#waaromlezen

SIL is veel meer dan alleen complexe faalkansberekeningen. Je leest hier welke aspecten belangrijker zijn

Wat SIL concreet inhoudt voor de procesindustrie anno 2019

Instrumentele beveiligingen

Bij SIL wordt vaak nog een-op-een gedacht aan complexe faalkansberekeningen. Die faalkansberekeningen horen er wel bij, maar diverse andere aspecten zijn van meer belang. In dit artikel zijn enkele van die aspecten beschreven. ▻ Herman Jansen

Een voorbeeldje: sommige bedrijven maken bij het SIL-testen gebruik van een HART-communicator. Dat is zinvol omdat zo makkelijk gecontroleerd kan worden of de range van transmitters juist is ingesteld en of de transmitter juist reageert op een gedetecteerde transmitterfout. Ten behoeve van het testen van de tripwaarde wordt vervolgens de transmitter in simulatiemodus gebracht, waardoor getest kan worden of de beveiliging wel actief wordt bij de juiste meetwaarde. Maar: als de simulatiemodus niet correct gestopt wordt, blijft de transmitter overbrugd - ook als de HART-communicator verwijderd is - zonder dat een alarm of melding dit aangeeft. De testformulieren worden naar tevredenheid afgetekend en de procesinstallatie blijft onbeveiligd achter. Dat na een functietest de beveiliging niet meer functioneert, is onacceptabel!

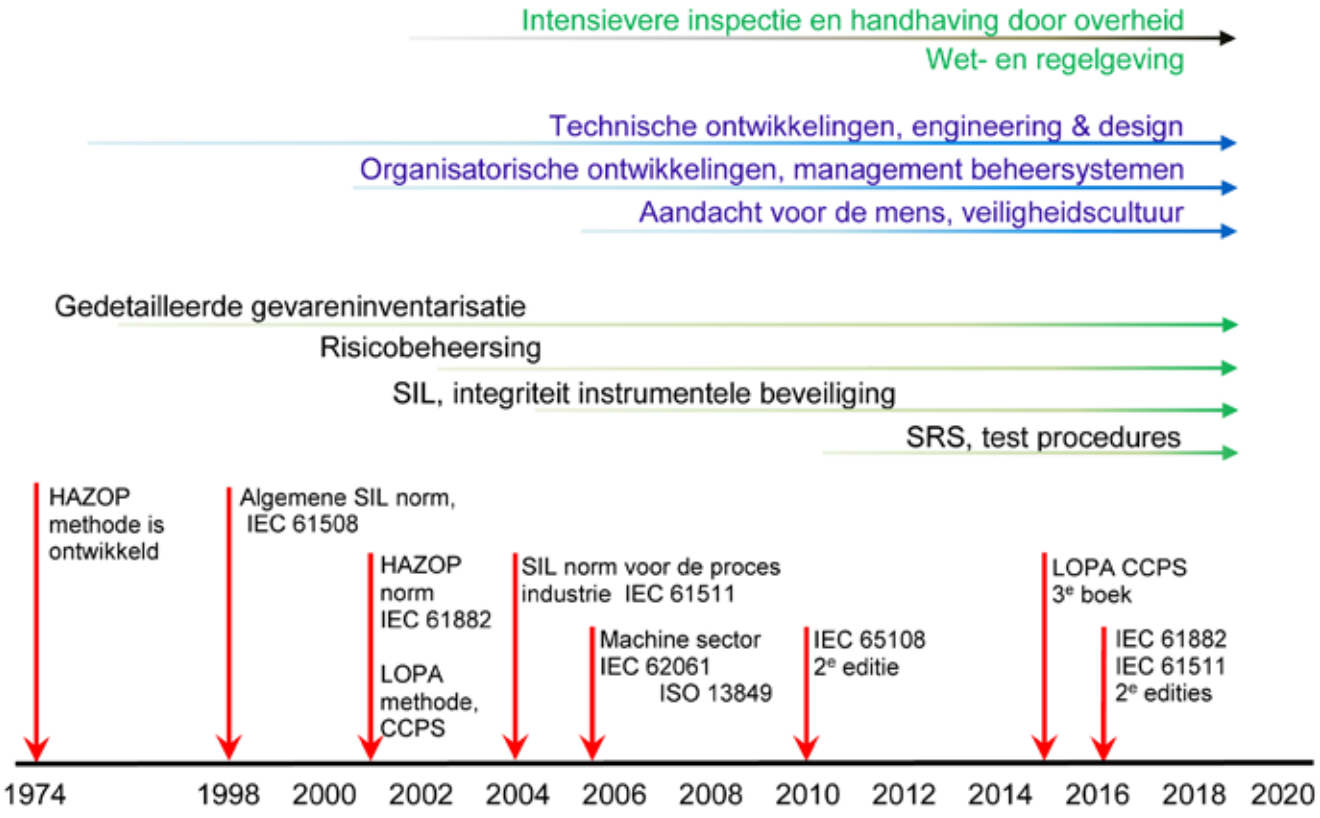
De schrijver van dit artikel tijdens een SIL-uitvoeringsverificatie bij DSM in Emmen.

Ontwikkeling

Ruim een halve eeuw geleden werden (al) betrouwbare ‘hardwired logic solvers’ ontwikkeld en toegepast, onder andere in de olie- en gasindustrie. Het ‘fail safe’ principe stond centraal. Analoge sensoren werden toen nog bij voorkeur niet gebruikt voor beveiligingen. In de tweede helft van de vorige eeuw groeide de behoefte aan instrumentele beveiligingen die aantoonbaar betrouwbaar waren, niet alleen de logic solver maar ook de sensoren, de kleppen en de motoren die de procesinstallatie moeten veiligstellen. Mechanische beveiligingen - zoals veerveiligheden - waren en zijn relatief simpel, instrumentele beveiligingen daarentegen laten niet zien dat ze betrouwbaar zijn.

Integriteitseisen werden geformuleerd en de IEC 61508 werd ontwikkeld en twintig jaar geleden uiteindelijk uitgegeven. IEC 61511 - de SIL-norm specifiek voor de procesindustrie - volgde enige jaren later. Deze SIL-normen zijn door de procesindustrie enorm omarmd en de implementatie daarvan is in relatief korte tijd heel voortvarend verlopen. Een groot compliment aan de initiatiefnemers en opstellers van de SIL-normen.

In de SIL-normen gaat het om vier integriteitsklassen. Een SIL1-beveiliging geeft een risicoreductie van in ieder geval 10 (101). Dat houdt in dat als een gevaarlijk scenario gemiddeld eens per 15 jaar optreedt, deze met een adequate SIL1-beveiliging minder vaak dan eens per 150 jaar zal optreden. Een SIL2-beveiliging reduceert risico met minimaal een factor 100 (102). Bij SIL3 is de risicoreductie in ieder geval 1000 (103). Sommige bedrijven hanteren naast de formele SIL1/2/3 ook nog SILa. Een interlock in het procesregelsysteem is



△ Fig.1 Ontwikkeling procesveiligheid.

hierbij een typische SILa voorziening. SIL4 beveiligingen zijn uitzonderlijk, waarbij het een grote uitdaging is deze te ontwerpen en te realiseren.

Functional Safety

De term 'SIL' komt (natuurlijk) veel voor in de SIL-normen, maar de term 'Functional Safety' komt vaker voor. Het ontwerpen en realiseren van een beveiligingsfunctie luistert nauw. Welke sensoren, waar plaatsen, welke tripsettingen? Hoe kan de procesinstallatie worden veiliggesteld? In dit artikel wordt Functional Safety vanuit twee invalshoeken benaderd. De organisatorische en de technische invalshoek.

Natuurlijk gaat het uiteindelijk om het ontwerp en de techniek van de instrumentele beveiliging. Hiermee wordt een betrouwbare SIL-beveiliging gerealiseerd met een voldoende lage technische faalkans. Het technische aspect is belangrijk maar de organisatie rondom de instrumentele beveiliging is misschien wel belangrijker. De organisatorische faalkans zou groter kunnen zijn dan de technische faalkans. Voor de goede orde: de technische faalkans, de 'PFDavg' moet berekend en getoetst worden. Organisatorische onvolkomenheden worden niet gekwantificeerd.

Een voorbeeld van een technische fout is een defecte sensor. Enkele voorbeelden van organisatorische fouten (de SIL-normen hebben het dan over 'systematic failures'):

- Door een ontwerpfout worden niet alle toevoeren gesloten bij een overvulbeveiliging.
- Een onjuiste SIL-classificatie waardoor een beveiliging te 'licht' wordt ontworpen.
- De sluittijd van een tijd-kritische klep krijgt geen aandacht.
- Een sensor met een onjuist meetprincipe wordt ingezet (bijvoorbeeld een niveausensor dat niet door schuim in een tank kan 'kijken').
- Tijdens de engineering is geen aandacht voor het uitgangspunt dat een diagnosefout ('dangerous detected failure') altijd een actie tot gevolg moet hebben.
- Een programmeur maakt een foutje in de applicatie software van de plc.
- Het binnenwerk van de klep in een overdrukbeveiliging lekt, doordat het materiaal niet bestand is tegen de corrosieve inwerking van het medium.
- De beveiliging is in onvoldoende mate onafhankelijk.
- Onvolledige testprocedure.

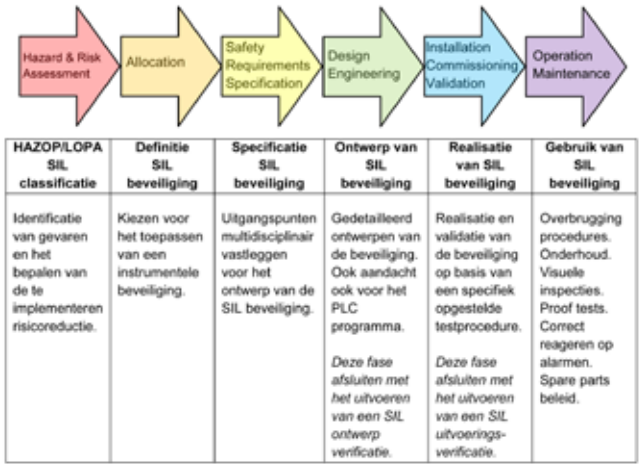
Organisatorische aspecten

Kort samengevat gaat het om deugdelijke management-systemen en competente medewerkers gedurende alle lifecycle fasen van instrumentele beveiligingen. De management-systemen moeten er voor zorgen dat de benodigde activiteiten worden uitgevoerd en dat geborgd wordt dat een gemaakte fout (tijdig) wordt ontdekt.

Hazard & Risk Assessment

Tijdens het proces van gevarenidentificatie - bijvoorbeeld door een HAZOP-studie - zal een bedrijf zich bewust worden van de zogenaamde 'Loss Of Containment' scenario's, waarbij stoffen of energie uit de installatie vrijkomen of onbedoeld in de installatie komen. Het betreft dan meestal een veiligheidsissue. De risicobepaling kan resulteren in een noodzakelijke risicoreducerende maatregel. ▶

△ Fig. 2 Aspecten van een instrumentele beveiliging.



HAZOP/LOPA SIL classificatie	Definitie SIL beveiliging	Specificatie SIL beveiliging	Ontwerp van SIL beveiliging	Realisatie van SIL beveiliging	Gebruik van SIL beveiliging
Identificatie van gevaren en het bepalen van de te implementeren risicoreductie.	Kiezen voor het toepassen van een instrumentele beveiliging.	Uitgangspunten multidisciplinair vastleggen voor het ontwerp van de SIL beveiliging.	Gedetailleerd ontwerpen van de beveiliging. Ook aandacht ook voor het PLC programma. *Deze fase afsluiten met het uitvoeren van een SIL ontwerp verificatie.*	Realisatie en validatie van de beveiliging op basis van een specifiek opgestelde testprocedure. *Deze fase afsluiten met het uitvoeren van een SIL uitvoerings-verificatie.*	Overbrugging procedures. Onderhoud. Visuele inspecties. Proof tests. Correct reageren op alarmen. Spare parts beleid.

△ Fig.3 Fases waarin instrumentele beveiliging tot stand komt.

De SIL-normen geven informatief aan - niet dwingend - hoe je tot een SIL-klasse kunt komen. In principe gebeurt dat 'risk based': hoe groter het risico, des te hoger de SIL-klasse. De HAZOP-methodiek werd in 1974 geïntroduceerd. Het inschatten en beheersen van risico's kwam pas goed op gang vanaf 2003 met de risicograaf uit de SIL-norm. De LOPA-methodiek (Layer Of Protection Analysis) werd ook twintig jaar geleden ontwikkeld. Ook de implementatie van LOPA heeft een enorme boost gekregen door de SIL-normen.

In de procesindustrie worden deze methodieken al lang niet meer alleen toegepast voor de SIL-classificatie van instrumentele beveiligingen. Risicograaf en LOPA worden ingezet om alle procesmatige risico's te beheersen - procesveiligheid als ook machineveiligheid. Het inzetten van een instrumentele beveiliging als risicoreducerende maatregel is dan een mogelijkheid.

Allocation

Met 'Allocation' wordt bedoeld dat bepaald moet worden hoe risicoreducerende maatregelen moeten worden ingevuld. Gekozen kan worden voor een instrumentele beveiliging. Pas dan komen we in het werkgebied van 'Functional Safety' en SIL.

'In de afgelopen 25 jaar zijn grote stappen gezet'

Safety Requirements Specification

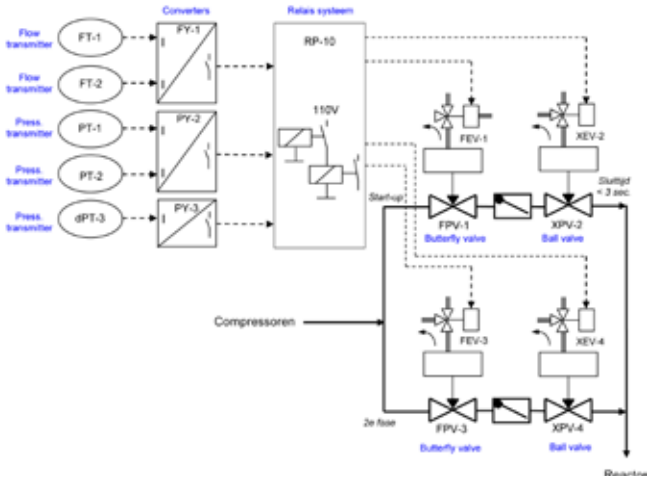
Het opstellen van een Safety Requirements Specification of SRS neemt over het algemeen niet veel tijd in beslag. Een SRS is bij voorkeur kort en bondig. Toch geeft de SIL-norm aan: 'The development of the SRS is one of the most important activities of the whole safety lifecycle'. In een SRS worden alle relevante uitgangspunten voor de instrumentele beveiliging(en) multidisciplinair bepaald en vastgelegd.

Het belang van de SRS wordt gelukkig steeds meer onderkend. Tijdens een HAZOP/LOPA-studie wordt bepaald dat een risicoreducerende maatregel nodig is. In de SRS moet het SIL-niveau en eventueel aanvullend de minimale risicoreductiefactor of de maximale faalkans aangegeven worden. Er dient te worden aangegeven welke sensoren het potentiële gevaar moeten detecteren en bij welke tripwaarde(n) de beveiliging geactiveerd moet worden. Ook moet precies zijn aangegeven hoe de beveiliging de procesinstallatie moet veiligstellen; welke motoren moeten stoppen en welke kleppen moeten sluiten of juist moeten openen. Soms maakt een alarm deel uit van een beveiliging. Of kleppen lekdicht moeten zijn en hoe snel deze kleppen dicht moeten lopen. Of tracing nodig is van de meetleiding om stollen van het medium te voorkomen. Of er overbruggingen benodigd zijn, bijvoorbeeld ten behoeve van onderhoud of opstart. Bij voorkeur wordt in de SRS al aangegeven of voorzieningen geïmplementeerd moeten worden om later de beveiliging te kunnen testen.

In de SRS worden de uitgangspunten gedefinieerd die in de volgende fase - Design & Engineering - worden uitgewerkt. Maar ook voor het valideren van de SIL-beveiliging wordt de SRS gebruikt.

Design & Engineering

In de 'Design & Engineering' fase wordt de SIL-beveiliging tot in detail ontworpen. Gebruikelijk wordt vervolgens in deze fase het ontwerp 'SIL-geverifieerd' door een onafhankelijke SIL-professional. In de norm wordt deze verificatie een 'Functional Safety Assessment, stage 2' genoemd. Ook in deze fase zijn competentie en managementsystemen



△ Fig.4 Schematische weergave.

belangrijk. Een ervaren instrumentengineer zal de juiste instrumenten specificeren. Bij voorkeur gebruikmakend van 'proven technology'. De SIL-norm heeft het dan over 'prior use devices'. Het is noodzakelijk dat eventuele ontwerpfouten zich openbaren voor de ingebruikneming. Controle door een collega - peer review - kan nodig zijn. De specifieke programmering van de safety-plc laat zich vaak lastig controleren. In ieder geval moet de betreffende systeemengineer aantoonbare competentie hebben - bijvoorbeeld beschikken over relevante opleidingscertificaten en ervaring. Bij de SIL-ontwerp- en/of uitvoeringsverificatie dient hierop getoetst te worden.

Installation, commissioning and validation

Instrumentele beveiligingen kunnen het verschil maken tussen leven en dood. Daarom dienen deze gedetailleerd getest te worden, het zogenaamde proof-testen. Proof-test-procedures moeten kwalitatief goed zijn. Dit is geen 'nice to have dingetje' maar een kritische factor. Het opstellen van goede testprocedures is vaak moeilijk. Het vereist een multidisciplinaire aanpak.

In sommige faalkans-rekenprogramma's kan een Proof Test Coverage factor ingevoerd worden. Deze factor geeft aan hoe goed het proof-testen uitgevoerd wordt. Een lage Proof Test Coverage factor zorgt ervoor dat de berekende faalkans van een beveiliging groter wordt. Het gevaar is aanwezig dat slecht testen gecompenseerd wordt door vaker slecht te testen om zo de berekende faalkans weer gunstiger te krijgen. Het kan zijn dat de testprocedure beschrijft om een transmitter los te nemen en te vervangen door een stroombron waarmee getest kan worden of de instrumentele beveiliging op de juiste stroomwaarde actief wordt. Waarbij de transmitter en de meetleidingen niet getest worden. Een onvolledige test van de SIL-beveiliging is niet acceptabel.

SIL uitvoeringsverificatie

Ook in deze fase is verificatie gewenst. De norm heeft het dan over een 'Functional Safety Assessment, stage 3' De SIL- uitvoeringsverificatie wordt onder andere standaard door bedrijven als Dow, DSM en USG uitgevoerd. De SIL-uitvoeringsverificatie is niet de validatie van de SIL-beveiligingen maar de controle of de validatie op juiste wijze heeft plaatsgevonden en na de validatie de beveiliging weer 'op scherp' is gezet. Deze uitvoeringsverificatie bestaat onder andere uit de controle van de testprocedures, of deze zijn afgetekend al dan niet met relevante opmerkingen en een visuele inspectie van de beveiliging in de plant. Het blijkt dat een dergelijke verificatie niet zelden noodzakelijk is.

Operation and Maintenance

Gemakshalve gaan we bij SIL uit van constante faalgegevens en geven daarbij aan dat als de levensduur van een instrument bijna is verstreken, deze moet worden vervangen. Dat is makkelijker gezegd dan gedaan. Instrumenten zijn helaas niet voorzien van een indicatie met de 'resterende lifetime'. Wat is de verouderingssnelheid, wat is de invloed van erosie, corrosie, trillingen, stress, temperatuurwisselingen? Bij een instrument dat jaarlijks wordt getest, kan redelijkerwijs de vinger aan de pols gehouden worden. Bij SIL3 HIPPS-systemen - HIPPS staat hier voor High Integrity Pressure Protection System - is het gebruikelijk dat na circa zes jaar de afsluiters worden gedemonteerd en intern worden geïnspecteerd op onvolkomenheden, een zogenaamde overhaul.

Hoe moet omgegaan worden met een instrumentele beveiliging die op leeftijd is, met een proof-test interval van zes jaar? Bij maintenance-afdelingen is vaak de eerste focus op het in bedrijf houden van de installatie, niet op het 'gezond houden' van de instrumentele beveiligingen. Tot in hoeverre wordt het veiliger als een specifiek niet SIL-gecertificeerd instrument in een agressieve omgeving - dat bewezen heeft goed te functioneren - wordt vervangen door een nieuw SIL-gecertificeerd type dat werkt met een ander meetprincipe? Daarvoor is het nodig het 'end of lifetime' aspect te bespreken en een strategie te kiezen. Dat kan leiden tot het voortijdig vervangen van instrumenten of extra tussentijdse inspecties/controles.

Technische aspecten

De onderstaande criteria zijn van belang tijdens de ontwerp-verificatie.

Identificatie van de beveiliging

Voor de SIL ontwerpverificatie moet duidelijk zijn welke sensoren en final elements deel uitmaken van de beveiliging en hoe redundante configuraties functioneren. Daarnaast is het nodig te weten hoe de beveiliging in detail is opgebouwd en met welke componenten.

Functionele controle

De beveiliging moet bij een potentieel gevaar de proces-installatie veiligstellen. Als er geen SRS is, zal gecontroleerd moeten worden aan de hand van de P&ID's, het HAZOP report en het risk assessment report.

De tripinstellingen van sensoren moeten juist bepaald zijn. Overbruggingen zijn eigenlijk niet gewenst. Kleppen moeten snel genoeg sluiten en mogelijk lekdicht zijn. Ook het toetsen van de programmering van de safety-plc maakt deel uit van de functionele controle. ▶

Onafhankelijkheid
Het komt voor dat afsluiters en sensoren deel uitmaken van een SIL-beveiliging alsook de normale procesregeling. Voorop staat dat falen van - een onderdeel van - het regelsysteem het veilig functioneren van de SIL-beveiliging nooit negatief mag kunnen beïnvloeden. De SIL-norm geeft aan: 'A device used by the process control system shall not be used by the instrumental safeguard, unless an analysis has been carried out to confirm that the overall risk is acceptable'. Het opstellen van deze 'analysis' is weleens lastig. Om hier pragmatisch, snel en goed mee om te kunnen gaan zijn er vuistregels opgesteld.

Systematische fouten
'Prior use' instrumenten hebben aantoonbaar bewezen goed te functioneren. Het meetprincipe, de toegepaste materialen en omgevingscondities luisteren vaak nauw, zeker bij specifieke applicaties. IEC 61511 geeft aan deze 'prior use' instrumenten te evalueren en te documenteren. Als 'Prior use' instrumenten niet zijn toegepast, zal getoetst moeten worden op basis van IEC 61508. Dat houdt in dat de instrumenten moeten voldoen aan een 'Systematic Capability' klasse. In een SIL2-beveiliging moeten de instrumenten voldoen aan SC-2. De instrumentleverancier heeft hierin een grote verantwoordelijkheid. De leverancier moet onder andere een deugdelijk kwaliteitssysteem hebben. De SIL-norm heeft het zelfs over een 'Functional Safety Management System'.

Architectuur
Redundantie wordt vereist bij SIL3 en soms ook al bij SIL2. Deze architectuureis staat los van de faalkansberekening. De meeste eindgebruikers werken (nog) niet met zogenaamde 'prior use' aanpak. Dat betekent dat de architectuur tabellen uit de IEC 61508 gebruikt worden met instrument type A/B, 'Safe Failure Fraction' en 'Hardware Fault Tolerance'. Het toepassen van één enkele industriële sensor in een SIL2-beveiliging is op basis van IEC 61508 vaak niet acceptabel, ook al is de faalkans laag - tenzij de sensor SIL2-gecertificeerd is.

Faalkansberekening
Faalkansen kunnen berekend worden met complexe software, die bijvoorbeeld gebruikmaakt van Markov-modellering. Naast de faalsnelheden van de instrumenten, worden common cause factoren ingegeven alsook de mission time van het instrument en de proof test coverage factor alsmede de tijd benodigd voor het testen. De faalkans wordt dan zeer precies berekend. De common cause factor is echter een grove inschatting, de mission time ook, evenals de proof test coverage factor. Het voegt niet veel toe om met complexe software de faalkansen te berekenen. Het gebruik van vereenvoudigde formules is meestal goed genoeg!

Grote stappen

In de afgelopen 25 jaar zijn grote stappen gezet met de ontwikkeling en implementatie van SIL-normen. De procesveiligheid is daardoor flink toegenomen. Het besef is echter nog beperkt aanwezig dat het bij instrumentele beveiligingen niet alleen gaat om de technische aspecten maar ook om de organisatie gedurende de diverse lifecyclefasen. Kort samengevat houdt dat in: weten welke activiteiten uitgevoerd moeten worden en deze laten uitvoeren door vakmensen! Het opstellen van een SRS is zo'n activiteit. Maar ook het maken van goede testprocedures, zowel voor de initiële validatie als ook voor de daarna periodiek uit te voeren proof-tests.

De programmering van de safety-plc blijft een punt van aandacht. Hoe kan zeker gesteld worden dat de plc in alle situaties juist functioneert? Het is een zinvolle overweging om een ontwerp met complexe functionaliteit eerst te controleren op een simulatie systeem met schakelaars en lampen. Een andere aan te bevelen stap - die de meeste bedrijven nog niet gezet hebben, is het definiëren en toepassen van zogenaamde 'prior use' devices.

Kortom, veel goede ideeën zijn ontwikkeld, ervaringen zijn opgedaan en goede inzichten zijn verworven. Bedrijven kunnen hiermee hun voordeel opdoen! ■

www.consiltant.com

INFORMATIE