Het doorgronden van SIL & PL met behulp van het V-model

Functionele veiligheid in de machinebouw

kader
Consultancy & Interim

Bekijk het op
kader.nl

Bekijk het op
kader.nl

Inleiding

Functionele veiligheid beschrijft hoe een deel van de veiligheid van een machine kan en mag worden toevertrouwd aan een besturingssysteem. De automatisering van machines heeft grote stappen gemaakt sinds de intrede van de machinerichtlijn en de introductie van de eerste noodstoprelais. Zo is de veiligheids-PLC inmiddels niet meer weg te denken, worden systemen complexer en veiligheidscomponenten steeds slimmer. Zonder kennis van veiligheidsgerelateerde onderdelen is het tegenwoordig bijna onmogelijk om nog een besturingssysteem te ontwerpen. Met deze brochure helpen we je een stukje op weg.

Of je een machinebouwer bent of een eindgebruiker die een vinger aan de pols wil houden bij de leverancier van een nieuwe machine, wij helpen je graag met jouw vraagstukken of projecten over functionele veiligheid. Dit kan in de vorm van advies, coaching of begeleiding van klantspecifieke projecten.

In de brochure vind je

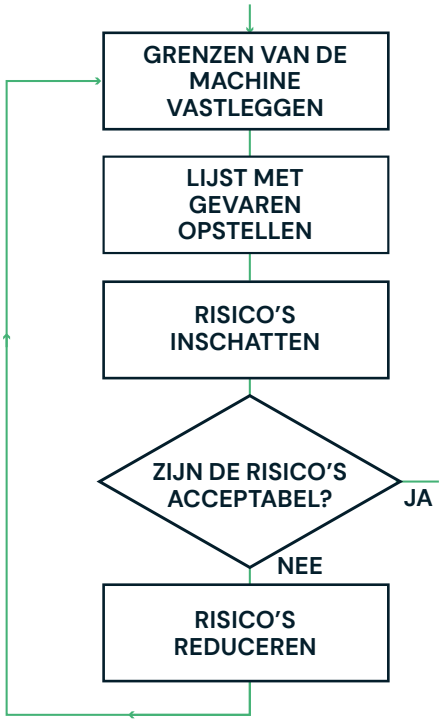
Contact
Heb je na het lezen van de informatie nog vragen, of wil je een offerte aanvragen? Neem dan gerust contact met ons op.

Telefoonnummer 030 243 64 64
kader.nl | sales.kceni@kader.nl

Wij helpen je graag!

Veiligheidsfuncties

Risicobeoordeling
De risicobeoordeling is een belangrijk instrument om tot een veilige machine te komen. Het is noodzakelijk om hiermee al vroeg in het ontwerptraject te starten. Alleen op die manier kunnen de juiste stappen worden doorlopen om risico's te reduceren. Het komt helaas vaak voor dat de risicobeoordeling pas aan het eind wordt opgesteld, vaak in de vorm van een checklist. Effectieve maatregelen (in het machineontwerp) kunnen dan niet meer genomen worden.



Risico's reduceren in 3 stappen

1. Verbeter het ontwerp, zorg dat het gevaar er niet meer is.
2. Voeg een beveiliging toe, het gevaar kan niet worden weggenomen maar de blootstelling wordt verminderd.
3. Verstrek informatie, er is nog een gevaar met blootstelling, veilig werken vereist bijvoorbeeld instructie en persoonlijke beschermingsmiddelen.

Grenzen

Leg eerst de grenzen van de machine vast, met voldoende detail:
voorzien gebruik, redelijkerwijs voorzienbaar verkeerd gebruik, fysieke grenzen van de machine, gebruikers, bedrijfsmodi, omgevingsomstandigheden, service-intervallen, toegankelijkheid, afmetingen, massa's, cyclustijden, eigenschappen van materialen in de machine enzovoorts.

Lijst met gevaren

Identificeer 'alle' gevaren in de machine, zonder rekening te houden met eventuele beveiligingen. Ga nog geen oplossingen bedenken! Beschouw alle fasen in de levenscyclus van de machine en alle taken die aan de machine worden uitgevoerd. Identificeer gevaren in de vorm van scenario's.

Inschatten van de risico's

Als een gevaar weinig letsel kan veroorzaken of er is nauwelijks blootstelling aan dat gevaar zal het risico lager zijn. Schat voor elk gevaar in hoe groot het risico is. Gebruik een methode zoals risicograaf of Kinney&Wiruth.

EN ISO 12100
Safety of machinery - General principles for design - Risk assessment and risk reduction

Functionele veiligheid

Een vaste afscherming is een voorbeeld van een beveiligingsmaatregel. Hoewel er eisen zijn aan vaste afschermingen heeft dit niets met SIL of PL te maken. Pas als een beveiliging uitgevoerd wordt door een besturingssysteem, spreken we van een veiligheidsfunctie. Elke veiligheidsfunctie krijgt een benodigd PL (a-e) of SIL (1-3) level. De veiligheidsfunctie wordt opgedeeld in subsystemen (ingang – logische eenheid – uitgang) waarbij elk subsysteem een architectuur moet hebben die robuust genoeg is voor het te behalen level. Daarnaast moet de opgetelde faalkans van de subsystemen laag genoeg zijn. Onafhankelijk van de berekening moet ook aandacht besteed worden aan diverse kwalitatieve aspecten.

Performance level PL
EN ISO 13849-1/2
Safety of machinery
Safety-related parts of control systems

Safety integrity level SIL
EN IEC 62061
Safety of machinery – Functional safety of safety-related control systems

Systematische werkwijze
Dit V-model is een voorbeeld van de systematische aanpak van functionele veiligheid binnen een project. Fouten worden voorkomen door een goed specificatie-, ontwerp- en realisatietraject met een aantal controlemomenten. Doorlopen en vastleggen van deze stappen is nodig om aan te tonen dat het benodigde SIL- of PL niveau behaald is. Zorg voor een wijzigingsprotocol zodat bij een wijziging, indien nodig, wordt terugverwezen naar de relevante ontwerpstappen. Houd documenten en revisies onder configuratiemanagement. De opsommingen in de toelichtingen hieronder zijn slechts hoofdlijnen. Maak het model passend voor het project, niet complexer dan noodzakelijk en leg de werkwijze vooraf vast in een plan. Het einddoel is een veilige en werkbare machine, bij alle taken, dus niet alleen voor de operator maar ook bijvoorbeeld voor technici en schoonmakers. Wanneer (functionele) veiligheid als hinderlijk wordt ervaren, leidt dat vaak tot creatieve manieren om de werkzaamheden op een andere manier toch uit te kunnen voeren. Neem veiligheid en werkbaarheid daarom vanaf de start mee in het ontwerptraject!

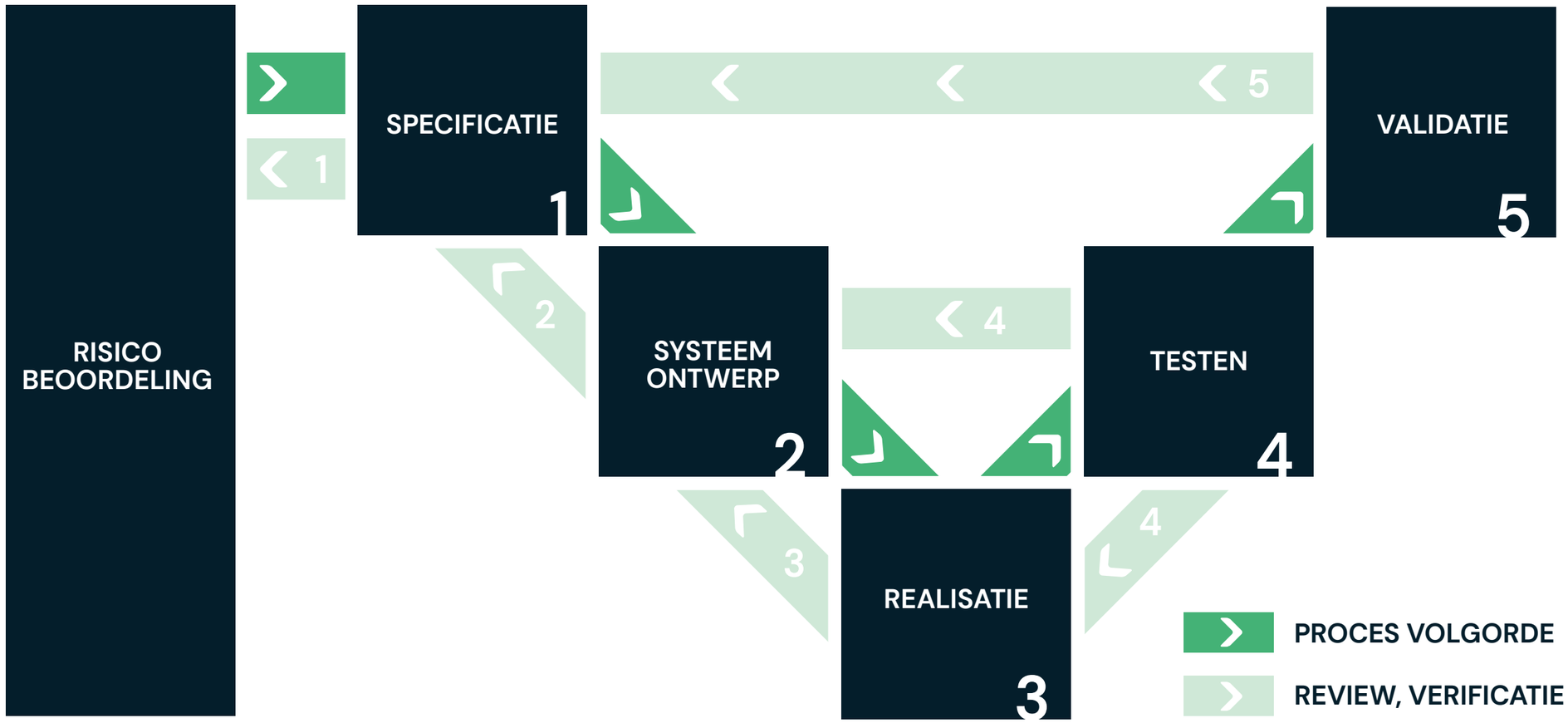
1 Specificeer elke veiligheidsfunctie.
Functionaliteit & aanspreekfrequentie.
Benodigde level met onderbouwing.
Omgevings- en gebruiksomstandigheden.
Gebruiksmodi en uitzonderingen.

2 Ontwerp de veiligheidsfuncties.
Subsystemen, componenten, architectuur en diagnose.
Specificatie en ontwerp van veiligheidssoftware.

3 Maak tekeningen (elektrisch, pneumatisch, hydraulisch).
Info voor de gebruiksaanwijzing.
Bouwen van de machine.
Programmeren veiligheidssoftware.

4 Test de I/O van de veiligheidsPLC, inclusief instellingen en diagnose. Test de redundantie van de subsystemen, introduceer fouten, controleer diagnose.
Test alle veiligheidsfuncties.

5 Controleer het ontwerptraject, testrapporten en andere documentatie.
Zijn alle stappen in het model doorlopen en gedocumenteerd en zijn de verificatiestappen uitgevoerd en afgerond?



Zijn alle veiligheidsfuncties die uit de risicobeoordeling volgen volledig gespecificeerd met oog op het risico dat door de veiligheidsfunctie gereduceerd word?
Passen de gespecificeerde omgevingsomstandigheden bij de grensbeschrijving?
Is de specificatie volledig? 1

Is de gekozen architectuur robuust genoeg (categorie / SILCL)?
Is de berekende faalkans laag genoeg (PFHD)?
Zijn componenten onderling compatibel?
Zijn de componenten bestand tegen de te verwachten omgevingsomstandigheden?
Zijn alle veiligheidsfuncties en specificaties volledig in het ontwerp opgenomen, zowel hard- als software? 2

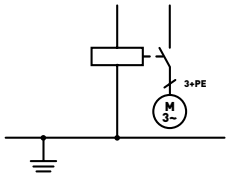
Zijn alle componenten uit het systeemontwerp correct in de tekeningen opgenomen?
Zijn deze componenten toegepast conform de gebruiksaanwijzing van het component?
Is de diagnose op de juiste manier verwerkt?
Is de hardware conform tekeningen gerealiseerd (geen extra componenten toegevoegd bijvoorbeeld)? 3

Functioneert het veiligheidsgerelateerde deel van het besturingssysteem zoals beschreven in het ontwerp?
Functioneren alle componenten zoals voorzien tijdens de realisatie en montage? 4

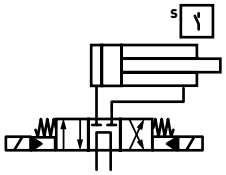
Hebben we gebouwd wat gespecificeerd is? 5

Architectuur en faalkans

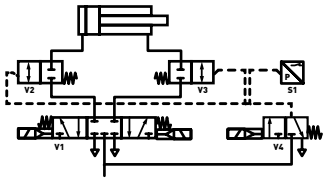
Robuuste architectuur, per subsysteem
Hoewel een enkelvoudig systeem een hele lage faalkans kan hebben is het niet mogelijk om met deze architectuur een hoog level te bereiken. Voor de lage levels (PL a, PL b, PL c of SIL 1) is een enkelvoudige architectuur meestal voldoende. De hogere levels (PL d, PL e, SIL2 of SIL3) worden doorgaans met een redundante architectuur met diagnose uitgevoerd. Een getest enkelvoudig systeem (dus met diagnose) is in de praktijk moeilijk realiseerbaar, omdat het vaak niet mogelijk is om na diagnose van een fout het systeem naar een veilige toestand te brengen. In de vier voorbeelden hieronder wordt steeds een uitgang subsysteem beschreven.



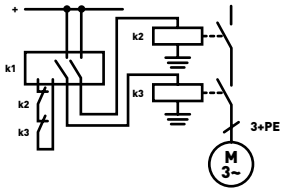
Enkelvoudig systeem
Één gevaarlijke fout, in dit geval het verkleven van de motorcontactor, leidt tot verlies van de veiligheidsfunctie.
De kwaliteit van dit subsysteem is volledig afhankelijk van de kwaliteit van de motorcontactor.
Gebruik daarom 'beproefde componenten'.
PL categorie 1; SIL HFT0 SILCL 1.



Getest enkelvouwdig systeem
De correcte werking van het hydraulische stuurventiel wordt indirect terug-gekoppeld door sensor S. Bij falen van het stuurventiel kan bijvoorbeeld het hydraulische aggregaat worden gestopt om de cilinder alsnog veilig tot stilstand te brengen.
Let op: er zijn strikte eisen aan de foutreactie en de testfrequentie.
PL categorie 2; SIL HFT0 SILCL 1, 2 of 3.



Redundant systeem met lage DC waarde
Het stuurventiel met gesloten middenstand kan de cilinder stilzetten (kanaal 1). De blokkeerventielen, aangestuurd door een extra stuurventiel, kunnen dat ook (kanaal 2). Tenminste één van beide kanalen moet functioneren om de cilinder te stoppen. Sommige, maar niet alle fouten kunnen worden gedetecteerd.
PL categorie 3; SIL HFT1 SILCL 2 of 3.



Redundant systeem met hoge DC waarde
Door de mechanisch gedwongen verbreekcontacten van de contactors K2 en K3 terug te koppelen naar de veiligheidsbesturing worden fouten met hoge zekerheid gedetecteerd. De machine zal na het falen van een kanaal niet meer kunnen opstarten.
PL categorie 4; SIL HFT1 SILCL 3.

Categorie
Classificatie van de gebruikte architectuur gebaseerd op redundantie, diagnose en reactie op fouten.
Wordt alleen gebruikt in de PL-norm.

Hardware fault tolerance (HFT)
De mate van redundantie waarbij HFT0 niet bestand is tegen fouten en HFT1 bestand is tegen 1 fout.

Safe failure fraction (SFF)
De som van het percentage veilige fouten (waarbij bijvoorbeeld de machine veilig stopt als gevolg van de fout) en het percentage gevaarlijke fouten dat gedetecteerd wordt (zodat de machine in een veilig toestand gebracht kan worden).

Sil claim limit (SILCL)
Geeft voor elk subsysteem aan tot welk SIL niveau deze architectuur mag worden toegepast. SILCL wordt via een tabel bepaald op basis van HFT en SFF.

Lage faalkans

Per subsysteem wordt de kans op toevallig gevaarlijk falen (Random Hardware Failure) bepaald of berekend. De som van de faalkansen van de subsystemen vormen de faalkans van de veiligheidsfunctie. Deze moet laag genoeg zijn voor het benodigde level.

Gevaarlijk falen Met een component dat gevaarlijk faalt is een machine niet meer naar de veilige toestand te brengen.	Een contactor die blijft plakken (kan niet uitschakelen) is gevaarlijk gefaald omdat deze een motor niet kan stoppen. Een contactor die een doorgebrande spoel heeft (kan niet inschakelen) is veilig gefaald omdat deze een motor niet kan starten.	
PFH_D Kans, per uur, dat het subsysteem gevaarijk faalt.	De PFH_D (Probability of dangerous Failure per Hour) van de veiligheidsfunctie wordt berekend door de PFH_D van alle subsystemen op te tellen. Als de PFH_D waarde niet door de leverancier opgegeven wordt, moet deze bepaald worden met behulp van de variabelen hieronder.	
$MTTF_D$ Gemiddelde tijd, in jaren, tot het gevaarlijk falen van een component.	**λ_D** Kans, per uur, dat een component gevaarlijk faalt.	$MTTF_D$ (Mean Time To Failure dangerously) en λ_D zijn gedurende de te bepalen levensduur (een bepaalde tijd of aantal schakelingen) constant. Dan geldt $MTTF_D$ is $1/\lambda_D$. Aan het einde van deze levensduur moeten componenten preventief worden vervangen omdat λ_D daarna snel zal stijgen en $MTTF_D$ snel zal dalen.
B_{10D} Statistisch aantal schakelingen (voor elektromechanische componenten) waarna 10% van de componenten gevaarlijk heeft gefaald.	**nop** of **c** Aantal keer schakelen (voor dit component) per jaar (nop) of per uur (c).	Met de B_{10D} en de nop (number of operations) of c-waarde is met een eenvoudige formule de $MTTF_D$ of λ_D waarde te berekenen.
RDF het percentage fouten dat gevaarlijk is ten opzichte van alle fouten.	Als bijvoorbeeld een contactor een B_{10} waarde van 1.000.000 heeft met een RDF (Ratio of Dangerous Failure) van 73% dan is: $B_{10D} = B_{10}/RFD = 1.000.000 / 0{,}73 = 1.369.863$	
DC Het percentage gevaarlijke fouten dat door de diagnose wordt gedetecteerd.	Een redundant subsysteem is pas zinvol als fouten worden gedetecteerd. Afhankelijk van de gebruikte techniek van foutdetectie wordt een DC (Diagnostic Coverage) waarde toegekend aan redundante subsystemen. De combinatie van faalkans ($MTTF_D$ of λ_D), architectuur en terugkoppeling (DC) wordt gebruikt in de bepaling van de PFH_D waarde van het subsysteem.	

Goed vakmanschap

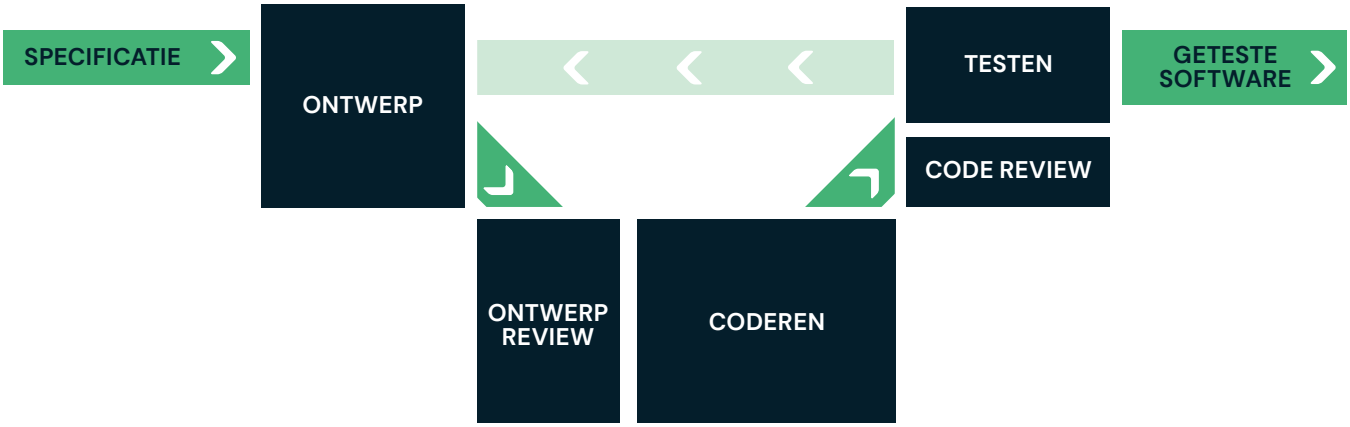
Als een contactor faalt omdat er teveel stroom loopt of een schakelaar faalt omdat deze niet bestand is tegen de omgevingsomstandigheden, dan is dat geen toevallig falen maar een direct gevolg van een fout ontwerp. Deze fouten zijn dus systematisch. Het vervangen van de schakelaar door een (identieke) nieuwe schakelaar lost het probleem niet op. Bij het berekenen van de faalkans is altijd het uitgangpunt dat de componenten precies op de juiste manier worden toegepast, zoals dit door de leverancier in de datasheet is vermeld.
Pas basis- en beproefde veiligheidsprincipes toe zoals:
kies geschikte materialen en componenten; gebruik datasheets en manuals; installeer de voorgeschreven beveiligingen tegen te hoge stroom, druk, temperatuur etc.; zorg voor de juiste lucht en oliekwaliteit bij hydraulische en pneumatische systemen; houd rekening met omgevingscondities.

CCF Bepaal of voldoende aandacht is besteed aan het voorkomen van Common Cause fouten met behulp van een checklist.	Een Common Cause fout is één fout die beide kanalen laat falen, zoals een overbelasting waardoor 2 contactors tegelijk blijven kleven. Voor PL moet een bepaald aantal punten worden gescoord in de checklist, voor SIL volgt uit de checklist nog een factor β die gebruikt wordt in de PFH_D berekening.

Software in veiligheidsPLC's

Software

Alleen door een goed ontwerptraject kunnen fouten in software worden voorkomen. Gebruik het V-model (lifecycle activities) en zorg dat de werkwijze past bij de complexiteit en omvang van het systeem. Hieronder een vereenvoudigd V-model dat specifiek gericht is op software in veiligheidsPLC's. De leverancier voorziet dan in een structuur met een programmeertaal en geteste functieblokken.



Specificatie

De specificatie van de software omvat vooral de specificatie van de veiligheidsfuncties en het ontwerp van de hardware (architectuur & functionaliteit). Deze worden aangevuld met enkele PLC specificaties en een verwijzing naar de coding standards.

Ontwerp

Het ontwerp van de software bevat onder andere:

- De PLC I/O inclusief redundantie, testpulsen, discrepantie en diagnose.
- De architectuur van de software waarmee alle veiligheidsfuncties worden ingevuld.
- De logica van de veiligheidsfuncties, gebruik een systematische methode zoals 'cause & effect' diagram.
- Functies voor het detecteren van fouten zoals looptijdbewaking, plausibiliteit en feedback.
- De interactie met de reguliere PLC door commando- en statusbits.

Ontwerp review & coderen

Het is belangrijk dat het ontwerp volledig is. De programmeur voert een review uit en mag het ontwerp niet aanvullen of aanpassen. Het programma wordt geschreven op basis van het ontwerp en de coding standards als leidraad. De programmeur heeft de specifieke kennis die nodig is voor de gebruikte veiligheidsPLC en moet in staat zijn om de software op een leesbare, begrijpelijke manier te implementeren. Aan een programma dat er eenvoudig uitziet, en dat daardoor goed te testen en te onderhouden is, kan het vakmanschap van een goede programmeur herkend worden!

Code review & testen

Leesbare software, gebaseerd op een goed ontwerp laat zich prima reviewen. Is het software ontwerp correct en compleet vertaald naar code? Zijn de coding standards toegepast? Bij een veiligheidsPLC zijn er specifieke taken aan de I/O toebedeeld die alvast kunnen worden gecontroleerd en getest (I/O test). Bij redundante (sub) systemen is de diagnose in het ontwerp beschreven, laat een fout optreden en controleer of de juiste actie in gang gezet wordt (fault insertion testing). Activeer bijvoorbeeld een lichtscherm om te testen of een aandrijving stopt. Hier is de controle op de reactietijd van belang maar ook op de bedrijfsmodi, muting en andere overbruggingen of uitzonderingen (functionele test). Maak in de testplannen onderscheid tussen testen die bijvoorbeeld gesimuleerd, op een proefopstelling of aan de machine worden uitgevoerd.

Configuratiemanagement

Het PLC programma, met de juiste signature, wordt onder configuratiemanagement (CM) geplaatst. Het is gebruikelijk om vast te leggen welke versie van de software bij welke klant draait. Maar CM omvat veel meer. Als ergens versie 8 van de veiligheidssoftware draait, moet vastliggen waarom van versie 7 naar versie 8 is gegaan, de reden van de wijziging, of de specificatie is aangepast, wat er gewijzigd is in het ontwerp, wie de wijziging heeft uitgevoerd, welk testrapport erbij hoort en of er weer verificatie- en validatiestappen zijn uitgevoerd. Dus in principe vallen alle stappen binnen het V-model (hard- en software) onder CM. Eisen, ontwerp, code, testrapporten, plannen en procedures moeten voorwaarts en achterwaarts traceerbaar zijn van specificatie tot validatie. Zorg voor een wijzigingsprotocol zodat deze werkwijze wordt geborgd gedurende de levensduur van de machine. Voorkom ongeoorloofde wijzigingen!

De gebruiksaanwijzing van de machine

Dit is een omvangrijk document, of eigenlijk een serie van documenten, dat alle informatie bevat die de gebruiker nodig heeft om de machine goed en veilig op zijn plaats te krijgen, te gebruiken, te onderhouden, te repareren en te demonteren. Dus inclusief de operator handleiding, de service handleiding, de installatie instructies, de elektrische schema's, transportgegevens enzovoorts. In veel normen is terug te vinden wat er specifiek voor dat onderwerp in de gebruiksaanwijzing moet worden opgenomen. Onderstaande items mogen, op grond van de SIL- of PL norm, tenminste verwacht worden in de gebruiksaanwijzing van een machine.

Over Kader Group

Kader Group verbetert de kwaliteit, veiligheid en duurzaamheid van organisaties, zodat een ieder goed kan zorgen voor mens, milieu en maatschappij. Dat doen we met onze consultancy & interim diensten, digitale oplossingen en opleidingen op de gebieden kwaliteit, veiligheid & gezondheid, cyber security en milieu & duurzaamheid. Onze missie: het creëren van een veilige en duurzame leefomgeving om door te geven aan toekomstige generaties. We zijn daarin pragmatisch, innovatief, persoonlijk en vakkundig.

Kader Group startte in 1994 en bestaat inmiddels uit ruim 200 gedreven medewerkers. Vanuit onder meer 3 business units helpen wij onze opdrachtgevers bij te dragen aan een betere leefomgeving:

- Academy
- Consultancy & Interim
- Digital

Bekijk het op
kader.nl

Ook interessant voor jou?

**Ben je benieuwd waar we je jou bij kunnen ondersteunen?
Wellicht zijn onderstaande onderwerpen interessant!**

Opleiding

Basistraining SIL machinebouw en FSDT/TIA-ST

Na de training ben je in staat om veiligheidsfuncties op te stellen en het behalen van het SIL level aan te tonen door berekeningen. Door de praktische oefeningen met de tools krijg je een goed begrip van hoe de SIL norm kan worden toegepast.

Meer informatie ›

Dienst

Functionele Veiligheid in de machinebouw

Of je een machinebouwer bent of een eindgebruiker die een vinger aan de pols wil houden bij de leverancier van een nieuwe machine, wij helpen je graag met jouw vraagstukken of projecten over functionele veiligheid. Dit kan in de vorm van advies, coaching of begeleiding van klantspecifieke projecten.

Meer informatie ›

Opleiding

Performance Level en SISTEMA training

Na de PL en SISTEMA training ben je in staat om veiligheidsfuncties te ontwerpen en uit te werken. Je kunt het te behalen PL level aantonen door berekeningen in SISTEMA. Door de praktische oefeningen met SISTEMA weet je hoe de PL norm kan worden toegepast.

Meer informatie ›

Kader Almelo

Bedrijvenpark Twente 301
7602 KL Almelo
0546 536 800

Kader Breda

Stadionstraat 32
4815 NG Breda
076 5040 340

Kader Harderwijk

Prins Mauritslaan 45c
3843 AJ Harderwijk
0341 43 08 48

Kader Zeist

Dijnselburgerlaan 2
3705 LP Zeist
030 243 64 64

kader.nl | sales.kceni@kader.nl

V.1122