Inleiding Functionele Veiligheid in de Procesindustrie

(conform de NEN-EN-IEC-61511

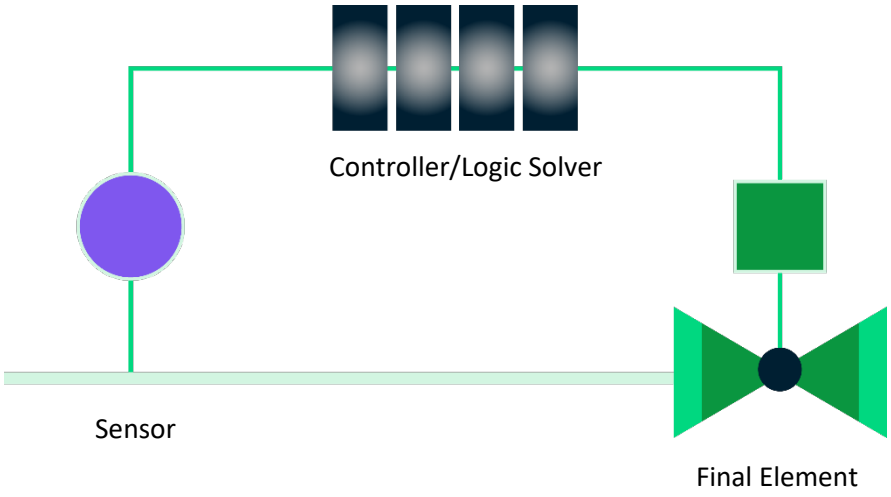
13 augustus 2024

kader
framework for positive change

Inhoudsopgave

1. Inleiding

In de procesindustrie worden instrumentele beveiligingen gebruikt om de processen en installaties te beveiligen wanneer het proces niet meer onder controle is. Een instrumentele beveiliging bestaat uit een of meer opnemers, een logic solver, en een of meer stuurorganen. Deze beveiligingen kunnen worden uitgevoerd in het control system (DCS, BPCS) of in aparte veiligheidssystemen, afhankelijk van de benodigde risico reductie. Wanneer deze risico reductie een factor >10 moet zijn, dan is in Nederland gebruikelijk om de normserie NEN-EN-IEC61511 in samenhang met de NEN-EN-IEC61508 te gebruiken, ook wel de SIL-methodiek genoemd. Deze norm wordt internationaal als BBT (best beschikbare techniek) gezien en daarvoor veelvuldig gebruikt. Daarnaast wordt bovenstaande norm in diverse PGS-en (Publicatiereeks Gevaarlijke Stoffen) genoemd als normatieve referentie en daarmee dus verplicht om mee te werken.



Figuur 1: Typical van een instrumentele beveiliging

Bij veel bedrijven is er de misvatting dat een SIL beveiliging een belangrijkere beveiliging is dan een beveiliging die wordt geïmplementeerd in het DCS/BPCS en daarmee meer aandacht behoeft. Daarnaast probeert men onder de SIL range te blijven, omdat wordt aangenomen dat een SIL beveiliging veel extra eisen met zich mee brengt. Hierbij wordt vergeten dat de meeste stappen in het design en onderhoud exact hetzelfde zijn. Denk hierbij bijvoorbeeld aan documentatie, berekeningen, eisen aan competenties, verificatie, etc.

Ondanks dat de NEN-EN-IEC61511 norm in principe alleen geldt wanneer een beveiliging een risico reductie factor (RRF) van >10 heeft, zijn de principes ook uitermate goed toepasbaar bij beveiligingen die een kleinere risico reductie factor hebben en bijvoorbeeld in het DCS/BPCS worden uitgevoerd. Hierbij speelt tevens mee dat er geen specifieke internationale norm voor instrumentele beveiligingen met een RRF <10 beschikbaar is.

De NEN-EN-IEC61511 is een sector specifieke norm onder de paraplu van de functionele veiligheidsnorm NEN-EN-IEC61508 en is gericht op de proces industrie. De norm-serie beschrijft alle stappen die genomen moeten worden voor het ontwerp, selectie van componenten, installatie, bedrijven en onderhouden van een instrumentele beveiliging. Daarnaast beschrijft de norm ook de

voorwaarden waaraan bedrijven/personen, die een rol hebben in het tot stand komen en in stand houden van een instrumentele beveiliging, moeten voldoen. Dit wordt ook wel het Functional Safety Management (FSM) genoemd en is daarmee een kwaliteitssysteem. Mede door dit kwaliteitssysteem kan uiteindelijk worden gesteld dat de betrouwbaarheid van een instrumentele beveiliging voldoende hoog en de waarschijnlijkheid van fouten gemaakt door mensen voldoende laag is.

Zowel de NEN-EN-IEC61508 en de NEN-EN-IEC61511 zijn normen die aangeven wat gedaan of geïmplementeerd moet worden, en geven daarmee de gebruiker van de normen de vrijheid om te bepalen hoe ze dat doen. Dat is meteen ook het grote nadeel omdat iedereen dus deels een eigen interpretatie kan geven, maar ook dat documentatie niet een vaste opmaak heeft.

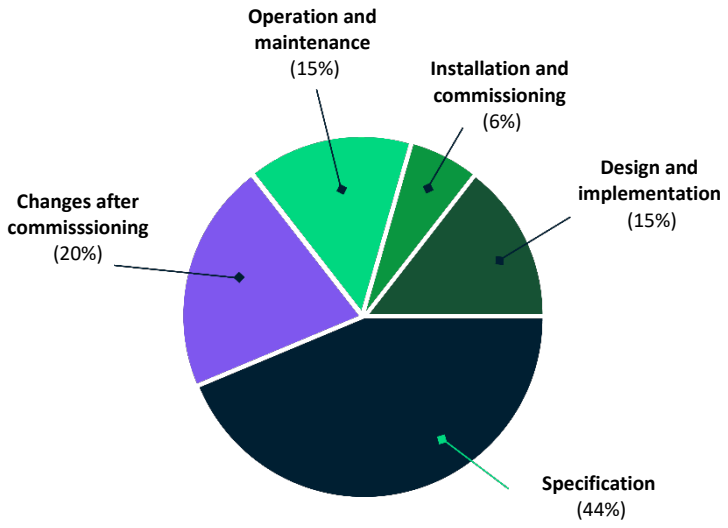
In de volgende hoofdstukken wordt ingegaan op enkele belangrijke onderwerpen van de norm.

2. Functional Safety Management

De basis en kwaliteit van iedere beveiliging ligt in hoe zaken geregeld zijn met betrekking tot procedures zoals competentie management, verificatie, templates, document control etc. Wanneer de beveiliging uitgevoerd wordt als instrumentele beveiliging, wordt dit Management of Functional Safety (FSM) genoemd. In de NEN-EN-IEC61511 wordt gesteld dat bij elke activiteit tijdens ontwerp, installatie, bedrijf en onderhoud vooraf nagedacht moet worden wie en wat daarvoor nodig is. Om te bepalen welke activiteiten er zijn, is in de norm een Safety Life Cycle (SLC) gedefinieerd (in hoofdstuk 4 wordt aan de SLC aandacht geschonken). Dit heeft allemaal tot doel om systematische fouten te voorkomen of te reduceren. Dat houdt dus in dat vastgelegd moet worden wie welke taak/activiteit mag uitvoeren en welke competentie deze persoon daarvoor nodig heeft, wie mag een review uitvoeren, wat moet worden opgeleverd na een bepaalde taak, welk template moet gebruikt worden enzovoorts.

> Het is wel voor te stellen dat wanneer een persoon iets ontwerpt of monteert met zijn kennis en ervaring dat dit mogelijk kan leiden tot een foutief design of installatie. Daarom is een verificatie, door middel van een review of een test, door een tweede (competente) persoon, noodzakelijk om eventuele fouten/onvolkomenheden te identificeren en samen met de eerste persoon te herstellen.
>
> Hetzelfde geldt voor bijvoorbeeld het gebruik van voorbereide templates. Als in het verleden goed is nagedacht wat allemaal vastgelegd moet worden, kunnen bepaalde aspecten niet over het hoofd worden gezien. Hierdoor is er een kleinere kans dat een mogelijk niet werkende beveiliging wordt afgeleverd. Natuurlijk met de voorwaarde dat de template een goede verificatie heeft gehad.

Uit onderstaande figuur blijkt dat de incidenten, waar het beveiligingssysteem niet adequaat ingegrepen heeft, kunnen worden teruggevoerd op alle fases van de SLC. Daaruit kan worden geconcludeerd dat FSM voor iedere fase van groot belang is.



Figuur 2: Primary cause by phase (from: Health and Safety Executive HSG238 Out of Control)

Als zaken niet gedocumenteerd zijn, is het uitgangspunt dat het niet uitgevoerd is. Documentatie is in de norm NEN-EN-IEC61511 daarom ontzettend belangrijk. Alle documentatie van gevarenstudie en ontwerp tot en met periodiek testen dient beschikbaar te zijn tijdens de gehele levensduur van de instrumentele beveiliging.

Naarmate een hogere SIL gevraagd wordt, worden ook de eisen aan het FSM hoger. Dit is natuurlijk heel logisch aangezien een hogere betrouwbaarheid wordt gevraagd. Betrouwbaarheid is niet alleen afhankelijk van de gebruikte componenten, maar natuurlijk ook van de andere partijen die een rol hebben in het ontwerp en installatie van de instrumentele beveiliging en van de eindgebruiker (operations en onderhoud). Wanneer (één van) de betrokken partijen geen FSM systeem hebben, moet helaas geconcludeerd worden dat de instrumentele beveiliging niet conform de norm is en daarmee kan geen SIL worden geclaimd.

> Voor fabrikanten van veiligheidscomponenten is de (NEN-EN-)IEC61508 van toepassing. Ook in deze norm wordt ook een FSM (bij de fabrikant) verplicht gesteld. De kwaliteit van die FSM systemen wordt uitgedrukt in Systematic Capability (SC) en loopt van SC1 (laag) tot en met SC4 (hoog).

Een FSM systeem kan als een “stand-alone” systeem worden opgetuigd waarbij procedures specifiek worden geschreven. Echter wanneer een bedrijf al een kwaliteitssysteem (zoals ISO9001) heeft, zijn daarin al veel van de verplichte onderdelen van een FSM systeem geïmplementeerd en kan met relatief kleine aanpassingen geschikt gemaakt worden voor het gebruik onder de NEN-EN-IEC61511. Samengevat bestaat een FSM systeem dus uit drie belangrijke onderdelen en worden internationaal vaak de 3 P’s genoemd:

- Mensen (People)
- Procedures
- Papier(werk)

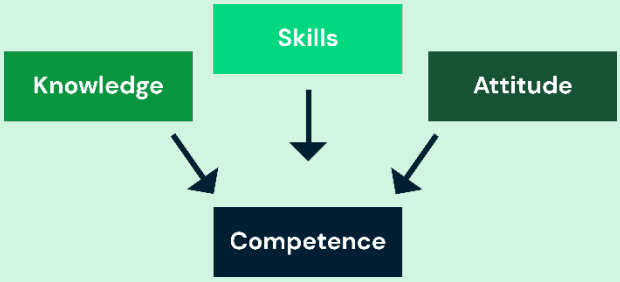
3. Competentie

“Een beveiliging van een industriële installatie is bedacht, ontworpen en/of onderhouden door iemand die hiervoor niet is opgeleid of toegerust.”

Hoeveel vertrouwen in het correct functioneren van een (instrumentele) beveiliging geeft bovenstaande stelling? Het is natuurlijk te hopen dat elke beveiliging ontworpen is en/of onderhouden wordt door mensen die competent zijn. De NEN-EN-IEC61511 eist dat iedereen die betrokkenheid heeft met een instrumentele beveiliging competent moet zijn en moet weten welke verantwoordelijkheden ze hebben. Maar wanneer is iemand dan competent en hoe moet dit inzichtelijk worden gemaakt?

Voor competent bestaan verschillende definities.
De beste definitie luidt als volgt:

“Geschikt voor het uitoefenen van zijn functie. Iemand die beschikt over alle competenties die in een functie vereist worden. In staat om kennis, houding en vaardigheden zodanig te combineren dat het leidt tot succesvol optreden in een bepaalde functie.”



Een bestuurder van een auto dient een rijbewijs te hebben. Het rijbewijs wordt behaald door een stuk theorie (over de wetgeving, betekenis van borden, etc) en een deel praktijk. Als zowel een theorie als een praktijk examen met goed gevolg is afgelegd, wordt gesteld dat deze persoon de kennis en vaardigheid heeft en wordt competent verklaard om alleen de weg op te kunnen. En toch zien we heel regelmatig mensen de meest gekke capriolen uithalen. Hierbij laten we even in het midden of dat komt door gebrek aan:

- Kennis - wetgeving is veranderd of kennis van de wetgeving is weggezakt;
- Vaardigheden - te weinig rijden of nog nooit in een bepaalde situatie geweest;
- Houding – afgeleid zijn of bewust niet aan de regels houden.

Competent zijn houdt dus in dat niet iedereen zomaar geschikt is om te werken aan een (instrumentele) beveiliging, want het niet succesvol optreden in een bepaalde functie (denk aan engineering, installatie, operations, onderhoud maar ook aan management) kan zomaar leiden tot een niet werkende beveiliging. In de NEN-EN-IEC61511 wordt dan ook aangegeven dat de benodigde competenties van zowel personen, afdelingen als organisaties van te voren moeten worden bepaald. De benodigde competenties zijn natuurlijk afhankelijk van zaken zoals het industriële proces wat beveiligd moet worden, welke technologie gebruikt wordt, uit welke componenten de beveiliging bestaat en de SIL.

Zoals al eerder aangegeven, geeft de NEN-EN-IEC61511 alleen doelstellingen. In dit geval is het dus dat mensen competent moeten zijn. De norm geeft (helaas) geen competentielijstjes per taak of rol, maar laat dit over aan de partijen die betrokken zijn bij de instrumentele beveiliging. Veel van de benodigde competenties liggen wel redelijk voor de hand, zoals bepaalde trainingen die gevolgd moeten zijn, aantal jaren ervaring (wellicht is het beter om in plaats van jaren ervaring het aantal keer ervaring met een bepaalde activiteit of component als eis te hebben), bewijs dat activiteiten gedaan zijn onder supervisie en dat de supervisor een positieve beoordeling heeft gegeven, goed in documenteren van (test)resultaten.

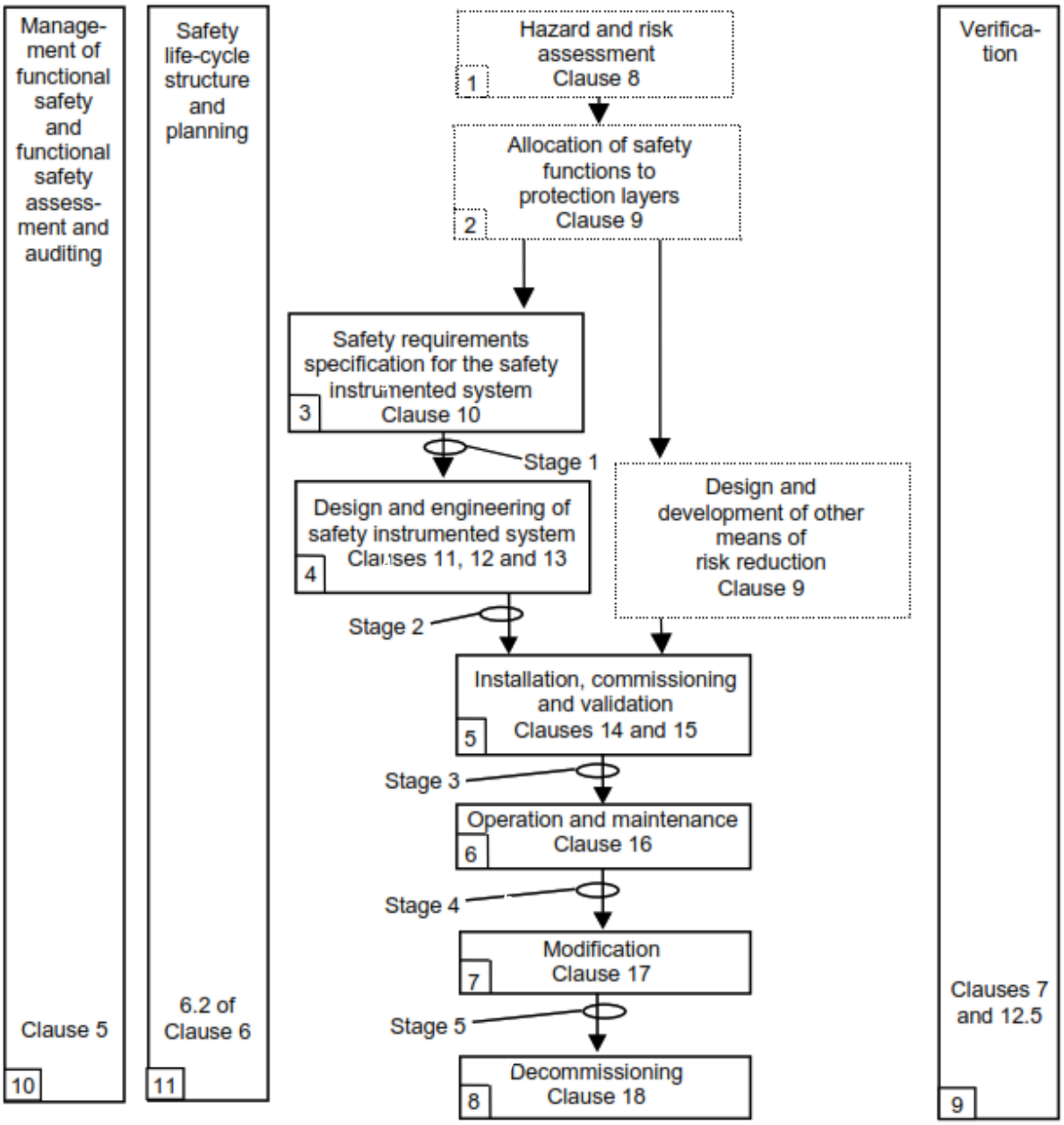
Als bekend is welke competenties voor een bepaalde taak benodigd zijn, moet de persoon, die de taak gaat uitvoeren, daar ook aan voldoen en dat moet aantoonbaar gemaakt worden. Dat betekent dus dat competentiemanagement geïmplementeerd moet worden. Hierbij geeft de organisatie aan dat een persoon een activiteit kan uitvoeren, maar tevens ligt er een verantwoordelijkheid bij de persoon dat deze geen activiteiten uitvoert waar hij/zij niet competent (genoeg) voor is.
Daarnaast heeft de norm bepaald dat periodiek moet worden beoordeeld of personen nog wel competent zijn. Waar natuurlijk wel enige logica in zit. Wanneer je niet dagelijks met een activiteit bezig bent, zal de kennis en/of kunde langzaam verdwijnen. Maar ook voor mensen die juist wel dagelijks met een activiteit bezig zijn, kunnen op basis van de automatische piloot bezig zijn en mogelijk zichzelf langzamerhand een verkeerde werkwijze aanleren. Dus een regelmatige opfriscursus of beoordeling van een bepaalde activiteit, zorgt voor het aantoonbaar maken van de competenties van een persoon.

> Om nog even terug te komen op het voorbeeld van de automobilist. Als het al even geleden is dat het rijbewijs behaald is, dan zijn er diverse wijzigingen geweest, zoals nieuwe borden geïntroduceerd, andere vervoersmiddelen op de weg gekomen. De overheid brengt niemand persoonlijk op de hoogte van de wijzigingen. Wat is de status van kennis van de gemiddelde automobilist? Of zijn we een beetje laks geworden en hebben we onze eigen rijstijl ontwikkeld (anders dan wat aangeleerd is)? Met andere woorden zijn we nog competent om de weg op te gaan?

Belangrijk is dus dat wanneer aan een instrumentele beveiliging wordt gewerkt dat het bekend is welke competenties nodig zijn en dat de personen die eraan werken deze competenties hebben. Bij trainingen stellen we weleens de vragen: “Ben je competent en hoe weet je dat?” en “Volg je altijd de procedure (tot de letter)?” In de praktijk zien we dan zelden dat competentiemanagement geïmplementeerd is. En zonder competentiemanagement is het dus niet aan te tonen dat mensen competent zijn voor hun activiteit binnen het ontwerp, installatie, bedrijf en onderhoud van de beveiliging. Zoals in het vorige hoofdstuk aangegeven blijkt dat het toch regelmatig voorkomt dat een beveiliging niet functioneert. Dus wellicht moeten we dan toch concluderen dat de stelling waarmee dit hoofdstuk mee begon eigenlijk toch wel (te) vaak de realiteit is.

4. Safety Life-cycle

In voorgaande hoofdstukken is ingegaan op het management van functionele veiligheid (FSM) volgens de norm NEN-EN-IEC61511. Eén van de onderdelen die daarbij hoort is het concept van de Safety Life-cycle (SLC). De hele norm is geschreven rondom dit concept. Middels de SLC worden de verschillende fases van elkaar gescheiden en geeft daarmee logische structuur. Zoals zoveel eisen uit de norm kan het concept van de SLC ook weer worden toegepast op elke andere beveiliging. De NEN-EN-IEC61511 heeft onderstaande generieke Safety Life-cycle geadopteerd waaromheen alle eisen zijn gedefinieerd.



Figuur 3: Safety Life-cycle – figure 7 van de NEN-EN-IEC61511)

De start van elke beveiliging begint bij een gevaren- en risico analyse (box 1 in bovenstaande figuur). Wanneer een proces niet inherent veilig ontworpen kan worden, moeten maatregelen worden geïntroduceerd om het risico tot het acceptabele niveau te krijgen. Elk van deze maatregelen wordt een beveiligslaag (box 2). Daarmee wordt elke beveiligingslaag even belangrijk omdat, wanneer één van deze beveiligingslagen niet aanwezig is of niet functioneert, onvoldoende risico reducerende maatregelen zijn getroffen en daarmee het rest risico te hoog is. De NEN-EN-IEC61511 geeft voor deze stappen in de SLC geen gedetailleerde eisen over de uitvoering aangezien hiervoor andere normen invulling aan geven (denk bv. aan NEN-EN-IEC 61882 voor HAZOP). Echter aangezien de gevaren- en risico analyse de basis vormt voor elke instrumentele beveiliging worden er wel degelijk minimale eisen aan deze studie gesteld. Beveiligingslagen die niet instrumenteel worden uitgevoerd, vallen ook onder andere normen.

Wanneer een beveiligingslaag wordt uitgevoerd als een instrumentele beveiliging dan moet eerst bekend zijn welke eisen aan deze beveiliging worden gesteld (box 3). Deze eisen hebben betrekking tot de functionaliteit, maar ook aan de betrouwbaarheid. Als deze eisen bekend zijn kan het ontwerp en de engineering worden uitgevoerd (box 4). Vervolgens wordt de volledige beveiliging geïntegreerd, getest en gevalideerd ten opzichte van de gestelde eisen (box 5). Als alles goed is, begint de operationele fase (box 6). Hier moet zowel operations als onderhoud ervoor gaan zorgen dat de instrumentele beveiliging blijft werken conform de eisen en het ontwerp. Meestal is de levensduur van een fabrieksproces zo'n 20 jaar. In deze 20 jaar worden regelmatig modificaties uitgevoerd waardoor het noodzakelijk is om de instrumentele beveiliging te herzien (box 7) en tot slot kan het zijn dat de beveiliging uit bedrijf moet worden genomen (box 8).

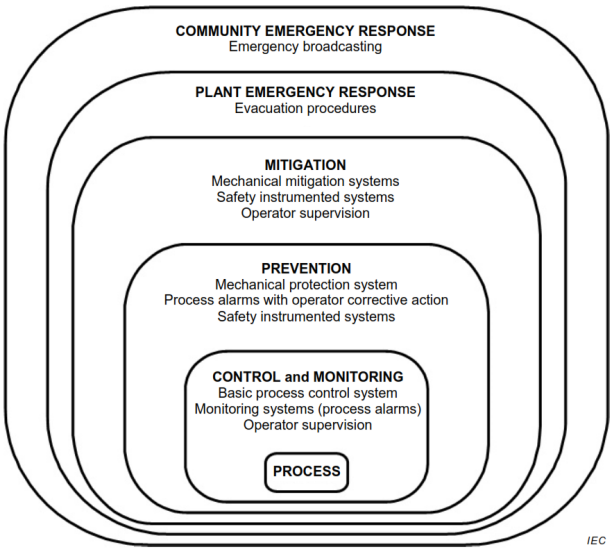
Door de SLC op deze manier te organiseren kan voor iedere fase duidelijk omschreven worden welke input nodig is, welke activiteiten uitgevoerd moeten worden, welke competenties benodigd zijn en uiteindelijk wat het resultaat (bv. documentatie of programmatuur) van de fase moet zijn. Wanneer de SLC op de juiste manier wordt toegepast, wordt het werk gestructureerd uitgevoerd. Aan het eind van een fase uit de SLC moet worden geverifieerd dat alle vooraf gedefinieerde resultaten van die fase aanwezig zijn. Daarmee wordt voorkomen dat bepaalde essentiële stappen worden overgeslagen of dat een fase begint met te weinig of inconsistente input informatie waardoor een instrumentele beveiliging foutief ontworpen, geïnstalleerd of onderhouden wordt.

In de volgende hoofdstukken zullen de verschillende fases van de SLC worden uitgediept, beginnend met de gevaren- en risico analyse.

5. Gevaren- en risico analyse

In het vorige hoofdstuk ging het over de Safety Life-cycle (SLC). De eerste stap om tot een (instrumentele) beveiliging te komen is het uitvoeren van een gevaren- en risico analyse (box 1 vanuit de SLC). Tijdens zo'n analyse worden alle gevaren in kaart gebracht en vervolgens worden de risico's ingeschaald. Wanneer het risico te hoog is, moeten risico reducerende maatregelen genomen worden. In de procesindustrie wordt hiervoor meestal de HAZOP (HAZard and OPerability studie) methode in combinatie met een risico analyse methode gebruikt. Veel gebruikte risico analyse methoden zijn de risicomatrix, risicograaf of Layer of Protection Analysis (LOPA). In het informatieve deel 3 van de NEN-EN-IEC61511 serie worden deze methodes kort uitgelegd aan de hand van een voorbeelden voor risico criteria. Veel bedrijven nemen deze risico criteria zonder aanpassing over, maar vergeten dat de risico criteria wel moeten worden aangepast naar bv. wetgeving, corporate waarden of mogelijke voorwaarden vanuit verzekeraars. Wanneer risicobeoordelingen worden gedaan aan de hand van incorrecte risico criteria zal ook de uitkomst van de beoordeling incorrect zijn, waardoor kans is op te conservatieve resultaten (resulterend in hogere kosten) of te positieve resultaten (resulterend in te hoog rest risico).

De NEN-EN-IEC61511 geeft niet aan welke methode gebruikt moet worden, maar geeft wel aan wat minimaal tijdens zo'n analyse beschreven moet worden. Naast de gevaren (en oorzaken) moeten de kans en consequenties worden beschreven van elk scenario. Bij veel bedrijven wordt bij de gevaren- en risico analyses alleen gekeken naar 'normal operation' modus en worden de gevaren die aanwezig zijn tijdens start-up en shutdown, onderhoud, procesverstoringen en een noodstop niet behandeld of slecht sporadisch aangestipt (zeker niet methodisch onderzocht). De NEN-EN-IEC61511 geeft aan dat deze bedrijfscondities wel degelijk beschreven dienen te worden. Wanneer alle risico's in kaart zijn gebracht, moeten ook alle maatregelen (beveiligingen) worden beschreven (box 2 vanuit de SLC). Waarbij natuurlijk rekening moet worden gehouden met de arbeidshygiënische strategie.



Figuur 4: Generieke beveiliginglagen – figure 9 van de NEN-EN-IEC61511-1

Als gekozen is om de beveiliging instrumenteel uit te voeren en de benodigde risico reductiefactor is groter dan 10, wordt deze beveiliging een Safety Instrumented Function (SIF) genoemd en valt deze onder de NEN-EN-IEC61511. De benodigde risico reductie factor geeft vervolgens aan welke SIL behaald moet worden en daarmee is meteen ook bepaald wat de gemiddelde kans van falen mag zijn wanneer deze beveiliging zou moeten werken (Probability of Failure on Demand (PDFavg)).

SIL	Risico Reductie Factor	PFDavg
1	>10 tot ≤ 100	$\geq 10^{-2}$ tot $< 10^{-1}$
2	>100 tot ≤ 1.000	$\geq 10^{-3}$ tot $< 10^{-2}$
3	>1.000 tot ≤ 10.000	$\geq 10^{-4}$ tot $< 10^{-3}$
4	>10.000 tot ≤ 100.000	$\geq 10^{-5}$ tot $< 10^{-4}$

Tabel 1: Relatie SIL Risico Reductie Factor en PFDavg

In het hele proces van het aanbrengen van beveiligingslagen worden wel enkele restricties gegeven door de NEN-EN-IEC61511. Wanneer een beveiligingslaag in een BPCS (basic process control system) wordt uitgevoerd en de beveiliging in dit control systeem niet conform de NEN-EN-IEC61511 is opgebouwd, mag een maximale risico reductie factor van 10 (dit moet wel onderbouwd zijn) worden genomen in de gevaren studie. Daarnaast wordt een limitatie gegeven voor het aantal BPCS beveiligingen die meegenomen mogen worden in een scenario. Wat vooral heel belangrijk wordt gevonden in de norm is dat de beveiligingen onafhankelijk zijn van de oorzaak van het scenario.

Omdat de NEN-EN-IEC61511 gaat over instrumentele beveiligingen, waarvan de besturing in een computersysteem (bv. PLC) wordt gebouwd, moeten voor dit systeem ook de cyber security risico's in kaart worden gebracht. Hiervoor verwijst de norm naar bv. de NEN-EN-IEC62443 serie.

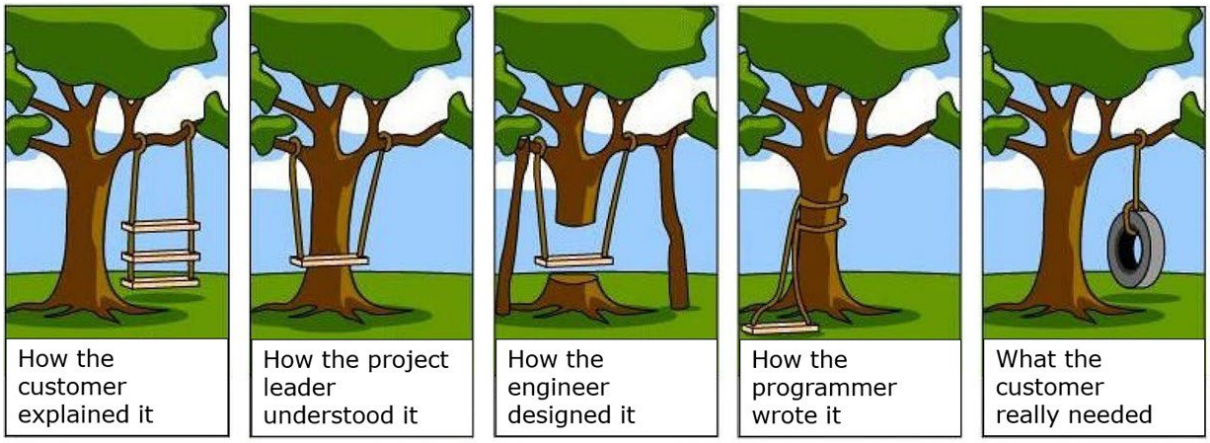
Als de gevaren- en risico analyses uitgevoerd zijn en de verschillende (instrumentele) beveiligingen zijn geïdentificeerd, moeten deze ontworpen worden. Daarvoor moet een specificatie gemaakt worden. In de norm wordt dit een Safety Requirements Specification genoemd.

6. Safety Requirements Specification

De eerste stappen in de SLC zijn dus de gevaren- en risico analyse en het bepalen van beveiligingslagen. Tijdens de gevaren- en risico analyse is bepaald dat een beveiliging instrumenteel uitgevoerd wordt en dat deze een risico-reductiefactor heeft die groter is dan 10. De volgende stap is het specificeren van de SIF (box 3 van de SLC).

Zoals aangehaald in hoofdstuk 2, blijkt dat de meeste oorzaken, waarom een SIF niet functioneert, terug te voeren zijn op de specificatie. De norm geeft daarom ook aan dat een Safety Requirements Specification (SRS) zo moet wordt opgesteld dat de vereisten duidelijk, accuraat, verifieerbaar, onderhoudbaar en uitvoerbaar zijn. De norm geeft niet aan dat dit in één document moet, maar het heeft natuurlijk wel zeer grote voordelen. Wanneer alle informatie verdeeld is over diverse documenten moet de ontwerper, operator of onderhoudsmedewerker ook maar toevallig weten dat in een ander document essentiële informatie staat.

Het volgende plaatje wordt vaak gebruikt om aan te tonen dat een duidelijke specificatie heel belangrijk is. Zeker wanneer meerdere partijen bij het ontwerp betrokken zijn, kunnen zaken wel eens heel erg anders geïnterpreteerd worden.



De NEN-EN-IEC61511 heeft voor een SRS geen format beschikbaar, maar geeft wel een flinke lijst van zo'n 30 punten waar mogelijk vereisten uit komen die noodzakelijk zijn om tot een functionele en betrouwbare beveiliging te komen. Dit gaat o.a. over de logica, proof testing, betrouwbaarheid, bypasses etc. Het gaat te ver om hier alle punten te behandelen. Toch willen we een tweetal punten onder de aandacht brengen die vaak niet goed worden doordacht of omschreven.

- Responstijd en process safety time: Het is in algemeen wel bekend dat het gewenst is dat de SIF zijn volledig actie heeft uitgevoerd voordat het proces zover uit de hand is gelopen dat het leidt tot een gevaarlijke situatie, waarbij het medium uit de installatie komt. Om dus iets te kunnen zeggen over de benodigde snelheid van reageren van de SIF, moet eerst bekend zijn hoeveel tijd er beschikbaar is. De beschikbare tijd wordt ook wel de process safety time genoemd. De process safety time is afhankelijk van de instelling van de tripsetting en de snelheid van het proces (bv. hoe snel stijgt een druk of temperatuur in het worst case scenario). Wanneer de process safety time niet gespecificeerd is aan het begin van het design en deze berekening op een later tijdstip

pas wordt uitgevoerd, kan het zijn dat met de gekochte componenten de responstijd langer is dan de process safety time. Dat betekent dan weer dat nieuwe componenten moeten worden aangeschaft of dat de tripsetting moet worden aangepast (vaak met als gevolg dat deze dichtbij de normale procescondities komt te liggen, waardoor het aantal 'onnodige' trips omhoog gaat)

- Resetten na een shutdown: Als een shutdown heeft plaatsgevonden door een trip vanuit een SIF, moet de SIF (vaak het stuurorgaan) ook weer gereset worden om verder te gaan met de productie. Heel vaak heeft de trip een oorzaak die onderzocht moet worden en zou het gevaarlijk zijn om bij een gezond signaal van de sensor direct weer met de productie te starten. Daarom wordt een SIF vaak met software en/of hardware vergrendeling toegepast die handmatig moet worden gereset. Er kunnen natuurlijk ook redenen zijn om een SIF juist automatisch te resetten wanneer het proces weer binnen de normale procescondities komt. Per SIF moet hier een keus in gemaakt worden.

Naast de specificeren van de vereisten voor een SIF, geeft de norm ook aan dat een specificatie gemaakt moet worden voor het software deel van de logic solvers (application program).

De SRS zou in elke fase van de SLC weer in beeld moeten komen. Bij het ontwerp moet iets bedacht worden wat voldoet aan de vereisten en dat moet vervolgens natuurlijk gevalideerd worden. Zijn de vereisten niet vastgelegd dan valt er weinig te valideren. Dan moeten ook de procedures en werkwijze van operations en onderhoud voldoen aan de eisen vanuit de SRS. En wanneer modificaties worden uitgevoerd moet bekend zijn of vereisten aangepast moeten worden of dat de modificatie juist aan één of meer van de vereisten zou moeten voldoen. Helaas wordt de SRS nog te vaak niet gemaakt of is het een document wat in een kast of mapje op het netwerk verdwijnt en er nooit meer uit komt. Daardoor weet niemand precies meer wat de vereisten zijn en mogelijk daarvan gaat afwijken, met als uiterste gevolg dat een beveiliging niet meer functioneert wanneer dat nodig is.

Wanneer de SRS opgesteld is, kan begonnen worden met het eigenlijke design van de SIF.

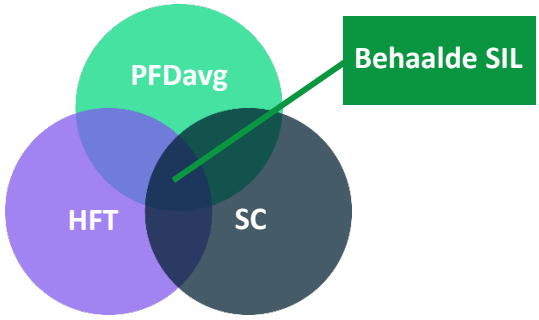
7. Design

Vanuit een gevaren- en risicobeoordeling komt de noodzaak voor een instrumentele beveiliging (SIF). Dan worden de vereisten bepaald en vastgelegd in de specificatie (Safety Requirements Specification - SRS) en pas daarna kan het ontwerp van de SIF pas echt beginnen. In de Safety Life-cycle (SLC) van de NEN-EN-IEC61511 is dit box 4.

Gedurende de ontwerpfase wordt de benodigde hardware bepaald en gekocht, wordt de applicatie geprogrammeerd in de logic solver en moet er getest worden. Wanneer naar de norm gekeken wordt gaan de meeste pagina's over deze fase, wat natuurlijk te verklaren is doordat in deze fase de meeste keuzes gemaakt moeten worden. Ook voor de ontwerpfase geldt dat deze inleiding op het onderwerp te kort is om alles uit te leggen, maar de hoofdlijn is dat het design conform de specificatie moet zijn en moet functioneren. Daarbij komt vervolgens dat de norm voor het design ook eisen geeft met betrekking tot de betrouwbaarheid (SIL) van de SIF. De behaalde SIL bestaat uit drie factoren die allemaal moeten voldoen aan de minimaal benodigde SIL.

Deze factoren zijn:

- Berekening van de kans op falen bij een aanspraak op de veiligheidsfunctie (PFDavg)
  (noot: uitgangspunt van dit artikel is een aanspraakfrequentie <1x per jaar)
- Hardware Fault Tolerance (HFT)
- Systematic Capability (SC)



Over elk van de bovenstaande factoren kan ook weer heel veel geschreven worden en aan elk zitten weer uitzonderingen. Daarom beperken we dit tot een korte algemene uitleg van deze begrippen.

Berekening van de kans op falen bij een aanspraak op de veiligheidsfunctie (PFDavg)

Elk component dat onderdeel is van de SIF – dus van sensor, via logic solver tot en met het stuurorgaan (en alles waar daartussen zit) kan falen, waardoor de veiligheidsfunctie niet meer uitgevoerd kan worden. De faalgegevens van een component worden opgegeven door de fabrikant of zijn bepaald door de eindgebruiker. Hierbij moet opgemerkt worden dat de faalgegevens van fabrikant (al dan niet met een certificaat van een certificerende instantie) en/of eindgebruikers heel vaak veel te positief zijn en dat deze op juistheid beoordeeld en wanneer nodig aangepast moeten worden, voordat deze worden gebruikt. Daarnaast gelden de faalgegevens alleen bij installatie en onderhoud zoals voorgeschreven in het instructie- en/of veiligheidshandleiding (hoeveel ontwerpers lezen deze documenten?). Met de juiste faalgegevens, proof test interval etc. moet een berekening uitgevoerd worden waaruit dan een gemiddelde "Probability of Failure on Demand" (PFDavg). Dit moet voor ieder component uit de SIF gedaan worden en vervolgens moeten alle PFDavg opgeteld worden om de totale PFDavg van de SIF te bepalen. Deze moet vervolgens kleiner zijn dan de

benodigde SIL. De berekeningen kunnen uitgevoerd worden met (dure) software pakketten, maar ook met versimpelde vergelijkingen.

Hardware Fault Tolerance (HFT)

De Hardware Fault Tolerence is afhankelijk van de gebruikte architectuur en geeft weer hoeveel componenten er kunnen falen voordat de veiligheidsfunctie niet meer uitgevoerd kan worden. Door redundantie toe te passen kan vervolgens een hogere betrouwbaarheid behaald worden.

> Voorbeeld: In een meting wordt één sensor gebruikt. Wanneer deze een defect/fout heeft waardoor bijvoorbeeld een te lage waarde door gegeven wordt, terwijl de werkelijke proceswaarde al voorbij het trip point is, dan kan de SIF zijn veiligheidsfunctie niet uitvoeren. Deze functie kan dus geen enkele fout in de hardware permitteren, zonder dat de SIF faalt (HFT=0). Door een extra sensor toe te voegen en 'voting' toe te passen waardoor bij een defecte sensor de andere sensor nog wel de juiste waarde kan doorgeven, wordt wel een fout toegestaan en daarmee wordt HFT = 1 bereikt.

In de normen NEN-EN-IEC61511 en NEN-EN-IEC61508 is middels tabellen opgenomen wat de minimale HFT moet zijn om een bepaalde betrouwbaarheid (SIL) te kunnen claimen en dat is afhankelijk van de gekozen componenten. Dus moet de HFT zo gekozen worden dat de benodigde SIL behaald wordt.

Systematic Capability (SC)

De NEN-EN-IEC61511 geeft aan dat wanneer componenten gebruikt gaan worden in een SIF dat de fabrikanten van deze componenten dan minimaal ook een FSM moeten hebben. Zoals al in hoofdstuk 2 beschreven, wordt dit uitgedrukt in de Systematic Capability (SC). Alle componenten die gebruikt worden in de SIF moeten een minimale SC hebben die gelijk is aan de benodigde SIL.
Tijdens het design van de SIF komt het nogal eens voor dat door bovenstaande factoren aanpassingen gedaan moeten worden. Zo kan het zijn dat additionele componenten moeten worden geïnstalleerd of dat de beoogde componenten vervangen moeten worden door 'betere' componenten. Daarom is het aan te raden om de verificatie van de behaalde SIL zo vroeg mogelijk uit te voeren, zodat een eventuele aanpassing zo min mogelijk vertraging en/of financiële gevolgen heeft.

Als het design is afgerond en alle componenten aanwezig zijn, kan de installatie, commissioning en validatiefase starten.

8. Installatie, commissioning en validatie

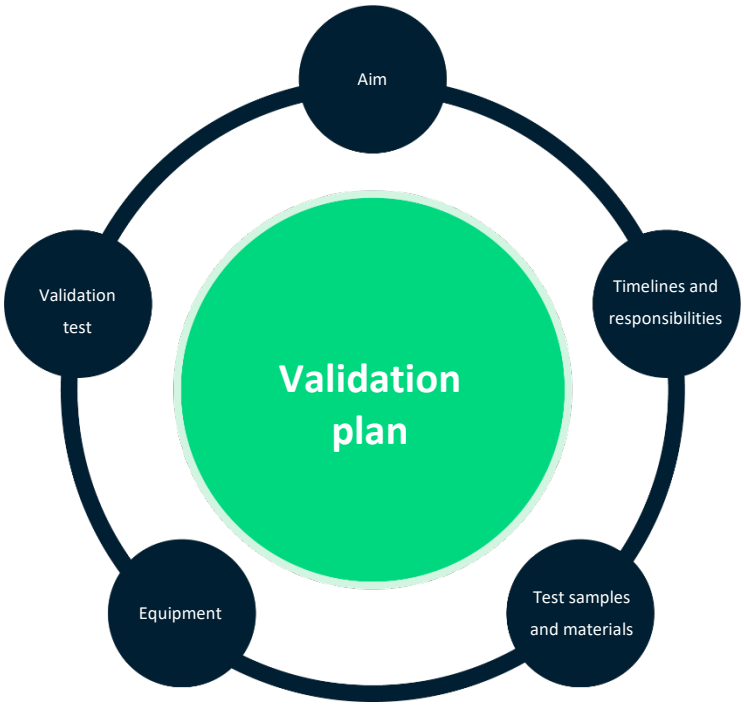
Inmiddels is vanuit de gevaren- en risico inventarisatie een Safety Requirements Specification (SRS) opgesteld, is het ontwerp uitgevoerd en zijn alle componenten ingekocht.

Dan wordt het tijd om alles te gaan installeren en de commissioning activiteiten uit te voeren (box 5 uit de SLC). Belangrijk tijdens het installeren is het opvolgen van de installatie- en/of veiligheidshandleiding. Voor de meeste monteurs zal het voor het installeren van componenten niet uitmaken of een component wordt toegepast in procesbesturing of in een veiligheidsfunctie aangezien het heel vaak dezelfde types worden gebruikt. Maar meestal moet er wel een extra handeling (bv. het omzetten van een dipswitch) worden uitgevoerd om het component ook als een veiligheidscomponent te mogen classificeren.

Als alles is geïnstalleerd, kunnen de commissioning activiteiten plaatsvinden. Hier wordt gekeken of alles juist geïnstalleerd is incl. eventuele aarding en dat alle transport/verpakkingsmaterialen verwijderd zijn. Verder is het een check dat alle kalibraties zijn uitgevoerd en de juiste instellingen zijn geconfigureerd en dat alles signalen en componenten operationeel zijn. Deze commissioning activiteiten moeten allemaal gedocumenteerd worden.

> Wanneer de benodigde risicoreductie vanuit de gevaren- en risico analyse verdeeld is over meerdere beveiligingslagen (bijvoorbeeld een afblaasventiel) is het essentieel dat de overige beveiligingen ook geïnstalleerd zijn om uiteindelijk te starten met een voldoende veilig systeem.

Voordat dan ook echt opgestart kan worden, moet het veiligheidssysteem nog worden gevalideerd door middel van inspectie en testen. Daarvoor moet een plan gemaakt zijn. Dit plan wordt gevoed en aangevuld in elke fase in de SLC. Het plan moet in principe voorzien in dat de SIF functioneel is en alle andere vereisten zoals beschreven in de SRS. Daarnaast moet goed beschreven worden op welke wijze gevalideerd kan worden zonder dat het gevaar oplevert. Wellicht moeten er ook nog additionele equipment worden geïnstalleerd om bepaalde zaken te testen (denk aan het testen van het lekdebiet van afsluiters).
Wanneer testen en/of controlepunten worden uitgevoerd, moeten de test- of controlepunt resultaten gedocumenteerd worden.



Wat heel vaak vergeten wordt bij het valideren van de beveiliging is dat naast dat alle documentatie van voorgaande fases beschikbaar moet zijn ook documentatie voor de volgende fase aanwezig moeten zijn. In de operationele (en onderhouds) fase moeten namelijk de operators en het onderhoudspersoneel wel weten wat benodigd is voor het in stand houden van de beveiliging. Dit kunnen procedures zijn voor het plaatsen van overbruggingen, maar bijvoorbeeld ook proof test procedures (die misschien wel een paar jaar later pas nodig zijn) moeten al geïmplementeerd zijn.

Er kan alleen opgestart worden wanneer uit de validatie gebleken is dat de SIF conform de SRS is uitgevoerd en de beveiliging(en) functioneel zijn.

9. Operations en onderhoud

Alle activiteiten en tijd die in de voorgaande fases, van gevaren- en risico inventarisatie, specificatie, design, installatie tot en met de validatie, van de Safety-Lifecycle (SLC) zijn besteed, hadden tot doel om in de operationele fase (box 6 van de SLC) een werkende en betrouwbare SIF te hebben. In de NEN-EN-IEC61511 wordt de operationele- en onderhoudsfase relatief summier beschreven, maar deze fase duurt het langst (meestal wordt een installatie voor zo'n 20 jaar ontworpen) van alle fases. In de operationele- en onderhoudsfase van een SIF zijn een paar zaken belangrijk, namelijk:
Het bedrijven en onderhouden van de SIF conform de specificatie

- Vergaren van gebruikersdata met betrekking tot het aantal keer van een aanspraak op de veiligheidsfunctie
- Vergaren van gebruikersdata met betrekking tot de faaldata van componenten
- Het lijkt niet veel, maar bovenstaande houdt wel in dat flink wat procedures geïmplementeerd moeten zijn.

Ook in deze fase is competentie weer erg belangrijk. De operators en onderhoudsmedewerkers zijn vanaf dit moment namelijk verantwoordelijk dat de SIF blijft functioneren. Dit impliceert meteen dat deze personen moeten weten wat de SIF's (en andere beveiligingen zijn) zijn, hoe deze werken en welke gevaren er afgedekt worden. Daarnaast moet duidelijk zijn welke componenten tot de SIF behoren, zodat er niet zomaar wijzigingen, waarvan de invloed niet beoordeeld is, worden aangebracht. Voor elk van deze personen geldt dat vooraf bekend moet zijn welke verantwoordelijkheden ze hebben en welke taken uitgevoerd mogen worden. Voor de verschillende taken moeten dan ook procedures (of werkinstructies) aanwezig zijn, denk hierbij aan (proof) test procedures, overbruggingsprocedures, reactie op een alarm van de diagnostiek etc.

> Bovenstaande geldt ook voor onderhoud wat uitbesteed wordt aan bijvoorbeeld de fabrikant van specifieke componenten (of installaties). Voor veel componenten geldt dat deze ingezet kunnen worden voor procesregeling of als beveiliging. Het onderhoud door de fabrikant zal hetzelfde worden uitgevoerd en wellicht zal het component opnieuw afgesteld worden. Als dit component is opgenomen in een beveiliging is wellicht een extra check nodig op correcte installatie, kalibratie etc. (zeker bij een hoge SIL) zodat zeker is dat het component weer zal reageren zoals opgenomen in de SRS. Zeker bij de meer complexere installaties/componenten komt vaak een allrounder (die dan alles moet weten over mechanische componenten, elektronica, elektriciteit, programmeren) in plaats van een specialist voor de beveiliging zoals deze geïnstalleerd is.

Als de organisatie ingesteld is om een beveiliging betrouwbaar en functioneel te houden, kan het alsnog zijn dat de beveiliging uiteindelijk niet de benodigde risico reductie haalt. In de gevaren- en risico inventarisatie is namelijk een aanname gedaan over het aantal keer per jaar dat deze beveiliging noodzakelijk is om in te grijpen. Bij een goed ontworpen procesinstallatie, zal dat niet heel vaak zijn. Maar het kan natuurlijk voorkomen dat bijvoorbeeld door het wijzigen van de kwaliteit van grondstoffen of door een verkeerde inschatting van de prestaties van een nieuwe installatie in werkelijkheid blijkt dat de beveiliging veel vaker wordt aangesproken dan de aanname uit de

gevaren- en risico inventarisatie. Hierdoor kan eventueel het initiële risico hoger uitkomen en zal meer risico reductie nodig zijn. Een ander gevolg kan zijn dat blijkt dat de SIF vaker dan 1x per jaar wordt aangesproken, dan gaat SIF van low demand mode naar high demand mode. Uiteindelijk leidt een hogere aanspraakfrequentie (wat de oorzaak ook is) tot een aanpassing van de SRS, met als gevolg dat dit consequenties kan hebben voor de architectuur en/of gebruikte componenten van de SIF. Het is dus van groot belang (en noodzakelijk) om de afwijkingen in de procescondities bij te houden en regelmatig naast de gevaren- en risico inventarisatie te leggen om te zien of aanpassingen gedaan moeten worden.

Een andere oorzaak van het niet behalen van de risico reductie kan liggen in het feit dat de aangenomen faaldata van de componenten in werkelijkheid niet blijkt te kloppen en dat deze veel vaker falen in een bepaalde omgeving (bv. hogere temperaturen, straling etc) of door het proces zelf (mogelijk vervuiling, schuim, erosie etc). De NEN-EN-IEC61511 eist dat de faaldata van de geïnstalleerde componenten wordt verzameld tijdens de gebruiksfase. Deze moet periodiek worden vergeleken met de aangenomen faaldata tijdens het design (zie hoofdstuk 7). Daaruit kan blijken dat met de nieuwe faaldata de benodigde risico reductie (gekoppeld aan de PFDavg) niet meer wordt behaald. Ook dan zijn er weer aanpassingen van de SIF nodig. Mogelijk kan een vervanging van een soortgelijk component van andere fabrikant of kan het verlagen van de proof test interval uitkomst bieden, maar het kan ook veel ingrijpender zijn en moet een meetprincipe of de architectuur worden aangepast.

Aan het verzamelen van de faaldata kan ook een positieve kant zitten. Wellicht blijkt uit de faaldata ook dat de onderhoudsfrequentie mogelijk naar beneden bijgesteld kan worden, wat lagere leidt tot lagere onderhoudskosten).

Het blijkt dat tijdens de levensduur van een installatie of een SIF vaak modificaties (moeten) worden uitgevoerd. Het volgende hoofdstuk gaat in op deze modificaties.

10. Modificaties

Inmiddels is bijna het eind van de Safety Life-cycle (SLC) van de NEN-EN-IEC61511 bereikt. Initieel is een gevaren- en risico inventarisatie geweest. Daarop is de specificatie (SRS) van de instrumentele beveiliging (SIF) geschreven. Nadat deze ontworpen en geïnstalleerd is, is de SIF operationeel geworden. In de vorige hoofdstuk is al gebleken dat tijdens de operationele fase door verkeerde aannames in het design mogelijk aanpassingen (box 7 in de SLC) gedaan moeten worden. Maar dat zijn zeker niet de enige redenen voor modificaties aan de SIF. Het kan ook zijn dat door veranderingen in onder andere wet- en regelgeving, verandering in de aanwezigheid van mensen in of nabij de installatie (bijvoorbeeld tijdens voorbereiding van turnarounds, tijdens bouwactiviteiten of een verhoogde frequentie van operatorrondes) of veranderingen elders in het proces waardoor bijvoorbeeld het proces of misschien alleen de process safety time verandert. Dit laatste kan veroorzaakt worden door het plaatsen van een pomp met een hoger debiet of door een andere routing van het leidingwerk etc. Heel vaak wordt een modificatie van/voor een beveiliging (in dit geval een SIF) niet herkend of onderkend, doordat het onbekend is wat onderdeel uitmaakt van de voorwaarden van goed functioneren van de beveiliging(en). Voorbeelden die veelvuldig voorkomen zijn:

- Het vervangen van een component door een vergelijkbaar component (maar niet like-for-like). Dit kan gevolgen hebben voor instellingen, response tijd, SIL verificatie (vanwege andere faaldata), proof test procedures en zelfs de training van onderhoudsmedewerkers. Wanneer dus deze factoren niet vooraf worden geanalyseerd is het mogelijk dat ofwel de SIF niet meer functioneel ofwel dat deze minder betrouwbaar is.
- Verandering van de bemensing in de installatie. Tijdens de gevaren- en risico analyse wordt heel vaak alleen naar de operators gekeken, maar in de voorbereiding van of na een turnaround lopen veel meer mensen in de installatie, zo zijn daar de mensen die de steigers bouwen, de isolatie verwijderen of terugplaatsen, verven etc. Maar het kan ook dat er bouwketen worden geplaatst waar mensen vergaderen of schaften. Hierdoor neemt het risico van de verschillende scenario's toe (door een grotere kans op een dode vanwege de langere aanwezigheid van personen of door een groter effect met meerdere doden).
- Aanpassingen in een ander deel van de fabriek, waarbij voorbij gegaan wordt aan het verifiëren van de beveiligingen up- of downstream. Als voorbeeld het veranderen van waaiers in de pomp of het plaatsen van een zwaardere motor van de pomp. Dit kan effect hebben op het debiet en druk van de pomp. Hierdoor kunnen nieuwe gevaren worden geïntroduceerd die niet in de oorspronkelijke gevaren- en risico studies aanwezig waren (het is bv. mogelijk dat met een andere waaier of motor de opvoerhoogte verandert, waardoor het design van het leidingwerk of apparatuur niet meer toereikend is en een beveiliging geplaatst moet worden), maar het kan ook dat bestaande beveiligingen sneller moeten werken of een grotere doorvoer moeten hebben. Soortgelijk is het aanpassen van een Cv van een (regel)klep of het veranderen van doorstroombegrenzers.

Wanneer een modificatie noodzakelijk is, moet daarom een impact analyse gedaan worden. In een impact analyse moet gekeken worden naar de totale impact op mogelijk het introduceren van nieuwe gevaren, een verandering voor de specificatie waardoor mogelijk een nieuw ontwerp moet worden gemaakt. Maar het kan ook een aanpassing in een document zijn of dat een test uitgevoerd moet worden. Als blijkt dat er een impact op veiligheid is, zal bepaald moeten worden in welke fase van de SLC dit moet gebeuren en zal vanaf daar weer verder gegaan moeten worden.

> Als nieuwe gevaren worden geïntroduceerd, zal in de SLC naar de gevaren- en risico inventarisatie teruggegaan moeten worden. Wordt alleen een component voor een like-for-like component is wellicht alleen een test en een aanpassing in een onderhoudsdatabase nodig en kan volstaan worden met de installatie, commissioning en validatie fase.

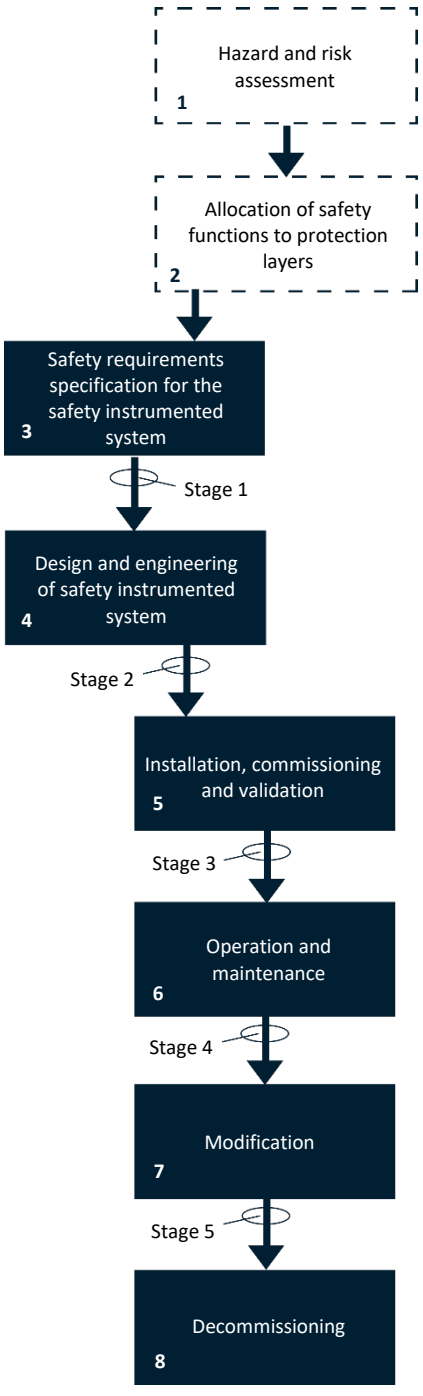
En zoals al eerder benoemd, is documentatie essentieel. Dus zowel de impact analyse als alle activiteiten die gedurende modificatie worden uitgevoerd moeten gedocumenteerd en bewaard worden.

De laatste fase van de SLC is decommissioning (uit bedrijf stellen) van de SIF. In essentie is dit een speciale vorm van modificatie en zal daarom niet behandeld worden.

De verschillende fases van de SLC zijn nu allemaal besproken. Binnen de SLC is echter ook een soort van gate review opgenomen. Dit worden Functional Safety Assessments genoemd. In het volgende hoofdstuk meer hierover.

11. Functional Safety Assessment

In de voorgaande hoofdstukken is de hele Safety Life-cycle (SLC) van de NEN-EN-IEC61511 doorgenomen. Daarbij is aangegeven dat dit een hele logische werkwijze is in de ontwikkeling van een instrumentele beveiliging. In de SLC zit tevens een project structuur verwerkt met stage gate reviews. Deze worden in de norm Functional Safety Assessments (FSA) genoemd. In de SLC worden deze als “stage” met een nummer aangegeven. De volgende stages zijn geïdentificeerd:



- Stage 1: Nadat de gevaren- en risico analyse is uitgevoerd, de benodigde beveiligingslagen zijn geïdentificeerd en de safety requirement specification (SRS) is ontwikkeld (na box 3 van de SLC);
- Stage 2: Nadat het Safety Instrumented System (SIS) ontworpen is (na box 4 van de SLC);
- Stage 3: Nadat de installatie, (pre-)commissioning en validatie van de SIS uitgevoerd is en de operationele- en onderhoudsprocedures zijn ontwikkeld (na box 5 van de SLC);
- Stage 4: Nadat operationele- en onderhoudservaring is opgedaan (tijdens box 6 van de SLC);
- Stage 5: Na modificaties (na box 7 van de SLC).

De norm heeft bepaald dat FSA stages 3, 4 en 5 verplicht zijn. Dat betekent dus ook dat stage 1 en 2 niet verplicht zijn. Maar als stage 1 en 2 worden overgeslagen, moeten deze gedaan worden tijdens FSA stage 3. Tijdens de FSA kan een bevinding zijn dat bepaalde zaken in een SLC fase niet juist of compleet zijn uitgevoerd en daardoor kan de volgende fase niet gestart worden. Wanneer bijvoorbeeld een bevinding wordt gevonden in de SRS en dit wordt pas ontdekt vlak voordat opgestart wordt, is dit kostbaar en heeft dit impact op de planning. Het is dus aan te raden om ook de FSA’s van stage 1 en 2 uit te voeren, zodat eventuele re-work en vertraging voorkomen wordt.

Het primaire doel van een FSA is om zeker te stellen dat aan alle eisen van de norm en van de interne procedures is voldaan en dat daarmee de vereiste SIL wordt bereikt voor de geïdentificeerde SIF’s. Een FSA moet daarom uitgevoerd worden door een onafhankelijk(e) persoon of team. Daarnaast

moet minimaal één persoon een senior status hebben. Alle personen moeten natuurlijk ook weer competent zijn en alles moet gedocumenteerd worden.

FSA stage 3 wordt vaak ook wel de Pre-Startup-Safety Review (PSSR) genoemd. Hierbij is het belangrijk om, door middel van de assessment, te bevestigen dat alle van belang zijnde stappen zijn uitgevoerd. Deze stappen houden in dat de basis de gevaren- en risico analyse is. Alle aanbevelingen uit deze studie geïmplementeerd zijn in de beveiligingen. Als tijdens het project nog wijzigingen zijn geweest, dat deze op de juiste manier uitgevoerd zijn. Dat de beveiligingen zijn ontworpen en geinstalleerd conform de SRS en dat dit gevalideerd is. En tot slot dat de benodigde informatie (en trainingen) door de operators en het onderhoudspersoneel ontvangen is.

FSA stage 4 wordt periodiek uitgevoerd tijdens de operationele fase. De focus van deze FSA ligt heel erg op de instandhouding van de SIF. Hierbij wordt vooral gekeken of operations en onderhoud het werk uitvoeren zoals bedacht was tijdens het design nog wel kloppen. Daarnaast wordt de implementatie van het Functional Safety Management (FSM) beoordeeld.

FSA stage 5 moet uitgevoerd na een modificatie en heeft als uitgangspunt de impact analyse (zie vorige hoofdstuk). Op basis daarvan moeten alle modificatie werkzaamheden correct uitgevoerd zijn en volgt vervolgens eigenlijk voor een groot deel de PSSR (FSA stage 3).

Wanneer in de SLC fases de informatie op de juiste manier gedocumenteerd is, is de ervaring dat een FSA relatief snel kan. Maar de praktijk is meestal toch wat weerbarstiger en blijkt dat veel zaken niet geheel juist uitgevoerd en/of gedocumenteerd zijn.

12. Conclusie

We hebben getracht een inleiding vanuit de NEN-EN-IEC61511 te geven in de activiteiten die nodig zijn om een instrumentele beveiliging te ontwerpen en te bedrijven. Het is in ieder geval van toepassing op instrumentele beveiligingen met een benodigde betrouwbaarheid van SIL 1 of hoger. Maar ons inziens kan en moet dit voor iedere (instrumentele) beveiliging toegepast worden.

Wij zijn ons bewust dat dit in de uitvoering soms lastig is en op veel weerstand stuit. Wij hebben echter wel de hoop dat Functionele Veiligheid in de procesindustrie (nog) serieuzer genomen wordt en dat we uiteindelijk in een veiligere wereld komen te werken en wonen.

Contact

Heb je na het lezen van de informatie nog vragen of wil je een offerte aanvragen? Neem dan gerust contact met ons op.

Telefoonnummer: 088 - 99 51 200
kader.nl | sales.kceni@kader.nl