besloten om een apart pakket te maken van alle elektrische tekeningen, die te maken hebben met het veiligheidssysteem. Omdat dit niet in E-plan kan is er besloten om gebruik te maken van Autocad. De elektrische tekeningen zijn te zien in bijlage XXV.

8.5 Stap 5: Installatie, inbedrijfstellen en validatie

Voor de installatie, inbedrijfstelling en validatie van het veiligheidssysteem moeten een aantal taken verricht worden. Allereerst kan er na het kiezen van de onderdelen al een verificatie gedaan worden. Hierin worden een aantal waarden van de SIF's berekend om te kijken of ze voldoen aan de eisen in het SRS. Daarna kan de installatie van die onderdelen en de bekabeling plaatsvinden volgens de gemaakte tekeningen. Na de installatie kan het geheel inbedrijfgesteld worden en kan er een validatie plaatsvinden. De validatie zal gebeuren aan de hand van een aantal documenten waarin staat wat er gecontroleerd moet worden.

8.5.1 Design verificatie

Voor de verificatie moeten er een aantal berekeningen gemaakt worden. Deze berekeningen zijn een controle om te kijken of de gekozen onderdelen voldoen aan de eisen die gesteld zijn in het SRS. Onderstaand wordt de methode voor het berekeningen uitgelegd en de uitkomsten vermeld. De berekeningen zelf zijn toegevoegd in bijlage XXVI. Voor deze berekeningen zijn een aantal waarden nodig:

- λsd [$/10^9\ uur$] (de veilige gedetecteerde faalcijfers)
- λsu [$/10^9\ uur$] (de veilige ongedetecteerde faalcijfers)
- λdd [$/10^9\ uur$] (de gevaarlijke gedetecteerde faalcijfers)
- λdu [$/10^9\ uur$] (de gevaarlijke ongedetecteerde faalcijfers)
- T1 [uur] (de proof test interval)
- MTTR [uur] (de mean time to restauration)
- HFT (hardware fault tolerance)
- Type element (A of B)

De faalcijfers geven aan hoe vaak een component kan falen. Deze zijn opgesplitst in veilig falen en gevaarlijk falen. De veilige fouten zijn fouten die veroorzaakt worden door de veiligheidscomponenten zelf. Wanneer bijvoorbeeld een input op de veiligheidsPLC faalt, wordt de volledige kaart spanningsloos gemaakt. Op deze input hoeft dan geen sensor aangesloten te zitten, dus er zal nooit een gevaarlijke situatie gecreëerd worden. Gevaarlijke fouten zijn fouten waarbij het veiligheidssysteem de installatie niet naar een veilige toestand kan brengen bij een demand. Omdat sommige componenten diagnose hebben en omdat alle componenten een proof test moeten ondergaan, kunnen sommige fouten ontdekt worden. Daarvoor is er tussen gevaarlijke fouten en veilige fouten ook nog eens onderscheid gemaakt in gedetecteerde en ongedetecteerde fouten. De faalcijfers zijn terug te vinden in de certificaten of de safety manuals van de componenten. De waarden T1 en MTTR zijn waarden die overgenomen moeten worden uit de SRS. De hardware fault tolerance is een waarde hoeveel fouten een component kan tolereren voordat de SIF actie moet gaan ondernemen. Dit heeft vooral te maken met redundante componenten en de voting die gebruikt wordt. Zijn er geen redundante componenten, zoals in dit geval, dan is de hardware fault tolerance altijd 0. Daarnaast moet er opgelet worden of het component software bevat (type B element) of dat het component geen software bevat (type A element). Dit is terug te vinden in het certificaat of de safety manual van het component.

De SIL waarden van elke SIF

Voor de onderstaande berekeningen wordt uitgegaan dat alle componenten in de SIF's gecertificeerd zijn. Omdat er in dit project echter geen nieuwe kleppen toegevoegd zijn, kan de SIL waarde nooit boven 0 uitkomen. Er wordt echter aangenomen dat de kleppen proven in use zijn. Dat wil zeggen dat ze door jarenlang gebruikt ook een SIL classificatie kunnen krijgen. Dit moet normaal gesproken zeer uitvoerig gedocumenteerd en bewezen worden. Dat is in dit project niet mogelijk omdat de kleppen maar af en toe gebruikt worden, en er is geen documentatie bijgehouden over het falen van de kleppen bij een demand. De huidige kleppen zijn echter wel beschikbaar met een SIL certificaat als ze nieuw besteld worden. De faalcijfers in die SIL certificaten worden aangehouden voor de berekeningen.
Naast de kleppen zijn de splitters ook niet gecertificeerd. Hiervan worden de waarden uit de FMEDA gebruikt. De FMEDA is een document dat opgesteld wordt door dezelfde instanties die de SIL certificering van componenten doen. Het is een document dat vaak wordt opgesteld om te bewijzen dat een onderdeel proven in use is of in een geconditioneerde testruimte getest is. De faalcijfers die in de FMEDA van de splitter staan, zullen gebruikt worden voor de berekeningen.

Om te kijken of de SIF voldoet aan de SIL waarde die in het SRS geëist is moeten drie stappen uitgevoerd worden. De eerste stap is een berekening van de PFD waarde, waar uiteindelijk het SIL niveau mee opgezocht kan worden. Om de PFD van de volledige SIF te berekenen worden de volgende formules gebruikt:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} * \left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} * MTTR \qquad PFD = (\lambda_{DU} + \lambda_{DD}) * t_{CE} \qquad RRF = \frac{1}{PFD_{sys}}$$

Deze formules komen uit de norm en zijn afgeleid en vereenvoudigd van een aantal zeer ingewikkelde formules. Deze formules gelden ook alleen bij een voting van 1oo1, voor elke andere voting zijn ook andere formules beschikbaar in de norm. Met deze formules wordt van elk component in de SIF, de PFD en waarde berekend. Door deze bij elkaar op te tellen kom je op de PFD waarde van de volledige SIF (PFDsys). Omdat de PFD waarde niet echt tot de verbeelding spreekt kan er ook een risico reductie factor berekend worden. Deze factor geeft aan hoeveel keer een risico gereduceerd wordt door de SIF. Aan de hand van Tabel 8-8 kan bij de PFD en RRF waarde de SIL waarde van de SIF gevonden worden. De resultaten zijn te zien in Tabel 8-10, Tabel 8-11 en Tabel 8-12.

SIL	PFD	Risk Reduction Factor
1	$10^{-1} - 10^{-2}$	10 - 100
2	$10^{-2} - 10^{-3}$	100 – 1.000
3	$10^{-3} - 10^{-4}$	1.000 – 10.000
4	$10^{-4} - 10^{-5}$	10.000 – 100.000

Tabel 8-8: Vergelijking SIL, PFD en RRF

De tweede stap is het opzoeken en berekenen van SIL waarde voor Architectural Constraints. Daarvoor wordt gebruik gemaakt van Tabel 8-9.

Safe Failure Fraction (SFF)	Type A element Hardware Fault Tolerance (HFT)			Type B element Hardware Fault Tolerance (HFT)		
	0	1	2	0	1	2
<60%	SIL 1	SIL 2	SIL 3	N. A.	SIL 1	SIL 2
60% - <90%	SIL 2	SIL 3	SIL 4	SIL 1	SIL 2	SIL 3
90% - <99%	SIL 3	SIL 4	SIL 4	SIL 2	SIL 3	SIL 4
≥99%	SIL 3	SIL 4	SIL 4	SIL 3	SIL 4	SIL 4

Tabel 8-9: Architectural Constraints

Om nu uit de tabel de SIL waarde te kunnen halen, moet de safe failure fraction berekend worden. Dit kan door het toepassen van de volgende formule:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} * 100\%$$

Ook deze formule komt uit de norm. Door deze formule op elk component toe te passen komt er een SFF uit die gebruikt kan worden in de tabel. Voor elk component krijg je dus een SIL waarde. De SIL waarde van de SIF zal dan gelijk zijn aan de laagste SIL waarde van alle componenten in die SIF (een ketting is zo sterk als de zwakste schakel). Uitkomst van deze berekening is te zien in Tabel 8-10, Tabel 8-11 en Tabel 8-12.

De derde stap is het opzoeken van de SIL waarde voor Systematic Capability. Deze zijn te vinden op de certificaten of in de safety manual van de componenten. Ook hier geld dat de SIL waarde van de SIF, gelijk is aan de laagste SIL waarde van alle componenten. De uitkomst van deze stap is te zien in Tabel 8-10, Tabel 8-11 en Tabel 8-12.

De mean time to fail spurious

Omdat het ongewenst en ongepland uitschakelen van een installatie, of deel van een installatie, heel duur kan zijn wordt er ook gekeken naar de mean time to fail spurious (MTTFs). Dit is de hoeveelheid per tijdseenheid dat een installatie uitvalt terwijl er niets mis is in het proces. De uitval wordt dan veroorzaakt door fouten in de apparatuur in het veiligheidssysteem. Om te berekenen hoeveel tijd (in jaren) dat er tussen de spurious trips zit, wordt er gebruik gemaakt van de volgende formule:

$$STR = \lambda_{SD} + \lambda_{SU} + \lambda_{DD}$$

Om de spurious trip rate van de hele SIF te krijgen moeten de veilige faalcijfers en de dangerous detected faalcijfers van alle componenten in de SIF bij elkaar opgeteld worden. Het getal wat daar uitkomt, is het aantal keren dat de installatie kan falen in 10^9 uur. Dit moet dus omgerekend worden naar een aantal jaren tussen twee spurious trips. Daarvoor wordt de volgende formule gebruikt:

$$MTTFs\ (jaren) = \frac{10^9}{STR * 8760}$$

De uitkomst van deze berekening voor alle SIF's is te zien in Tabel 8-10, Tabel 8-11 en Tabel 8-12.

Responstijd

In het SRS is aangegeven dat de reactietijd van het veiligheidssysteem en van het proces niet meer mocht zijn dan 25% van de proces veiligheidstijd. Er moet gecontroleerd worden of dat klopt bij het gebruik van de gekozen componenten.

$$totale\ responstijd = \frac{\Sigma responstijden\ componenten}{proces\ veiligheidstijd} * 100\%$$

De uitkomst van deze berekening voor alle SIF's is te zien in Tabel 8-10, Tabel 8-11 en Tabel 8-12.

SIF 1: Temperatuur		
Controlepunten	Eis SRS	Uitkomst
PFD		1,85E-04
RRF		5402,05
SIL classificatie	SIL 1	SIL 3
SIL Arch. Constraints	SIL 1	SIL 1
SIL Syst. Capability	SIL 1	SIL 2
SIL totaal	SIL 1	SIL 1
MTTFs [jaar]	< 10	72,80
Proces veiligheidstijd [s]		600
Response tijd [s]		1,736
Percentage	< 25%	0,29%
Voldoet aan alle eisen?	ja	

Tabel 8-10: Uitkomsten design verificatie SIF 1

SIF 2: Druk		
Controlepunten	Eis SRS	Uitkomst
PFD		1,93E-04
RRF		5190,87
SIL classificatie	SIL 1	SIL 3
SIL Arch. Constraints	SIL 1	SIL 1
SIL Syst. Capability	SIL 1	SIL 2
SIL totaal	SIL 1	SIL 1
MTTFs [jaar]	< 10	61,61
Proces veiligheidstijd [s]		5
Response tijd [s]		1,026
Percentage	< 25%	20,52%
Voldoet aan alle eisen?	ja	

Tabel 8-11: Uitkomsten design verificatie SIF 2

SIF 3: Niveau		
Controlepunten	Eis SRS	Uitkomst
PFD		3,00E-04
RRF		3336,63
SIL classificatie	SIL 1	SIL 3
SIL Arch. Constraints	SIL 1	SIL 1
SIL Syst. Capability	SIL 1	SIL 2
SIL totaal	SIL 1	SIL 1
MTTFs [jaar]	< 10	54,94
Proces veiligheidstijd [s]		187
Response tijd [s]		0,936
Percentage	< 25%	0,50%
Voldoet aan alle eisen?	ja	

Tabel 8-12: Uitkomsten design verificatie SIF 3

Voor bovenstaande berekeningen is gebruik gemaakt van de bronnen uit Tabel 8-13.

Component	Document	Bron
Temperaturetransmitter TMT82	SIL certificaat	("TÜV", TMT82 SIL certificate, 2014)
	Safety manual	("Endress&Hauser", TMT82 safety manual, 2014)
	Datasheet / manual	("Endress&Hauser", TMT82 Tecnical information, 2014)
Pressuretransmitter PMC71	SIL certificaat	("TÜV", PMC71 SIL certificate, 2014)
	Safety manual	("Endress&Hauser", PMC71 safety manual, 2014)
	Datasheet / manual	("Endress&Hauser", PMC71 Technical information, 2014)
Levelswitch FTL51	SIL certificaat	("TÜV", FTL51 + FEL 57 + FTL 325P, 2014)
	Safety manual	("Endress&Hauser", FTL51 en FTL325P Functional safety manual, 2014)
	Datasheet / manual	("Endress&Hauser", FTL51 Technical information, 2014)
Levelswitch versterker FTL325P	SIL certificaat	Zie SIL certificaat FTL51
	Safety manual	Zie safety manual FTL51
	Datasheet / manual	("Endress&Hauser", FTL325P Technische informatie, 2014)
VeiligheidsPLC F35 3	SIL certificaat & safety manual	("TÜV", TÜV EC type examination Certificate & Safety manual, 2014)
	Datasheet / manual	("HIMA", 2014)
Remote I/O	SIL certificaat & Safety manual	Zie SIL certificaat en safety manual veiligheidsPLC
	Datasheet / manual	Zie datasheet veiligheidsPLC
Splitters KDF2-CR4-1.2O	FMEDA rapport	("Exida", KFD2-CR4-1.2O exida functional safety assessement, 2014)
	Safety manual	("Pepperl&Fuchs", KFD2-CR4-1.2O functional safety manual, 2014)
	Datasheet / manual	("Pepperl&Fuchs", KFD2-CR4-1.2O datasheet, 2014)
Valve SC-G-327B103-24V/DC	SIL certificaat & Safety manual	("Exida", Asco 327 SIL certificate & Assessement report, 2014)
	Datasheet / manual	("Asco", 2014)
Actuator Norbro 40R	SIL certificaat & Safety manual	("Exida", Norbro 40R SIL certificate & Assessement report, 2014)
	Datasheet / manual	("Flowserve", Norbro 40R, 2014)

Klep Worcester F54	SIL certificaat & Safety manual	("Exida", Worcester F54 SIL certificate & Assessement report, 2014)
	Datasheet / manual	("Flowserve", Worcester 54 serie , 2014)

Tabel 8-13: Bronnen gebruikt voor de design verificatie

8.5.2 Validatie

Voor de validatie van dit project zijn twee stappen nodig. Allereerst wordt er een veld verificatie gedaan om te controleren of alles volgens het ontwerp is geïnstalleerd. Daarna zal de validatie gedaan worden om te controleren of de installatie met het toegevoegde veiligheidssysteem voldoet aan alle gestelde eisen in de norm en de documentatie van het veiligheidssysteem.

De veld verificatie

Een veld verificatie is bedoeld om te controleren of de volledige installatie klaar is om inbedrijfgesteld te worden. Hierin wordt gekeken naar de inbouw van alle componenten en de verwijdering van verpakkingsmaterialen of beschermingsmaterialen. Ook wordt er gekeken naar de kalibratie van de sensoren en of daar een wachtwoord of iets dergelijks op zit. Alle onderwerpen die gecontroleerd moeten worden, moeten in een document vastgelegd worden. Het document moet de eisen uit de norm bevatten en goedgekeurd worden door de stagebegeleider om gebruikt te kunnen worden. Daarna kan het document, vóór de inbedrijfstelling, doorlopen en ondertekend worden ter goedkeuring.

De validatie

Nadat de installatie inbedrijfgesteld is kan de validatie gedaan worden. Deze is bedoeld om te controleren of alle functies die toegevoegd zijn, werken zoals vooraf beschreven is. Hiervoor wordt ook een document gemaakt dat de eisen uit de norm en de eisen uit het SRS bevat. Dit document moet goedgekeurd zijn voordat het gebruikt kan worden voor de validatie. De validatie wordt binnen bedrijven ook vaak de SAT ofwel Site Acceptance Test genoemd. In de validatie wordt samen met de opdrachtgever de installatie gecontroleerd op de werking in alle verschillende modi. De functie van de oude installatie moeten daarbij behouden blijven, en het toegevoegde systeem moet voldoen aan de eisen die gesteld zijn in het SRS. Dit document moet dus volledig doorlopen worden en getekend worden door zowel de opdrachtnemer als de opdrachtgever ter goedkeuring.

De documenten voor de veld verificatie en de validatie zijn nog niet gemaakt. De voortgang van deze documenten en alle andere werkzaamheden voor de realisatie voor dit project zullen besproken worden in het volgende hoofdstuk.

9 Realisatie

Voor de realisatie van dit project is een planning gemaakt waarin gebruik gemaakt wordt van fasen en mijlpalen. In dit hoofdstuk zal de globale fasering van die planning te zien zijn en zal per fase verteld worden hoe deze volbracht is of nog volbracht moet worden (paragrafen 9.1 en 9.2). Daarna zal de voortgang in het project besproken worden waarin aangetoond wordt hoe in de laatste weken de realisatie voltooid gaat worden (paragraaf 9.3). Tot slot worden de risico's besproken die in dit project zijn voorgekomen (paragraaf 9.4).

9.1 Globale fasering

In Tabel 9-1 is te zien hoe het verloop van de stage ingedeeld is. Hierin wordt getoond in welke weken de fasen plaatsgevonden hebben en wanneer de mijlpalen plaatsgevonden hebben.

Week	Fase / mijlpaal	Beschrijving	Toelichting
34-04	F0	Schooldocumenten maken	Deze fase loopt over het gehele project en er wordt nog aan gewerkt
34-35	F1	Voorbereidingsfase	Inlezen documenten, bestuderen opdracht
36-47	F2	Onderzoeksfase	Het onderzoeken van de norm en de installatie, het uitwerken van de deelvragen
37	M1	Inleveren PID	Deze is ingeleverd en goedgekeurd
39-49	F3	Ontwerpfase	Ontwerpen van het veiligheidssysteem en maken van de standaarddocumenten die nodig zijn
47	M2	Analyserapport	Dit verslag heeft wat vertraging opgelopen en is later klaar dan de originele planning aangaf
39	M3	Standaarddocument risicoanalyse	Het standaarddocument van stap 1 is gecontroleerd en goedgekeurd
41	M4	Risicoanalyse uitgevoerd	Het ingevulde standaarddocument is goedgekeurd
41	M5	Standaarddocument Allocatieblad	Het standaarddocument van stap 2 is gecontroleerd en goedgekeurd
42	M6	Inleveren reflectieverslag en prof. Funct.	De beoordeling is uitgevoerd en samen met een reflectieverslag ingeleverd
43	M7	Allocatie uitgevoerd	Het ingevulde standaarddocument is goedgekeurd
46	M8	Standaarddocument SRS	Het standaarddocument van stap 3 is nog niet gecontroleerd, wel volledig gemaakt
47	M9	SRS ingevuld	Het SRS is ingevuld voor het project maar nog niet goedgekeurd
49-02	F4	Realisatiefase	Installeren, in bedrijf stellen en valideren van het ontwerp
49	M10	Ontwerp veiligheidssysteem	Het ontwerp is nog niet volledig, een aantal tekeningen moeten nog bijgevoegd worden
51	M11	Standaarddocument validatie / FAT / SAT	Een standaarddocument voor stap 5 is nog niet gemaakt
50	M12	Inleveren eindverslagen	Het eindverslag wordt nog aangepast naar gelang het project vordert
02	M13	FAT / SAT	Het opleveren en valideren van het project wordt gedaan wanneer het ontwerp gerealiseerd is
01-03	F5	Afrondingsfase	Het in orde brengen van alle documentatie die van belang is bij de nieuwe installatie

03	M14	Overdracht documentatie en afsluiting	Als de validatie gedaan is worden alle documenten opgeleverd aan Actemium
04	M15	Presentatie en verdediging	Na het goedkeuren van het eindverslag wordt de presentatie gemaakt en de verdediging gehouden

Tabel 9-1: Globale fasering

9.2 Realisatie per fase

Fase 0 Schooldocumenten maken, wordt gebruikt om alle documenten die voor school gemaakt moeten worden te plannen. Dit is wat apart gehouden van de onderdelen die vooral voor Actemium van belang zijn. Deze fase bestaat uit vier mijlpalen namelijk M1 inleveren PID, M6 inleveren reflectieverslag en professioneel functioneren 1e keer, M12 inleveren eindverslagen (hieronder valt het afstudeerverslag en het reflectieverslag met de bijbehorende beoordeling professioneel functioneren) en M15 de presentatie en de verdediging. Voor het PID zijn de eerste weken van het project gebruikt. Hier is voornamelijk de opdracht goed onderzocht en daarbij is een hoofdvraag en een aantal deelvragen naar voren gekomen. Het professioneel functioneren is halverwege het project ingevuld door de stagebegeleider. Op deze beoordeling is gereflecteerd en dit is verwerkt in het reflectieverslag. Het afstudeerverslag is het huidige document en is opgebouwd uit onder andere het analyserapport, het ontwerprapport met daarnaast alle aanvullende hoofdstukken. De tweede professioneel functioneren beoordeling is inmiddels ook al gedaan en is verwerkt in een reflectieverslag. De presentatie zal gemaakt worden wanneer dit verslag goedgekeurd is.

Fase 1 Voorbereidingsfase, is vooral voor de voorbereiding op de onderzoeksfase. In deze fase is er ingelezen in de standaard bedrijfsdocumenten voor nieuwe werknemers en in de opdracht en de normen. Uiteindelijk valt deze fase ook samen met het PID, waar hoofd- en deelvragen gesteld zijn die uiteindelijk in de volgende fase onderzocht moeten worden. Er zijn geen specifieke mijlpalen in deze fase.

Fase 2 Onderzoeksfase, is voor het onderzoeken van alle hoofd- en deelvragen die in het PID naar voren zijn gekomen. Vooral het onderzoek naar de installatie en de normen is van groot belang in deze fase omdat deze bepalend zijn voor de ontwerpfase. De mijlpaal van deze fase is M2 het analyseverslag. In het analyseverslag zijn de deelvragen beantwoord door het onderzoeken van de normen, de installatie en de overige onderwerpen uit de onderzoeksvragen. De inhoud van het analyseverslag is toegevoegd aan het eindverslag onder het hoofdstuk analyse. Omdat het onderzoek veel meer inhield als vooraf verwacht is deze fase uitgelopen.

Fase 3 Ontwerpfase, loopt voor een deel gelijktijdig met de onderzoeksfase. Dit is gedaan omdat er vaak nog vragen bijkomen na het onderzoeken en bij het starten van de eerste ontwerpen. In deze fase is het ontwerp gemaakt die de installatie gaat verbeteren. De mijlpalen van deze fase zijn M3 het standaarddocument risicoanalyse, M4 de risicoanalyse uitgevoerd, M5 het standaarddocument allocatieblad, M7 de allocatiebladen ingevuld, M8 het standaarddocument SRS, M9 het SRS ingevuld en M10 het ontwerp van het veiligheidssysteem. Voor de risicoanalyse is in het analyserapport onderzocht welke methoden er gebruikt kunnen worden, en is uiteindelijk een methode gekozen die toegepast is in het project. Voor het allocatieblad is in het analyserapport onderzocht welke methoden er gebruikt kunnen worden, en is uiteindelijk een methode gekozen die toegepast is in het project. Voor het SRS zijn de eisen en een voorbeeld van Actemium gebruikt om het standaarddocument op te zetten. Dit standaarddocument is uiteindelijk ingevuld voor het project. Daarna is er gestart met het ontwerpen door middel van berekeningen, tekeningen aanpassen en uitzoeken van onderdelen.

Fase 4 Realisatiefase, zal het ontwerp gebouwd gaan worden op de installatie. Hierin wordt dus de realisatie, het in bedrijf nemen en het testen van de installatie gedaan. De mijlpalen van deze fase zijn M11 de standaarddocumenten voor de validatie / FAT / SAT en M13 de uitgevoerde validatie / FAT / SAT. Het

installeren zal gebeuren door een monteur van Actemium die daarbij gebruik maakt van het ontwerp van de afstudeerster. Wanneer dit gereed is wordt er een FAT of SAT test gedaan, maar wordt er ook gevalideerd of alle onderdelen goed gekozen zijn. De validatie bestaat uit het opnieuw berekenen van alle belangrijke waarden als de PFDavg. Daaruit moet blijken of de onderdelen die gebruikt zijn inderdaad zorgen voor voldoende risico reductie in de ProcessCell. De FAT of SAT is bekijken of alles gebouwd is zoals het ontworpen is, en daarnaast bekijken of alles voldoet aan de eisen die gesteld zijn in de voorgaande documentatie.

Fase 5 Afrondingsfase:

In de afrondingsfase moet er gezorgd worden dat alle documentatie op de juiste plek staat en up to date zijn. Ook zullen er misschien handleidingen of dergelijke gemaakt worden die van belang zijn voor de overdracht van dit project. Mijlpaal in deze fase is M14 de overdracht en afronding. Aangezien de documentatie in dit project zo belangrijk was, is elk gemaakt stuk gecontroleerd en goedgekeurd door de leidinggevende. Daardoor zouden alle documenten up to date moeten zijn dus zal de overdracht niets anders zijn dan de goedgekeurde documenten en het ontwerp in de juiste mappen zetten.

9.3 Voortgang

Omdat om het moment van schrijven van dit verslag, de realisatie niet gereed is zal hier weergegeven worden wat de stand van zaken is. Daarna zal beschreven worden welke vervolgstappen er nog genomen gaan worden om de realisatie voor de einddatum van het project nog af te ronden.

Stand van zaken

Op het moment van schrijven is het ontwerp voor het veiligheidssysteem volledig gereed en geverifieerd. In de installatie zijn de PLC, de remote I/O en de klemmenstroken ingebouwd. De kabels zijn al binnen en kunnen ook gelegd worden, maar daarvoor moet er een monteur beschikbaar zijn binnen Actemium. De splitters, shunts en ventielen zijn al in bestelling, en voor de sensoren wordt druk gecommuniceerd met Endress en Hauser, over een mogelijke sponsoring. Op de ventielen zit echter een langere levertijd waardoor de installatie nog niet volledig afgemaakt kan worden. Ook de software, het document voor de veld verificatie en het document voor de validatie zijn nog niet gemaakt.

Hoe nu verder

Het totaal realiseren van het project zal afhankelijk zijn van de komende weken in dit project. Om toch een oplevering te doen wordt de volgende planning aangehouden:

- In week 51 wordt de PLC geprogrammeerd en getest volgens de eisen in het SRS. Het testen van de PLC zal gebeuren in de algemene testruimte binnen Actemium. Daarnaast zal er gestart worden met het maken van de documenten voor de veld verificatie en de validatie. Tijdens deze werkzaamheden zal er door een monteur, zover mogelijk, de bekabeling in de installatie gelegd en aangesloten worden.
- In week 52 worden de documenten van de verificatie en de validatie afgemaakt.
- In week 02 worden alle documenten gecontroleerd en zal er in ieder geval op de geschreven software een officiële verificatie en validatie plaatsvinden. Hierbij wordt de I/O gesimuleerd door middel van bijvoorbeeld potmeters, drukknoppen en lampjes. Daarbij zal een van de begeleiders de veld verificatie en validatie mee afnemen en ondertekenen ter goedkeuring.
- In week 03 worden de ventielen verwacht. Deze kunnen dan ingebouwd en aangesloten worden. Omdat alle bekabeling al gelegd is, kan het aansluiten nog door de afstudeerder zelf gedaan worden. De ventielen kunnen dan ook de veld verificatie en validatie ondergaan zoals dit met de software ook gedaan is. Hierbij worden de inputs gesimuleerd door middel van bijvoorbeeld potmeters en drukknoppen.
- Week 04 is de week waarin de afstudeerpresentatie plaatsvindt. In deze presentatie zal kort verteld worden hoe de realisatie in de laatste weken verlopen is. Daarbij worden de afgetekende veld verificatie en de validatie documenten meegenomen worden.

Omdat de levertijd van de sensoren waarschijnlijk te lang is om dit binnen de afstudeerstage nog te kunnen realiseren, is de enige realisatie in dit project de software en de ventielen.

9.4 Risico's

In het PID zijn een aantal risico's bepaald die invloed kunnen hebben op het project. Van deze risico's zijn er een aantal werkelijkheid geworden in het project. In Tabel 9-2 en Tabel 9-3 is weergegeven welke risico's zijn voorgekomen in dit project. Daaronder staat een toelichting op hoe het risico is voorgekomen en hoe het opgelost is.

Risico	Kans	Gevolg	Oplossing
De onderzoeken duren te lang	Aanwezig	Vertraging in het project	Hulp vragen aan experts binnen het bedrijf, buiten bedrijfsuren doorwerken.
Toelichting	De onderzoeken die gedaan zijn, hebben veel langer geduurd dan gepland is. Daardoor is er minder tijd besteed aan andere delen in het eindverslag en is de deadline in gevaar gekomen. Om dit op te lossen is buiten bedrijfsuren stevig doorgewerkt om toch alles op tijd af te krijgen.		
Communicatie naar begeleiders is niet goed	Aanwezig	Informatie wordt niet tijdig doorgegeven	Wekelijks een momentje plannen om de begeleiders in te lichten over de voortgang
Toelichting	In het begin van het project was er veel zelfstandigheid vanuit de afstudeerster en was het niet nodig om wekelijks of zelfs twee wekelijks een vergadermoment te plannen. De stagebegeleider heeft uiteindelijk aangegeven niet op de hoogte te zijn van de werkzaamheden van de afstudeerster en heeft toen besloten om toch twee wekelijks een momentje te plannen om de voortgang te bespreken. Daardoor wordt hij op de hoogte gehouden en weet hij hoe het gaat met het project.		

Tabel 9-2: Interne risico's

Risico	Kans	Gevolg	Oplossing
De begeleiders zijn niet bereikbaar of beschikbaar	Aanwezig	Dringende vragen niet beantwoord	Op tijd contact opnemen met begeleiders bij vragen. Via andere wegen proberen contact op te nemen.
Toelichting	De begeleiders binnen Actemium hebben natuurlijk ook de eigen werkzaamheden binnen het bedrijf naast het begeleiden van de afstudeerster. Vooral op momenten dat volgens de planning een document beoordeeld of goedgekeurd moest worden kwam het wel eens voor dat de begeleiders geen tijd hadden. Binnen het project is dan gewoon doorgewerkt en regelmatig langsgegaan bij de begeleiders om alsnog de documenten te laten beoordelen of goedkeuren.		
Materiaal niet op tijd geleverd	Aanwezig	Vertraging in het project	Op tijd materialen bestellen, spoed erachter zetten
Toelichting	Het materiaal wat gebruikt wordt is geen standaard materiaal. Daarom is vroegtijdig in het project, voordat het ontwerp gemaakt is, al gekozen voor de onderdelen. Op deze manier is er een kans dat de onderdelen nog op tijd geleverd kunnen worden. Voor de onderdelen die niet op tijd komen; deze zullen na afloop van de afstudeerstage nog aangesloten worden zodat het demo model toch afgemaakt wordt.		

Andere verplichtingen als terugkomdagen of interne cursussen duren te lang	Gering	Vertraging in het project	Goed plannen. Zorgen dat alles duidelijk in de planning staat, desnoods planning tussentijds bijwerken.
Toelichting	Na het maken van de planning zijn er nog een aantal verplichtingen bijgekomen die vooraf niet voorzien waren. Onder andere door die verplichtingen is wat vertraging in het project ontstaan. Een aantal van die verplichtingen is een driedaagse cursus voor de IEC61511 / IEC61508 norm en de Actemium Automation Awards.		
Het ontwerp valt ver buiten het budget (€5000, -)	Gering	Geen realisatie van het ontwerp	Geen. Beschrijven waarom deze realisatie niet goedgekeurd wordt in het eindverslag.
Toelichting	Bij het kiezen van de onderdelen zijn nog een aantal tegenslagen voorgekomen. Twee van de sensoren die al in de procesinstallatie zaten werken met Profibus. Deze moeten ook aan de SIS aangesloten worden, maar die werkt alleen met een 4-20mA signaal. Daarom moeten die twee sensoren vervangen worden door nieuwe sensoren met een 4-20mA uitgang zodat ze zowel op het BPCS als op de SIS aangesloten kunnen worden. Daardoor valt echter de totale prijs hoger uit dan verwacht, maar de onderdelen zijn uiteindelijk wel besteld.		

Tabel 9-3: Externe risico's

10 Eindproduct

Als het volledige project klaar is komt daar een eindproduct uit. De eindproducten voor deze opdrachten zijn de standaarddocumenten voor de risicoanalyse, de allocatiebladen en het SRS, en het fysieke veiligheidssysteem. In dit hoofdstuk wordt beschreven wat de resultaten zijn van deze opdracht, wordt er een evaluatie gegeven, wordt er een conclusie gegeven en worden de aanbevelingen getoond.

10.1 Resultaat

De standaard documenten die gemaakt zijn voor dit project zijn bedoeld voor Actemium om te werken als leidraad. Bij nieuwe of bestaande klanten kan Actemium haar eigen documenten in huisstijl van Actemium gebruiken. Daarnaast staan alle onderdelen die nodig zijn om te voldoen aan de normen in die documenten. Bij goed gebruik van die documenten is het dus niet tot nauwelijks meer nodig om in de norm zelf te kijken, maar kan het project door middel van de documentatie voldoen aan de norm. De standaarddocumenten die gemaakt zijn, zijn de risicoanalyse, het allocatieblad en het SRS.

Het veiligheidssysteem is op het moment van schrijven nog niet toegevoegd. Wanneer dit toegevoegd wordt kan het demo model van de ProcessCell op veel verschillende manieren gebruikt worden. Met het toegevoegde veiligheidssysteem kunnen klanten, leerlingen, studenten en eigen personeel kennismaken met veiligheidssystemen, met de veiligheidsPLC van HIMA en met de documentatie die bij een veiligheidssysteem van toepassing is. Het demo model kan ook gebruikt worden om studenten, leerlingen en eigen personeel te leren een veiligheidsPLC te programmeren. Gezien de ProcessCell ook voor scholen gebruikt wordt om oefeningen uit te voeren zal het veiligheidssysteem gedeeltelijk ongewenste situaties tegengaan die voor kunnen komen bij die oefeningen.

10.2 Evaluatie en conclusie

De standaard documenten zijn constant in overleg met de expert binnen Actemium opgesteld, om de documenten te laten voldoen aan zijn eisen en wensen. Voor elk gemaakt document is dan ook een goedkeur formulier getekend. Er is nog geen ervaring met het gebruik van de standaarddocumenten dus het kan zijn dat Actemium die in de toekomst nog aan wil passen aan de gebruikerservaringen.

De documenten zijn geschikt om te gebruiken in elke vorm van procesautomatisering die valt binnen de IEC61511. De invulling van de documenten zijn gebaseerd op de norm in samenwerking met Actemium en zijn voor iemand die ervaring heeft in veiligheidssystemen eenvoudig te gebruiken.

De methoden die gebruikt zijn voor het maken van de standaarddocumenten zijn bepaalt door Actemium. Het kan echter zijn dat andere methoden meer geschikt zijn, afhankelijk van de klant waar Actemium voor werkt. De keuze voor de HAZOP methode en de gekalibreerde risicograaf zijn voor dit project dus goed, maar ook daar kan in de toekomst de mening over veranderen.

Het veiligheidssysteem is nog niet volledig toegevoegd. Als het veiligheidssysteem toegevoegd wordt zoals het ontworpen is, voldoet het aan de eisen en wensen van Actemium. Het is dan echter geen volledig veiligheidssysteem omdat de kleppen en splitters die gebruikt worden geen SIL classificatie hebben, waardoor de volledige loops niet als SIL waardig worden beschouwd.

Uitbreiding is zeker mogelijk gezien er nog een aantal I/O vrij is op de PLC en de remote I/O en er kunnen nog tot 64 remote I/O's toegevoegd worden aan het veiligheidssysteem. Wel moet er dan een andere voeding en een nieuwe kast bijgeplaatst worden gezien de ruimte in de kast beperkt is en de voeding niet voldoende sterk is voor meer apparatuur.

Conclusie
De standaarddocumenten die zijn gemaakt in dit project zijn voorlopig goed om te gebruiken in projecten waar een veiligheidssysteem nodig is. Als het veiligheidssysteem ingebouwd is kan dit gebruikt worden voor klanten, leerlingen, studenten en medewerkers als voorbeeld en als educatieve oplossing.

10.3Aanbevelingen

Als de standaard documenten gebruikt zullen gaan worden door medewerkers met ervaring, zijn de documenten op zichzelf voldoende om een project te kunnen engineeren. Gezien er vanuit Actemium de intentie is om meerdere medewerkers ervaring op te laten doen in projecten die moeten voldoen aan de norm, kan het handig zijn om een soort handleiding te schrijven, hoe gebruik gemaakt kan worden van de standaard documenten. Bij medewerkers waar de norm nog nieuw is moet echter wel altijd de norm aangehouden en bestudeerd worden, voordat gebruik gemaakt kan worden van de standaarddocumenten.
De documenten zijn gemaakt zoals de norm nu is, maar het kan zijn dat er nieuwe versies van de norm uitgebracht worden. De documenten moeten dan een update krijgen zodat ze voldoen aan de laatste versie van de norm. Dit geld voor zowel de documenten in het Nederlands als de documenten in het Engels.

De methoden die gekozen zijn door Actemium, zijn voornamelijk gekozen omdat dat bekende methoden zijn. Het is echter mogelijk dat een klant of Actemium zelf later een andere voorkeur krijgt. Wanneer dat gebeurt, moeten er nieuwe standaarddocumenten gemaakt worden die de nieuw gekozen methoden ondersteunen.

Het veiligheidssysteem wat toegevoegd zal gaan worden zal niet voldoen aan de SIL classificatie omdat een aantal onderdelen niet gecertificeerd zijn. In de toekomst kan het daarom goed zijn om alle componenten in het veiligheidssysteem te vervangen door SIL gecertificeerde componenten. Alleen dan kan Actemium een volledig gecertificeerd demo model laten zien aan haar klanten. Daarnaast werkt het veiligheidssysteem slechts met drie risico’s in de ProcessCell. In de toekomst is het verstandig om de volledige ProcessCell te bewerken zodat ook alle andere risico’s gereduceerd kunnen worden. Waar dan wel rekening mee gehouden moet worden is de voeding die nu voor het veiligheidssysteem gekozen is zoals aangegeven in paragraaf 8.4.2.

11 Proces en planning

Om het project zo goed mogelijk uit te voeren is het handig om een bepaalde projectaanpak te volgen of er zelf een te bedenken. Ook een planning is zeer belangrijk bij het uitvoeren van het project. In dit hoofdstuk is beschreven wat de projectaanpak is, wordt de strokenplanning beschreven en getoond, wordt er een klein stukje verteld over de kosten binnen dit project en wordt er een projectevaluatie gemaakt op basis van het project tot nu toe ten opzichte van de start van het project.

11.1 Projectaanpak

De methodiek die gebruikt is in dit project is het stappenplan uit de IEC61511 gecombineerd met de projectmethodiek van Roel Grit. De stappen in de norm zijn ingedeeld in de fasen die beschreven staan in het boek projectmanagement van Roel Grit (Grit, 2011) . Het bijhouden van uren is wekelijks gedaan om te bepalen wat de voortgang is en of er taken uitlopen. Per week wordt er een deadlinelijst (zie Tabel 11-1) bijgewerkt en gecontroleerd om de taken die de meeste prioriteit hebben in een kort overzicht te hebben. In bijlage XXVII is de volledige deadlinelijst toegevoegd. Voor de strokenplanning is gebruik gemaakt van Excel. Dit omdat MS-project op de computer niet beschikbaar was en omdat plannen in Excel ook goed gaat. Deze planning wordt minimaal wekelijks ingekeken en bijgewerkt wanneer dit nodig is. Op dit moment is deze planning acht keer aangepast omdat er taken zijn bij gekomen of omdat er andere veranderingen plaatsvonden.

Deadlinelijst						
Fase	Taak	Omschrijving	Dat. Gepl.	Dat. werkelijk	status	opmerkingen
2. Onderzoek	2	Onderzoek IEC61508 / IEC61511	26-9-2014	19-11-2014	Klaar	Loopt uit, zie deelvragen
2. Onderzoek	2	Deelvraag 1a	26-9-2014	7-10-2014	Klaar	Loopt uit, wordt tijdens ontwerpen verder afgemaakt
2. Onderzoek	2	Deelvraag 1b	26-9-2014	19-11-2014	Klaar	Loopt uit, wordt tijdens ontwerpen verder afgemaakt
2. Onderzoek	2	Deelvraag 1c	26-9-2014	22-9-2014	Klaar	
2. Onderzoek	2	Deelvraag 1d	26-9-2014	17-11-2014	Klaar	Loopt uit, wordt tijdens ontwerpen verder afgemaakt
2. Onderzoek	2	Deelvraag 2a	26-9-2014	18-9-2014	Klaar	

Tabel 11-1: Deadlinelijst voorbeeld

11.2 Strokenplanning

Op de pagina's 79 tot en met 81 is de strokenplanning weergegeven. Er is in deze planning onderscheid gemaakt tussen werkzaamheden die voor school van belang zijn of werkzaamheden die voor Actemium van belang zijn. In het bovenste blok is te zien welke documenten er gemaakt en ingeleverd moeten worden. Er is daarbij rekening gehouden met het gebruik van concept versies omdat alles nagekeken moet worden door, in ieder geval, de stagebegeleider voordat het opgestuurd wordt. Het onderste blok geeft de werkzaamheden weer die nodig zijn om de opdracht te voltooien voor Actemium. De volledige planning is opgedeeld in fasen en mijlpalen. Bij de fasen is voor elke fase een andere kleur gebruikt om duidelijk te maken welke deeltaken bij een bepaalde fase hoort. De mijlpalen zijn aangegeven in het rood om deze extra te laten opvallen. Er is bij elke taak een start en einddatum ingevuld en in de kolom Volt. kan er door middel van een pull down menu aangegeven worden hoe ver de taak gevorderd is. Zo kan er niet alleen in de deadlinelijst bijgehouden worden of alles nog op schema loopt maar ook in de planning. In bijlage XXVIII is de eerste planning toegevoegd.

F= Fase / M = Mijlpaal

					Wk34 - aug '14					Wk35 - aug '14					Wk36 - sep '14					Wk37 - sep '14					Wk38 - sep '14					Wk39 - sep '14					Wk40 - sep '14					Wk41 - okt '14				
					M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V
Nr	Taak	Startdat.	Einddat.	Volt.	18	19	20	21	22	25	26	27	28	29	1	2	3	4	5	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	1	2	3	6	7	8	9	10
0	Afstudeertraject	18-8-2014	23-1-2015	80%																																									
F0	School documenten maken	18-8-2014	9-1-2014	100%																																									
1	PID concept	20-8-2014	5-9-2014	100%																																									
2	PID final	8-9-2014	12-9-2014	100%																																									
M1	inleveren PID		12-9-2014	V																																								
3	Invullen proffesioneel functioneren 1e keer	6-10-2014	10-10-2014	100%																																									
4	reflectieverslag concept	13-10-2014	17-10-2014	100%																																								
M6	Inleveren reflectieverslag en prof. Functioneren 1e keer		17-10-2014	V																																								
5	Invullen proffesioneel functioneren 2e keer	1-12-2014	5-12-2014	100%																																									
6	reflectieverslag final	8-12-2014	12-12-2014	100%																																								
7	afstudeerverslag concept	15-9-2014	28-11-2014	100%																																								
8	afstudeerverslag final	1-12-2014	12-12-2014	100%																																								
M12	inleveren eindverslagen		12-12-2014	V																																								
9	Presentatie maken	15-12-2014	26-12-2014	0%																																								
10	Presentatie oefenen	5-1-2015	16-1-2015	0%																																								
M15	presentatie en verdediging		23-1-2015																																									
F1	Voorbereidingsfase	18-8-2014	29-8-2014	100%																																								
1	Inlezen bedrijfsdocumentatie	18-8-2014	19-8-2014	100%																																									
2	Inlezen opdracht en normen	18-8-2014	29-8-2014	100%																																								
F2	Onderzoeksfase	29-8-2014	21-11-2014	100%																																								
1	Cursus programeren in een Hima PLC	25-9-2014	26-9-2014	100%																																									
2	onderzoeken normen IEC61508 / IEC61511	15-9-2014	21-11-2014	100%																																									
3	Onderzoeken bestaande installatie	15-9-2014	17-11-2014	100%																																									
4	Cursus normen IEC61508 / IEC61511	27-10-2014	30-10-2014	100%																																									
M2	Analyserapport		21-11-2014	V																																								
F3	Ontwerpfase	22-9-2014	14-10-2014	100%																																								
1	Stap 1 Risicoanalyse	22-9-2014	3-10-2014	100%																																									
M3	Standaarddocument risicoanalyse		26-9-2014	V																																								
M4	Risicoanalyse uitgevoerd		3-10-2014	V																																								
2	Stap 2 Toewijzen veiligheidsfuncties	6-10-2014	24-10-2014	100%																																								
M5	Standaarddocument allocation sheet		10-10-2014	V																																								
M7	Allocation uitgevoerd		24-10-2014	V																																								
3	Stap 3 SRS opstellen	20-10-2014	14-11-2014	100%																																								
M8	Standaarddocument SRS		14-11-2014	V																																								
M9	SRS uitgevoerd		21-11-2014	V																																								
4	Stap 4 Ontwerpen SIS systeem + aanpassen tekeningen	10-11-2014	5-12-2014	100%																																								
M10	Ontwerp veiligheidssysteem		5-12-2014	V																																								
F4	Realisatiefase	1-12-2014	9-1-2015	20%																																								
1	Stap 5 Instal., in bedrijf stellen en valideren/verificeren	1-12-2014	26-12-2014	40%																																								
M11	Standaarddocument / FAT/ SAT / Field verification		19-12-2014																																								
M13	FAT / SAT / Field verification		9-1-2015																																									
F5	Afrondingsfase	29-12-2014	16-1-2015	0%																																								
1	Alle documenten afmaken (Zie o.a. Fase 0)	29-12-2014	9-1-2014	0%																																								
M14	Overdracht documenten en afsluiting		16-1-2014																																									

F= Fase / M = Mijlpaal

					Wk42 - okt '14					Wk43 - okt '14					Wk44 - okt '14					Wk45 - nov '14					Wk46 - nov '14					Wk47 - nov '14					Wk48 - nov '14					Wk49 - dec '14				
					M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V
Nr	Taak	Startdat.	Einddat.	Volt.	13	14	15	16	17	20	21	22	23	24	27	28	29	30	31	3	4	5	6	7	10	11	12	13	14	17	18	19	20	21	24	25	26	27	28	1	2	3	4	5
0	Afstudeertraject	18-8-2014	23-1-2015	80%																																									
F0	School documenten maken	18-8-2014	9-1-2014	100%																																									
1	PID concept	20-8-2014	5-9-2014	100%																																									
2	PID final	8-9-2014	12-9-2014	100%																																									
M1	inleveren PID		12-9-2014	V																																								
3	Invullen proffesioneel functioneren 1e keer	6-10-2014	10-10-2014	100%																																									
4	reflectieverslag concept	13-10-2014	17-10-2014	100%																																								
M6	Inleveren reflectieverslag en prof. Functioneren 1e keer		17-10-2014	V																																								
5	Invullen proffesioneel functioneren 2e keer	1-12-2014	5-12-2014	100%																																									
6	reflectieverslag final	8-12-2014	12-12-2014	100%																																								
7	afstudeerverslag concept	15-9-2014	28-11-2014	100%																																								
8	afstudeerverslag final	1-12-2014	12-12-2014	100%																																								
M12	inleveren eindverslagen		12-12-2014	V																																								
9	Presentatie maken	15-12-2014	26-12-2014	0%																																								
10	Presentatie oefenen	5-1-2015	16-1-2015	0%																																								
M15	presentatie en verdediging		23-1-2015																																								
F1	Voorbereidingsfase	18-8-2014	29-8-2014	100%																																								
1	Inlezen bedrijfsdocumentatie	18-8-2014	19-8-2014	100%																																								
2	Inlezen opdracht en normen	18-8-2014	29-8-2014	100%																																								
F2	Onderzoeksfase	29-8-2014	21-11-2014	100%																																								
1	Cursus programeren in een Hima PLC	25-9-2014	26-9-2014	100%																																								
2	onderzoeken normen IEC61508 / IEC61511	15-9-2014	21-11-2014	100%																																								
3	Onderzoeken bestaande installatie	15-9-2014	17-11-2014	100%																																								
4	Cursus normen IEC61508 / IEC61511	27-10-2014	30-10-2014	100%																																								
M2	Analyserapport		21-11-2014	V																																								
F3	Ontwerpfase	22-9-2014	14-10-2014	100%																																								
1	Stap 1 Risicoanalyse	22-9-2014	3-10-2014	100%																																								
M3	Standaarddocument risicoanalyse		26-9-2014	V																																								
M4	Risicoanalyse uitgevoerd		3-10-2014	V																																								
2	Stap 2 Toewijzen veiligheidsfuncties	6-10-2014	24-10-2014	100%																																								
M5	Standaarddocument allocation sheet		10-10-2014	V																																								
M7	Allocation uitgevoerd		24-10-2014	V																																								
3	Stap 3 SRS opstellen	20-10-2014	14-11-2014	100%																																								
M8	Standaarddocument SRS		14-11-2014	V																																								
M9	SRS uitgevoerd		21-11-2014	V																																								
4	Stap 4 Ontwerpen SIS systeem + aanpassen tekeningen	10-11-2014	5-12-2014	100%																																								
M10	Ontwerp veiligheidssysteem		5-12-2014	V																																								
F4	Realisatiefase	1-12-2014	9-1-2015	20%																																								
1	Stap 5 Instal., in bedrijf stellen en valideren/verificeren	1-12-2014	26-12-2014	40%																																								
M11	Standaarddocument / FAT/ SAT / Field verification		19-12-2014																																								
M13	FAT / SAT / Field verification		9-1-2015																																									
F5	Afrondingsfase	29-12-2014	16-1-2015	0%																																								
1	Alle documenten afmaken (Zie o.a. Fase 0)	29-12-2014	9-1-2014	0%																																								
M14	Overdracht documenten en afsluiting		16-1-2014																																								

F= Fase / M = Mijlpaal

					Wk50 - dec '14					Wk51 - dec '14					Wk52 - dec '14					Wk1- dec '15					Wk02 - jan '15					Wk03 - jan '15					Wk04 - jan '15				
					M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V	M	D	W	D	V
Nr	Taak	Startdat.	Einddat.	Volt.	8	9	10	11	12	15	16	17	18	19	22	23	24	25	26	29	30	31	1	2	5	6	7	8	9	12	13	14	15	16	19	20	21	22	23
0	Afstudeertraject	18-8-2014	23-1-2015	80%																V	r	i	j															
F0	School documenten maken	18-8-2014	9-1-2014	100%																V	r	i	j															
1	PID concept	20-8-2014	5-9-2014	100%																V	r	i	j															
2	PID final	8-9-2014	12-9-2014	100%																V	r	i	j															
M1	inleveren PID		12-9-2014	V																V	r	i	j															
3	Invullen proffesioneel functioneren 1e keer	6-10-2014	10-10-2014	100%																V	r	i	j															
4	reflectieverslag concept	13-10-2014	17-10-2014	100%																V	r	i	j															
M6	Inleveren reflectieverslag en prof. Functioneren 1e keer		17-10-2014	V																V	r	i	j															
5	Invullen proffesioneel functioneren 2e keer	1-12-2014	5-12-2014	100%																V	r	i	j															
6	reflectieverslag final	8-12-2014	12-12-2014	100%																V	r	i	j															
7	afstudeerverslag concept	15-9-2014	28-11-2014	100%																V	r	i	j															
8	afstudeerverslag final	1-12-2014	12-12-2014	100%																V	r	i	j															
M12	inleveren eindverslagen		12-12-2014	V																V	r	i	j															
9	Presentatie maken	15-12-2014	26-12-2014	0%																V	r	i	j															
10	Presentatie oefenen	5-1-2015	16-1-2015	0%																V	r	i	j															
M15	presentatie en verdediging		23-1-2015																	V	r	i	j															
F1	Voorbereidingsfase	18-8-2014	29-8-2014	100%																V	r	i	j															
1	Inlezen bedrijfsdocumentatie	18-8-2014	19-8-2014	100%																V	r	i	j															
2	Inlezen opdracht en normen	18-8-2014	29-8-2014	100%																V	r	i	j															
F2	Onderzoeksfase	29-8-2014	21-11-2014	100%																V	r	i	j															
1	Cursus programeren in een Hima PLC	25-9-2014	26-9-2014	100%																V	r	i	j															
2	onderzoeken normen IEC61508 / IEC61511	15-9-2014	21-11-2014	100%																V	r	i	j															
3	Onderzoeken bestaande installatie	15-9-2014	17-11-2014	100%																V	r	i	j															
4	Cursus normen IEC61508 / IEC61511	27-10-2014	30-10-2014	100%																V	r	i	j															
M2	Analyserapport		21-11-2014	V																V	r	i	j															
F3	Ontwerpfase	22-9-2014	14-10-2014	100%																V	r	i	j															
1	Stap 1 Risicoanalyse	22-9-2014	3-10-2014	100%																V	r	i	j															
M3	Standaarddocument risicoanalyse		26-9-2014	V																V	r	i	j															
M4	Risicoanalyse uitgevoerd		3-10-2014	V																V	r	i	j															
2	Stap 2 Toewijzen veiligheidsfuncties	6-10-2014	24-10-2014	100%																V	r	i	j															
M5	Standaarddocument allocation sheet		10-10-2014	V																V	r	i	j															
M7	Allocation uitgevoerd		24-10-2014	V																V	r	i	j															
3	Stap 3 SRS opstellen	20-10-2014	14-11-2014	100%																V	r	i	j															
M8	Standaarddocument SRS		14-11-2014	V																V	r	i	j															
M9	SRS uitgevoerd		21-11-2014	V																V	r	i	j															
4	Stap 4 Ontwerpen SIS systeem + aanpassen tekeningen	10-11-2014	5-12-2014	100%																V	r	i	j															
M10	Ontwerp veiligheidssysteem		5-12-2014	V																V	r	i	j															
F4	Realisatiefase	1-12-2014	9-1-2015	20%																V	r	i	j															
1	Stap 5 Instal., in bedrijf stellen en valideren/verificeren	1-12-2014	26-12-2014	40%																V	r	i	j															
M11	Standaarddocument / FAT/ SAT / Field verification		19-12-2014																	V	r	i	j															
M13	FAT / SAT / Field verification		9-1-2015																	V	r	i	j															
F5	Afrondingsfase	29-12-2014	16-1-2015	0%																V	r	i	j															
1	Alle documenten afmaken (Zie o.a. Fase 0)	29-12-2014	9-1-2014	0%																V	r	i	j															
M14	Overdracht documenten en afsluiting		16-1-2014																	V	r	i	j															

11.3 Calculatie uren en kosten

Voor elk project wordt er een uren calculatie en een kosten calculatie gemaakt voordat het project start. Wanneer een project normaal gesproken aangevraagd wordt zal er een offerte afgegeven worden waarin de kosten weergegeven worden die gemaakt zullen worden om het project af te maken. Onderstaand wordt aangegeven wat uiteindelijk de kosten zijn voor dit project en wat het totaal aantal uren zijn voor dit project.

Kosten calculatie

Er is in dit project een bepaald budget uitgetrokken voor de hardware die nog besteld moet worden en voor bewerkingen die aan de installatie gedaan moeten worden. Er wordt echter geen uurloon gerekend voor de uitvoerende ingenieur omdat het een leertraject is. Toch kan er gekeken worden naar de kosten die de opdrachtgever betaalt om de student deze afstudeeropdracht te laten doen. Hier wordt gekeken naar de volgende onderdelen:

- Duur van het project 22 weken of +/- 5 maanden.
- Loon per maand €340
- Reiskostenvergoeding woon/werkverkeer €0,19 per kilometer tot 20 kilometer enkele reis.
- Woon / werkverkeer 40km per dag
- Overige kosten (huur, gas, water, licht, printerpapier enz.) zijn wat moeilijker in te schatten. In deze situatie wordt er gebruik gemaakt van 20% van het maandloon dat er per maand bijkomt aan overige kosten.

5 maanden x €340 maandloon	€1700, -
22 weken x 5 dagen / week x 40 km / dag x €0,19 / kilometer	€836, -
5 maanden x 20% van €340 maandloon	€340, -
Totale kosten	€2876, -

Tabel 11-2: Kosten afstudeerproject

In Tabel 11-2 is te zien dat wordt uitgekomen op een bedrag van bijna €3000,-. Voor de materiaalkosten is een kostprijsberekening gedaan tijdens het bestellen van de onderdelen. Deze is te zien in Tabel 11-3.

Onderdelen overzicht				
Aantal	Onderdeel	Leverancier	Prijs/stuk	Prijs
1	Temperaturetransmitter TMT82	Endress + Hauser	€ 278,02	€ 278,02
1	Pressuretransmitter PMC71	Endress + Hauser	€ 1.126,85	€ 1.126,85
1	Levelswitch FTL51	Endress + Hauser	€ 653,73	€ 653,73
1	Levelswitch versterker FTL325P	Endress + Hauser	€ 418,80	€ 418,80
1	VeiligheidsPLC F35 3	HIMA	€ -	€ -
1	Remote I/O	HIMA	€ -	€ -
1	Shunt 500Ω 982220067	HIMA	€ 27,20	€ 27,20
2	Splitters KDF2-CR4-1.2O	Pepperl + Fuchs	€ 150,00	€ 300,00
1	Analoge inputs	Phoenix Contact	€ -	€ -
8	Valve SC-G-327B103-24V/DC	Asco	€ 325,00	€ 2.600,00
1	Kleinmateriaal + installatie uren	Actemium	€ 300,00	€ 300,00
			Totaal	€ 5.704,60

Tabel 11-3: Kostprijsberekening

In het PID is aangegeven dat er een budget was van €5000,- voor alle materialen die nog besteld moesten worden. Door enkel de onderdelen die besteld worden is het budget overschreden. Bovendien komen er nog kosten bij voor de installatiemonteur en overige klein materiaalkosten als de DIN rail en afstandsbusjes. Daarvoor zijn de kosten geschat op €300,-. De totale kostprijs voor Actemium voor dit project is dus ongeveer €8600,-

Uren calculatie

Zoals hierboven en in het PID beschreven is de voorgeschreven tijd voor dit project 22 weken. Het totaal aantal uren dat dus gereserveerd staat voor dit project komt neer op 40 uur x 22 weken = 880 uur. Op het moment van schrijven van dit verslag zijn er 17 weken verstreken, maar is er ook thuis nog extra gewerkt. Volgens de planning komt het totaal neer op de geplande 21 weken omdat er een week tussen kerst en oud en nieuw vrij gepland staat, maar het werk thuis komt er nog extra bij. De tijd die nu al verbruikt is komt neer op ongeveer 800 uur. Als daar de overige weken nog bijgeteld worden komt het uit op 960 uur totaal. Gezien dat 80 uur, die meer gemaakt zijn, thuis gemaakt zijn zal dit niet in rekening gebracht worden bij Actemium.

11.4Projectevaluatie

De methoden die gekozen zijn voor dit project sluiten mooi op elkaar aan, waarbij het stappenplan uit de IEC61511 norm onderverdeeld kan worden in de fasen die gebruikt worden vanuit projectmanagement van Roel Grit. Het enige lastige was dat de eerste twee stappen uit de norm, de analyse van een veiligheidssysteem betreft terwijl het in dit project ook al een ontwerp is vanwege de standaarddocumenten.

De indeling in de planning voor de werkzaamheden bij Actemium is goed gemaakt, op het maken van de documentatie na. Dat is door de vele werkzaamheden bij Actemium verschoven waardoor het maken van het analyserapport zo lang heeft geduurd. De controle van de planning is goed gegaan, bij elke afgeronde fase of behaalde mijlpaal is de planning bijgewerkt. Er is minder gebruik gemaakt van de deadline lijst omdat de planning op zichzelf voldoende was voor het bijhouden van de voortgang. In het verleden is gebleken dat een deadlinelijst zeer nuttig is als er in groepsverband gewerkt wordt, maar dit blijkt dus voor een eenpersoons project geen toegevoegde waarde te hebben.

De kosten in dit project zijn een stuk hoger uitgevallen dan vooraf verwacht was. De prijs van SIL geclassificeerde onderdelen zijn over het algemeen duurder dan normale onderdelen, maar daar was rekening mee gehouden. De extra kosten zitten vooral in de sensoren die vervangen moeten worden en in de hoeveelheid ventielen die nodig zijn. De stagebegeleider heeft de drie risico's gekozen op basis van moeilijkheid, maar ook op het eenvoudig implementeren en de kleine hoeveelheid aanpassingen en toevoegen van onderdelen in de installatie. De aanpassingen en onderdelen bleken er echter meer te zijn dan verwacht wat een extra kostenpost met zich meebracht.

Het aantal uur wat gespendeerd is in dit project zullen waarschijnlijk ook hoger uitvallen dan verwacht. De werkzaamheden buiten de verslagen om namen al zoveel tijd in beslag dat dit moeilijk te combineren viel met het schrijven van het verslag. Om dit probleem op te vangen is het verslag gedeeltelijk thuis gemaakt. Daarnaast zijn er tijdens het project nog werkzaamheden toegevoegd als de cursus van de IEC61508 / IEC61511 norm en de Actemium Automation Awards. Daarvoor is de planning aangepast maar dit resulteerde dat andere taken plaats moesten maken, waardoor deze weer te laat klaar waren. Het bepalen van de onderdelen is nog wel naar voren gehaald omdat de levertijd van SIL waardige componenten langer is dan van normale componenten. Daardoor zijn de componenten al bepaald voordat het standaarddocument van het SRS gemaakt is. Dat is op sommige punten wel makkelijker geweest, onder andere om het SRS in te vullen voor het project, maar is geen goede volgorde bij het engineeren van een veiligheidssysteem.

12 Reflectie

In dit hoofdstuk zal teruggeblikt worden op de afstudeerstage en de opdracht. Er zal bekeken wordt wat ik als afstudeerder van de opdracht vond en hoe ik gepresteerd heb in de opdracht.

Wat ik er van vond

Bij de start van de opdracht heb ik de opdracht anders gezien dan hij uiteindelijk bleek te zijn. De verwachtingen in het begin waren voornamelijk het kort doornemen van de normen, het maken van de standaarddocumenten en als kern het programmeren van de PLC. Nu blijkt echter dat de normen de kern van de opdracht zijn. De meeste tijd is in dit project gespendeerd aan het bestuderen van de norm en het maken van de standaarddocumenten.

De meeste moeite heb ik gehad met het onderzoeken van de normen. Deze zijn geschreven in een officiële taal (taal die gebruikt wordt voor belangrijke documenten als normen en wetgevingen) en in het Engels. Daardoor vond ik het moeilijk om alles om te zetten in begrijpbaar Nederlands. Daarnaast zijn er termen gebruikt in de norm die heel begrijpbaar zijn in het Engels, maar omgezet naar het Nederlands juist niet duidelijk waren. Hierbij doel ik op woorden als demand, spurious trip enz.

Ondanks dat de verwachting anders, en de taal uit de norm soms moeilijk te begrijpen / vertalen was, heb ik met plezier en grote interesse gewerkt aan deze opdracht. Ik ben ook erg blij dat ik mee mocht doen met de cursus functionele veiligheid die aangeboden is door HIMA. Deze cursus heeft mij erg veel geholpen bij het krijgen van meer inzicht in wat er allemaal komt kijken bij een veiligheidssysteem. Ik ben dan ook trots op de resultaten die zijn voortgekomen uit dit project.

Mijn prestaties

Ik denk dat ik over het algemeen goed gepresteerd heb in deze opdracht. Het goed overleggen met anderen heeft er toe geleid dat alle standaarddocumenten en het veiligheidssysteem goedgekeurd zijn door Actemium. Daarnaast heb ik grote inzet en interesse getoond in de werkzaamheden in dit project. In de cursus vond ik dat ik alles goed kon volgen, ondanks dat de cursus voor experts in functionele veiligheid was.

Wat betreft de functionele vaardigheden ben ik zeer zelfstandig geweest in dit project. Ik ben alle gemaakte afspraken nagekomen en ik heb me flexibel opgesteld ten opzichte van medewerkers binnen Actemium. Daarnaast heb ik alle projectrollen binnen het project goed vervuld en heb ik daarbij planningen aangepast, overlegd met andere werknemers om een gezamenlijk einddoel te bereiken, zelf geschikte projectmethodieken gekozen en projectspecifieke documentatie opgeleverd.

Afkortingen

Afkorting	:	Betekenis
λdd	:	Dangerous detected faalcijfers
λdu	:	Dangerous undetected faalcijfers
λsd	:	Safe detected faalcijfers
λsu	:	Safe undetected faalcijfers
BPCS	:	Basic Process Control System
CCA	:	Cause Consequence Analysis
CIOS	:	Centrale I/O Server
CPU	:	Central Processing Unit
E / E / PE	:	Elektrisch / Elektronisch / Programmeerbaar Elektronisch
EPCU	:	EduLab Process Control Unit
FAT	:	Factory Acceptance test
FMEA	:	Failure Mode and Effect Analysis
FMEDA	:	Failure Modes Effects and Diagnostics Analysis
HAZOP	:	HAZard and OPerability study
HFT	:	Hardware Fault Tolerance
IEC	:	International Electrotechnical Commission
I/O	:	Inputs en Outputs
MOS	:	Maintenance Overrides Switch
MSDS	:	Material Safety Data Sheet
MTTFs	:	Mean Time To Fail spurious
MTTR	:	Mean Time To Restauration
P&ID	:	Process and Instrumentation Diagram
PFD	:	Probability of Failure on Demand
PIAS	:	Process Instrumentation Arbitration System
PID	:	Project Initiatie Document
PLC	:	Programmable Logic Controller
POS	:	Process Overrides Switch
RRF	:	Risico Reductie Factor
RTD	:	Resistance Temperature Detector
SAT	:	Site Acceptance Test
SCADA	:	Supervisory Control And Data Acquisition
SFF	:	Safe Failure Fraction
SIF	:	Safety Instrumented Function
SIL	:	Safety Integrity Level
SIS	:	Safety Instrumented System
SRS	:	Safety Requirements Specification
STR	:	Spurious Trip Rate

Begrippen

Begrip	:	Betekenis
λ safe detected	:	De hoeveelheid gedetecteerde veilige fouten in een component.
λ safe undetected	:	De hoeveelheid ongedetecteerde veilige fouten in een component.
λ dangerous detected	:	De hoeveelheid gedetecteerde gevaarlijke fouten in een component.
λ dangerous undetected	:	De hoeveelheid ongedetecteerde gevaarlijke fouten in een component.
Allocatie	:	Toewijzen, in dit geval toewijzen van veiligheidsfuncties aan beschermingslagen.
Applicatiesoftware	:	De software die door een ingenieur ontworpen is voor de installatie waar het veiligheidssysteem betrekking op heeft.
Arbitrage	:	Een scheidsrechter die in dit geval bepaald wie en signalen mag versturen.
Achitectural constraints	:	Wanneer een component een bepaald SIL niveau kan halen, kan het zijn dat dit SIL niveau gebaseerd is op een redundante opstelling. Er zijn dus beperkingen aan een enkele opstelling, wat architectural constraints wordt genoemd.
Base	:	Een stof die een pH waarde hoger dan 7,5 heeft.
Basic process control system	:	Het “normale” besturingssysteem van een installatie.
Batch	:	Een bepaalde hoeveelheid goederen of producten die in een keer geproduceerd worden
Besturingssysteem	:	Een pakket van programma’s/apparatuur om een installatie te laten functioneren.
Business unit	:	Onderdeel van een bedrijf dat gegroepeerd is rondom een bepaalde activiteit, productgroep of technologie.
Cause consequence analysis	:	Een methode om risico’s te vinden in bijvoorbeeld een procesinstallatie.
Central processing unit	:	Het hart van een computer of in dit geval een PLC. Deze voert alle basisbewerkingen en controles uit in een PLC.
Centrale I/O server	:	Een PLC die alle signalen uit het veld ontvangt, omzet naar ethernet en doorstuurt naar de drie BPCSen.
Clausule	:	Een soort hoofdstukken waarmee de norm is ingedeeld.
Common cause failure	:	Het falen van apparatuur door een gemeenschappelijke bron.
De-energize to trip	:	Wanneer iets spanningsloos wordt op het moment dat er iets fout gaat, bijvoorbeeld een uitgangskaart die spanningsloos wordt als er een fout in die kaart zit.
Deadlinelijst	:	Een lijst waar alle data is weergegeven waarop een taak af moet zijn.
Demand	:	Een aanvraag vanuit een installatie, bijvoorbeeld een aanvraag om een klep te sluiten.
Destilleren	:	Een scheidingsmethode voor vloeistofmengsels die werkt met de verschillende kookpunten van de componenten.
EduLab	:	Een ruimte binnen Actemium Veghel bedoelt voor educatieve doeleinden.
Edulab process control unit	:	In feite is dit een computer (als in een desktop computer) en die bepaald door middel van het PIAS systeem welke welk BPCS het proces mag besturen.
Energize to trip	:	Wanneer iets juist spanning moet krijgen op het moment dat er iets fout gaat, bijvoorbeeld een sprinkler systeem.
Exotherme reactie	:	Een chemische reactie of fysisch proces waarbij warmte vrijkomt.
Factory acceptance test	:	Een test van het systeem die vaak binnen een bedrijf gedaan wordt door iemand die niet aan het project heeft meegewerkt.

Failure mode and effect analysis	:	Een methode om risico's te vinden in bijvoorbeeld een procesinstallatie.
Failure mode effect and diagnostic analysis	:	Een testmethode om te kijken wat voor faalcijfers een component heeft.
Functionele veiligheid	:	een deel van de totale veiligheid die afhankelijk is van het correct functioneren van E/E/PE componenten of systemen.
Hardware	:	Fysieke machine eenheden zoals mechanische en elektronische onderdelen van een machine of installatie.
Hardware fault tolerance	:	Het aantal fouten dat getolereerd kan worden voordat de SIS de installatie naar een veilige toestand moet gaan.
Hazard and operability study	:	Een methode om risico's te vinden in bijvoorbeeld een procesinstallatie.
Implementeren	:	Een nieuw systeem of beleid invoeren en in gebruik nemen.
Inputs / Outputs	:	Ingangen en uitgangen, in dit geval op een PLC. Op ingangen kan bijvoorbeeld een aanwezigheidssensor aangesloten worden en op uitgangen een motor.
Integreren	:	Het samenvoegen van verschillende delen tot een goed werkend geheel.
Interbus	:	De interne communicatie tussen de I/O en het kopstation van Phoenix Contact.
International electrotechnical commission	:	Het bedrijf dat verantwoordelijk is voor het opzetten van de IEC normen.
Kalibratie	:	Het ijken van een sensor of ander component, bijvoorbeeld het instellen van het meetbereik en dergelijke.
Logic solver	:	Een groep in een veiligheidssysteem die bestaat uit bijvoorbeeld een PLC en een remote I/O.
Machinerichtlijn	:	Een verzameling van eisen waaraan machines moeten voldoen.
Maintenance overrides switch	:	Wanneer een SIF niet hoeft te werken omdat hij in onderhoud is wordt er vaak iets ingebouwd waarmee de SIF uitgeschakeld wordt maar dat het proces zelf wel door kan werken.
Material safety data sheet	:	Een blad wat voor gevaarlijke stoffen geschreven wordt, met daarin de handelmethoden voor lekken, verbranden enz.
Mean time to fail spurious	:	De tijd die tussen twee spurious trips zit.
Mean time to restauration	:	De tijd die nodig is om falende apparatuur te vervangen of repareren. Dit is de tijd vanaf het moment dat het defect geconstateerd is tot het gerepareerd is, dus inclusief verzendtijd van onderdelen, reistijd van monteurs enz.
Methodiek	:	Leer van een te volgen methode bij onderzoek of onderwijs.
NAMUR	:	Voor mechanische NAMUR, dit is een aansluitmethode waardoor een ventiel direct op een klep gemonteerd kan worden als ze beide een NAMUR aansluiting hebben. Voor elektrische NAMUR, dit is een signaal protocol die de diagnose van sensoren beter maken. Het normale signaal ligt tussen de 4-20mA, op 3,8mA en 20,5 mA is de sensor buiten bereik maar werk nog wel. Onder de 3,6mA is het kabelbreuk en boven de 21mA is het kortsluiting.
Norm	:	Een richtinggevende indicator met een algemeen afgesproken grootheid waarnaar een organisatie zich richt
pH	:	Dit is een maat voor de zuurtegraad in een vloeistof
Probability of failure on demand	:	De mogelijkheid van falen bij een aanvraag op een component.
Proces automatisering	:	De geautomatiseerde besturing van continu processen of batchprocessen

Process and instrumentation diagram	:	Een technische tekening die schematisch laat zien hoe alle onderdelen in een installatie met elkaar verbonden zijn en hoe de leidingen lopen
ProcessCell	:	Alle apparatuur die nodig is binnen een installatie om een of meerdere batches te maken
Process instrumentation arbitration system	:	Het bij Actemium ontworpen programma om te bepalen welk BPCS de installatie mag besturen.
Process overrides switch	:	Wanneer een SIF nog niet hoeft te werken omdat er in het proces een bepaalde waarde nog niet bereikt
Programmable logic controller	:	Een apparaat wat geprogrammeerd kan worden om bijvoorbeeld door middel van de aangesloten aanwezigheidssensor een aangesloten motor te laten draaien
Project initiatie document	:	Het startdocument van een afstudeertraject dat gemaakt wordt om anderen inzicht te geven in de uit te voeren opdracht
Profibus	:	Een 2 draads industriële datacommunicatiestandaard waarmee automatiseringscomponenten informatie kunnen uitwisselen
Proof test	:	Een test die controleert of een component nog functioneert zoals het bedoeld is
Pull down menu	:	Een selecteermethode waarbij na het klikken op een pijl een lijst naar voren komt met de mogelijkheden die te selecteren zijn
Reactor	:	Een chemische / natuurlijke installatie om er een chemische of nucleaire reactie in te laten plaatsvinden
Reflux	:	Het terug laten vloeien van condensaat bij het verwarmde product
Resistance temperature detector	:	Dit is een manier van temperatuur meten. Hiervoor wordt een materiaal gebruikt waarvan de weerstand veranderd als de temperatuur veranderd. Door de stroomverandering te meten kan de temperatuursverandering bepaald worden.
Revisie	:	Herstellen en nakijken van in dit geval documenten. Elke revisie krijgt een hoger nummer
Risico reductie factor	:	De factor die aantoont hoe vaak een risico gereduceerd wordt.
Safe failure fraction	:	De hoeveelheid veilige fouten van het totaal aantal fouten
Safety instrumented function	:	Een veiligheidsfunctie is een set van instrumentatie die gezamenlijk een SIL classificatie hebben en die gebruikt worden om het risico van een specifiek gevaar te reduceren.
Safety instrumented system	:	Een systeem dat bestaat uit een of meerdere SIF's. Vaak bestaat een SIS uit verschillende SIF's met verschillende SIL classificaties.
Safety integrity level	:	Een manier om aan te geven wat het niveau van presteren is voor een veiligheidsfunctie of instrument.
Safety lifecycle	:	De veiligheidslevenscyclus van een proces of een installatie
Safety manual	:	Een document dat verplicht is bij een SIL certificaat. In dat document staan onder andere de testresultaten van een component
Safety requirements specification	:	Een document waarin de eisen staan die aangeven wat er nodig is om de betreffende installatie aan de norm te laten voldoen
Shutdown	:	Het afsluiten / uitschakelen van een procesinstallatie.
Site acceptance test	:	Een test van het systeem die op locatie bij de klant gedaan wordt in het bijzijn van de klant zodat die ziet dat alles aan zijn wensen en eisen voldoet.
Software	:	Een verzamelnaam voor programmatuur, zowel besturingssystemen als toepassingsprogramma's.
Solenoid	:	Een schakelmethode waar gebruik gemaakt wordt van elektromagnetisme.
Spurious trip	:	Een actie van een veiligheidssysteem die komt door een defect in een van de componenten, in plaats van een gevaarlijke situatie in een installatie.

Spurious trip rate	:	De hoeveelheid spurious trips in een installatie, ofwel hoe vaak een installatie naar een veilige toestand gaat zonder een daadwerkelijk gevaar.
Supervisory control and data acquisition	:	Een methode om een installatie te visualiseren voor het gebruik door een operator of medewerker van de betreffende installatie
Systematic capability	:	Dit is de SIL waarde die gegeven wordt aan componenten waar de software ook bij meegenomen wordt. De SIL waarde van de software kan niet verhoogt worden door redundantie. De systematic capability geeft dus aan wat het maximale SIL niveau kan zijn van de software en de hardware.
Systematische geschiktheid	:	Zie systematic capability
Utiliteitssoftware	:	De software die meegeleverd wordt met de onderdelen die gebruikt kunnen worden voor een veiligheidssysteem
Validatie	:	Het controleren of alles wel voldoet aan de eisen die gesteld zijn. Wordt bij functionele veiligheid gedaan door collega's of door de klant in samenwerking met de engineer
Veiligheidssysteem	:	Een besturing die volledig onafhankelijk van een BPCS werkt om de veiligheid te garanderen
Verificatie	:	Het controleren of alles wel voldoet aan de eisen die gesteld zijn. Wordt bij functionele veiligheid gedaan door de ingenieur zelf
Voting	:	Als twee sensoren bij elkaar hetzelfde meten kan het zijn dat er altijd één van de twee die moet werken, ofwel er mag er één uitvallen. Dit wordt 1oo2 of 1 out of 2 genoemd en dat is de voting van meerdere sensoren
Xorter	:	Een sorteerband die gedoneerd is door VanDerLande Industries aan Actemium om als educatieve opstelling te gebruiken

Afbeeldingenindex

Tabellenindex

Bronnen

"Actemium". (2014, januari). Algemene presentatie Actemium nl - 2014 (intern document). Veghel, Noord-Brabant, Nederland.

"Actemium". (2014). *Over Actemium*. Opgeroepen op augustus 20, 2014, van Actemium: http://www.actemium.nl/over-actemium/

"Asco". (2014, november 6). *Solenoid valves 327.* Opgehaald van asconumatics.eu: http://www.asconumatics.eu/images/site/upload/_en/pdf1/80107gb.pdf

"Endress&Hauser". (2014, november 6). *FTL325P Technische informatie.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/level-measurement/29464?highlight=FTL325P

"Endress&Hauser". (2014, november 6). *FTL51 en FTL325P Functional safety manual.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/level-measurement/29464?highlight=FTL325P

"Endress&Hauser". (2014, november 6). *FTL51 Technical information.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/level-measurement/29466?highlight=FTL51

"Endress&Hauser". (2014, november 5). *PMC71 safety manual.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/pressure/PMC71?highlight=PMC71

"Endress&Hauser". (2014, november 5). *PMC71 Technical information.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/pressure/PMC71?highlight=PMC71

"Endress&Hauser". (2014, november 11). *TMT82 safety manual.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/Temperature-measurement-thermometers-transmitters/Temperature-transmitter-TMT82-HART?highlight=TMT82

"Endress&Hauser". (2014, november 11). *TMT82 Tecnical information.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/Temperature-measurement-thermometers-transmitters/Temperature-transmitter-TMT82-HART?highlight=TMT82

"Exida". (2014, november 6). *Asco 327 SIL certificate & Assessement report.* Opgehaald van Exida.com: http://www.exida.com/SAEL/ASCO_327

"Exida". (2014, november 5). *KFD2-CR4-1.2O exida functional safety assessement.* Opgehaald van Pepperl-fuchs.nl: http://www.pepperl-fuchs.nl/netherlands/nl/classid_1824.htm?view=productdetails&prodid=54132

"Exida". (2014, december 11). *Norbro 40R SIL certificate & Assessement report.* Opgehaald van Exida.com: http://www.exida.com/SAEL/Flowserve_Norbro_33_39_40_40R_Series

"Exida". (2014, december 11). *Worcester F54 SIL certificate & Assessement report.* Opgehaald van Exida.com: http://www.exida.com/SAEL/Flowserve_Worcester_51_52

"Flowserve". (2014, december 12). *Norbro 40R.* Opgehaald van Flowserve.com: http://www.flowserve.com/files/Files/Literature/ProductLiterature/FlowControl/Norbro/norbro%2040r.pdf

"Flowserve". (2014, december 12). *Worcester 54 serie .* Opgehaald van Flowserve.com: http://www.flowserve.com/files/Files/Literature/ProductLiterature/FlowControl/WorcesterControls/WCEBR0005-01.pdf

"HIMA". (2014, oktober 17). *Himatrix F35 03 & Himatrix F3 DIO 20/8 02.* Opgehaald van Hima.com: http://www.hima.com/Products/HIMatrix/Documentation__HIMatrix_default.php

"Pepperl&Fuchs". (2014, november 20). *KFD2-CR4-1.2O datasheet.* Opgehaald van Pepperl-fuchs.nl: http://www.pepperl-fuchs.nl/netherlands/nl/classid_1824.htm?view=productdetails&prodid=54132

"Pepperl&Fuchs". (2014, november 5). *KFD2-CR4-1.2O functional safety manual.* Opgehaald van Pepperl-fuchs.nl: http://www.pepperl-fuchs.nl/netherlands/nl/classid_1824.htm?view=productdetails&prodid=54132

"PQRI". (2014, oktober 7). *HAZOP training guide.* Opgehaald van www.pqri.org: http://www.pqri.org/pdfs/MTC/HAZOP_Training_Guide.pdf

"Rockwell.Automation". (2002, maart). *PLC vs Safety PLC.* Opgehaald van rockwellautomation.com: http://discover.rockwellautomation.com/Files/PLC-vs-Safety-PLC-Fundamental-and-Significant-Differences.pdf

"Sigma-aldrich.com". (2014). *NaOH.* Opgeroepen op september 17, 2014, van sigma-aldrich: http://www.sigmaaldrich.com/catalog/search?interface=All&term=naoh&N=0&mode=partialmax&focus=product&lang=en&region=NL

"SWC". (2014, 11 17). *Aanvaardbaar risico*. Opgehaald van woorden-boek.nl: http://www.woorden-boek.nl/woord/aanvaardbaar%20risico
"TÜV". (2014, november 6). *FTL51 + FEL 57 + FTL 325P.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/level-measurement/29466?highlight=FTL51
"TÜV". (2014, november 5). *PMC71 SIL certificate.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/pressure/PMC71?highlight=PMC71
"TÜV". (2014, november 11). *TMT82 SIL certificate.* Opgehaald van Endress.com: http://www.nl.endress.com/nl/Tailor-made-field-instrumentation/Temperature-measurement-thermometers-transmitters/Temperature-transmitter-TMT82-HART?highlight=TMT82
"TÜV". (2014, oktober 17). *TÜV EC type examination Certificate & Safety manual.* Opgehaald van Hima.com: http://www.hima.com/Products/HIMatrix/Documentation__HIMatrix_default.php
"Vierpool". (2014, 11 25). *signaalconditionering*. Opgehaald van vierpool.nl: http://www.vierpool.nl/signaalconditionering/bewaken-van-meetsignalen-met-pr-electronics.html
"Wikipedia.nl". (2014, maart 20). *Moscow methode*. Opgeroepen op augustus 25, 2014, van Wikipedia.nl: http://nl.wikipedia.org/wiki/MoSCoW-methode
"Wikipedia.nl". (2014, september 7). *Natriumhydroxide*. Opgeroepen op september 17, 2014, van Wikipedia.nl: http://nl.wikipedia.org/wiki/Natriumhydroxide
Achatot. (2012, april 4). *EduLab*. Opgeroepen op augustus 20, 2014, van EduLab wiki: http://wiki.edu-lab.nl/(S(4vaclh55yc5pt1550i2bcqbl))/Edulab.ashx
Achatot. (2012, april 10). *EduLabProcess*. Opgeroepen op augustus 21, 2014, van EduLab wiki: http://wiki.edu-lab.nl/EduLabProcess.ashx
Achatot. (2012, april 5). *EduLabXorter*. Opgeroepen op augustus 21, 2014, van EduLab wiki: http://wiki.edu-lab.nl/EduLabXorter.ashx
Assmann, I. C., & Kroonen, I. M. (2009, maart). *Kennisdocument industriele procesbeveiliging.* Opgeroepen op september 18, 2014, van Relevant.nl: https://relevant.nl/download/attachments/4096942/IPO+Kennisdocument.pdf?version=1
Gould, J. (2000). *review of hazard identification techniques.* Opgehaald van www.hse.gov.uk: http://www.hse.gov.uk/research/hsl_pdf/2005/hsl0558.pdf
Grit, R. (2011). *Projectmanagement.* Groningen: Noordhoff Uitgevers bv Groningen / Houten.
IEC. (2014, augustus 18). NEN-EN-IEC61508-1:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61508-2:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61508-3:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61508-4:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61508-5:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61508-6:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, september 22). NEN-EN-IEC61508-7:2010 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61511-1:2005 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61511-2:2005 en. Geneve, Geneve, Zwitserland.
IEC. (2014, augustus 18). NEN-EN-IEC61511-3:2005 en. Geneve, Geneve, Zwitserland.
IEC. (2014, oktober 2). NEN-IEC61882. Geneve, Geneve, Zwitserland.
Laar, H. v. (2011, december 20). Stageverslag EduLabProcess V0.5 (intern document). Veghel, Noord-Brabant, Nederland.
Lent, J. v. (2011, augustus 12). Safety Requirement Specifications (intern document). Veghel, Noord-Braband, Nederland.
Lent, J. v. (2014, september 22). Lead engineer hardware. (M. Leijten, Interviewer)
OSP, Z.-m. (2014, september 11). *Ernstige ongevallen met chemische producten*. Opgehaald van www.zero-meridean.nl: http://www.zero-meridean.nl/overzicht_inc_chemie.php
Peters, J. (2014, juni 4). Afstudeerverslag Aanpassen processcell EduLab V1.00 (intern document). Veghel, Noord-Brabant, Nederland.
Pietersen, C. (2014, oktober 7). *25 jaar later (Bijlage 4).* Opgehaald van www.tripodincidentanalyse.nl: http://www.tripodincidentanalyse.nl/1404
Pietersen, I. C. (2008, december 6). *procesveiligheid.* Opgeroepen op september 18, 2014, van tripodincidentanalyse.nl: http://www.tripodincidentanalyse.nl/1438_Incidenten%20en%20TRIPOD%20analyse%20NPT%20artikel%20%20deel%202.pdf

Pranger, J. (2008, december 18). *Procesveiligheid en arbeidsveiligheid.* Opgeroepen op september 18, 2014, van kcbv.com: http://www.kcbv.com/wp-content/uploads/2014/02/Procesveiligheid-en-Arbeidsveiligheid181208.pdf

Smits, L. M. (2009, september 21). Functional Specification EduLab Process V1.09 (intern document). Veghel, Noord-Brabant, Nederland.

Verburg, B. (2014, augustus 18). Client manager. (M. Leijten, Interviewer)

With, N. d. (2012, februari 1). *PMA 1-2-2012 pag. 4-7.* Opgehaald van Automatie-PMA.com: http://automatie-pma.com/pma-1-2-2012/

With, N. d. (2012, mei). *PMA 5-2012 pag.4-6.* Opgehaald van Automatie-PMA.com: http://automatie-pma.com/pma-5-2012/