

Werkschakelaars en LoTo(To)

Correct uit is het nieuwe in – IV

In dit vierde artikel wordt aandacht besteed aan de besturing via de veiligheids-PLC van de remote-lototo-unit. Hierbij worden enkele details van de

besturing nader beschouwd met als uitgangspunt de norm IEC/CD1 62061¹. Vervolgens zal op basis van de remote-lototo-functie dieper ingegaan worden

op de besturingslogica in relatie tot enkele mogelijke storingen.

Paul Hoogerkamp, Pouw Jongbloed
en Aart van Ginkel

Uitgangspunten

Zonder diepgaande beschouwing over de risicoclassificatie kan worden gesteld dat deze (veiligheids) besturingssoftware zodanig betrouwbaar moet zijn dat deze aan de hoogste betrouwbaarheidsklasse van de EN-ISO 13849-1 (PLe) of EN 62061² (SIL3) moet voldoen. Tevens is gekozen voor de validatie/verificatiemethode zoals deze is beschreven in de IEC 62061 die binnenkort voor een eerste commentaarronde zal verschijnen als IEC/CD1 62061. In die norm staat de keuzetabel voor de eisen die passen bij het gekozen (veiligheids) softwarelevel (afbeelding 1, geel-omrande kolom). Door de keuze van een zogenoemd 'pre-assesed hardware platform' en 'pre-assesed software' kan PLe of SIL3 worden bereikt. In dit geval wordt gebruikgemaakt van de PNOZmulti met de bijbehorende software.

Risico

Voor deze remote-lototo is met behulp van de door de fabrikant van de PLC geleverde programmatuur de besturingssoftware gerealiseerd. In feite wordt

met behulp van de programmatuur de besturingslogica opgebouwd. Het maken en het wijzigen van besturingssoftware is eenvoudig en snel te realiseren. Met name door deze snelheid van werken neemt het risico op systematische fouten toe. Mede daarom wordt in de norm EN 62061 gehamerd op het maken van correcte specificaties en bijbehorende testspecificaties alvorens te coderen. Na het coderen volgt het testen van de code en vervolgens het implementeren van de code in de uiteindelijke besturing die vervolgens kan worden gevalideerd. De methodiek gericht op het vermijden van fouten in het ontwerp (zogenoemde systematische fouten) is beschreven in het IFA report 2/2016³ door middel van het verkorte V-model.

Elektrische veiligheid

Uitgangspunt voor de besturingssoftware is dat aan de basiseisen voor elektrische veiligheid is voldaan en dat de remote lototo-unit functioneert binnen de randvoorwaarden van de componenten. Dergelijke beschouwingen zijn terug te vinden in de EN-ISO 13849-2 tabel D1 (basisprincipes), D2 (beproefde principes) en D3 (beproefde componenten) en zijn ook in de IEC/CD1 62061 vermeld in tabel B2 (afbeelding 3).

Vandaar dat in het vorige artikel de opmerking is gemaakt dat:

'de aders van de meetcontacten naar de PU3Z zodanig gelegd (zijn – red.) dat kortsluiting tussen de fase(n) als gevolg van een losse ader niet is te verwachten.

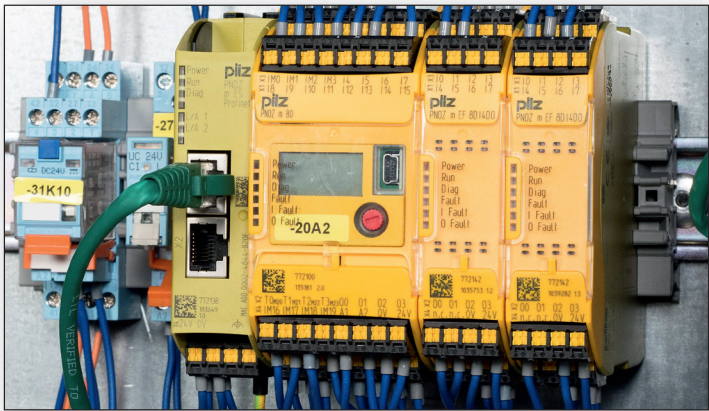
Maar eveneens geldt dit voor de zeer gevaarlijke situatie dat de PU3Z ten onrechte 0 V signaleert doordat de ader losgeraakt is of contact maakt met aarde. Tevens dienden de aders bestand te zijn tegen een hogere temperatuur om te voorkomen dat de bovengenoemde fouten kunnen ontstaan. Een en ander conform de eisen van de EN 61439-1 met betrekking tot maatregelen om sluitingen naar aarde of onderling te voorkomen. Omdat het niveau SIL3 (PLe) moet worden ge-

Software Level		A						B			C		
Software-Route		B1	B2	B3	B4	B5	C1	C2	C3				
Maximum SIL achievable		3	2	2	1	1	-	3	2	3			
Maximum PL achievable		e	d	d	c	c	b	e	d	e			
Software designed and tested according to	IEC 61508		x					x					
	this standard	x		x	x	x	x		x	x			
	diversity required			x						x			
Software platform	pre-assesed	x						*	*	*			
	not designed explicitly for safety application		x	x	x	x	x						
	diversity required		x	x	x								
Hardware platform	pre-assesed	x						**	**	**			
	not designed explicitly for safety application		x	x	x	x	x						
	diversity required		x	x	x								
	HFT		1	1	1	0	0				1		
category according to ISO 13849-1			3	3	3	2	B				3/4		

* If a software platform is used, e.g. an operating system, it has to satisfy the requirements of a functional safety standard.

** The hardware platform has to satisfy the requirements of a functional safety standard.

Afbeelding 1. Tabel 7 uit de IEC/CD1 62061.



Afbeelding 2. De veiligheids-PLC (PNOZmulti) met een koppeling naar een veldbus (links).

haald is tevens van belang dat niet één en dezelfde persoon de software maakt én ook controleert. Bij ‘software level A’ kan echter worden volstaan met controle door een onafhankelijke derde. Controle door een onafhankelijke derde (bijvoorbeeld een Notified Body) is raadzaam (afbeelding 4). Bij de in de tabel weergegeven X1/X2 wordt de opmerking geplaatst dat een onafhankelijke derde ook noodzakelijk kan zijn in het kader van de complexiteit en/of de projectomvang.

Besturingssoftware: de basis

De voorgaande uitgangspunten en de eisen voor de software op basis van de IEC/CD1 62061 leiden tot de specificatie van de functies binnen de remote-lototo-unit; het uitschakelen van de werkschakelaar waardoor de hoofdstroom wordt onderbroken en de kortsluitvermogensunit wordt ingeschakeld en vervolgens de groene LED oplicht. In het actie/activiteiten-overzicht (tabel 1) wordt dit nader toegelicht en wordt tevens in de laatste kolom verwezen naar de afbeeldingen met de besturingslogica. Voordat de genoemde remote-lototo-functie wordt uitgevoerd moet deze remote-lototo-unit bedrijfs-gereed staan. Dit betekent onder andere dat de 24 V-voeding correct moet functioneren. In deze eerste cyclus (afbeelding 5) wordt duidelijk hoe de lay-out met functieblokken er uitziet en hoe deze onderling zijn verbonden. Door middel van de veiligheidssoftware worden functiebouwstenen gerealiseerd. In afbeelding 5 is bijvoorbeeld bouwsteen 1 een zogenoemde NAND-poort⁴ afgebeeld. Vanuit die bouwsteen wordt het stuurspanningssignaal naar de pulstimer (bouwsteen 2) geleid en vervolgens wordt dat signaal samen met het stuurspanningssignaal gebruikt als input voor een NOR-poort (bouwsteen 3) die de LED (stuurspanning aanwezig) laat knipperen of continu branden.

N.B.: Als het stuurspanningssignaal naar de NAND-poort (zekering doorgebrand van de 24 V voeding) afwezig is (Laag) zal deze LED dus

Avoidance of systematic failures	
Measure	Comment/Examples
Proper selection, combination, arrangements, assembly	The right component for the application and used in the correct way (instruction for use of the component manufacturer): Position switches useable for this application?
Wiring, interconnections	See instruction for use of the component manufacturer; measures against short-circuit failures
Correct dimensioning and shaping	Electrical overdimension: Load of contactors correct?
Hardware design review	Analysis of plausibility and considering the instruction for use of the component manufacturer)
Simulation	Not possible, but instead of the hardware design review
Control of systematic failures	
Measure	Comment/Examples
Voltage variations and interruptions	Hardware design acc. to IEC 60204-1
Effects of the physical environment and EM immunity	Hardware design acc. to IEC 60204-1; see instruction for use of the component manufacturer
Effects of temperature increase or decrease	See instruction for use of the component manufacturer; if necessary including relevant hints into the information for use of the safety function
Use of de-energization	Switching off of the motor by actuating the position switches
Well-trieed safety principles	
- Failure detection by automatic tests	Monitoring of two position switches and two contactors; short-circuit detection
- Operation in the positive mode	Positively driven contacts of the position switches

Afbeelding 3. Systematic Integrity –example overview (IEC/CD1 62061 Tabel B.2).

Minimum level of independence	Required PL/SIL for the software design up to			
	PL b	PL c / SIL 1	PL d / SIL 2	PL e / SIL 3
Other Person	X	sufficient only for SW level A for combination of pre-assessed software modules	sufficient only for SW level A for combination of pre-assessed software modules	not sufficient
Independent person	possible but not necessary	X	X1	sufficient only for SW level A for combination of pre-assessed software modules
Independent department	possible but not necessary	possible but not necessary	X2	X1
Independent organisation	possible but not necessary	possible but not necessary	possible but not necessary	X2

Afbeelding 4. Minimum level of independence for review, testing and verification activities (IEC/CD1 62061 Tabel 8).

knipperen, want de pulstimer krijgt dan door de invertering van het ingangssignaal door de NAND-poort juist een ‘Niet Laag’ of te wel ‘Hoog’ signaal. Deze LED voor de indicatie ‘Stuurspanning OK’ is overigens niet wezenlijk voor de veiligheid van de remotelototo-unit, maar het signaal ‘Stuurspanning OK’ is wel degelijk van belang voor de overige besturingscycli. Het blokje ‘Stuurstroom OK’ (afbeelding 5, bouwsteen 4) wordt elders in

het programma mede gebruikt om te controleren of er storingen in een deel van de voedingsspanning is opgetreden (afbeelding 6).

Opgemerkt wordt dat hierbij het inverse signaal (afbeelding 6, bouwsteen 4) 'Stuurstroom OK' (in feite 'Stuurstroom NOK') wordt gebruikt samen met de signalen 'Hoofdstroom storing' (bouwsteen 1), de inverse van 'Deurvergrendeling diagnose' (bouwsteen 5) en 'Deurvergrendeling overbrugd' (bouwsteen 5), en de 'Spanningsstoring' (bouwsteen 6) om een signaal te genereren die het inschakelen blokkeert. Pas als er geen storing is wordt dit signaal 'Hoog' gemaakt. Dit signaal kan wederom als input worden gebruikt om bepaalde acties uit te voeren, zoals het schakelen van een LED of het blokkeren van de uitschakeling.

Besturingssoftware: enkele details

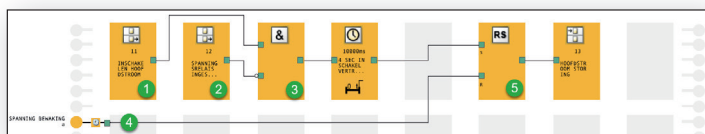
De besturingssoftware moet dus een aantal checks uitvoeren alvorens de groene lamp mag gaan branden als teken dat de vergrendeling (slot met label) mag worden aangebracht. Tussentijdse storingen die tot een onveilige situatie leiden moeten zijn voorkomen of uitsluitend kunnen leiden tot een veilige situatie. Aangezien de vermogensautomaten een bi-stabiele schakelaar hebben met daaraan gekoppelde hulpcontacten, is altijd de status van de schakelaar te achterhalen in die controlecyclus. In afbeelding 7 is dit weergegeven door de 'Normally Open'- en 'Normally Closed'-contacten, de meest linkse bouwstenen, die

'divers' en redundant worden ingelezen en bewaakt. In afbeelding 8 is de cyclus weergegeven voor de bewaking wanneer de hoofdstroom mag worden ingeschakeld. Dit deel van de besturing bewaakt de in- en uitschakeltijden van de componenten. Onder andere het door de motor opwinden van de veer die noodzakelijk is voor de bediening van de vermogensautomaten.

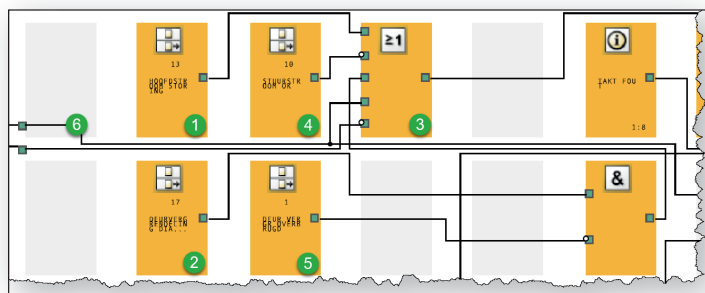
Al dit soort interne controles moeten sequentieel worden afgewerkt alvorens 'groen licht' te geven. Tevens moet worden bedacht dat op ieder moment in die cyclus een spanningsdip of storing kan optreden en die mag nooit tot een gevaarlijke situatie leiden. Als de remote-werkschakelaar in de uitgeschakelde stand (vergrendeld) is kan dit dus uitsluitend hebben kunnen plaatsvinden als de vermogensschakelaar was uitgeschakeld én de kortsluitvermogensschakelaar was ingeschakeld. Vandaar dat als laatste in de cyclus de groene lamp wordt ingeschakeld (afbeelding 9) en deze LED knippert als de vermogensschakelaar nog niet is afgeschakeld (afbeelding 8, bouwsteen 1) en (AND-poort, bouwsteen 3) de spanning nog niet voldoende laag is (bouwsteen 2), en vervolgens of (OF-poort, bouwsteen 5) de vermogensschakelaar echt is uitgeschakeld (bouwsteen 5). Als aan alle voorwaarden is voldaan zal de OF-poort (bouwsteen 5) 'Laag' zijn en wordt de knipperfrequentie uitgeschakeld. Op dat moment is eveneens zeker dat de kortsluitvermogensschakelaar is ingeschakeld en de vermogensschakelaar van het afgaande veld is uitgeschakeld.

Actie / activiteit	Status	Resultaat	Opmerkingen	Afb.
Remotelototo-unit bedrijfs gereed	De unit is in bedrijf en de witte LED licht op	Stuurspanning OK	Als de indicatie van de stuurspanning niet aanwezig is kan de LED kapot zijn of een zekering gesprongen. Als de zekering is gesprongen van de veiligheids PLC en er geen voeding is kan ook de besturing niet functioneren. De remotelototo-unit staat dan in een bepaalde stand waarbij de werkschakelaar óf is ingeschakeld óf is uitgeschakeld en vergrendeld. Vandaar dat na het opkomen van de 24V voeding als eerste via een interne controleloop de status worden gecontroleerd. Pas als deze controle is gerealiseerd kan het signaal 'geen storing' worden afgegeven.	5
Werkschakelaar op de remote unit wordt uitgezet	Werkschakelaar in de 'Off' positie	De contacten in de werkschakelaar worden verbroken en dat wordt door de besturing waargenomen	De logica in de besturing gaat de vermogensschakelaar in de 'Off' positie zetten. Dit kan alleen als er tussentijds geen storingen optreden. Treden er tussentijds storingen op dan wordt bij het opstarten eerst de vermogensschakelaar in de voeding uitgeschakeld als deze al niet uitgeschakeld was en de kortsluitvermogensschakelaar ingeschakeld als deze nog niet ingeschakeld was. N.B.: door de bi-stabiele standen van de vermogensschakelaars blijft de eenmaal (in)geschakelde stand behouden onafhankelijk van de mogelijke spanningsuitval of storingen.	6
Vermogensschakelaar	Vermogensschakelaar wordt door de besturing afgeschakeld	De hoofdstroom is onderbroken	De spanningvoerende fasen zullen op enig moment na het afschakelen een voldoende lage spanning voeren. Wanneer deze spanning wordt gedetecteerd door de nulspanningsdetectie op de fasen (PU3Z) zal, na een bepaald tijdsverloop, de kortsluitvermogensschakelaar worden ingeschakeld.	7
Kortsluit vermogensschakelaar	Kortsluit vermogensschakelaar wordt door de besturing ingeschakeld	Kortsluiting tussen actieve delen onderling en na de aarding is gemaakt	Zodra de kortsluiting tussen actieve delen onderling en na de aarding is gemaakt en er geen enkele storing is opgetreden kan de groene lamp worden geactiveerd.	8
Groene controle lamp	Unit is veilig afgeschakeld	Groene LED licht op	Na het aanbrengen van slot en label in de daarvoor bestemde opening van de werkschakelaar is de procedure van de remote lockout/tagout volbracht. Omdat de werkschakelaar bij de motor is geplaatst en duidelijk is gemarkeerd, is de eventuele tryout hiermee ook veilig uitgevoerd en kan er veilig worden gewerkt aan het afgaande veld.	

Tabel 1. Het actie/activiteiten-overzicht van de remote-lototo-unit.



Afbeelding 5. Start van de besturingscyclus: Stuurstroom OK.



Afbeelding 6. 'Stuurstroom OK'-signaal als ingang voor het afhandelen van storingen.

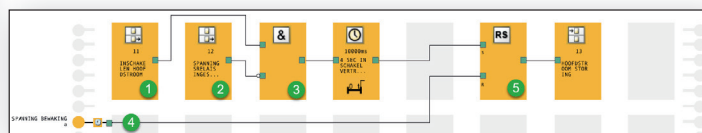
Tot slot

Uit de hiervoor vermelde details blijkt dat een niet al te ingewikkelde schakeling met duidelijke schakelvoorwaarden juist door het beschouwen van de mogelijke fouten al snel complex wordt. In feite gaat in die toenemende complexiteit het meeste werk zitten. Om de kans op details over het hoofd te zien, en mede daardoor de kans op gevaarlijk falen heel klein te maken is een formele en structurele werkwijze noodzakelijk. Deze werkwijze om van de algemene functionele specificatie in detail de overige specificaties af te leiden en rekening te houden met 'gevaarlijke' storingen, defecten of falen van componenten wordt in het eerder genoemde 'IFA report' beschreven. In het volgende artikel zal aan deze zogenoemde oorzaak-gevolgmatrix om software te specificeren aandacht worden besteed. Kortom – ook in de besturingssoftware zijn diverse aspecten die een veiligheidstechnische achtergrond hebben. Deze aspecten zijn en worden overigens niet uitputtend behandeld, maar zijn wel onderdeel van een omvangrijk technisch constructiedossier. Vandaar dat evenals in voorgaande artikelen telkens de waarschuwing onderaan deze pagina wordt getoond.

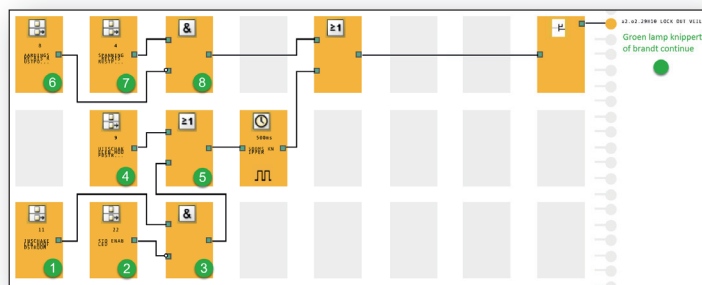
Op het Safety Event (www.engineersonline.nl/safetyevent) van 9 mei aanstaande in het Evoluon in Eindhoven (Evoluon) worden diverse alternatieven voor de remote-lototo getoond. Zie ook www.remotelototo.nl.



Afbeelding 7. Onderdeel van de cyclus: inlezen van de hulpcontacten.



Afbeelding 8. Onderdeel van de cyclus: bewaking in- en uitschakeltijden van de componenten.



Afbeelding 9. Groene lamp als laatste item in de besturingscyclus.

Voetnoten

¹ Door de samenwerking tussen de werkgroepen van ISO en IEC ten aanzien van de veiligheidsgelateerde besturing zal onder andere het validatiegedeelte gemeenschappelijk worden opgesteld.

² Titel van EN 62061 en EN-ISO 13849.

³ IFA report 2/2016 is te downloaden op <http://publikationen.dguv.de/dguv/pdf/10002/rep0216.pdf>. Tevens zijn de voorbeelden uit dat rapport te downloaden via http://www.dguv.de/medien/ifa/de/pub/rep/pdf/reports2016/softwarebeispiele_ifa-report_2-2016.zip.

⁴ https://nl.wikipedia.org/wiki/Logische_poort



Waarschuwing

De auteurs willen er nadrukkelijk op wijzen dat het klakkeloos nabouwen zonder de noodzakelijke achtergrond informatie van de getoonde schema's of afbeeldingen leidt tot gevaarlijke situaties. Zelfs indien men over de nodige kennis op elektrisch gebied beschikt is dit geen garantie of de in de schakeling verborgen veiligheidsmaatregelen correct worden toegepast. Voor mogelijke gevolgen indien, deze waarschuwing wordt genegeerd, wordt door de auteurs en MYbusinessmedia geen enkele aansprakelijkheid aanvaard.