DE TOEPASSING VAN SIL

POSITION PAPER VAN HET SIL PLATFORM

AUTOMATIE

REPRINT

NEN

SIL Platform

Willem van der Bijl (Safety Consultant en M.D. PRODUCA Consultancy) & Henry Verwey (Sr. Safety Consultant Verwey Safety Services)
nl.linkedin.com/in/willemvanderbijl

Drieluik SIL - Deel 1

Toepassing SIL

De toepassing van SIL in de procesindustrie wordt steeds belangrijker. Het SIL Platform is opgericht om de industrie hierbij te ondersteunen. De visie van het platform is verwerkt in een SIL Platform Position Paper om met de industrie te delen. Automatie biedt u deze visie aan als drieluik. In deze uitgave deel 1 over de basis van SIL implementatie en systematische ontwerpbenadering.

Het is de bedoeling van het SIL Platform om een SIL gerelateerd document uit te geven. De doelstelling van het SIL Platform Position Paper is om de markt te informeren en om bewustwording te creëren over specifieke aspecten van het toepassen van SIL in de procesindustrie. Dit document geeft basisinformatie over de implementatie van SIL en de relevante terminologie. Het richt zich vooral op het SIL verificatieproces om de nagestreefde integriteit van SIL circuits vast te stellen.

Onderwerpen

1 Basis van SIL Implementatie
2 Systematische ontwerpbenadering
3 Storingsgegevens van instrumenten
4 Het gebruik van de Diagnostic Coverage (DC) factor en de Safe Failure Fraction (SFF)
5 Hardware safety integrity randvoorwaarden aan de architectuur
6 Verificatiebeproevingen van Safety Instrumented Systems
7 Safety lifecycle management

In deel 1 van dit drieluik worden de hoofdstukken 1 en 2 en de inleiding behandeld. In deel 2 volgen de hoofdstukken 3 en 4, en de overige drie hoofdstukken worden in het laatste deel behandeld.

Over het SIL Platform

Het SIL Platform is een onafhankelijke groep van ervaren gebruikers en aanhangers van de SIL filosofie volgens IEC 61508:2010 en IEC 61511:2003 in de Nederlandse procesindustrie. Het SIL Platform is onderdeel van de Nederlandse normcommissie NEC 65 'Industrieel meten, regelen en automatiseren', die de Nederlandse inbreng verzorgt in het internationale werk van IEC/TC 65 'Industrial measurement, control and automation'. Op dit moment telt het SIL Platform veertig leden. Zij vertegenwoordigen eindgebruikers, ingenieursbureaus, leveranciers, fabrikanten en consultancy bedrijven.

Meer informatie
I: www.nen.nl en E: rianne.boek@nen.nl

Hoofdstuk 1 Basis van SIL Implementatie

Wat vormt de basis van SIL implementatie?

Het is gebruikelijk om procesinstallaties te laten draaien op maximale opbrengst, optimale capaciteit en minimaal risiconiveau. Key Performance Indicatoren worden gebruikt om realistische targets en doelstellingen te meten en te controleren. Een methode om risico's te kwantificeren, is een tiental jaren geleden geïntroduceerd onder de naam SIL, wat staat voor Safety Integrity Level. Eigenlijk kan SIL worden gezien als een numerieke aanduiding van het risiconiveau, op een schaal van SIL 1 tot en met SIL 4. In overeenstemming hiermee is dit ook het integriteitsniveau van een veiligheidssysteem dat het risico reduceert.

Tijdens een studie naar gevaren en bedrijfsvoering (HAZOP, hazard and operability) worden potentiële risico's per procesknooppunt vastgesteld, die als juist en volledig zullen moeten worden geverifieerd. HAZOP is een gestructureerd en systematisch onderzoek van een gepland of bestaand proces of uitvoering van werkzaamheden met als doel om gevaren te kunnen identificeren en te evalueren. De volgende stap is een risicobeoordeling, ook wel een SIL Classificatie genoemd. Vanwege verificatie-eisen moet deze gescheiden zijn van de HAZOP studie. Bij een SIL Classificatie worden risicografieken of risicomatrices die horen bij het type activiteiten, bedrijf en proces, als referentie gebruikt. Wanneer risico's als 'acceptabel' worden geclassificeerd, is geen verdere actie nodig. In het geval van een onacceptabel risico wordt de grootte vastgesteld in factoren van tien. SIL 1 betekent dat het risico van dat procesknooppunt een factor 10 te hoog is. Bij SIL 2 is het risiconiveau een factor 100 te hoog enzovoorts.

De consequentie van de SIL Classificatie is dat wanneer een gevarenknooppunt een risiconiveau van SIL 2 heeft, u verplicht bent om dat risico met minimaal een factor 100 te verminderen om tot een acceptabel risiconiveau te komen. Deze factor wordt risicoreductiefactor (RRF, risk reduction factor) genoemd. SIL gerelateerde risicoreductie wordt, per definitie, bereikt met elektrische, elektronische of programmeerbare elektronische (E/E/PE) veiligheidssystemen. Het proces wordt bewaakt door het zogenaamde sensorelement, gewoonlijk een meetzender. Zodra het proces een bepaalde veiligheidswaarde overschrijdt, moet een uitvoerelement dit zodanig beïnvloeden dat het risicolopend proces wordt teruggebracht in een veilige toestand. Een logische verwerkingseenheid is geprogrammeerd om een uitgangstoestand naar een klep of relaiskontakt (uitvoerelement) over te brengen indien een ingang een ingestelde waarde overschrijdt. Het onderling verbonden sensorelement, de logische verwerkingseenheid en het uitvoerelement worden het veiligheidscircuit genoemd, en deze voert de Safety Instrumented Function (SIF) uit. Gezamenlijk vormen deze componenten het Safety Instrumented System, ofwel SIS. Het Safety Integrity Level, SIL, is per definitie gerelateerd aan de Safety Instrumented Function (SIF), en niet aan de individuele componenten.

Hoe realiseer ik een geschikte SIL implementatie?

Gedurende het SIL Classificatieproces worden SIL niveaus gekoppeld aan specifieke procesgevaren, die op hun beurt de eisen voor de integriteit van de Safety Instrumented Function (SIF) en de gerelateerde apparatuur bepalen. Het moet duidelijk zijn dat HAZOP, SIL Classificatie en SIL Verificatie behandeld moeten worden met dezelfde hoge mate van importantie en kwaliteit. In de volgende hoofdstukken van dit document wordt ingegaan op het belang en de bronnen van storingsfrequentiegegevens, certificering van instrumenten, statistische berekeningen, testprincipes, interpretatie van diagnostische gegevens, ofwel het circuitontwerp, storingsanalyse en gegevensverwerking, wat leidt tot de onderbouwing van de integriteit van het veiligheidscircuit.

‘Met dit position paper informeert het SIL Platform de markt en creëert het bewustwording over specifieke aspecten van het toepassen van SIL in de procesindustrie.’

Hoofdstuk 2 Systematische ontwerpbenadering

Een systematische ontwerpbenadering is er op gericht om het optreden van systematische fouten te elimineren. Systematische fouten zijn op deterministische wijze gerelateerd aan een bepaalde oorzaak die alleen weggenomen kan worden door wijziging van het ontwerp, het fabricageproces, operationele procedures of andere relevante factoren.

Waarom?

Onderzoek toont aan dat de meerderheid van storingen in regelsystemen die leiden tot incidenten, wordt veroorzaakt door storingen die voorkomen hadden kunnen worden indien een systematische, risicogebaseerde ontwerpbenadering zou zijn toegepast over de hele levenscyclus van het systeem. Zie ‘Out of Control’, gepubliceerd door HSE, voor details.

Valkuilen

Incomplete specificaties en te veel focus op berekeningen zijn de belangrijkste valkuilen bij het realiseren van een systematische ontwerpbenadering. Deze worden hieronder verder toegelicht.

Incomplete specificaties

Ingenieurs zijn getraind om oplossingen te bedenken. Dit kan echter leiden tot een drang om over te gaan tot de ontwerpfase voordat een complete set specificaties is opgesteld. Het onderzoek waaraan hierboven wordt gerefereerd, toont aan dat 44 procent van de incidenten kan worden toegeschreven aan tekortkomingen in de specificaties van het regelsysteem. De meest voorkomende tekortkomingen zijn een slechte analyse van gevaren van de apparatuur binnen het regelsysteem en een ontoereikende beoordeling van de invloed van verschillende storingen van het regelsysteem op de specificaties.

Te veel focus op berekeningen

Betrouwbaarheidstechniek is gebaseerd op statistiek. Bij het berekenen van de PFD zijn waardes voor bepaalde factoren nodig, bijvoorbeeld de diagnostic coverage en de common cause storingen, binnen bepaalde condities. Alleen als aan deze condities wordt voldaan, zal een berekening van de PFD een betrouwbaar resultaat opleveren. De geldigheid van deze aangenomen condities ten opzichte van de werkelijke condities waarbinnen het systeem functioneert, moet zorgvuldig geverifieerd worden.

Realisatie

Om een systematische ontwerpbenadering te realiseren, moet aan een aantal voorwaarden worden voldaan. Deze worden hieronder verder uitgelegd.

Betrokkenheid management

Essentieel bij het realiseren van een systematische ontwerpbenadering is de betrokkenheid van het management. Deze moet aanwezig zijn voor elke fase van de safety lifecycle. Het management is verantwoordelijk voor:

> het vaststellen van het beleid en de strategie ten aanzien van veiligheid,
> het evalueren van de resultaten ten aanzien van veiligheid,
> het organiseren van de communicatie binnen de organisatie,
> het opzetten van een veiligheidsmanagementsysteem dat er voor zorgt dat daar waar safety instrumented systemen worden gebruikt, het personeel in staat is om het proces in een veilige toestand te brengen en/of te houden,
> het trainen van de personen die betrokken zijn bij activiteiten gedurende de 'safety lifecycle', om er voor te zorgen dat deze competent zijn,
> het implementeren van procedures voor ontwerp-, validatie- en beoordelingsactiviteiten.

Adequate specificaties

Een belangrijke en normatieve eis is het opstellen van de Safety Requirement Specification, SRS genoemd. De SRS is een erg belangrijk document omdat alle relevante gegevens voor elke specifieke SIF, inclusief gedetailleerde gegevens van elk element en een diagram van het Veiligheidscircuit, verzameld en opgenomen moeten worden.

Eisen aan de Safety Requirement Specificaties zijn dat deze duidelijk, precies, verifieerbaar, onderhoudbaar en haalbaar moeten zijn. De specificaties moeten zo geschreven zijn dat ze gemakkelijk te begrijpen zijn voor degenen die er mee werken. De specificaties moeten alle fasen van de 'safety lifecycle' omvatten.

De veiligheidseisen (SRS: 61511-1, 10.3.1) moeten bijvoorbeeld de volgende onderdelen bevatten:
> Een beschrijving van de safety instrumented function
> Een definitie van de veilige toestand van het proces
> De responsietijd voor een safety instrumented function om een proces in een veilige toestand te brengen
> De wijze van bedrijfsvoering (op afroep/continu)
> Uitschakelen (of in sommige gevallen, bekrachtigen) om het proces stil te leggen
> De eisen voor het resetten van de SIS na een shutdown
> De eisen aan de software
> De omgevingsomstandigheden (temperatuur, EMC, schokken, trillingen, elektrostatische ontlading)
> Common cause (beta factor) gegevens
> Tijdsduur van de verificatiebeproeving
> Gemiddelde tijd nodig om te repareren (MTTR)

In de volgende uitgave van Automatie worden hoofdstuk 3 en 4 van het SIL Platform Position Paper verder uitgewerkt. In deel 2 van dit drieluik leest u alles over storingsgegevens van instrumenten en over het gebruik van de Diagnostic Coverage (DC) factor en de Safe Failure Fraction (SFF). ■

Hans van Dongen (SIS & Alarm Management Guardian Du Pont de Nemours) & André Fijan (Sr. Safety Consultant Fluor BV)
nl.linkedin.com/pub/hans-van-dongen/5/798/2b6
nl.linkedin.com/in/andrefijan

Toepassing SIL

Drieluik SIL Platform Position Paper: deel 2

De toepassing van SIL in de procesindustrie wordt steeds belangrijker. Het SIL Platform is opgericht om de industrie hierbij te ondersteunen. De visie van het platform is verwerkt in een SIL Platform Position Paper om met de industrie te delen. Automatie biedt u deze visie aan als drieluik. In deze uitgave deel 2 over storingsgegevens van instrumenten en over het gebruik van de Diagnostic Coverage (DC) factor en de Safe Failure Fraction (SFF).

Het is de bedoeling van het SIL Platform om een SIL gerelateerd document uit te geven. De doelstelling van het SIL Platform Position Paper is om de markt te informeren en om bewustwording te creëren over specifieke aspecten van het toepassen van SIL in de procesindustrie. Dit document geeft basisinformatie over de implementatie van SIL en de relevante terminologie. Het richt zich vooral op het SIL verificatieproces om de nagestreefde integriteit van SIL circuits vast te stellen. De volgende onderwerpen komen aan bod:

1 Basis van SIL Implementatie
2 Systematische ontwerpbenadering
3 Storingsgegevens van instrumenten
4 Het gebruik van de Diagnostic Coverage (DC) factor en de Safe Failure Fraction (SFF)
5 Hardware safety integrity randvoorwaarden aan de architectuur
6 Verificatiebeproevingen van Safety Instrumented Systems
7 Safety lifecycle management

In deel 2 van dit drieluik worden de hoofdstukken 3 en 4 behandeld. In deel 3 volgen de hoofdstukken 5, 6 en 7.

Over het SIL Platform

Het SIL Platform is een onafhankelijke groep van ervaren gebruikers en aanhangers van de SIL filosofie volgens IEC 61508:2010 en IEC 61511:2003 in de Nederlandse procesindustrie. Het SIL Platform is onderdeel van de Nederlandse normcommissie NEC 65 'Industrieel meten, regelen en automatiseren', die de Nederlandse inbreng in het internationale werk van IEC/TC 65 'Industrial measurement, control and automation' verzorgt. Op dit moment telt het SIL Platform veertig leden. Zij vertegenwoordigen eindgebruikers, ingenieursbureaus, leveranciers, fabrikanten en consultancy bedrijven.
Meer informatie: I www.nen.nl, E rianne.boek@nen.nl

Hoofdstuk 3 Storingsgegevens van instrumenten

Storingsgegevens van instrumenten zijn gegevens van de fabrikant die informatie geven over de te verwachten betrouwbaarheid en integriteit van elk element in een SIF-circuit. Deze informatie bestaat uit vier parameters: gevaarlijke gedetecteerde storingen, gevaarlijke niet-gedetecteerde storingen, ongevaarlijke gedetecteerde storingen en ongevaarlijke niet-gedetecteerde storingen. Deze worden respectievelijk aangeduid met λdd, λdu, λsd, λsu. Deze parameters worden uitgedrukt in het aantal storingen per tijdseenheid (uur of jaar). Storingsgegevens van instrumenten zijn belangrijk, omdat ze worden gebruikt bij het berekenen van de integriteit van de veiligheid van safety instrumented functions.

Valkuilen

De grootste valkuil bij het gebruik van storingsgegevens van instrumenten is het toepassen van de getallen als absolute gegevens. Het gebruik van storingsgegevens van instrumenten vraagt om een beoordeling van de geldigheid van de beschikbare gegevens onder de daadwerkelijk heersende bedrijfsomstandigheden. De volgende aspecten hebben invloed op de geldigheid van de beschikbare gegevens.

Beperkte bronnen

In de praktijk bepalen fabrikanten de storingsgegevens van instrumenten op basis van verschillende bronnen. Bijvoorbeeld de teruggestuurde instrumenten en apparaten. In de praktijk zal echter slechts een klein gedeelte van alle falende instrumenten worden teruggestuurd naar de fabrikant. Dit leidt tot niet-realistische storingsgegevens van instrumenten.

Bedrijfsomstandigheden

Storingsgegevens van instrumenten worden bepaald onder specifieke bedrijfsomstandigheden. Als de daadwerkelijk optredende bedrijfsomstandigheden – zoals de aanwezigheid van chemische stoffen of het optreden van extreme temperaturen – anders zijn dan de bedrijfsomstandigheden waaronder de storingsgegevens zijn bepaald, geven de storingsgegevens geen goede weergave van de werkelijkheid.

Verschil in daadwerkelijk gebruik instrument of apparaat

De storingsgegevens van instrumenten kunnen informatie bevatten die niet relevant is voor het daadwerkelijke gebruik van het instrument of het apparaat. Bijvoorbeeld, een apparaat dat in staat moet zijn om 10^7 maal te schakelen gedurende zijn levenscyclus, zou in het daadwerkelijke gebruik slechts uitgeschakeld hoeven te worden na vijf jaar in bedrijf te zijn geweest. Het is goed denkbaar dat het apparaat in zijn bekrachtigde toestand blijft staan door remanent magnetisme. Het is duidelijk dat voor deze toepassing de storingsgegevens van het instrument niet de relevante informatie verschaffen.

Correct gebruik

Storingsgegevens van instrumenten mogen nooit als absolute gegevens worden opgevat, maar moeten worden gebruikt rekening houdend met alle relevante bedrijfsomstandigheden. Men moet zich er altijd van vergewissen in welke mate de beschikbare instrument storingsgegevens geldig zijn voor de bedrijfsomstandigheden waaronder het instrument of apparaat gebruikt zal gaan worden.

Storingsgegevens van instrumenten moeten worden beschouwd in relatie tot systematische storingen en de Systematic Capability (SC). Systematische storingen zijn storingen die, op een deterministische manier gerelateerd aan bepaalde oorzaken, alleen kunnen worden geëlimineerd door een modificatie van het ontwerp, of het fabricageproces, bedrijfsprocedures, documentatie of andere relevante factoren. De SC wordt gedefinieerd als een maat, zijnde het vertrouwen dat de systematic safety integrity van een element aan de eisen voldoet van de gespecificeerde target SIL, met betrekking tot de gespecificeerde veiligheidsfunctie van het element (wanneer het element/apparaat wordt toegepast volgens de instructies in de betreffende Veiligheidshandleiding voor het element/apparaat). De SC wordt uitgedrukt op een schaal van SIL 1 tot 4 (SC 1 tot 4). De Veiligheidshandleiding, die wordt geleverd door de fabrikant, bevat alle benodigde informatie over een veiligheidselement, hoe het te gebruiken in een specifieke procestoepassing binnen de gegeven specificaties en alle informatie betreffende berekeningen en een beoordeling van de Systematic Capability en FSM (Functional Safety Management).

Elke SIF moet voldoen aan vier in de norm gestelde hoofdeisen ten aanzien van:
Random hardware storingen --> in het totale veiligheidscircuit, uitgedrukt in de PFD waarde, waarmee ook het bereikte SIL niveau wordt aangegeven
Systematische storingen (software, productie, testen en modificaties) --> uitgedrukt in de Systematic Capability (SC 1-4)
Beperkingen ten aanzien van de architectuur --> een normatieve kwaliteitsfactor die betrekking heeft op de storingsgegevens van de hardware
Functional Safety Management (FSM) systeem geïmplementeerd in de productie-eenheden van de producent van de elementen die gebruikt worden in de veiligheidscircuits --> in de praktijk een beoordelingsrapport van de productielocatie dat stelt dat de fabrikant een ISO 9001/2/3 certificaat heeft met uitgebreide modificatie- en product beproevingsprocedures

Hoofdstuk 4 Gebruik DC factor en SFF

De Diagnostic Coverage (DC) factor wordt in IEC 61511-1 (sectie 3.2.15) gedefinieerd als de verhouding van de gedetecteerde storingsfrequentie tot de totale storingsfrequentie van de component of het subsysteem, zoals gedetecteerd door diagnostische tests. De DC omvat geen van de fouten die door verificatiebeproevingen gevonden worden. De formule voor DC is:
DC = (λsd + λdd) / (λsd + λdd + λsu + λdu)

Waarin:

λsd = veilige gedetecteerde storingsfrequentie
λsu = veilige niet-gedetecteerde storingsfrequentie
λdd = gevaarlijke gedetecteerde storingsfrequentie
λdu = gevaarlijke niet-gedetecteerde storingsfrequentie

Voor veiligheidstoepassingen kan het volgende onderscheid worden gemaakt:
DCs = λsd / (λsd + λsu)
DCd = λdd / (λdd + λdu)

De Safe Failure Fraction (SFF) wordt gedefinieerd in IEC 61511-1 (sectie 3.2.65.1) als de fractie van de totale random hardware storingsfrequentie van een apparaat die resulteert in een veilige storing of een gedetecteerde gevaarlijke storing. De SFF wordt op een soortgelijke manier gedefinieerd in IEC 61508-4 (sectie 3.6.15) als een eigenschap van een veiligheidsgerelateerd element dat wordt gedefinieerd door de verhouding van de gemiddelde storingsfrequenties van veilige plus gevaarlijke gedetecteerde storingen en de veilige plus gevaarlijke storingen. Daarom kan de SFF als een soort kwaliteitsfactor worden gezien van de afgeleide storingscijfers. De formule voor SFF is:
SFF = (λsd + λsu + λdd) / (λsd + λdd + λsu + λdu)

Merk op dat het enige verschil tussen DC en SFF de component + λsu is. Voor mechanische apparaten is per definitie DC = 0, en SFF = λsu / (λsu + λdu). In dit geval betekent een hoge SFF een relatief hoge frequentie van oneigenlijk stilleggen van het proces!

Belangrijk

De DC factor wordt gebruikt om de componenten van de totale storingsfrequentie te splitsen in gedetecteerde en niet gedetecteerde componenten. Een aanbieder op de markt kan de DC (of de DCs en DCd) en de totale veilige en gevaarlijke storingsfrequenties publiceren, of hij kan de individuele storingsfrequenties (λsd, λdd, λsu, λdu) publiceren. Het laatste heeft de voorkeur.

De SFF wordt gebruikt om de hardware fout tolerantie te definiëren, dat wil zeggen de vereiste hardware redundantie. Een aanbieder op de markt kan de SFF en de totale veilige en gevaarlijke storingsfrequenties publiceren, maar de individuele storingsfrequenties zouden altijd gepubliceerd moeten worden.

De individuele storingsfrequenties en de DC en SFF factoren worden gebruikt om de gemiddelde waarde van de kans op een storing op afroep te berekenen (Probability of Failure on Demand, PFDavg). Deze waarde toont de integriteit aan van het veiligheidscircuit die de Safety Instrument Function (SIF) uitvoert. Componentstoringen van een SIF kunnen resulteren in een veilige procestoestand, zoals een oneigenlijke shutdown, of een gevaarlijke procestoestand. Componentstoringen van een SIF kunnen wel of niet door de SIF worden gedetecteerd voordat er zich een procesafroep voordoet.

Valkuilen

Gedetecteerde storingen
Wanneer de SFF gebruikt wordt bij SIL verificatie berekeningen, wordt aangenomen dat gevaarlijke gedetecteerde storingen beschouwd kunnen worden als veilige storingen. Dat wil zeggen dat het proces gedwongen naar de veilige toestand wordt gebracht of de operator neemt een alternatieve actie. In de praktijk is dit niet altijd het geval. Een voorbeeld is een zender die automatisch een interne fout detecteert, gewoonlijk BAD_PV genoemd. De vraag is wat het Safety Instrumented System zou moeten doen als er een BAD_PV wordt gedetecteerd. Alarmeren of het proces stilleggen? Het proces stilleggen is veilig, maar deze oneigenlijke stillegacties verminderen de beschikbaarheid van de procesinstallatie. Alarmering kan veilig zijn onder bepaalde voorwaarden. Als de operator tijd en middelen beschikbaar heeft om binnen de procestijd adequaat te reageren op deze kritische alarmen. Als dit niet het geval is, moet het stilleggen van het proces volgen omdat in de berekeningen van de SFF deze aanname is meegenomen.

Nauwkeurigheid van storingsfrequentiegegevens
De storingsfrequentiegegevens, de DC factor(en) en SFF worden gewoonlijk bepaald door de aanbieder van het instrument of op verzoek van de aanbieder van het instrument door onafhankelijke organisaties zoals TÜV of Exida, gebaseerd op

laboratoriumtesten of (mathematische) Failure Modes, Effects & Diagnostics Analysis (FMEDA). Laboratoriumtesten kunnen de storingsfrequentie parameters niet nauwkeurig vaststellen, omdat de real-life voorwaarde van een SIF niet nauwkeurig kan worden gesimuleerd in een laboratoriumtest. In werkelijkheid (real-life) wordt een SIF typisch niet meer dan een keer in de tien jaar geactiveerd (low demand bedrijf) of gedurende verificatiebeproeving met regelmatige intervallen.

FMEDA

De FMEDA is een mathematische benadering, gebaseerd op het instrumentontwerp met standaard componenten en op uitgebreide componentstoringen databases. De invloed van procesomstandigheden, zoals trillingen en temperatuurschommelingen, wordt gewoonlijk niet meegenomen. Effecten van storingen in componenten zijn echter gebaseerd op praktische ervaring binnen de door de aanbieder gespecificeerde bedrijfsomstandigheden. Soms worden de zogenaamde No-effect storingen of No-part storingen ook meegenomen als veilige storingen, gedetecteerd of niet-gedetecteerd. IEC 61508 (2010) vereist expliciet dat deze storingen geen rol spelen in de berekening van de Diagnostic Coverage of de Safe Failure Fraction (IEC-61508-2 (2010), bijlage C). Het is daarom vereist om te verifiëren dat de FMEDA is gebaseerd op de laatste editie.

In de praktijk bewezen

Als alternatief mogen eindgebruikers storingsfrequentiegegevens gebruiken die verzameld zijn uit praktijkervaring of uit commerciële databases en die gebaseerd zijn op praktijkervaring (bijvoorbeeld OREDA), en de DC factor en SFF uit die gegevens afleiden. Helaas is dat alleen mogelijk voor instrumenten die ongeveer tien jaar of langer in gebruik zijn vanwege voor de hand liggende redenen.

Hoe gebruik ik de DC en SFF correct?

> Bij het bepalen van de DC mogen alleen diagnostische tests meegenomen worden die zijn uitgevoerd met de vereiste of hogere frequenties (IEC-61508-2, secties 7.4.4.1.4 en 7.4.4.1.5).

> De DC voor mechanische apparatuur is per definitie 0, en de SFF is λsu / totale storingsfrequentie. Met andere woorden, een hoge SFF impliceert een relatief hoge frequentie van oneigenlijk stilleggen van het proces.

> Als de SFF wordt gebruikt in uw berekeningen, onderzoek dan of gevaarlijke gedetecteerde storingen inderdaad als veilige storingen mogen worden behandeld.

> De SFF en de DC zouden gebaseerd moeten zijn op IEC-61508 Editie 2.0 (2010), omdat deze de No-part en No-effect storingen uitsluit. Anders kunnen de SFF en de DC te optimistische waarden hebben.

In de volgende uitgave van Automatie worden hoofdstuk 5, 6 en 7 van het SIL Platform Position Paper verder uitgewerkt. In deel 3 van dit drieluik leest u alles over hardware safety integrity randvoorwaarden aan de architectuur, verificatiebeproevingen van Safety Instrumented Systems en safety lifecycle management. ■

Rens Wolters (Application Specialist SIL/HIPPS Mokveld Valves BV), Herman Jansen (Senior Safety Consultant ConSILtant) & Willem van der Bijl (Voorzitter SIL Platform & M.D. Produca Consultancy BV) ***Vertaling: NEN***

Toepassing SIL

Drieluik SIL Platform Position Paper: deel 3

De toepassing van SIL in de procesindustrie wordt steeds belangrijker. Het SIL Platform is opgericht om de industrie hierbij te ondersteunen. De visie van het platform is verwerkt in een SIL Platform Position Paper om met de industrie te delen. Automatie biedt u deze visie aan als drieluik. In deze uitgave deel 3 over hardware safety integrity randvoorwaarden aan architectuur, verificatiebeproevingen van Safety Instrumented Systems en safety lifecycle management.

Het is de bedoeling van het SIL Platform om een SIL gerelateerd document uit te geven. De doelstelling van het SIL Platform Position Paper is om de markt te informeren en om bewustwording te creëren over specifieke aspecten van het toepassen van SIL in de procesindustrie. Dit drieluik geeft basisinformatie over de implementatie van SIL en de relevante terminologie. Het richt zich vooral op het SIL verificatieproces om de nagestreefde integriteit van SIL circuits vast te stellen. De volgende onderwerpen komen aan bod:

1. Basis van SIL Implementatie
2. Systematische ontwerpbenadering
3. Storingsgegevens van instrumenten
4. Het gebruik van de Diagnostic Coverage (DC) factor en de Safe Failure Fraction (SFF)
5. Hardware safety integrity randvoorwaarden aan de architectuur
6. Verificatiebeproevingen van Safety Instrumented Systems
7. Safety lifecycle management

In het laatste deel van dit drieluik worden de hoofdstukken 5, 6 en 7 behandeld.

Over het SIL Platform

Het SIL Platform is een onafhankelijke groep van ervaren gebruikers en aanhangers van de SIL filosofie volgens IEC 61508:2010 en IEC 61511:2003 in de Nederlandse procesindustrie. Het SIL Platform is onderdeel van de Nederlandse normcommissie NEC 65 'Industrieel meten, regelen en automatiseren', die de Nederlandse inbreng in het internationale werk van IEC/TC 65 'Industrial measurement, control and automation' verzorgt. Op dit moment telt het SIL Platform veertig leden. Zij vertegenwoordigen eindgebruikers, ingenieursbureaus, leveranciers, fabrikanten en consultancy bedrijven.
Meer informatie: I www.nen.nl, E rianne.boek@nen.nl

Hoofdstuk 5 'Hardware safety integrity' randvoorwaarden aan de architectuur

Editie 2010 van de IEC 61508 definieert twee manieren om de vereiste Hardware Fout Tolerantie (HFT) aan te tonen. Route 1H is geschikt voor elektronische systemen, terwijl route 2H kan worden gebruikt voor zowel elektronische als mechanische apparatuur.

Volgend op de Probability of Failure on Demand (PFD) berekening om te verzekeren dat de PFD van het circuit in lijn is met de vereiste SIL, definiëren de randvoorwaarden aan de architectuur – zoals vastgelegd in de IEC standaard – het aantal elementen in het circuit.

Valkuilen

In methode 1H (IEC 61508-2 sectie 7.4.4.2) wordt de Safe Failure Fraction (SFF) van het systeem gebruikt om de vereiste HFT te definiëren. Zoals hierboven aangegeven, is de SFF niet echt toepasbaar op mechanische toestellen, die gewoonlijk als eindelement voorkomen. De nieuwe definitie van het diagnostische testinterval is specifiek voor elektronische apparatuur en kan niet worden toegepast op mechanische toestellen.

In de 'low demand' situatie is het vereist dat het diagnostische testinterval korter is dan de in de berekening gebruikte Mean Time To Restore (MTTR), minus de tijd om de vastgestelde storing te herstellen. Hoewel als MTTR vaak 8 tot 24 uur wordt gehanteerd, is dit moeilijk te bereiken voor niet-elektronische apparatuur.

Methode 1H definieert de HFT gebaseerd op twee tabellen, een voor apparatuur van type A en de ander voor apparatuur van type B. Volgens IEC 61508-2 (secties 7.4.4.1.2 en 7.4.4.1.3) is de definitie van type A of type B gebaseerd op de complexiteit van het element. Onderdelen met microprocessoren en software zijn van type B. Mechanische apparatuur en elektronische apparatuur zonder microprocessoren en software zijn in principe van type A. Deze selectie kan voor mechanische apparatuur ook afhangen van het gebruik en moet zorgvuldig worden bekeken. Bijvoorbeeld een groot formaat klep/actuator die in tientallen seconden sluit, wordt als type A apparatuur beschouwd. Echter, indien dezelfde apparatuur moet sluiten binnen enkele seconden, zijn er geen betrouwbare storingsgegevens. Dan moet vanwege de toepassing de apparatuur geclassificeerd worden als apparatuur van type B.

Zodra de SFF en het type A of B zijn gedefinieerd, kan de vereiste HFT van het apparaat in de tabel worden gevonden.

Correcte realisatie

De nieuwe methode 2H (IEC 61508-2 sectie 7.4.4.3) is gebaseerd op eerder gebruik of op het feit dat deze in de praktijk is bewezen, zoals ook is omschreven in IEC 61511 versie 2003. In toepassingen die een SIL 3 (in de high demand of de low demand situatie) of een SIL 2 (alleen in de high demand situatie) vereisen, is een HFT van 1 – en dus een 1oo2 configuratie – vereist (wanneer het element zich in de praktijk heeft bewezen).

Hoewel de term 'in de praktijk bewezen' heel duidelijk is, geeft de IEC specifieke eisen (IEC 61508-2, sectie 7.4.10). Om het 'gebruik te bewijzen', moeten statistische gegevens beschikbaar zijn voor dezelfde toepassing, hetzelfde procestype of toepassingsprofiel, en alle aspecten van de toepassing en veiligheidsmissie moeten worden geverifieerd. Bijvoorbeeld in het geval dat storingsgegevens beschikbaar zijn, gebaseerd op normale bediening of op normaal schakelgedrag en de toepassing vereist nu dat het onderdeel voor langere tijd in dezelfde positie blijft, kan de term 'in de praktijk bewezen' niet langer worden gebruikt.

Het laatste deel is feitelijk ook van toepassing op methode 1H waar gerelateerde storingsgegevens vereist zijn (IEC 61508-2, sectie 7.4.9.3). Gerelateerd betekent dat dat er voldoende vertrouwen moet zijn dat de apparatuur geschikt is voor de toepassing.

Hoofdstuk 6 Verificatiebeproevingen van Safety Instrumented Systems

Verificatiebeproevingen zijn periodieke tests om gevaarlijke verborgen storingen in een veiligheidssysteem aan te tonen. Verificatiebeproevingen zullen niet gedetecteerde storingen (als deze er zijn) in een Safety Instrumented System aan het licht brengen, zodat indien nodig het systeem (zo snel mogelijk) kan worden hersteld naar de oorspronkelijk ontworpen functionaliteit.

Valkuilen

Gebruik van software rekentools

Sommige geavanceerde PFD software rekenprogramma's kunnen de consequenties van een Proof Test Coverage factor (PTC) < 100 % berekenen, zowel de PTC als de levensduur van de SIF moet ingevoerd worden.
Het is echter mogelijk dat het mathematische model niet volledig de werkelijke situatie weergeeft, omdat een ontoereikende PFD als gevolg van gebrekkige tests in het mathematische model, gecompenseerd kunnen worden door frequentere (gebrekkige) verificatiebeproevingen.

Correcte uitvoering

Test interval

Het interval van de verificatiebeproevingen is gerelateerd aan de gemiddelde PFD van de SIF. Om te voldoen aan de eisen van

de vastgestelde target SIL van een SIF, mag het interval van de verificatiebeproevingen de testperiode die in de berekeningen is gebruikt, niet overschrijden. Gebruikelijk zijn één, twee, drie of vier jaar.

Tests

Een volledige functionele verificatiebeproeving (PTC van 100%, dat is een volledige proces-tot-proces test) moet altijd de doelstelling zijn. Sensoren moeten getest worden, indien mogelijk door het variëren van de proceswaarde. Indien gescheiden kanalen worden gebruikt, moeten voor elk kanaal afzonderlijke tests worden uitgevoerd.

Indien lekkage van kleppen tot een gevaarlijk scenario leidt, moet de mate van afsluiting van de klep ook aan een verificatiebeproeving onderworpen worden. Als het proces veiligheidstijdkritisch is, moet de SIF responsetijd ook getest worden.

Correcte realisatie

Safety Requirements Specification (SRS)

De Safety Requirements Specification moet behalve de standaard ontwerpoverwegingen, ook de eisen, beperkingen, functies en voorzieningen van iedere SIF bevatten om het periodieke verificatiebeproeven van elke SIF mogelijk te maken. Het interval van de verificaiebeproeving moet worden gedefinieerd, gebaseerd op onderhoudsprocedures en PFD berekening. In het bijzonder, wanneer online verificatiebeproeven vereist is, moeten testvoorzieningen een integraal onderdeel zijn van het SIF ontwerp om het mogelijk te maken te testen op niet gedetecteerde storingen.

Als test- en/of bypassvoorzieningen in de SIF zijn opgenomen, moeten deze aan twee voorwaarden voldoen.

Ten eerste moet de SIF worden ontworpen in overeenstemming met de onderhouds- en testeisen gedefinieerd in de Safety Requirement Specification. Ten tweede moet de operator gewezen worden op elke bypass die onderdeel vormt van de SIF middels een alarm- en/of een werkprocedure. Het gebruik van bypasses moet zoveel mogelijk worden voorkomen.

Procedures voor onderhoud en verificatiebeproevingen

Verificatiebeproevingen moeten gedocumenteerd zijn in de onderhoudsprocedures, met inbegrip van:

- Wanneer verificatiebeproevingen moeten worden uitgevoerd.
- De acties die moeten worden uitgevoerd voor de verificatiebeproeving van een SIF. Voor elke SIF moeten geschreven, gedetailleerde procedures voor de verificatiebeproeving worden ontwikkeld om alle gevaarlijke storingen te vinden. Deze geschreven testprocedures moeten elke stap omschrijven die moet worden uitgevoerd, en moeten de correcte werking van elke sensor en eindelement, logische acties en alarmen en signaleringen bevatten. De ontwikkeling van de procedures voor de verificatiebeproeving is een zeer belangrijke multidisciplinaire maatwerkactiviteit, en moet voorafgaand aan de initiële inbedrijfstelling worden uitgevoerd.
- De acties en beperkingen die nodig zijn om een onveilige toestand te voorkomen en/of de gevolgen van een gevaarlijke gebeurtenis tijdens onderhoud of bedrijfsvoering. Bijvoorbeeld, welke aanvullende beperkende maatregelen moeten worden toegepast wanneer het nodig is om een systeem te bypassen voor testen of onderhoud?
- Kalibratie van sensoren.
- Testapparatuur die gebruikt wordt tijdens normale onderhoudsactiviteiten, wordt op de juiste manier gekalibreerd en onderhouden.

Correcte uitvoering geschikte verificatiebeproevingen Safety Instrumented Systems

Verificatiebeproeven

Periodieke verificatiebeproevingen moeten worden uitgevoerd volgens de beschreven en goedgekeurde procedures voor de verificatiebeproeving. De totale SIF moet worden getest, met inbegrip van sensoren, logische verwerkingseenheid en eindelement(en). Verschillende onderdelen van de SIF kunnen verschillende testintervallen nodig maken, bijvoorbeeld, de logische verwerkingseenheid kan een ander testinterval vereisen dan de sensoren of eindelementen. Elke onvolkomenheid die wordt gevonden tijdens het verificatiebeproeven, moet op een veilige en tijdige manier worden gerepareerd.

Elke verandering aan de applicatielogica vereist volledig verificatiebeproeven. Uitzonderingen hierop zijn toegestaan indien een geschikte beoordeling en testen van het gewijzigde deel uitgevoerd wordt om te verzekeren dat de veranderingen correct zijn uitgevoerd.

Gedurende de verificatiebeproeving dient de SIF ook visueel geïnspecteerd te worden, om te verzekeren dat er geen ongeautoriseerde wijzigingen en geen merkbare beschadigingen zijn (ontbrekende bouten of instrumentafdichtingen, roestende steunen, losse draden, gebroken buizen, defecte leidingverwarming en ontbrekende isolatie).

Documentatie verificatiebeproeving

De resultaten van elke verificatiebeproeving moeten worden vastgelegd om aan te tonen dat verificatiebeproevingen en inspecties zijn uitgevoerd zoals vereist. Deze rapporten moeten minimaal de volgende informatie bevatten:

- Beschrijving van de uitgevoerde testen en inspecties
- Datums van de testen en inspecties
- Naam van de persoon/personen die de testen, verificaties en inspecties hebben uitgevoerd
- Serienummer of een andere unieke identificatie van het geteste systeem (circuitnummer, labelnummer, apparaat-nummer, SIF-nummer)
- Resultaten van de testen en inspectie ('zoals aangetroffen' en 'zoals achtergelaten' condities)
- Corrigerende acties, indien deze er zijn
- Ondertekend bypass document, met datum en tijd dat de bypasses zijn aangebracht en verwijderd.

Hoofdstuk 7 Safety lifecycle management

De safety lifecycle omvat volgens de definitie in de norm de periode die begint met het conceptontwerp tot aan het moment dat het veiligheidssysteem buiten bedrijf wordt gesteld. De integriteit van een veiligheidssysteem wordt in eerste instantie bepaald tijdens de ontwerpfase. Deze integriteit zou in gevaar kunnen worden gebracht tijdens elke andere fase van de levenscyclus van het systeem, bijvoorbeeld tijdens de operationele fase. Safety lifecycle management garandeert dat de integriteit van een veiligheidssysteem behouden blijft gedurende alle fases van de levenscyclus van het systeem of installatie.

Valkuilen

Te weinig aandacht voor integrale veiligheid in latere fases in de levenscyclus

Wanneer het management besluit om de SIL filosofie over te nemen, wordt de meeste inspanning besteed aan het ontwerp en tijdens de installatiefase. Na de inbedrijfstelling en het opstarten begint de langste periode met een belangrijke SIL focus, de operationele fase. Het veiligheidscircuit wordt vaak niet met dezelfde accuratesse geïnspecteerd, getest en onderhouden als tijdens de ontwerpfase.

Overschrijden van testintervallen

Testen worden uitgevoerd om het adequaat functioneren van de SIP aan te tonen. Het testinterval is direct gerelateerd aan de PFD waarden van het veiligheidscircuit. Het uitstellen van de test buiten de oorspronkelijke testintervallen veroorzaakt direct een onacceptabel risico in dit circuit.

Correcte realisatie

Foutanalyse

Wanneer de test een storing laat zien, is het belangrijk om uit te zoeken wanneer de storing voor het eerst optrad en wat deze veroorzaakt heeft. Hiervoor is een gedetailleerde analyse nodig. Zijn er andere apparaten in de installatie die mogelijk hetzelfde probleem hebben?

Reparaties

De verificatiebeproeving is een periodieke test die wordt uitgevoerd om gevaarlijke verborgen storingen in een veiligheidssysteem aan het licht te brengen. Reparatie is noodzakelijk om het veiligheidssysteem te herstellen tot een volledige functionele toestand. Wees ervan bewust dat de effectiviteit van de verificatiebeproeving afhankelijk zal zijn van zowel het afdekken van de storingen als de effectiviteit van de reparatie. In de praktijk wordt het ontdekken van 100% van de verborgen gevaarlijke storingen niet eenvoudig bereikt. De doelstelling zou moeten zijn dat alle veiligheidsfuncties gecontroleerd worden in overeenstemming met de E/E/PE Safety Requirement Specification.

‘De toepassing van SIL vereist een continue en doorlopende activiteit gedurende de gehele levenscyclus van de procesinstallatie.’

Bedrijfsbeleid

Het is belangrijk om bedrijfsprocedures te hebben om SIL verificatiebeproevingen in te bouwen als de standaard praktijk binnen de betrokken afdelingen. Ten slotte willen we stellen dat de toepassing van SIL een continue en doorlopende activiteit vereist gedurende de gehele levenscyclus van de procesinstallatie. ■

AUTEURS

Willem van der Bijl	CH 01 & 07	Safety Consultant & M.D.	PRODUCA Consultancy BV
Henrie Verwey	CH 02	Sr. Safety Consultant	Verwey Safety Services
Hans van Dongen	CH 03	SIS & Alarm Management Guardian	Du Pont de Nemours
André Fijan	CH 04	Process Control & Safety Engineer	Fluor BV
Rens Wolters	CH 05	Application Specialist SIL/HIPPS	Mokveld Valves BV
Herman Jansen	CH 06	Process Safety Consultant	Consiltant BV

SIL Platform