Een standaard-PLC voor veiligheidsfuncties?

[tekst] **Lilian Vermeer**

Kun je een standaard-PLC inzetten voor veiligheidsfuncties, of moet dit altijd een veiligheids-PLC zijn? De veiligheidsnormen EN-ISO 13849-1:2008 en EN-IEC 62061 moeten op dit gebied duidelijkheid geven, maar dit blijkt in de praktijk lastig te zijn. "EN-ISO 13849-1 en de voorbeelden die het Duitse Institut für Arbeitsschutz heeft opgesteld om deze norm toe lichten, wekken de indruk dat een standaard-PLC is in te zetten voor veiligheidsfuncties. Dat is vaak niet verstandig", zegt Nick de With van Fusacon. Dat vinden ook andere deskundigen.

De standaard-PLC heeft al vele jaren een plaats in de automatiseringstechniek en kon op nagenoeg alle fronten de conventionele bedradings- en schakeltechniek verdringen. Dat kwam door een aantal belangrijke voordelen van een PLC ten opzichte van conventionele schakeltechniek zoals flexibiliteit, veelvuldige diagnosemogelijkheden en een geringere bedradingstijd en -moeite.

Tot ongeveer 1995 golden deze voordelen in de machinesector alleen voor het niet-veiligheidsgerelateerde deel van een besturing. De vele veiligheidsfuncties (noodstop, tweehandenbediening, hekbewaking, personendetectiesystemen enzovoorts) moesten op grond van de norm EN 60204-1:1997 zijn uitgerust met elektromechanische onderdelen met vaste bedrading. Enkele onderdelen, zoals logische eenheden voor tweehandenbediening, moesten volgens de oude Machinerichtlijn (98/37/EG) door een aangemelde instantie (Notified Body of NoBo) worden gecontroleerd. De NoBo voert dan een zogenaamd EG-typegoedkeuring uit op de veiligheidscomponent.

> PLC biedt belangrijke voordelen

In de loop der jaren hebben diverse leveranciers een aparte veiligheids-PLC ontwikkeld die het veiligheidsgerelateerde deel van een besturing kan uitvoeren. De nieuwe Machinerichtlijn (2006/42/EG) paste zich aan deze nieuwe ontwikkelingen aan en stelt dat nu alle veiligheidscomponenten met 'interne logica' (Bijlage IV punt 21), die afzonderlijk in de handel worden gebracht, moeten worden gecontroleerd door een Notified Body. Voorbeelden zijn de traditionele veiligheidsrelais, diverse programmeerbare veiligheidscomponenten, zoals veiligheids-PLC's, veilige frequentieregelaars, veiligheidsveldbussen, et cetera.

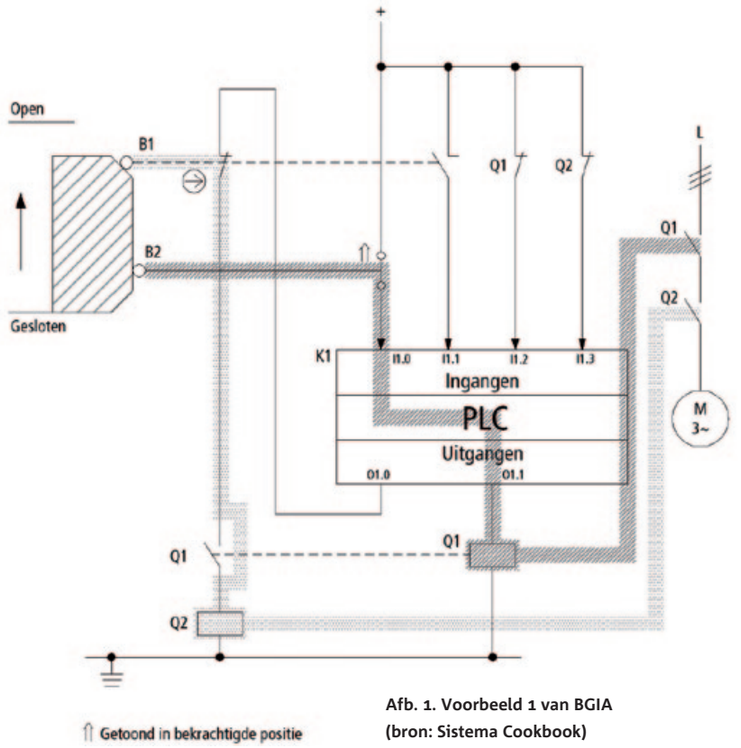
Normen en veiligheidssystemen

Om na te gaan welke eisen worden gesteld aan onderdelen van besturingssystemen met een veiligheidsfunctie in de machinesector (zoals de veiligheids-PLC) zijn verschillende normen te raadplegen: de normenreeks EN-IEC 61508 deel 1 tot en met 7, EN-ISO 13849-1:2008 en EN-IEC 62061.

In 2000 ontwierp de International Electrotechnical Commission (IEC) EN-IEC 61508, een uitgebreide internationale norm voor functionele veiligheid van elektrische/elektronische/programmeerbare elektronische systemen. De norm bestaat uit zeven delen (totaal 740 pagina's) en on-

De standaard-PLC heeft al vele jaren een plaats in de automatiseringstechniek. Hij is echter oorspronkelijk niet ontworpen voor veiligheidstechnische functies (foto: Rockwell Automation)

18-21_veiligheidplc.indd 18 02-10-13 09:21



Afb. 1. Voorbeeld 1 van BGIA (bron: Sistema Cookbook)

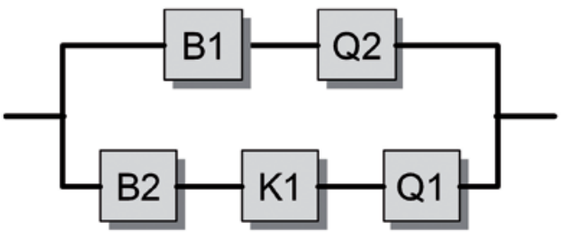
derkent vier SIL-niveaus (SIL 1 tot en met SIL 4). Elk SIL-niveau komt overeen met een bepaalde 'Probability of dangerous Failure per Hour' (PFHd, kans op gevaarlijk falen per uur). Hoe hoger het SIL-niveau, des te kleiner de kans dat het systeem faalt. Deze norm moet worden gezien als 'basic safety' publicatie voor normmakers. De procesindustrie heeft sinds 2003 een afgeleide versie ervan, EN-IEC 61511. Ook de machinesector heeft haar eigen norm, EN-IEC 62061 uit 2005.
Beide sectornormen beschrijven de eisen waaraan de veiligheidsapplicatie moet voldoen en verwijzen producenten van programmeerbare veiligheidscomponenten voor embedded software door naar de moedernorm EN-IEC 61508. Dit betekent dat de SIL-normen eisen dat, indien gebruik wordt gemaakt van programmeerbare componenten, deze moeten voldoen aan de eisen uit EN-IEC 61508.
Na de introductie van de faalkansberekening in EN-IEC 61508 besloot ook de International Organization for Standardization (ISO), vooral bekend van de mechanische normen, om deze methodiek op te nemen in de opvolger van ISO 13849-1:1999 (de ISO versie van EN 954-1:1996). Deze nieuwe ISO-norm, EN-ISO 13849-1:2008, voert naast een systeemgedrag ook een faalkansberekening in op basis van kwaliteit en zelfdiagnose. Zo zijn ook elektronica en software toe te passen in veiligheidsfuncties van machinebesturingen. Deze norm specificeert voor het gewenste veiligheidsniveau geen SIL-niveau maar een prestatieniveau, een 'performance level' (PLa, PLb, PLc, PLd of PLe).
De norm vereist alleen voor programmeerbare veiligheidscomponenten met het hoogste niveau (PLe) toepassing van EN-IEC 61508. Voor de lagere PL-niveaus is in hoofdstuk 4.6.3 een korte opsomming gegeven van de eisen waaraan systemen met embedded software moeten voldoen. Deze eisen zijn een vereenvoudigd aftreksel van de eisen uit EN-IEC 61508 deel 3 over embedded software.

Verschillende normen raadplegen

Voor onderdelen van besturingssystemen met een veiligheidsfunctie in de machinesector kunnen fabrikanten dus twee normen raadplegen: EN-ISO 13849-1:2008 (PL-norm) en de EN-IEC 62061:2005 (SIL-norm). In de praktijk ziet bijvoorbeeld Stephen Podeveyn van Rockwell Automation dat het grootste deel van zijn klanten (zo'n 80-85%) de PL-norm gebruikt en de rest voor SIL kiest. "Het is wat je gewend bent vanuit het bedrijf, maar in de praktijk maakt het niet uit."
Ook Wouter Leusden van Bosch Rexroth ziet een voorkeur voor de PL-norm: "Dat komt omdat wij behalve veiligheidscomponenten ook veiligheidsgerelateerde systemen ontwerpen voor hydrauliek en pneumatiek waarbij de SIL-norm niet bruikbaar is. De PL-norm leent zich voor alle aandrijfdisciplines die in een veiligheidsketen zijn verwerkt. Bij hydraulische of pneumatische aandrijvingen is de veiligheid van de gebruiker immers niet alleen afhankelijk van de goede werking van elektrische componenten maar ook van de hydraulische of pneumatische componenten."

Sistema kookboek

Voor de PL berekeningen heeft het Duitse Institut für Arbeitsschutz (IFA, voorheen BGIA genaamd) de Sistema softwaretool ontwikkeld. Deze tool (zie kader 1) biedt ontwerpers en controleurs van veilig-



Afb. 2 . Designated architecture van afbeelding 1 (bron: Sistema Cookbook)

Overzicht belangrijke links Sistema

SW tool	www.dguv.de/ifa/en/pra/softwa/sistema/index.jsp
Cookbook	www.dguv.de/ifa/en/pra/softwa/sistema/kochbuch/index.jsp
Examples	www.dguv.de/ifa/en/pra/bilder/circuit_examples.zip
Libraries	www.dguv.de/ifa/en/pra/softwa/sistema/bibliotheken/index.jsp

Voorbeeld 1, cookbook = voorbeeld 18 IFA report
www.dguv.de/ifa/en/pub/rep/pdf/rep07/biar0208/rep22008e.pdf

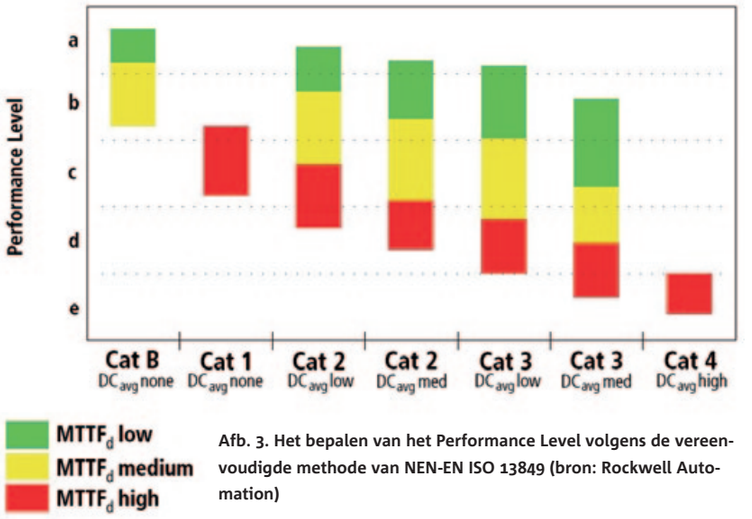
18-21_veiligheidplc.indd 19 02-10-13 09:21

heidsgerelateerde besturingsfuncties in machines uitgebreide ondersteuning bij de evaluatie van veiligheidsfuncties in het kader van EN-ISO 13849-1:2008. Om de toepassing van de tool te vereenvoudigen is het Sistema Cookbook uitgebracht.
Afbeelding 1 uit het cookbook toont een hekbewakingsschakeling voor een machine (**afb. 1**). Het hek is getekend in gesloten positie. Na inschakelen van de uitgangen O1.1 en O1.0 zullen contactoren Q1 en Q2 opkomen en gaat de motor draaien. Het veiligheidscircuit in **afbeelding 2** wordt gepresenteerd als 'designated architecture' van een tweekanaals categorie 3 systeem. Hierbij is kanaal 1 'hard wired' uitgevoerd via B1 en relais Q2 en kanaal 2 via B2 en de standaard-PLC en relais Q1. Schakelaar B1 en B2 en een NC-contact van Q1 en Q2 worden via ingangen ingelezen in de standaard-PLC. De volledige controle van de schakeling vindt dus plaats in de hard- en software van de standaard-PLC.
Het berekende Performance Level (PL estimated) voor afb. 1 komt volgens de IFA uit op een PFHd van $1{,}66.10^{-7}$ en voldoet dus aan niveau PLd (rekenkundig vergelijkbaar met SIL 2). Dit voorbeeld gaat uit van een aantal aannamen ten aanzien van de faalgegevens van de standaard-PLC, te weten: MTTF = 15 jaar, MTTFd = 30 jaar en de Diagnostic Coverage (DC) = 60%. DC is de verhouding tussen het aantal gedetecteerde gevaarlijke fouten gedeeld door het totaal aantal gevaarlijke fouten (ongedetecteerd + gedetecteerd).

Voorbeeld niet verantwoord!

De toepassing van de oplossing in afb. 1 is veiligheidstechnisch niet verantwoord, vindt Nick de With. "Allereerst heeft een standaard-PLC überhaupt geen interne diagnose waarmee de waarde van 60% DC zou kunnen worden gerechtvaardigd. Stel dat er één merkerbit is die bij een hoog niveau (logische 1) weergeeft of de diagnose van ingang (I1.0 tot en met I1.3) in orde is. Aangezien er geen interne diagnose is, wordt intern falen niet herkend en zal de motor door blijven draaien. Ten tweede is de aanname van een MTTFd van dertig jaar erg rooskleurig te noemen voor een complex product dat onbekend is en dat niet specifiek voor veiligheidsfuncties is gebouwd.
Ten derde zijn de embedded- en applicatiesoftware van de standaard-PLC nu veiligheidsgerelateerd, terwijl zeker is dat het programma in de embedded software oorspronkelijk niet geschreven is voor de uitvoering van veiligheidsfuncties! Daarnaast is de applicatiesoftware niet afgeschermd en eenvoudig toegankelijk voor elke programmeur met een programmeerpakket op zijn laptop."
Maarten Braadbaart van Sick deelt zijn mening. "Het hier besproken voorbeeld heeft een duidelijke redundante structuur. De controle wordt in dit voorbeeld volgens IFA verzorgd door het proces (lees PLC) en hier gaat de IFA uit van een DC van 60%. Daarnaast gaat de IFA er vanuit dat aan alle 'overige' eisen genoemd in 13849-1 wordt voldaan waaronder de genoemde software en programmeringseisen. Uiteindelijk komt de IFA dus op een Category 3 structuur uit en een Performance Level d (**afb. 3**)."

Diverse leveranciers hebben veiligheids-PLC's ontwikkeld die het veiligheidsgerelateerde deel van een besturing kan uitvoeren (foto: Pilz)



Afb. 3. Het bepalen van het Performance Level volgens de vereenvoudigde methode van NEN-EN ISO 13849 (bron: Rockwell Automation)

C-normen

Dieper ingaand op dit voorbeeld ziet Braadbaart een duidelijke relatie met een aantal C-normen, zoals de EN 1010-reeks voor papierverwerkende machines. "Hierin is het gebruik van standaard-PLC's voor veiligheidsfuncties al jaren toegestaan. Niet als zelfstandige veiligheidsbesturing, maar zoals in het voorbeeld in combinatie met additionele hard-wired circuits of zelfs met een tweede standaard-PLC ter bewaking van de eerste. Dit is precies zoals in EN 13849-1 6.2.6. Category 3 note 2 staat vermeld: C-type normen moeten meer richting geven aan de (on)mogelijkheid om fouten te detecteren. De C-norm (EN 1010) geeft in dit geval de mogelijkheid een standaard-PLC toe te passen om fouten te detecteren tot PLd. Deze norm schept echter ook de voorwaarden voor het gebruik van die standaard-PLC. Zonder zo'n C-norm wordt het haast onmogelijk een standaard-PLC te gebruiken.

Hoger SIL-niveau, lagere faalkans

De keuze van de IFA om dit voorbeeld te publiceren zonder verwijzing naar bijvoorbeeld relevante C-normen is daarom misschien ietwat ongelukkig."
De opmerkingen van De With over het gebruik van standaard-PLC's voor veiligheidsbesturing- en monitoringfuncties in het algemeen vindt Braadbaart gerechtvaardigd. Het moeten voldoen aan alle 'overige' eisen van EN 13849-1 is geen sinecure (vastlegging, uitvoering, validatie en borging in de gehele organisatie), zeker niet in het geval van zo'n complex product als een PLC. Braadbaart vraagt zich ook af hoe de IFA aan de waarden komt die ze in dit voorbeeld gebruikt voor

18-21_veiligheidplc.indd 20 02-10-13 09:22

een standaard-PLC. Het gebruik van standaard-PLC's voor veiligheidsbesturing- en monitoringfuncties raadt hij daarom af.

Complexe materie

Ook Henrie Verwey van Verwey Safety Services vindt de oplossingen die gegeven worden in de voorbeelden van IFA report niet erg handig en praktisch. "Wanneer je de veiligheid van een systeem gaat regelen met een gewone PLC moet je een deel via een ander circuit (hardware) laten lopen wil je bijvoorbeeld Performance Level c of d halen. Het is complexe materie en dan is de juiste kennis van zaken nodig, wil je het op een veilige manier uitvoeren."

"Bijna elke leverancier die componenten levert voor aandrijf- en besturingssystemen levert op dit moment ook 'fail safe' componenten, zoals veiligheidsrelais en -PLC's. Doordat er tegenwoordig veel concurrentie is op dit gebied, zijn deze componenten niet meer zo duur als vroeger. De leveranciers komen met aanbevelingen voor de manier van aansluiten van de componenten en garanderen op die manier de veiligheid. Ze nemen je veel werk uit handen met voorbeeldschakelingen, waarvan zij het Performance Level garanderen."

Stephen Podeveyn van Rockwell Automation voegt daar een zeer relevante opmerking aan toe: "Als je dit zélf ontwerpt, ben je ook zélf verantwoordelijk voor de veiligheid en moet je met getallen komen ($MTTF_d$ en DC). Het gebruik van gekeurde veiligheidscomponenten is veel gemakkelijker, want dan weet je tenminste dat je wat de veiligheid daarvan betreft goed zit. Ik kan me voorstellen dat grotere machinebouwers die hele grote aantallen produceren eerder geneigd zijn om eigen elektronica of standaard-PLC's te gebruiken. Zij hebben vaak ook de kennis in huis om dit veilig uit te voeren."

Geen standaard-PLC voor beveiliging

Verwey vraagt zich ook af of je goedkoper uit bent als je de veiligheid met een standaard-PLC en extra hardware regelt. "In het hiervoor genoemde voorbeeld met de hekbewaking moet je de bekabeling naar de hekschakelaars gescheiden aanleggen volgens de toelichting in het BGIA Report 2/2008e. Deze gescheiden aanleg van de bekabeling naar de veiligheidsschakelaars of een beschermde aanleg van de bekabeling is noodzakelijk om bepaalde fouten uit te kunnen sluiten. Dit is een dure oplossing. Veiligheidssystemen hebben juist voorzieningen om fouten in de bekabeling te detecteren en dus is dan een gescheiden aanleg niet nodig."

De opmerking over de bekabeling staat naast een aantal andere aannamen en voorwaarden bij het besproken voorbeeldschema voor hekbewaking. Als engineers dit voorbeeld voor hekbewaking toepassen en een bepaalde opmerking of aanname over het hoofd zien, heeft dit gevolgen voor het te behalen veiligheidsniveau (PL).

Het is vreemd dat er twee verschillende normen zijn die eigenlijk hetzelfde onderwerp behandelen, vindt Verwey. "Daarmee creëer je discussies over een belangrijk onderwerp als functionele veiligheid. En dat terwijl het doel van richtlijnen en normen is om duidelijkheid te scheppen en in heel de EU dezelfde (technische) regels te krijgen, zodat de handel binnen de EU wordt bevorderd."

Het samenvoegen en grondig herzien van deze twee normen waarmee een commissie nu aan de slag gaat, lijkt hem daarom zeer verstandig. "Het is belangrijk om daarbij vooral vanuit de gebruiker te denken zodat die er gemakkelijk mee aan de slag kan om de veiligheid op een verantwoorde manier te regelen."

Standaard- en veiligheids-PLC

De With benadrukt nog eens de eigenschappen van een veiligheids-PLC die de standaard-PLC niet heeft. "De veiligheids-PLC laat meerdere processoren (meestal twee) parallel werken. Pas wanneer ze allemaal dezelfde uitkomst geven, gaat hij zijn uitgangen aansturen. Doordat de fabrikant vaak processoren van verschillend fabricaat toepast, is de waarschijnlijkheid dat ze gelijktijdig dezelfde fout maken uitermate klein. Om toch zo snel mogelijk op eventuele willekeurige fouten (random failures) in te spelen, is de veiligheids-PLC voorzien van enkele tienduizenden zelftestfuncties in zowel de hardware als de software. Onder meer door middel van een watchdog, over- en onderspanningsbewaking en bitpatroontests, die cyclisch worden uitgevoerd.

Daarnaast wordt gebruikgemaakt van verschillende softwareteams die de embedded software (operating system, diagnostische software, support functies en libraries) voor elke processor apart ontwikkelen. Voor het programmeren van het veiligheidsapplicatieprogramma stelt de leverancier vaak een bibliotheek van NoBo gecertificeerde veiligheidsfunctieblokken ter beschikking."

Voor het beveiligen van deuren in industriële processen biedt Sick zowel elektromechanische schakelaars als contactloze schakelaars met magnetische, inductieve of transpondertechnologie (foto: Sick)

Conclusie

Het inzetten van een standaard-PLC voor veiligheidsfuncties wordt door de geraadpleegde deskundigen afgeraden. Zij stellen zonder uitzondering vraagtekens bij de aannamen (DC=60% en MTTFd=30 jaar) die door IFA in haar voorbeelden zijn aangenomen. Wie een standaard-PLC wil inzetten voor veiligheidsfuncties, neemt zelf de verantwoordelijkheid en moet ook zelf allerlei additionele veiligheidsmechanismen in hardware en software gaan inbouwen. Ook moet het geheel vastgelegd, gevalideerd en geborgd worden en dat is geen sinecure.

Bovendien is nog maar de vraag of men zonder de inzet van veiligheidscomponenten het vereiste veiligheidsniveau kan halen. De standaard-PLC bevat namelijk geen intern foutdetectiemechanisme en er is sprake van complexe componenten. Wie geen kennis heeft van de noodzakelijke maatregelen en deze verantwoordelijkheid dus niet aan kan, doet er uitermate verstandig aan om NoBo gecertificeerde veiligheids-PLC's of andere gecertificeerde componenten in te zetten voor veiligheidsfuncties omdat de veiligheidsfuncties hiermee betrouwbaarder en eenvoudiger te realiseren zijn. AT

Inlichtingen

Fusacon BV, tel.: (0347) 35 25 19, www.fusacon.nl
Institut für Arbeitsschutz, tel.: (+49) 2241 231 02, www.dguv.de/ifa/de/index.jsp#
Bosch Rexroth BV, tel.: (0411) 65 10 93, www.boschrexroth.nl
Sick BV, tel.: (030) 229 25 44, www.sick.nl
Verweij Safety Services BV, tel.: (0622) 93 20 56, www.verwey-training.nl
Rockwell Automation BV, tel.: (0297) 54 35 00, www.rockwellautomation.nl

18-21_veiligheidplc.indd 21 02-10-13 09:22