



Hoe krijgt onderhoud van beveiligingen gestalte?

Herman Jansen

SIL & Onderhoud

Tijdens de engineeringfase van industriële installaties krijgen gevarenidentificatie en risico-evaluatie (HAZOP/SIL brainstormsessies) terecht steeds vaker aandacht. De 'safety life cycle' eisen die worden gesteld aan in gebruik genomen installaties, worden echter in de praktijk vaak 'minder gestructureerd' opgevolgd. Hoe krijgt het noodzakelijke onderhoud van beveiligingen gestalte?

De focus die ligt op gevarenidentificatie en risico-evaluatie is een goede zaak. In de engineeringfase worden gevaren benoemd en risico's bepaald. Daaruit volgende SIL beveiligingen worden ontworpen en de betrouwbaarheid van deze beveiligingen wordt geverifieerd. Bij de SIL verificatie wordt rekening gehouden met alle mogelijke fouten die kunnen optreden in de beveiliging. Faalkansen worden bepaald en getoetst aan de NEN-EN-IEC 61508/61511. Vervolgens worden de beveiligingen gerealiseerd en in bedrijf genomen. Echter, onvoldoende onderhoud aan beveiligingen kan leiden tot een situatie van 'schijnveiligheid' en ernstige incidenten.

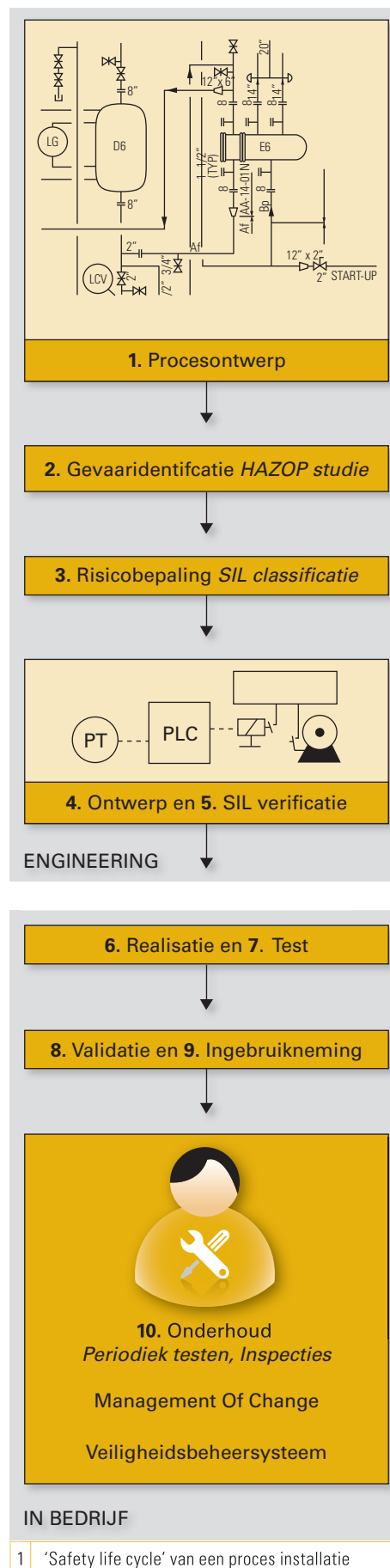
De 'safety life cycle': de engineering fase

In figuur 1 zijn de opeenvolgende 'safety life cycle' fasen schematisch weergegeven. Het (voorlopige) ontwerp van de procesinstallatie of de machine is vaak het startpunt van de 'safety life cycle' (stap 1). Vervolgens wordt vastgesteld wat de potentiële gevaren zijn. In de procesindustrie wordt vaak de HAZOP methodiek (Hazard & Operability Study) toegepast om te weten wat er (allemaal) mis kan gaan (stap 2). Daarna dienen de risico's bepaald te worden (stap 3). In de IEC 61508/61511 normen worden methodieken aangereikt om risico's te bepalen en uit te drukken als SIL. Er zijn vier niveaus: SIL 1 t/m SIL 4. Bij de risk assessment (ook wel SIL classificatie genoemd) wordt het risico bepaald voor veiligheid, milieu en soms ook voor financiële consequenties. Een te hoog risico moet gereduceerd worden door het proces aan te passen (inherent beveiligen) of door het aanbrengen van een mechanische en/of instrumentele beveiliging. Bij het ontwerpen van een SIL beveiliging (stap 4) krijgt de afkorting SIL betekenis: Safety Integrity Level. SIL geeft het betrouwbaarheidsniveau aan van de beveiliging.

Risk based ontwerpen houdt in dat hoe hoger het risico is, des te betrouwbaarder de desbetreffende beveiliging moet zijn.

SIL verificatie

SIL verificatie (stap 5) is het toetsen van een instrumentele beveiliging aan de betrouwbaarheidseisen van de IEC 61508/61511. Er zijn vijf criteria. Het eerste criterium is de identificatie van de beveiliging. Welke sensoren en welke final elementen maken deel uit van de beveiliging en uit welke componenten is de beveiliging opgebouwd? Ook elektrische onderdelen in MCC kunnen deel uitmaken van de beveiliging. Het tweede criterium heeft betrekking op de juiste functie. Het bepaalde SIL scenario is het uitgangspunt om te bepalen of een beveiliging adequaat is. Bijvoorbeeld bij een overvulbeveiliging van een tank moeten alle toevoerstroom gestopt worden. Beveiligingen moeten voldoende snel zijn. Sensoren dienen het potentiële gevaar tijdig te kunnen waarnemen. Bij voorkeur geen overbruggingen en fail safe opgezet. Het onafhankelijk opereren van regeling is het derde criterium. SIL beveiligingen dienen een onafhankelijke 'layer of protection' zijn. Met het vierde criterium wordt bedoeld op het feit dat de architectuur (redundantie) correct moet zijn. Met name bij de hogere SIL beveiligingen is redundantie van de beveiligingscomponenten verplicht. Zo zijn er weleens industriële transmitters nodig om SIL 2 te kunnen realiseren. Het laatste criterium is dat de faalkans op aanspraak van de totale beveiliging voldoende laag moet zijn. Iedere beveiliging moet een voldoende lage faalkans hebben. Met faalkans wordt bedoeld op de kans dat een beveiliging niet ingrijpt als dat zou moeten. Dit wordt de 'Probability of Failure on Demand' genoemd, of wel 'PFD'. Een benaderingsformule voor een enkelvoudige component is als volgt: $PFD = 0,5 \times \text{Faalsnelheid} \times \text{Testperiode}$. Dit betekent dat als er minder getest wordt dan oorspronkelijk is bepaald, de faalkans ontoelaatbaar hoog kan worden en de SIL klasse niet meer gehaald wordt. In de gegeven benaderingsformule wordt uitgegaan van perfect testen waarbij het na iedere test weer 100% zeker is dat de beveiliging perfect is. Bij gebruikmaking van SIL verificatie software wordt



- ▶ vaak een 'Proof test Coverage' ingevoerd ter compensatie van het feit dat perfect testen niet (altijd) mogelijk is.

De 'safety life cycle': de realisatie- en in bedrijfsfase

De volgende fase in de 'safety life cycle' is die van de realisatie (*stap 6*) en het testen (*stap 7*). Een zeer cruciaal moment in de 'safety life cycle' is het initiële, daadwerkelijk testen van beveiligingen. Functioneert de beveiliging? Complexe logic solvers moeten uitgebreid getest worden. Bij voorkeur tijdens de zogenaamde 'Factory Acceptance Test' en door gebruik te maken van simulatoren voor de ingangen en lampjes voor de uitgangen. Alle Shutdown functies moeten getest worden, ook als de overige ingangen in onlogische posities staan (bijvoorbeeld als een (gesimuleerde) kleppositie verkeerd staat). Redundante schakelingen (bijvoorbeeld 2 out of 3) moeten gedetailleerd getest wor-

om de tests en validatie goed voor te bereiden. Testprocedures moeten opgesteld worden.

Onderhoud, periodiek testen en inspecties (*stap 10*)

Onderhoud aan beveiligingen houdt het volgende in: het uitvoeren van preventieve activiteiten (schoonmaken van ventilatiesleuven, smeren bewegende delen, vervangen van onderdelen die aan het eind van de levensduur zijn), kalibratie van instrumenten, visuele inspecties, functietests en vervanging/reparatie van defecte onderdelen. Na de vaak intensieve voorgaande fasen (*stap 1 t/m stap 9*) komen we in de laatste fase die (vaak tientallen) jaren gaat duren. Gedurende deze fase zal keer op keer zeker gesteld moeten worden dat de ontworpen 'Functional Safety' nog steeds intact is (de beveiliging 'Loss of Containment' voorkomt) en in de tweede plaats dat de betrouwbaar-

Allereerst moet er iemand hoofdelijk verantwoordelijk worden gemaakt voor het onderhoud aan SIL beveiligingen. Uiteraard moet de betreffende persoon competent zijn en weten waar het om gaat. Een persoon kan alleen dan verantwoordelijkheid dragen als het onderhoud daadwerkelijk 'handen en voeten' krijgt.

Verder moet er een onderhoudsplan worden opgesteld specifiek voor de SIL beveiligingen (SIL beheersysteem). Onderhoudsactiviteiten moeten worden vastgesteld en worden ingepland. Tijdens de SIL classificatie/verificatie is bepaald welke sensoren, logic solvers en final elements deel uitmaken van SIL beveiligingen. Beveiligingen moeten periodiek geïnspecteerd en getest worden. Het onderhoudsplan moet voorzien in wat, hoe, wanneer en door wie onderhoudsactiviteiten, zoals inspectie en testen, uitgevoerd moeten worden. Ook moet er voor iedere beveiliging een testprocedure opgesteld

'In de laatste fase zal keer op keer zeker gesteld moeten worden dat de ontworpen 'Functional Safety' nog steeds intact is en dat de betrouwbaarheid nog steeds voldoende is.'

den. Deze gedegen en gedetailleerde wijze van testen is in de latere situatie wanneer installaties en beveiligingen reeds in gebruik genomen zijn, niet of nauwelijks meer mogelijk.

In gebruikneming (*stap 8*) en Validatie (*stap 9*)

Na realisatie in de procesinstallatie zullen toch in ieder geval één keer alle beveiligingen grondig getest moeten worden, vanaf de sensoren tot en met alle relevante 'final elements'. Deze validatie is essentieel omdat bij latere 'proof tests' gedetailleerd testen vaak niet meer mogelijk is door gebrek aan tijd, manpower en mogelijkheden. Belangrijk is

heid nog steeds voldoende is. Functieverlies kan optreden door een modificatie in de procesinstallatie, bijvoorbeeld in het geval van een infrarooddetector die een hittebron niet meer kan zien, omdat er een object tussen is geplaatst. De risicoreductie van een beveiliging kan ontoelaatbaar afgenomen zijn door slecht onderhoud, bijvoorbeeld als er minder (vaak) wordt getest dan aanvankelijk was aangenomen.

Belangrijke onderhoudsaspecten

In het onderstaande is puntsgewijs aangegeven welke stappen, handelingen en personen in deze 'safety life cycle' fase een prominente rol zouden moeten spelen.

worden. Vaak kan alleen getest worden als de procesinstallatie uit bedrijf is. Hoe moet getest worden, of nog duidelijker, hoe kan getest worden? Daar zal over nagedacht moeten worden. Het uitgangspunt is om zo volledig mogelijk fouten in de beveiligingen op te sporen.

Een ander belangrijk punt is dat er gezorgd moet worden dat de betreffende onderhoudsmensen voldoende inzicht hebben in de gevaren en de risico's. Ten behoeve van het bewustwordingsproces is het aan te bevelen een onderhoudsvertegenwoordiger te laten participeren in de HAZOP/SIL sessies. Het blijkt vaak dat de ontwikkelde inzicht-



Over de auteur

Ing. Herman Jansen (TÜV-certified Functional Safety Engineer) is senior consultant bij Safety Solutions Consultants BV in Apeldoorn.

ten, het hoe en waarom, de mensen die verantwoordelijk zijn voor het onderhoud, onvoldoende bereiken. Een bijkomend voordeel is dat de participerende onderhoudsvertegenwoordiger oog zal hebben voor potentiële problemen die betrekking hebben op onderhoud en testen. Voorzieningen om afsluiters te kunnen lektesten zullen bijvoorbeeld in de ontwerpfase meegenomen kunnen worden.

Voorts moet er gezorgd worden dat de betreffende onderhoudsmensen voldoende kennis en ervaring hebben van de beveiligingstechniek en basiskennis van de SIL theorie. Een beveiliging die uitsluitend is opgebouwd uit SIL 2 gecertificeerde componenten, hoeft nog niet te voldoen aan SIL 2. Een enkele SIL 2 gecertificeerde transmitter die gebruikt wordt voor zowel regelen als beveiligen, leidt niet tot een SIL 2 beveiliging. In SIL certificatie rapporten zijn vaak condities en restricties weergegeven. Het kan zijn dat een SIL gecertificeerd magneetventiel na vijf jaar vervangen moet worden. Tevens moet er een periodieke visuele inspectie uitgevoerd worden van alle beveiligingen. Is er mechanische schade, corrosie,

beschadigde bekabeling of klemmen, slechte heat tracing et cetera? Kunnen brand- en gasdetectoren nog steeds brand of gas waarnemen? Sommige bedrijven kiezen er voor om de sensoren en final elements visueel herkenbaar te maken, bijvoorbeeld door plaatsing van tagplaten met 'Safety Critical Instrument'.

Ook doen organisaties er verstandig aan om kalibratie en periodieke testen uit te voeren van alle beveiligingen. Er dient getest te worden volgens de opgestelde testprocedure (zie punt 3 hierboven). Een bedrijf kiest er voor om het setpoint van de sensor te verlagen tot onder het actuele niveau. Bij hogedruksensoren kan gebruik gemaakt worden van testgas waarvan de druk instelbaar is.

Verder moet er 'preventive and breakdown maintenance' uitgevoerd worden. Tijdens het uitvoeren van werkzaamheden aan een procesinstallatie die in bedrijf is, is het essentieel bewust te zijn van de potentiële gevaren en risico's. Zijn relevante 'spare parts' beschikbaar? Hoe wordt omgegaan met Maintenance Bypass Switches? Goed overleg met Operations is relevant. De leveranciers moeten aangeven hoe (preventief) onderhoud moet worden gepleegd.

Vervolgens moet de relevante informatie, zoals testresultaten en dergelijke, schriftelijk vastgelegd worden. Toezichhouders verlangen terecht dat een procesinstallatie aantoonbaar veilig is. Hoe, door wie en wanneer zijn de SIL beveiligingen getest? Wat zijn de bevindingen? Evaluatie wordt pas echt mogelijk als informatie wordt vastgelegd.

Tot slot, zeker niet onbelangrijk, moet er vinger aan de pols worden gehouden met Engineering en Operations. Evaluatie is noodzakelijk. Functioneren de beveiligingen zoals verwacht? Grijpt een beveiliging wel eens onterecht in? Is ergens een overbrugging of timer gewenst? Moeten optimalisaties geïmplementeerd worden? Het kan zijn

dat een gekozen meetprincipe in de praktijk matig blijkt te functioneren.

Samenvatting

Het is wijs om onderhoudsmensen al in een vroeg stadium te betrekken in het proces van bewustwording van de gevaren en risico's van een procesinstallatie en de functie van de beveiligingen daarin. Voorzieningen om (goed) te kunnen testen, dienen geïmplementeerd te worden. Testprocedures moeten zorgvuldig opgesteld worden. Een beheersysteem zal moeten functioneren. Onderhoud is maatwerk en mensenwerk. Toezicht is nodig en procedures moeten geborgd worden. ■

Meer info:

www.safety-sc.com, E.jansen@safety-sc.com