▽ De sluis van Terneuzen, echter niet die uit het praktijkvoorbeeld.

10 jaar SIL en PL in machinebouw

Rekentools bieden niet de gewenste veiligheid

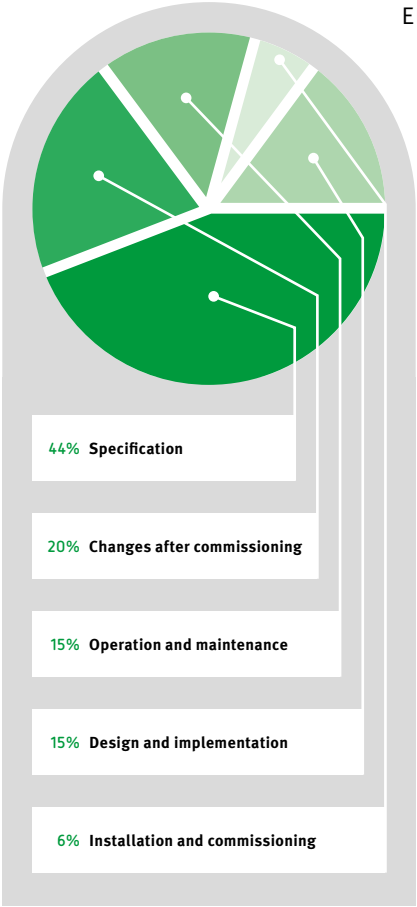
De machinebouw heeft nu zo'n kleine 10 jaar ervaring met de toepassing van de EN 62061 en/of de EN-ISO 13849-1 voor functionele veiligheid. Maar veel engineeringsbedrijven worstelen nog altijd met de toepassing van PL en SIL, zo blijkt uit het praktijkvoorbeeld in dit artikel. ▷ Ing. Nick de With

In 2005 werd de EN 62061 aangenomen, een jaar later de EN-ISO 13849-1. Deze normen classificeren respectievelijk het veiligheidsniveau in een Safety Integrity Level (SIL) en een Performance Level (PL). Beide zijn kort daarna geharmoniseerd onder de Machinerichtlijn 2006/42/EG. Toepassing ervan geeft het zogenaamde 'vermoeden van overeenstemming'.

Oorzaak falen machinebesturing

In het verleden werden machinebesturingen veelal uitgevoerd in elektromechanische relais, maar tegenwoordig wordt gebruikgemaakt van PLC- of PC-systemen met of zonder remote I/O. Ofschoon dergelijke systemen op dit moment als betrouwbaar worden ervaren, heeft bijna elke engineer of onderhoudsman wel eens meegemaakt dat een machine onverwacht opstartte of een onverwachte beweging maakte.

Door de Engelse Arbeidsinspectie HSE zijn 34 gevallen onderzocht van een falend besturingssysteem. Uit het onderzoek 'Out of Control' blijkt dat meer dan 75 procent van de fouten in de specificatie-, ontwerp- en installatiefase van het veiligheidscircuit ontstaan (zie figuur 1). Een webversie van deze publicatie is gratis te downloaden via www.hse.gov.uk/pubns/priced/hsg238.pdf. Uit resultaten van het onderzoek blijkt dat behalve 'random hardware' fouten (defect in hardware component), het merendeel van de fouten een systematisch karakter heeft. Je kunt dus stellen dat deze 'systematische' fouten onbewust door de mens aan het veiligheidscircuit worden toegevoegd. De oorzaken zijn verschillend van aard, maar kunnen bijvoorbeeld liggen in een onduidelijke vastlegging van de functionaliteit/timing van de veiligheidsfunctie, een onjuiste risicoanalyse, onduidelijke documentatie, bugs in de applicatie software enzovoorts.



Figuur 1 Hoofdoorzaken van falen in besturingssystemen ▷ *(bron: 'Out of Control' van Health and Safety Executive (HSE) United Kingdom)*

Getallengoochelaars

Er zijn op dit moment diverse marktpartijen, zoals trainingsinstituten en productleveranciers, die een SIL/PL-training aanbieden, waarbij wordt geleerd hoe de kans op gevaarlijk falen per uur (Probability of Dangerous Failure Hour, PFH_d) kan worden berekend. Voor de berekening van deze PFH_d is in beide normen voor elk type architectuur een aantal basisformules voorhanden. Bijvoorbeeld, de formule uit EN 62061 voor een niet-redundant systeem kan worden berekend met de formule $PFH_d = \lambda_{DU} \times 1h$. Hierbij is λ_{DU} de faalfrequentie van de gevaarlijke niet gedetecteerde fouten (DU = dangerous undetected).

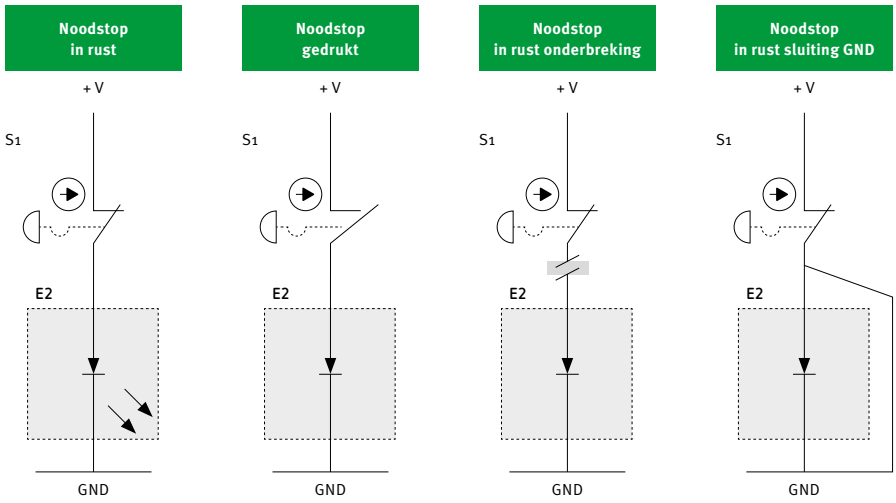
Er zijn intussen diverse softwaretools voorhanden waarmee de SIL/PL berekeningen kunnen worden gemaakt. De bekende tools zijn de Siemens Safety Evaluation Tool, de Pilz PAScal Safety Calculator en de IFA SISTEMA tool. Een aantal tools wordt kosteloos ter beschikking gesteld en een aantal tegen geringe kosten. De Pilz tool PAScal en de Siemens tool SET kunnen behalve de SIL-berekening ook de PL-berekening uitvoeren.

Veel adviesbureaus en bedrijven storten zich nu op de SIL/PL berekening met een dergelijke tool, maar vergeten de systematische fouten die in het ontworpen veiligheidscircuit kunnen sluipen. Na de uitleg van systematische fouten hieronder zal een echt voorbeeld uit de dagelijkse praktijk worden besproken. ▶

Systematische fouten

Een systematische fout is in veel gevallen een verborgen fout in het ontwerp of de implementatie van het ontwerp. Systematische fouten kunnen zowel in hard- als software en in elke fase van de levenscyclus van veiligheidssysteem optreden. Enkele voorbeelden zijn de keuze van een verkeerde ontwerpschakeling uit de leverancierscatalogus, het niet afzekeren van veiligheidscontacten van een veiligheidscircuit of het terugplaatsen van een foutieve zekering na een storing.

Systematische fouten kunnen permanent aanwezig zijn of alleen onder bepaalde omstandigheden optreden (intermitterende systematische fout). Een voorbeeld van een permanent aanwezige fout is een programmeerfout in het veiligheidsprogramma. De veiligheidsfunctie moet worden uitgevoerd als 'A of B' optreedt, terwijl de programmeur 'A en B' heeft geprogrammeerd. Als er geen test is gespecificeerd, zal deze fout altijd in de software blijven zitten.



Figuur 2 Eenkanalig noodstopcircuit volgens ruststroomprincipe *(bron: Training praktische toepassing van SIL en PL, FUSACON)*

Een intermitterende fout treedt daarentegen alleen op in bepaalde omstandigheden. Als die omstandigheden verdwijnen, zal de veiligheidsfunctie weer normaal functioneren. Een voorbeeld hiervan is een 'bus communication overload' in een veiligheidsveldbus. De veldbus is om een bepaalde reden overbelast en de veiligheidsfunctie is tijdelijk niet beschikbaar. Wanneer de overload verdwijnt, is alles weer normaal.

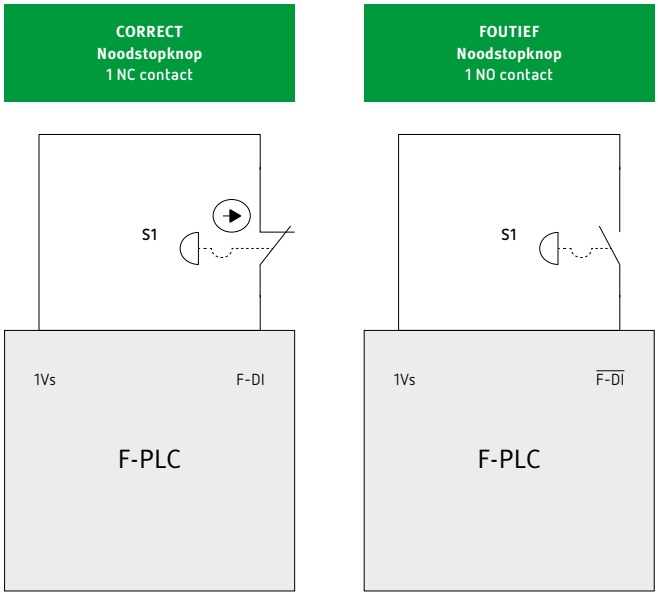
Noodstopcircuit

Een eenkanalig noodstopcircuit werkt op basis van het ruststroomprincipe. Dit is een beproefd principe en het betekent dat normaal (in rust) stroom loopt door het noodstopcontact (zie figuur 2).

Het noodstopcircuit is voor de eenvoud even voorgesteld als een noodstopknop met een LED lamp (lees: motor van de machine). De uitleg volgt van links naar rechts. Als de noodstopknop is uitgetrokken, is het verbreekcontact gesloten en loopt er stroom en licht de LED lamp op. Als de noodstop wordt ingedrukt, opent het verbreekcontact en wordt de stroom verbroken en gaat de lamp dus uit. Ook bij een onderbreking in de kabel gaat de lamp uit. Ook bij een sluiting naar de aarde (GND) onder het verbreekcontact gaat de lamp uit. Met andere woorden, het noodstopcircuit reageert op een onderbreking van de stroom door het contact en ook een sluiting naar aarde.

Als een noodstop wordt gekoppeld aan een veiligheids-PLC is er sprake van signaalbewaking over het contact. Het contact wordt dan gevoed vanuit de fail-safe ingangskaart met een pulserend signaal (1Vs). De signaalvorm wordt teruggelezen op een fail-safe digitale ingang en bewaakt. Hierdoor worden behalve onderbrekingen ook sluitingen naar een vreemde spanning vroegtijdig gedetecteerd.
In figuur 3 is in het linkervoorbeeld een noodstopknop met een verbreekcontact getekend en in het rechtervoorbeeld een noodstopknop met een maakcontact. Het linkervoorbeeld is correct, omdat dit werkt volgens het ruststroomprincipe en door de signaalbewaking alle fouten, uitgezonderd een overbrugging in de kabel, worden gedetecteerd.

Bij het rechtervoorbeeld moet het ingangssignaal in de logica geïnverteerd worden om de goede werking te krijgen. Deze aansluitmethode is om meerdere redenen niet correct. Ten eerste, de werking van het maakcontact berust op het arbeidsstroomprincipe. Ten tweede, een noodstopschakelaar heeft alleen mechanisch gedwongen verbreekcontacten. De juiste werking van maakcontacten is niet gegarandeerd. Ten derde, bij een onderbreking in de kabel zal bij indrukking van de noodstop geen afschakeling meer volgen. En tot slot wordt een sluiting naar de plus of naar de



Figuur 3 Eenkanalig noodstopcircuit op fail-safe PLC *(bron: Training praktische toepassing van SIL en PL, FUSACON)*

Over de Auteur

Ing. Nick de With is TÜV Certified Functional Safety Engineer en als Senior Consultant werkzaam bij Fusacon B.V. Hij is docent bij NEN en lid van de Nederlandse normcommissie NEC 44 en de internationale werkgroep IEC TC44/WG7. Meer informatie: www.fusacon.nl

aarde aan de onderzijde van de schakelaar pas gedetecteerd bij indrukking.

Praktijkvoorbeeld

Onlangs had een elektrotechnisch aannemer voor een bestaande sluis een nieuwe besturing met noodstopcircuit gebouwd. Het circuit bestond uit een noodstopknop met één verbreek- en één maakcontact, elk aangesloten op een fail-safe digitale ingang van een veiligheids-PLC (zie de middelste tekening in figuur 4). Het systeem werd door de aannemer doorgerekend met een softwaretool en zou volgens de aannemer makkelijk voldoen aan SIL 2.

De auditor van de opdrachtgever keurde het bewuste noodstopcircuit af en stelde voor dat de aannemer het circuit zou uitvoeren volgens het linkerplaatje van figuur 4. Bij het linkerplaatje wordt elk verbreekcontact vanuit de fail-safe PLC gevoed met een eigen dynamisch signaal, waardoor behalve onderbrekingen en vreemde spanningen ook een onderlinge sluiting tussen de 2 contacten vroegtijdig wordt gedetecteerd. De foutdiagnose is erg hoog en wordt door de fabrikant van de veiligheids-PLC gezet op een diagnostic coverage (DC, red.: dekkingsgraad van de foutanalyse) van groter dan 90 procent.

Het middelste schema uit figuur 4 kent de volgende problemen ten opzichte van het linkerschema. Deze aansluitmethode is om meerdere redenen niet correct. Ten eerste, de werking van het maakcontact berust op het arbeidsstroomprincipe. Ten tweede, een noodstopschakelaar heeft alleen mechanisch gedwongen verbreekcontacten. De juiste werking van maakcontacten is niet gegarandeerd. Ten derde, bij een onderbreking in de kabel van het maakcontact wordt dit niet vroegtijdig gedetecteerd. Ten vierde, een sluiting naar de plus of naar de aarde aan de onderzijde van de schakelaar wordt pas gedetecteerd bij indrukking. En tot slot, de aansluitmethodiek komt niet overeen met de user manual van de fail-safe digitale ingangskaart en de applicatievoorbeelden die de fabrikant ter beschikking stelt. Conclusie: het middelste schema uit figuur 4 resulteert slechts in een eenkanalig noodstopcircuit. Het rechterschema is helemaal foutief, omdat hier beide noodstopknoppen uitgevoerd zijn met een maakcontact.

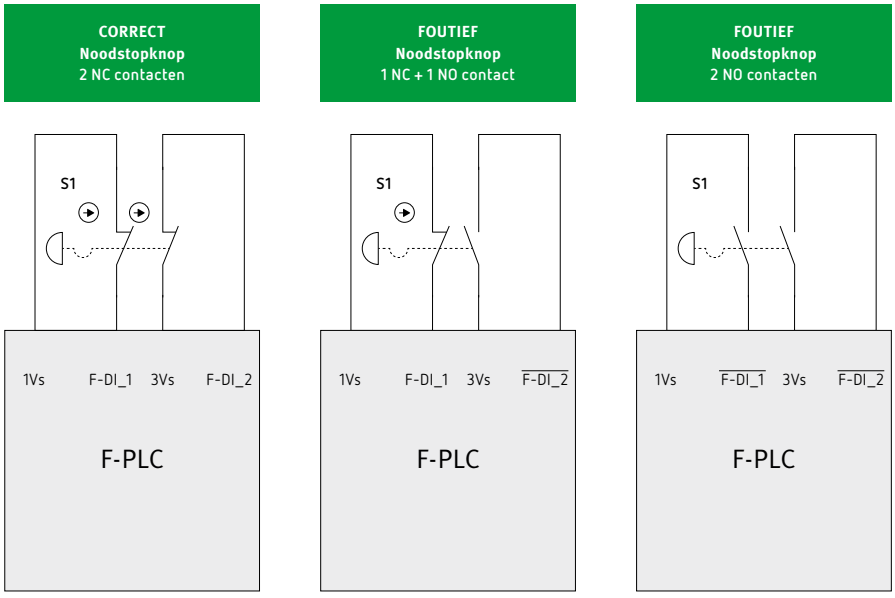
De aannemer bleef, ook na uitleg van de bovengenoemde problemen, bij hoog en bij laag volhouden dat de SIL rekensom klopt en dat de tweekanalige noodstop uit het middelste plaatje zonder problemen voor SIL 2 kan worden toegepast. Hij werd hierbij ondersteund door het ingenieursbureau dat de calculatie had uitgevoerd. Het is duidelijk dat de adviseur van het ingenieursbureau een zogenaamde ‘getallengoochelaar’ is, die de uitkomst van de SIL rekentool als ‘heilig’ verklaart.

Conclusie

Bij een veiligheids-PLC horen vaak meerdere gebruiks- en toepassingshandleidingen die door een Europese Notified Body, zoals TÜV Rheinland, IFA, AIB Vincotte, worden gecontroleerd op juistheid. Pas als de handleiding ook correct is, ontvangt de fabrikant op een component een EG-typegoedkeuring onder de Machinerichtlijn 2006/42/EG.

Bij onderzoek van de user manual van de digitale ingangskaart en de applicatie manual van de veiligheids-PLC bleek dat een tweekanalige noodstop werd afgedrukt als de linkertekening in figuur 4. Met toepassing van het middelste schema door de aannemer vervalt daarom de certificatie door de Notified Body van de fail-safe kaart. Hierdoor voldoet de oplossing niet aan het vereiste SIL-level, SIL 2.

Het bovenstaande voorbeeld is duidelijk een systematische ontwerpfout gebaseerd op een eigen interpretatie van veiligheid door de aannemer en het ingenieursbureau. Een opdrachtgever dient bij de audit van complexe veiligheidssystemen niet alleen te kijken naar de SIL berekening, maar ook naar de juiste toepassing van de componenten. ■



▽ Figuur 4 Tweekanalig noodstopcircuit op fail-safe PLC *(bron: Training praktische toepassing van SIL en PL, FUSACON)*