SAFEBOOK 5 VOOR MACHINES

Allen-Bradley

Guardmaster®

Veiligheidsgerelateerde besturings-systemen voor machines

Principes, normen en implementatie

(Revisie 5 van de Safebook-serie)

LISTEN. THINK. SOLVE.℠

Rockwell Automation

Veiligheidsgerelateerde machinebesturingssystemen

Inhoudsopgave

Hoofdstuk 1: Richtlijnen

Richtlijnen en wetgeving van de Europese Unie

Dit gedeelte dient als leidraad voor iedereen die met machineveiligheid te maken heeft, in het bijzonder wat betreft het gebruik van veiligheids- en vergrendelingssystemen binnen de Europese Unie. Dit gedeelte is bestemd voor de ontwerpers en gebruikers van industriële apparatuur.

Om het concept van een open markt te bevorderen binnen de Europese Economische Ruimte (EER) (die alle EU-lidstaten en nog drie landen omvat), zijn alle lidstaten verplicht om wetten op te stellen en toe te passen die de essentiële veiligheidseisen voor machines en het gebruik daarvan te definiëren.

Machines die niet aan deze eisen voldoen, kunnen niet aan of binnen EER-landen worden geleverd.

Er zijn verschillende Europese richtlijnen van toepassing op veiligheid van industriële machines en apparatuur. De twee meest relevante zijn:

1 De Machinerichtlijn

2 De Arbeidsmiddelenrichtlijn

Deze twee richtlijnen zijn rechtstreeks aan elkaar gerelateerd, omdat de essentiële veiligheids- en gezondheidseisen van de Machinerichtlijn kunnen worden gebruikt om de veiligheid van apparatuur in de Richtlijn voor het gebruik door werknemers van arbeidsmiddelen op de arbeidsplaats te waarborgen.

In dit gedeelte wordt op aspecten van beide richtlijnen ingegaan. Iedereen die zich bezighoudt met het ontwerp, de toevoer, inkoop of het gebruik van industriële apparatuur in of naar de EER en bepaalde andere Europese landen wordt aangeraden om zich vertrouwd te maken met de eisen van deze richtlijnen. Als er niet aan deze richtlijnen wordt voldaan, zullen de meeste leveranciers eenvoudig geen toestemming krijgen om machines aan deze landen te leveren, en zullen gebruikers in deze landen dergelijke machines niet mogen gebruiken.

Er bestaan nog andere Europese richtlijnen die van toepassing kunnen zijn op machines. De meeste van deze richtlijnen hebben betrekking op relatief specialistische aspecten, en zullen we hier dan ook buiten beschouwing laten. Het is echter van belang om hier op te merken dat, waar van toepassing, eveneens aan de eisen van deze richtlijnen dient te worden voldaan. Voorbeelden zijn onder meer: De EMC-richtlijn 2014/30/EC en de ATEX-richtlijn 2014/34/EC.

De Machinerichtlijn

De Machinerichtlijn is van toepassing op de levering van nieuwe machines en overige apparatuur, met inbegrip van veiligheidscomponenten. Het is verboden om binnen de EU machines te leveren die niet aan de bepalingen en eisen van deze richtlijn voldoen.

De breedste definitie van “machines” die in de richtlijn wordt gegeven, luidt als volgt: “een samenstel, voorzien van of bestemd om te worden voorzien van een aandrijfsysteem, maar niet op basis van rechtstreeks gebruikte menselijke of dierlijke spierkracht, van onderling verbonden onderdelen of organen waarvan er ten minste één kan bewegen, en die in hun samenhang bestemd zijn voor een bepaalde toepassing”

Aan de machine bevestigde CE-normering

De huidige Machinerichtlijn (2006/42/EC) heeft eind 2009 zijn voorganger (98/37/EC) vervangen. Deze richtlijn bevat verduidelijkingen en aanvullingen, maar de essentiële veiligheids- en gezondheidseisen zijn bijna niet gewijzigd. Er zijn een aantal wijzigingen opgenomen die samenhangen met veranderde technologieën en methoden. De reikwijdte van de richtlijn is vergroot door de opname van extra soorten apparatuur (bijv. bouwliften). De richtlijn bevat nu de expliciete eis dat door middel van een risicoanalyse vastgesteld moet worden welke veiligheids- en gezondheidseisen van toepassing zijn. Daarnaast zijn de procedures van de overeenstemmingsbeoordeling gewijzigd voor de in bijlage IV genoemde apparatuur. Gedetailleerde informatie over en een leidraad voor de definitie en alle andere aspecten van de Machinerichtlijn is te vinden op de officiële EU website:

http://ec.europa.eu/growth/sectors/mechanical-engineering/machinery/index_en.htm

De kernbepalingen van de oorspronkelijke richtlijn (98/37/EC) zijn op 1 januari 1995 van kracht geworden voor machines en op 1 januari 1997 voor veiligheidscomponenten.

De bepalingen van de huidige richtlijn (2006/42/EC) zijn van kracht geworden met ingang van 29 december 2009. De fabrikant of zijn gemachtigde vertegenwoordiger moet waarborgen dat geleverde apparatuur aan de richtlijn voldoet. Dit omvat:

- waarborgen dat aan de toepasselijke veiligheids- en gezondheidseisen uit Bijlage I van de richtlijn wordt voldaan;
- het samenstellen van een technisch dossier;
- het uitvoeren van een passende beoordeling van overeenstemming;
- het afgeven van een “EG-verklaring van overeenstemming”;
- het indien nodig aanbrengen van CE-markering;
- het zorgen voor veiligheidsinstructies

Essentiële veiligheids- en gezondheidseisen

Machine dient te voldoen aan essentiële veiligheids- en gezondheidseisen

Bijlage 1 van de richtlijn biedt een overzicht van essentiële veiligheids- en gezondheidseisen waaraan machines in relevante gevallen moeten voldoen. Dit overzicht heeft ten doel om ervoor te zorgen dat machines veilig zijn en op zodanige wijze ontworpen en gebouwd worden dat ze tijdens alle fasen van hun levenscyclus kunnen worden gebruikt, aangepast en onderhouden worden zonder dat dit gevaar oplevert voor mensen. De volgende tekst biedt een snel overzicht van een paar typische vereisten. Het is belangrijk om rekening te houden met alle gezondheids- en veiligheidseisen die in Bijlage 1 worden gegeven. Er moet een risicoanalyse worden uitgevoerd om te bepalen welke essentiële gezondheids- en veiligheidseisen van toepassing zijn op de betreffende apparatuur.

De veiligheids- en gezondheidseisen uit Bijlage 1 bieden een stelsel van maatregelen voor het elimineren van risico's:

(1) Inherent veilig ontwerp. Waar mogelijk dienen in het ontwerp risico's uitgesloten te worden. Indien dit niet mogelijk is, moeten **(2) aanvullende veiligheidsmaatregelen** genomen te worden zoals afschermingen met of zonder vergrendeling, lichtgordijnen, veiligheidsmatten enz. Alle overige risico's waar de bovengenoemde methoden geen oplossing voor bieden dienen te worden ingeperkt door middel van **(3) persoonlijke beschermingsmiddelen en/of training**. De machineleverancier dient aan te geven wat in dit verband wenselijk is.

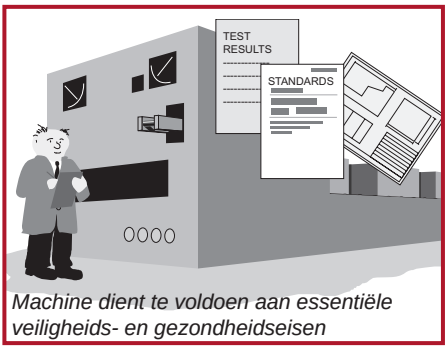
Voor de bouw en de bediening dienen geschikte materialen te worden gebruikt. De fabrikant dient voor afdoende verlichting en uitrusting te zorgen. De besturingssystemen dienen veilig en betrouwbaar te zijn. Machines mogen zich niet onverwacht in werking stellen, en dienen te worden uitgerust met een of meer noodstopvoorzieningen. Daarnaast moet men rekening houden met complexe installaties waarbij upstream- en downstreamprocessen invloed kunnen hebben op de veiligheid van een machine. Het uitvallen van de voeding of stuurstroom mag niet tot een gevaarlijke situatie leiden. Machines moeten stabiel zijn en in staat zijn om voorspelbare belastingen te weerstaan. Randen of oppervlakken die letsel kunnen veroorzaken, dienen te zijn afgedekt.

Er dient gebruik te worden gemaakt van afschermingen en veiligheidsvoorzieningen om bescherming te bieden tegen gevaren zoals bewegende onderdelen. Deze voorzieningen dienen stevig gebouwd te zijn en moeilijk te omzeilen. Vaste afschermingen dienen zodanig te zijn gemonteerd dat ze alleen met behulp van gereedschap kunnen worden verwijderd, en de bevestigingen moeten vastgezet zijn. Beweegbare afschermingen dienen te worden vergrendeld. Verstelbare afschermingen moeten zonder gebruik van gereedschap kunnen worden afgesteld.

Gevaren ontstaan uit elektrische of andere energiebronnen, inclusief opgeslagen energie, dienen te worden voorkomen. De kans op verwonding als gevolg van te hoge of te lage temperaturen, explosies, geluid, trilling, stof, gassen of straling dient minimaal te zijn. Op de machine dienen toepasselijke voorzieningen voor onderhoud en reparatie aanwezig te zijn. Op de machine dienen verder voldoende informatie- en waarschuwingsvoorzieningen aanwezig te zijn. De machine dient te worden geleverd met instructies voor een veilige installatie, veilig gebruik, veilige afstelling enzovoort.

Overeenstemmingsbeoordeling

De ontwerper of een andere verantwoordelijke rechtspersoon dient bewijs te overhandigen dat de overeenstemming met de essentiële veiligheids- en gezondheidseisen aantoont. In dit dossier dienen alle relevante gegevens te zijn opgenomen, zoals de testresultaten, tekeningen, specificaties enzovoort.



Machine dient te voldoen aan essentiële veiligheids- en gezondheidseisen

Een geharmoniseerde Europese (EN)-norm die is gepubliceerd in het Publicatieblad van de Europese Unie (PB) onder de Machinerichtlijn, en waarvan de beëindigingsdatum van de veronderstelling van overeenstemming niet is vervallen, voorziet in een veronderstelling van overeenstemming met bepaalde essentiële veiligheids- en gezondheidseisen. (Veel recente normen die in het Publicatieblad van de Europese Unie worden gepubliceerd, gaan vergezeld van een kruisverwijzing die de essentiële veiligheids- en gezondheidseisen aanduidt waarop de norm betrekking heeft). Als apparatuur in overeenstemming is met dergelijke actuele geharmoniseerde Europese normen, wordt de taak om aan te tonen dat de apparatuur in overeenstemming is met de essentiële veiligheids- en gezondheidseisen dan sterk vereenvoudigd. Bovendien kan de fabrikant in dat geval profiteren van een hogere mate van juridische zekerheid. Hoewel de eisen van deze normen niet in een wet zijn opgenomen, wordt fabrikanten sterk aanbevolen ervoor te zorgen dat hun producten aan deze eisen voldoen. Het aantonen van overeenstemming op basis van alternatieve methoden kan namelijk een uiterst complexe aangelegenheid zijn. Deze normen bieden ondersteuning voor de Machinerichtlijn en worden ontwikkeld door CEN (het Europees Comité voor Normalisatie) in samenwerking met ISO en door CENELEC (het Europees Comité voor elektrotechnische standaardisatie) in samenwerking met de IEC.

Er dient een grondige, gedocumenteerde risicoanalyse te worden uitgevoerd om te garanderen dat alle potentiële machinegevaren zijn beoordeeld. Op vergelijkbare wijze is het de verantwoordelijkheid van de machinefabrikant om ervoor te zorgen dat aan alle essentiële veiligheids- en gezondheidseisen wordt voldaan, zelfs aan de eisen die niet in de geharmoniseerde EN-normen worden vermeld.

Technisch dossier

De fabrikant of zijn gemachtigde vertegenwoordiger moeten een technisch dossier samenstellen waarin materiaal wordt opgenomen dat overeenstemming met de veiligheids- en gezondheidseisen aantoont. In dit dossier dienen alle relevante gegevens te zijn opgenomen, zoals de testresultaten, tekeningen, specificaties enzovoort.

Het is niet noodzakelijk dat alle informatie permanent op papier beschikbaar is. Het complete technisch dossier moet echter wel op verzoek van een deskundige autoriteit (een door een EU-land aangemelde instantie die de overeenstemming van de machines bewaakt) gecontroleerd kunnen worden.

Het technisch dossier moet ten minste de volgende documentatie bevatten:

1. Overzichtstekeningen van de apparatuur, met inbegrip van tekeningen van stuurstromen.

2. Gedetailleerde tekeningen, opmerkingen met betrekking tot berekeningen enz. die zijn vereist voor het controleren van de overeenstemming van de machine met de essentiële veiligheids- en gezondheidseisen.

3. Risicoanalysedocumentatie, waaronder een lijst met de essentiële veiligheids- en gezondheidseisen die op de machines van toepassing zijn, en een omschrijving van de geïmplementeerde veiligheidsmaatregelen.

4. Een lijst met toegepaste normen en andere technische specificaties die aangeeft welke essentiële veiligheids- en gezondheidseisen van toepassing zijn.

5. Een omschrijving van de methoden die worden gebruikt om machinegevaren te elimineren.

6. Indien van toepassing, technische rapporten of certificaten van een testfaciliteit of een andere instantie.

7. In het geval van een verklaring van overeenstemming met een geharmoniseerde Europese norm dient elk technisch rapport de relevante testresultaten te vermelden.

8. Een exemplaar van de gebruiksaanwijzing van de machine.

9. Indien van toepassing, de inbouwverklaring voor aanwezige niet-voltooide machines en de bijbehorende montage-instructies.

10. Indien van toepassing, exemplaren van de EG-verklaring van overeenstemming voor machines of andere producten die in machines zijn ingebouwd.

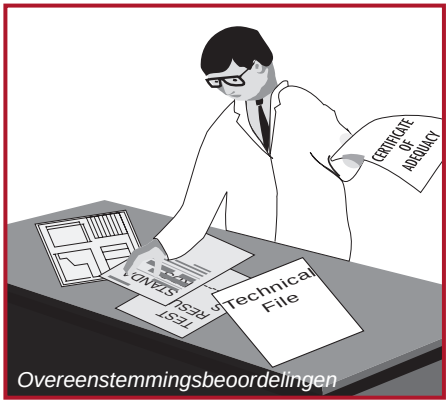
11. Een exemplaar van de EG-verklaring van overeenstemming.

In het geval van serieproductie moeten details met betrekking tot interne maatregelen (zoals kwaliteitssystemen) worden vermeld die de overeenstemming van alle geproduceerde machines waarborgen:

- De fabrikant dient zelf het noodzakelijke onderzoek uit te voeren en onderdelen, montagestukken of de voltooide machine testen om vast te stellen of de machine op basis van zijn ontwerp en bouw geschikt is om te worden geïnstalleerd en op veilige wijze in gebruik kan genomen worden.
- Hoewel het technisch dossier niet de vorm van één permanent dossier hoeft te hebben, moet de fabrikant in staat zijn om dit dossier binnen een redelijke periode samen te stellen en beschikbaar te maken. Het technisch dossier dient gedurende een periode van tien jaar na de productie van de laatste machine beschikbaar blijven.

In het technisch dossier hoeven geen gedetailleerde plannen of andere specifieke informatie over de onderdelen die voor de productie van de machine worden gebruikt te zijn opgenomen, tenzij deze informatie van essentieel belang is om de overeenstemming met de essentiële veiligheids- en gezondheidseisen te bewijzen.

Procedures voor de overeenstemmingsbeoordeling van machines in Bijlage IV



Overeenstemmingsbeoordelingen

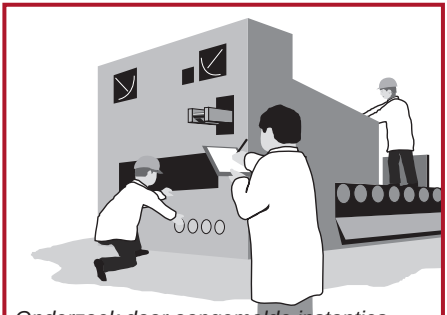
Op bepaalde typen machines zijn speciale maatregelen van toepassing. Deze machines worden vermeld in Bijlage IV van de richtlijn, en omvat gevaarlijke machines, zoals bepaalde houtbewerkingsmachines, persen, spuitgietmachines, ondergrondse apparatuur, reparatieliften voor voertuigen enzovoort.

In Bijlage IV zijn tevens bepaalde veiligheidscomponenten opgenomen, zoals veiligeheidsvoorzieningen die dienen om de aanwezigheid van personen te detecteren (bijv. lichtschermen) en logische eenheden die de werking van veiligheidsfuncties waarborgen.

In het geval van machines uit Bijlage IV die niet volledig overeenstemmen met de betreffende geharmoniseerde Europese normen, moet de fabrikant of zijn gemachtigde vertegenwoordiger een van de volgende procedures toepassen:

1. EG-typeonderzoek. Er moet een technisch dossier worden samengesteld en een exemplaar van de machine moet voor EG-typeonderzoek beschikbaar worden gesteld aan een aangemelde instantie (testinstelling). Als de machine aan de eisen voldoet, krijgt deze een testcertificaat voor het EG-typeonderzoek. De geldigheid van het certificaat moet om de vijf jaar opnieuw door de aangemelde instantie worden beoordeeld.

2. Volledige kwaliteitsborging. Er moet een technisch dossier worden samengesteld en de fabrikant moet bij het ontwerp, de fabricage, de eindinspectie en het testen gebruikmaken van een goedgekeurd kwaliteitssysteem. Het kwaliteitssysteem moet waarborgen dat de machines overeenstemmen met de bepalingen van de richtlijn. Het kwaliteitssysteem moet regelmatig door een aangemelde instantie worden gecontroleerd.



Onderzoek door aangemelde instanties

In het geval van machines die niet in Bijlage IV zijn opgenomen of machines die wel in Bijlage IV zijn opgenomen maar niet volledig overeenstemmen met de geharmoniseerde Europese normen, kan de fabrikant of zijn gemachtigde vertegenwoordiger ook een technisch dossier samenstellen en de overeenstemming van de apparatuur zelf beoordelen en zelf een verklaring van overeenstemming afgeven. Er moeten interne controles worden gehouden die waarborgen dat de gefabriceerde apparatuur in overeenstemming blijft.

Aangemelde instanties

In de EU is er een netwerk van aangemelde instanties die met elkaar overleggen en werken aan gemeenschappelijke criteria. Aangemelde instanties worden aangesteld door overheden, en niet door de branche. Informatie over organisaties met de status van aangemelde instantie is beschikbaar via:

http://ec.europa.eu/growth/tools-databases/nando/

Procedure voor EG-verklaringen van overeenstemming

De CE-markering moet aangebracht worden op alle geleverde machines. De machines dienen eveneens met een EG-verklaring van overeenstemming te worden geleverd.

De CE-markering geeft aan dat de machine voldoet aan alle toepasselijke Europese richtlijnen en dat de procedures van de overeenstemmingsbeoordeling zijn voltooid. Het is verboden in het kader van de Machinerichtlijn een CE-markering aan te brengen indien de machine niet aan de betreffende veiligheids- en gezondheidseisen voldoet.

De EG-verklaring van overeenstemming moet de volgende gegevens bevatten:

- Firmanaam en volledig adres van de fabrikant en indien van toepassing van zijn gemachtigde vertegenwoordiger;
- Naam en adres van de persoon die gemachtigd is om het technisch dossier samen te stellen; deze persoon moet gevestigd zijn in de Gemeenschap (in het geval van een fabrikant van buiten de EU kan dit de “gemachtigde vertegenwoordiger” zijn;
- Beschrijving en identificatie van de machine, waaronder generieke benaming, functie, model, type, serienummer en handelsbenaming;
- Een zin waarin uitdrukkelijk wordt verklaard dat de machine voldoet aan alle toepasselijke bepalingen van deze richtlijn en indien van toepassing een soortgelijke zin waarin wordt verklaard dat de machine in overeenstemming is met andere richtlijnen en/of toepasselijke bepalingen;
- Indien van toepassing, een verwijzing naar de toegepaste geharmoniseerde normen;
- Indien van toepassing, een verwijzing naar andere toegepaste technische normen en specificaties;
- (In het geval van machines uit Bijlage IV) indien van toepassing, de naam, het adres en het identificatienummer van de aangemelde instantie die het EG-typeonderzoek als bedoeld in Bijlage IX heeft uitgevoerd en het nummer van het certificaat van het EG-typeonderzoek;
- (In het geval van machines uit Bijlage IV) indien van toepassing, de naam, het adres en het identificatienummer van de aangemelde instantie die het in Bijlage X bedoelde systeem van volledige kwaliteitsborging heeft goedgekeurd;
- Plaats en datum van opstelling van de verklaring;
- Identiteit en handtekening van de persoon die gemachtigd is om namens de fabrikant of zijn gemachtigde vertegenwoordiger de verklaring op te stellen

EG-inbouwverklaring voor niet-voltooide machines

Als de apparatuur wordt geleverd om op een later tijdstip met andere onderdelen tot een complete machine te worden gemonteerd, moet er een INBOUWVERKLARING worden verstrekt. De CE-markering mag in dergelijke gevallen NIET worden aangebracht. De verklaring dient aan te geven dat de apparatuur pas in gebruik mag worden genomen wanneer is verklaard dat de machine waarin deze is ingebouwd aan de eisen van alle toepasselijke normen voldoet. Er moet een technisch dossier worden samengesteld en de niet-voltooide machine moet geleverd worden met gegevens die omschrijven onder welke voorwaarden de niet-voltooide machine in de afgewerkte machine moet worden ingebouwd. Dit dient om de veiligheid te waarborgen.

Deze optie is niet beschikbaar voor apparatuur die onafhankelijk kan functioneren of apparatuur die een wijziging van de functionaliteit van een machine inhoudt.

De inbouwverklaring moet de volgende gegevens bevatten:

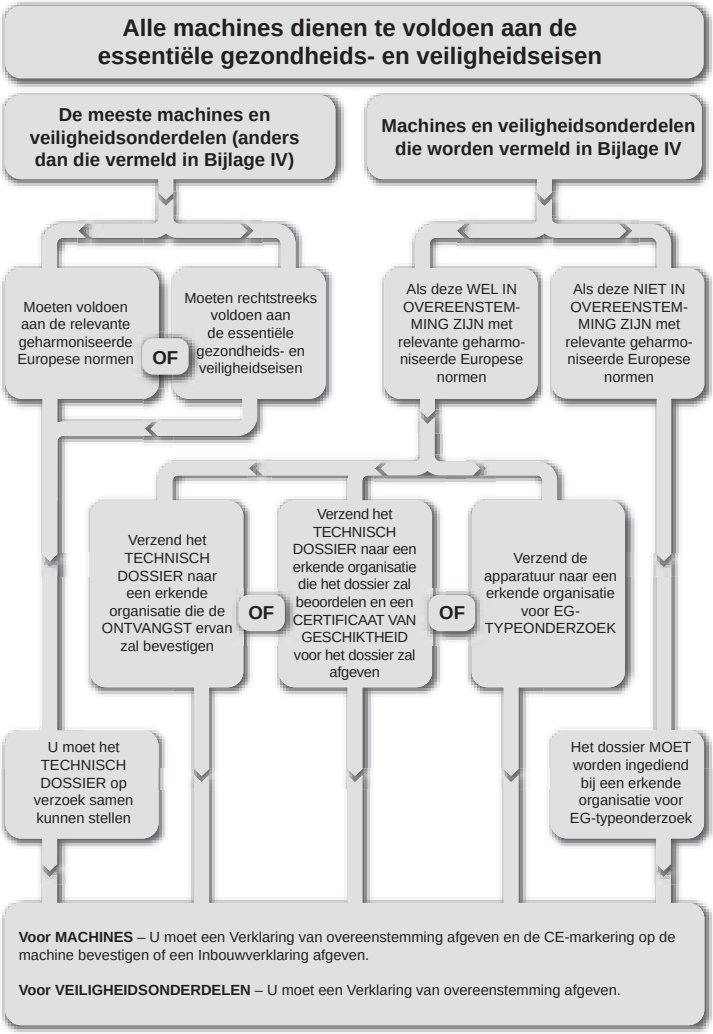
- Frimanaam en volledig adres van de fabrikant van de niet-voltooide machine en, indien van toepassing, van zijn gemachtigde vertegenwoordiger;
- Naam en adres van de persoon die gemachtigd is om de toepasselijke technische documenten samen te stellen; deze persoon moet gevestigd zijn in de Gemeenschap (in het geval van een fabrikant van buiten de EU kan dit de gemachtigde vertegenwoordiger zijn;
- Beschrijving en identificatie van de niet-voltooide machine, waaronder generieke benaming, functie, model, type, serienummer en handelsbenaming;
- Een zin waarin wordt verklaard welke essentiële eisen van deze richtlijn toegepast en vervuld zijn en dat de toepasselijke technische documenten overeenkomstig Bijlage VII, punt B zijn opgesteld en indien van toepassing een zin waarin wordt verklaard dat de niet-voltooide machine met andere toepasselijke richtlijnen overeenstemt;
- Een verbintenis om op met redenen omkleed verzoek van de nationale autoriteiten de relevante informatie over de niet-voltooide machine door te geven. Deze verbintenis bevat ook een vermelding van de wijze van doorgifte en laat de intellectuele-eigendomsrechten van de fabrikant van de niet-voltooide machine onverlet;
- Indien van toepassing, een verklaring dat de niet-voltooide machine niet in bedrijf mag worden genomen voordat voor de afgewerkte machine waarin deze zal worden ingebouwd, een verklaring van overeenstemming met de bepalingen van deze richtlijn voorhanden is;
- Plaats en datum van opstelling van de verklaring;
- Identiteit en handtekening van de persoon die gemachtigd is om namens de fabrikant of zijn gemachtigde vertegenwoordiger de verklaring op te stellen.

Machines afkomstig van leveranciers van buiten de EU – Gemachtigde vertegenwoordigers

Als een buiten de EU (of EER) gevestigde fabrikant machines naar de EU exporteert, moet hij een gemachtigde vertegenwoordiger aanwijzen.

Een gemachtigde vertegenwoordiger is elke in de Europese Gemeenschap gevestigde natuurlijke of rechtspersoon die van de fabrikant een schriftelijke volmacht heeft ontvangen om namens hem alle of bepaalde verplichtingen en formaliteiten in samenhang met de Machinerichtlijn uit te voeren.

De Arbeidsmiddelenrichtlijn van de Europese Unie



Waar de Machinerichtlijn is gericht op leveranciers van machines, is deze richtlijn (2009/104/EC) gericht op gebruikers van machines. Deze richtlijn is van toepassing op alle industriële sectoren en legt algemene verplichtingen op aan de werkgevers, gecombineerd met minimumeisen op het gebied van de veiligheid van arbeidsmiddelen. Alle EU-landen bepalen hun eigen wetgeving met betrekking tot de implementatie van deze richtlijn.

Als voorbeeld nemen we de toepassing van deze richtlijn in het Verenigd Koninkrijk onder de naam The Provision and Use of Work Equipment Regulations (vaak afgekort als P.U.W.E.R.). Hoewel de toepassingswijze per land kan verschillen, blijven de minimumeisen van kracht.

De artikelen van deze richtlijn bieden informatie over de soorten apparatuur en werkplekken waarop de richtlijn van toepassing is.

Daarnaast leggen deze richtlijn algemene verplichtingen op aan de werkgevers. Zo moeten de werkgevers zorg dragen voor veilige werkplekken, veilige en geschikte apparatuur beschikbaar stellen en deze apparatuur op de juiste wijze onderhouden. De gebruikers van de machines dienen op de juiste wijze over het gebruik van de machines te worden geïnformeerd en training te volgen voor veilig gebruik van de machine.

Nieuwe machines (en tweedehands machines die van buiten de EU afkomstig zijn) die na 1 januari 1993 zijn geleverd, moeten aan alle relevante productrichtlijnen voldoen, zoals bijvoorbeeld de Machinerichtlijn (behoudens relevante overgangsregelingen). Tweedehands apparatuur die van binnen de EU afkomstig is en voor de eerste keer op de werkplek wordt geleverd, moet onmiddellijk voldoen aan de minimumeisen die in een bijlage van de arbeidsmiddelenrichtlijn zijn opgenomen.

Opmerking: Bestaande en tweedehands machines die in hoge mate zijn herzien of gewijzigd worden als nieuwe apparatuur beschouwd. Het werk dat op deze machines wordt uitgevoerd dient dientengevolge in overeenstemming te zijn met de Machinerichtlijn (zelfs als deze machines voor intern gebruik zijn bestemd).

Een belangrijke eis van de richtlijn en wijst op de verantwoordelijkheid van de werkgever om een afdoend risicoanalyseproces uit te voeren zodat de machines geschikt en veilig zijn voor te uit te voeren werkzaamheden.

Het is een eis dat machines correct worden onderhouden. In de meeste gevallen houdt dit in dat er sprake dient te zijn van routinematig en gepland preventief onderhoud. Het wordt aanbevolen om een logboek bij te houden. Dit is met name belangrijk in gevallen waarbij het onderhoud en de inspectie van de apparatuur bijdraagt aan de voortdurende veiligheidsintegriteit van een veiligheidscomponent of -systeem.

De bijlage van de arbeidsmiddelenrichtlijn biedt algemene minimumeisen die van toepassing zijn op arbeidsmiddelen.

Als de apparatuur voldoet aan de toepasselijke productrichtlijnen, bijvoorbeeld de Machinerichtlijn, voldoet ze automatisch aan de bijbehorende machineontwerpeisen die in de minimumeisen van de bijlage.

Lidstaten mogen wetten aangaande het gebruik van arbeidsmiddelen uitvaardigen die hogere eisen stellen dan de minimumeisen in de arbeidsmiddelenrichtlijn.
Ga voor meer informatie over de arbeidsmiddelenrichtlijn naar de officiële website van de Europese Unie:

https://osha.europa.eu/en/legislation/directives/3

Amerikaanse richtlijnen

Dit gedeelte vormt een introductie tot een aantal machineveiligheidsrichtlijnen in de Verenigde Staten. De informatie in dit gedeelte dient louter als uitgangspunt. De lezers dienen zelf de eisen voor hun specifieke toepassingen te bestuderen en maatregelen te treffen om ervoor te zorgen dat hun ontwerpen, gebruiks- en onderhoudsprocedures en werkwijzen aan hun interne eisen en die van de nationale en regionale wet- en regelgeving voldoen.

Tal van Amerikaanse organisaties hebben als doel om de industriële veiligheid te bevorderen. Dit zijn onder meer:

1. Bedrijven die gebruikmaken van bestaande richtlijnen en hun eigen interne richtlijnen opstellen;

2. De Occupational Safety and Health Administration (OSHA);

3. Industriële organisaties, zoals de National Fire Protection Association (NFPA), de Robotics Industries Association (RIA) en de Association of Manufacturing Technology (AMT), ANSI die een lijst met erkende consensusnormen publiceert; en leveranciers van veiligheidsproducten en -oplossingen, zoals Rockwell Automation.

De Occupational Safety and Health Administration

De Occupational Safety and Health Administration (OSHA) is een van de belangrijkste Amerikaanse organisaties die de industriële veiligheid bevorderen. De OSHA werd in 1971 opgericht op basis van de aanname van een wet door het Amerikaanse congres. Deze wet heeft ten doel om veilige en gezonde werkomstandigheden te garanderen en personeel te beschermen. De wet machtigt de Amerikaanse minister van arbeid om verplichte veiligheids en gezondheids-normen op te stellen die van toepassing zijn op bedrijven die handel drijven tussen de staten onderling. Deze wet is van toepassing op werkzaamheden die worden uitgevoerd op werkplekken in Amerikaanse staten, het district Columbia, Puerto Rico, de Maagdeneilanden, Amerikaans-Samoa, Guam, het Trustgebied van de Pacifische Eilanden, Wake-eiland, het gebied van het buitenste continentaal plat zoals gedefinieerd in de wet inzake de gebieden van het buitenste continentaal plat, het Johnston-atol en de kanaalzone.

In Artikel 5 van deze wet worden de basiseisen uiteengezet. Elke werkgever dient aan elk van zijn werknemers werk en een werkplek te bieden. Het werk en de werkplek dienen vrij te zijn van erkende gevaren die naar alle waarschijnlijkheid kunnen resulteren in ernstig letsel of het overlijden van de werknemers, en dienen te voldoen aan de veiligheids en gezondheids-normen die door deze wet worden voorgeschreven.

Artikel 5 schrijft daarnaast voor dat elke werknemer dient te voldoen aan de veiligheids en gezondheids-normen en aan alle regels, richtlijnen en instructies die krachtens deze wet van toepassing zijn op zijn of haar handelingen en gedrag.

De OSHA-wet stelt zowel de werkgever als werknemer verantwoordelijk. In deze zin wordt in hoge mate afgeweken van de Machinerichtlijn, die voorschrijft dat leveranciers alleen machines op de markt mogen brengen die geen gevaren opleveren. In de Verenigde Staten kunnen leveranciers machines zonder veiligheidsvoorzieningenop de markt brengen. De gebruiker dient de veiligheidsvoorzieningen zelf aan te brengen om de machine veilig te maken. Hoewel deze werkwijze veel werd toegepast op het moment dat deze wet werd goedgekeurd, is de huidige trend dat fabrikanten machines met veiligheidsvoorzieningen leveren. De reden hiervan is dat het integreren van veiligheidsvoorzieningen in een machine veel efficiënter is dan het toevoegen van veiligheidsinrichtingen nadat de machine is ontworpen en gebouwd. De opstellers van normen proberen nu om de leverancier en de gebruiker veiligheidseisenmet elkaar uit te laten wisselen, zodat de resulterende machines niet alleen veilig, maar ook productiever zijn.

De Amerikaanse minister van arbeid heeft de bevoegdheid om alle normen waarover nationale overeenstemming bestaat als veiligheids en gezondheids-norm in te stellen. Dit geldt eveneens voor alle bestaande federale overheidsnormen, tenzij de instelling van een dergelijke norm niet zou resulteren in een verbetering van de veiligheid of gezondheid van specifiek aangewezen werknemers.

OSHA vervult deze taak door richtlijnen te publiceren in titel 29 van de Code of Federal Regulation (29 CFR). Normen die betrekking hebben op industriële machines worden door OSHA gepubliceerd in Part 1910 van 29 CFR. De normen zijn vrij beschikbaar op de OSHA-website op www.osha.gov. In tegenstelling tot de meeste normen, waarvan de naleving een vrijwillig karakter heeft, zijn de OSHA-normen wetten.

Belangrijke gedeelten die van toepassing op de machineveiligheid zijn:

- A – General (Algemeen)
- B – Adoption and Extension of Established Federal Standards (Instelling en uitbreiding van bestaande overheidsnormen)
- C – General Safety and Health Provisions (Algemene bepalingen ten aanzien van de veiligheid en gezondheid)
- H – Hazardous Materials (Gevaarlijke materialen)
- I – Personal Protective Equipment (Persoonlijke beschermingsmiddelen)
- J – General Environmental Controls – includes Lockout/Tagout (Algemene omgevingsveiligheidsmechanismen – inclusief lockout/tagout)
- O – Machinery and Machine Guarding (Machines en machineveiligheid)
- R – Special Industries (Speciale branches)
- S – Electrical (Elektrisch)

Een aantal OSHA-normen verwijzen naar vrijwillige normen. Het juridische gevolg van de opname via verwijzing is dat de materie wordt behandeld alsof deze volledig in het overheidsregister is gepubliceerd. Wanneer een norm waarvoor op nationale schaal overeenstemming is bereikt, als verwijzing in een van de subgedeelten wordt opgenomen, heeft deze norm ‘rechtskracht’.
Zo wordt er in Subgedeelte S verwezen naar NFPA 70, een vrijwillige norm die bekend staat als de US National Electric Code. Dit houdt in dat de eisen van de NFPA70-norm verplicht zijn gesteld.

Subgedeelte J van 29 CFR 1910.147 gaat in op de beheersing van gevaarlijke stroom. Deze richtlijn staat alom bekend als de Lockout/Tagout-norm. Een vergelijkbare vrijwillige norm is ANSI Z244.1. In grote lijnen schrijft deze norm voor dat de elektrische voeding van de machine dient te worden uitgeschakeld zodra er onderhouds- of reparatiewerkzaamheden op de machine worden uitgevoerd. Het doel is om onverwachte stroomvoorziening naar de machine of onverwacht opstarten van de machine te voorkomen, aangezien werknemers hierdoor letsel kunnen oplopen.

Werkgevers dienen een programma voor lockout/tagout op te stellen en procedures te gebruiken voor het uitrusten van stroomonderbrekende apparaten met de juiste lockout- of tagout-voorzieningen, en om anderzijds machines of apparatuur uit te schakelen om onverwachte stroomtoevoer, opstarten of vrijkomen van opgeslagen energie te voorkomen, zodat de werknemers geen lichamelijk letsel kunnen oplopen.

Kleine wijzigingen aan en bijstellingen van gereedschap en andere kleine onderhouds- en reparatieactiviteiten die tijdens normale productiewerkzaamheden plaatsvinden, vallen onder ANSI Z244 “Alternatieve maatregelen” indien er sprake is van herhaaldelijke routinewerkzaamheden die van essentieel belang zijn voor het gebruik van de apparatuur voor productiedoeleinden, mits de werkzaamheden worden uitgevoerd met behulp van alternatieve maatregelen die een effectieve bescherming garanderen. Dit wordt rechtstreeks ondersteund door OSHA in de “OSHA Minor Servicing Exception”. Alternatieve maatregelen zijn veiligheidsvoorzieningen zoals lichtschermen, veiligheidsmatten, deurvergrendelingen en vergelijkbare voorzieningen die voor veiligheidssystemen worden gebruikt. De uitdaging voor de ontwerper en de gebruiker van de machine is om vast te stellen hoe de uitdrukkingen “kleine onderhouds- en reparatieactiviteiten” en “herhaaldelijke routinewerkzaamheden die van essentieel belang zijn voor het gebruik van de apparatuur voor productiedoeleinden” dienen te worden geïnterpreteerd. Dit kan worden afgehandeld tijdens de Risicoanalyse.

Subgedeelte O gaat in op machines en machineveiligheid. Dit subgedeelte zet de algemene eisen voor alle machines en de eisen voor bepaalde specifieke machines uiteen. Toen de OSHA in 1971 werd opgericht, nam deze een groot aantal bestaande ANSI-normen over. Zo werd norm B11.1 inzake mechanische persen overgenomen in de vorm van norm 1910.217.

1910.212 is de algemene OSHA-norm voor machines. Deze norm schrijft voor dat een of meer maatregelen op het gebied van machineveiligheid dienen te worden genomen om de operator van de machine en andere werknemers binnen het machinegebied te beschermen tegen gevaren die worden veroorzaakt door de bedieningslocatie, grijppunten, ronddraaiende onderdelen, rondvliegende spaanders en vonken. Waar mogelijk moeten afschermingen op de machine worden aangebracht. Als deze afschermingen niet op de machine kunnen worden aangebracht, dienen zij elders te worden aangebracht. De afscherming mag zelf geen kans op ongevallen opleveren. Er moet er ook een gereedschap voor verwijdering vereist zijn, wanneer de afscherming moet worden verwijderd.
De “bedieningslocatie” is het machinegebied waar werkzaamheden worden uitgevoerd met betrekking tot het te verwerken materiaal. Als het gebruik van een machine gepaard gaat met de kans op letsel van werknemers dient de bedieningslocatie van

een veiligheidsinrichting te worden voorzien. De veiligheidsinrichting dient te voldoen aan alle relevante normen. Indien er geen specifieke normen op de veiligheidsinrichting van toepassing zijn, dient de veiligheidsinrichting op zodanige wijze te zijn ontworpen en gebouwd dat er tijdens de bedrijfscyclus geen lichaamsdelen van de operator in de gevarenzone kunnen komen.

Subgedeelte S (1910.399) biedt een overzicht van de elektrische richtlijnen van de OSHA. Een installatie of apparatuur is acceptabel voor de plaatsvervangende staatssecretaris van arbeid en wordt goedgekeurd volgens de betekenis van voornoemd subgedeelte S als deze apparatuur is geaccepteerd, gecertificeerd, op een lijst vermeld, van een label is voorzien of anderzijds als veilig is aangemerkt door een nationaal erkend testlaboratorium (NRTL).

Wat wordt verstaan onder “apparatuur”? Apparatuur is een algemene term die verwijst naar onder meer materiaal, bevestigingen, apparaten, voorzieningen, organen enzovoort, die worden gebruikt als onderdeel van of in samenhang met een elektrische installatie.

Wat wordt verstaan onder “vermeld”? Apparatuur is “vermeld” als het type ervan op een lijst wordt vermeld die (a) is gepubliceerd door een nationaal erkend testlaboratorium dat periodieke inspecties uitvoert van de productie van dergelijke apparatuur, en (b) aangeeft dat dergelijke apparatuur voldoet aan nationaal erkende normen of is getest en veilig is bevonden voor het desbetreffende gebruik.

Sinds augustus 2009 zijn de volgende bedrijven door de OSHA erkend als NRTL:

- Canadian Standards Association (CSA)
- Communication Certification Laboratory, Inc. (CCL)
- Curtis-Straus LLC (CSL)
- FM Approvals LLC (FM)
- Intertek Testing Services NA, Inc. (ITSNA)
- MET Laboratories, Inc. (MET)
- NSF International (NSF)
- National Technical Systems, Inc. (NTS)
- SGS U.S. Testing Company, Inc. (SGSUS)
- Southwest Research Institute (SWRI)
- TUV America, Inc. (TUVAM)
- TUV Product Services GmbH (TUVPSG)
- TUV Rheinland of North America, Inc. (TUV)
- Underwriters Laboratories Inc. (UL)
- Wyle Laboratories, Inc. (WL)

De bevoegde autoriteit (AHJ) heeft het laatste woord inzake de vereisten. Sommige staten zoals NY, CA en IL kennen bijvoorbeeld aanvullende vereisten.

Sommige Amerikaanse staten hebben hun eigen regionale OSHA’s en kennen mogelijk extra vereisten naast de OSHA-vereisten van de Amerikaanse overheid. 24 Amerikaanse staten, Puerto Rico en de Maagdeneilanden kennen door de OSHA goedgekeurde

overheidsplannen en hebben hun eigen normen en beleidsregels op het gebied van handhaving ingesteld. De normen die deze staten hebben ingesteld zijn in grote lijnen identiek aan de OSHA-normen van de Amerikaanse overheid. Sommige staten hebben echter andere machineveiligheidsnormen ingesteld, of beschikken over andere beleidsregels met betrekking tot de handhaving. Werkgevers dienen een historie van ongevallen en onregelmatigheden aan de OSHA te rapporteren. De OSHA verzamelt informatie over de frequentie van ongevallen en onregelmatigheden, stelt deze informatie beschikbaar aan lokale kantoren en gebruikt deze informatie om inspecties op prioriteit in te delen. De belangrijkste aanleidingen voor inspecties zijn:

- Dreigend gevaar
- Calamiteiten en overlijden
- Klachten van werknemers
- Branches met risicovolle activiteiten
- Lokale geplande inspecties
- Vervolginspecties
- Nationale en lokale aandachtsprogramma's

Overtredingen van de OSHA-normen kunnen in boetes resulteren. Het boetesysteem ziet er als volgt uit:

- Ernstige overtredingen: maximaal 7.000 dollar per overtreding
- Niet-ernstige overtredingen: per geval verschillend, maximaal 7.000 dollar
- Herhalingsovertreding: maximaal 70.000 dollar per overtreding
- Opzettelijke overtredingen: maximaal 70.000 dollar per overtreding
- Overtredingen die de dood ten gevolge hebben: verdere strafmaatregelen
- Verzuim om een probleemsituatie te herstellen: 7.000 dollar per dag

Canadese richtlijnen

In Canada wordt op regionaal niveau op de industriële veiligheid toegezien. Elke provincie kent en handhaaft haar eigen richtlijnen. Zo heeft Ontario de Occupational Health and Safety Act ingesteld. Dit is een veiligheids en gezondheids-wet die de rechten en verplichtingen van alle partijen op de werkplek uiteenzet. De belangrijkste doelstelling van deze wet is om werknemers te beschermen tegen gezondheids- en veiligheidsrisico's op het werk. De wet omvat procedures voor de omgang met gevaren op de werkplek, en voorziet in de handhaving van de wet waar niet op vrijwillige wijze volgens deze wet wordt gehandeld.

Een onderdeel van deze wet is gedeelte 7 van richtlijn 851, waarin de "Pre-Start Health and Safety review" wordt gedefinieerd, een gezondheids- en veiligheidsevaluatie voorafgaande aan het starten van de machine. Binnen Ontario is deze evaluatie verplicht voor elke nieuwe, herziene of gewijzigde machine, en er dient een rapport door een professionele ingenieur of specialist te worden opgesteld.

Hoofdstuk 2: Normen

Dit gedeelte behandelt een aantal kenmerkende, internationale en nationale normen die van toepassing zijn op machineveiligheid. Dit is geen uitputtend overzicht. Het is bedoeld om inzicht te bieden in de problemen op het gebied van machineveiligheid waarop normalisatie van toepassing is. Dit gedeelte moet gelezen worden in samenhang met het gedeelte over richtlijnen.

Landen in alle delen van de wereld werken samen aan de wereldwijde harmonisatie van normen. De gevolgen van hun inspanningen zijn met name voelbaar in het domein van machineveiligheid. De wereldwijde machineveiligheidsnormen worden beheerd door twee organisaties: de ISO en IEC. Hoewel er nog steeds regionale en nationale normen bestaan die in lokale behoeften voorzien, heeft er in de meeste landen een verschuiving plaatsgevonden naar het gebruik van de internationale normen die door de ISO en IEC zijn ontwikkeld.

De EN-normen (Europese normen) worden binnen alle EER-landen gebruikt. Alle nieuwe Europese normen zijn in overeenstemming met de ISO- en IEC-normen, en hebben in de meeste gevallen dezelfde tekst. Ook de VS refereren nu vaak aan IEC- en ISO-normen.

De IEC-normen hebben betrekking op elektrotechnische aangelegenheden. De ISO-normen hebben betrekking op alle overige aangelegenheden. De meeste geïndustrialiseerde landen zijn lid van IEC en ISO. De machineveiligheidsnormen worden opgesteld door werkgroepen waarin experts uit een groot aantal industrielanden deelnemen.

In de meeste landen hebben normen een vrijwillig karakter, in tegenstelling tot richtlijnen, die wettelijk verplicht zijn. Normen worden in de meeste gevallen gebruikt als praktische interpretatie van de richtlijnen. Om deze reden zijn de werelden van normen en richtlijnen nauw met elkaar verbonden.

ISO (Internationale Standaardisatie-Organisatie)

ISO is een niet-overheidsorganisatie die bestaat uit de nationale normeninstituten van de meeste landen van de wereld (157 landen op het moment van schrijven). Een centraal secretariaat in het Zwitserse Genève draagt zorg voor de coördinatie van het systeem. ISO ontwikkelt normen voor het efficiënter, veiliger en gezonder ontwerpen, produceren en gebruiken van machines. Daarnaast maken normen het handelsverkeer tussen landen eenvoudiger en eerlijker. ISO-normen worden aangeduid met de drie letters ISO.

De ISO-machinenormen worden op dezelfde manier ingedeeld als de EN-normen, namelijk op drie niveaus: Type A, B en C (zie het latere gedeelte over geharmoniseerde Europese normen).

Raadpleeg voor meer informatie de website van ISO op: *www.iso.org.*

IEC (Internationale Elektrotechnische Commissie)

De IEC is verantwoordelijk voor het opstellen en publiceren van internationale normen voor elektrische, elektronische en verwante technologie. Via de aangesloten leden bevordert de IEC internationale samenwerking met betrekking tot alle vraagstukken op het gebied van elektrotechnische normalisatie en verwante aangelegenheden, zoals de evaluatie van de naleving van de elektrotechnische normen.

Raadpleeg voor meer informatie de website van IEC op: *www.iec.ch*

Geharmoniseerde Europese normen (EN)

Deze normen gelden binnen alle EER-landen en worden ontwikkeld door de Europese normalisatieorganisaties CEN en CENELEC. Het gebruik van deze normen is vrijwillig. De meest directe weg om overeenstemming met de essentiële veiligheids- en gezondheidseisen van de Machinerichtlijn aan te tonen is echter om ervoor te zorgen dat het ontwerp en de productie van machines aan de richtlijnen van deze normen voldoen.

De EN-normen zijn onderverdeeld in 3 typen: A-, B- en C-normen.

Normen type A: zijn van toepassing op alle typen machines.

Normen type B: zijn onderverdeeld in 2 groepen.
Type B1-NORMEN: zijn van toepassing op specifieke ergonomische en veiligheidsaspecten van machines.
Type B2-NORMEN: zijn van toepassing op veiligheidscomponenten en veiligheidsvoorzieningen.

Type C-NORMEN: zijn van toepassing op specifieke typen of groepen machines.

Het is belangrijk om op te merken dat naleving van een C-norm vanzelf conformiteit veronderstelt met de EHSR's die onder die norm vallen. Wanneer een geschikte C-norm ontbreekt, kunnen A- en B-normen worden gebruikt als gedeeltelijk of volledig bewijs van overeenstemming met de essentiële veiligheids- en gezondheidseisen, namelijk door overeenstemming met relevante gedeeltes aan te tonen.

Er zijn afspraken gemaakt voor samenwerking tussen CEN/CENELEC en instellingen zoals ISO en IEC. Dit zou uiteindelijk moeten resulteren in gemeenschappelijke, wereldwijde normen. In de meeste gevallen kennen EN-normen hun tegenhanger in de vorm van een IEC- of ISO-norm. In de meeste gevallen zullen de twee teksten identiek zijn. Eventuele regionale verschillen worden aangestipt in de inleiding van de norm.

Raadpleeg voor een compleet overzicht van EN-machineveiligheidsnormen de volgende website:

http://ec.europa.eu/growth/single-market/european-standards/

Amerikaanse normen

OSHA-normen

Waar mogelijk stelt OSHA normen op basis van nationale overeenstemming in of stelt het bestaande overheidsnormen als veiligheidsnormen in. De verplichte bepalingen (het woord “shall” geeft aan dat een bepaling verplicht is) die via referentie in de normen zijn opgenomen, hebben dezelfde uitwerking als de normen die in Gedeelte 1910 worden vermeld. Zo wordt norm NFPA 70, waarover nationale overeenstemming is bereikt, vermeld als referentiedocument in Bijlage A van Subgedeelte S-Electrical van Gedeelte 1910 van 29 CFR. NFPA 70 is een vrijwillige norm die door de National Fire Protection Association (NFPA) is ontwikkeld. NFPA 70 staat ook bekend als de National Electric Code (NEC). Door opname in de norm zijn alle verplichte eisen binnen de NEC verplichte eisen van de OSHA.

ANSI-normen

Het American National Standards Institute (ANSI) treedt op als beheerder en coördinator van het vrijwillige normalisatiesysteem voor de Amerikaanse particuliere sector. Het is een besloten ledenorganisatie zonder winstoogmerk die wordt ondersteund door een diverse achterban van organisaties uit de private en publieke sector.

ANSI ontwikkelt zelf geen normen. Het bevordert de ontwikkeling van normen op basis van overeenstemming tussen gekwalificeerde groepen. Daarnaast zorgt ANSI ervoor dat de basisprincipes van overeenstemming, eerlijke procedures en openheid door de gekwalificeerde groepen worden bewaakt.
Deze normen worden aangemerkt als toepassingsnormen of constructienormen. Toepassingsnormen definiëren hoe een beveiliging op een machine moet worden toegepast. Voorbeelden zijn onder meer ANSI B11.1, een norm die informatie biedt over het gebruik van de machineveiligheid voor mechanische persen, en ANSI/RIA R15.06, een norm die het gebruik van machineveiligheid voor robots uiteenzet.

National Fire Protection Association

De National Fire Protection Association (NFPA) is opgericht in 1896. Deze organisatie heeft zich ten doel gesteld om de gevolgen van brand voor de kwaliteit van leven te verminderen door op wetenschappelijke principes gebaseerde richtlijnen en gedragsnormen, onderzoek en onderwijs op het gebied van brand en gerelateerde veiligheidsrisico’s te bevorderen. Om deze doelstelling te verwezenlijken, bevordert de NFPA een groot aantal normen. Twee belangrijke normen die betrekking hebben op industriële veiligheid en veiligheidsvoorzieningen zijn de National Electric Code (NEC) en de Electrical Standard for Industrial Machinery.

De National Fire Protection Association treedt sinds 1911 op als verantwoordelijke voor de NEC. De oorspronkelijke gedragsnorm werd opgesteld in 1897 als resultaat van de gezamenlijke inspanningen van verschillende belangengroepen op het gebied van elektriciteit, verzekeringen, bouwkunde en verwante disciplines. De NEC is sindsdien

regelmatig bijgewerkt. De norm wordt om de ongeveer drie jaar herzien. Artikel 670 van de NEC vermeldt een reeks van details met betrekking tot industriële machines en verwijst de lezer naar de Electrical Standard for Industrial Machinery, NFPA 79.

Norm NFPA 79 is van toepassing op elektrische/elektronische apparatuur, apparaten of systemen van industriële machines. Het doel van NFPA 79 is om gedetailleerde informatie te bieden met betrekking tot het gebruik van elektrische/elektronische apparatuur, apparaten of systemen die als onderdeel van industriële machines worden geleverd en om de veiligheid van mensen en goederen te bevorderen. NFPA 79 werd in 1962 officieel overgenomen door ANSI en toont qua inhoud sterke gelijkenis met de norm IEC 60204-1.

Machines waarop geen specifieke OSHA-normen van toepassing zijn, dienen vrij te zijn van bekende gevaren die in ernstig letsel of overlijden kunnen resulteren. Deze machines dienen op zodanige wijze te worden ontworpen en onderhouden dat ze aan de eisen van de toepasselijke branchenormen te voldoen. NFPA 79 is een norm die geldt voor machines waarop geen specifieke OSHA-normen van toepassing zijn.

Canadese normen

De CSA-normen vormen een weerslag van de overeenstemming op nationale schaal van fabrikanten en gebruikers, met inbegrip van fabrikanten, consumenten, detailhandelaars, vakbonden, beroepsorganisaties en overheidsinstellingen. Deze normen worden op brede schaal door de industrie en handel toegepast, en worden vaak overgenomen in de richtlijnen van gemeentes, provincies en federale overheden, met name als het gaat om gezondheid, veiligheid, bouw en milieu.

Personen, bedrijven en organisaties uit alle delen van Canada ondersteunen de ontwikkeling van normen door CSA door hun tijd en expertise beschikbaar te stellen aan CSA-comités en steunen de doelstellingen van de vereniging door hun ondersteunende lidmaatschap. De CSA omvat meer dan 7.000 vrijwilligers die aan comités deelnemen en 2.000 ondersteunende leden.

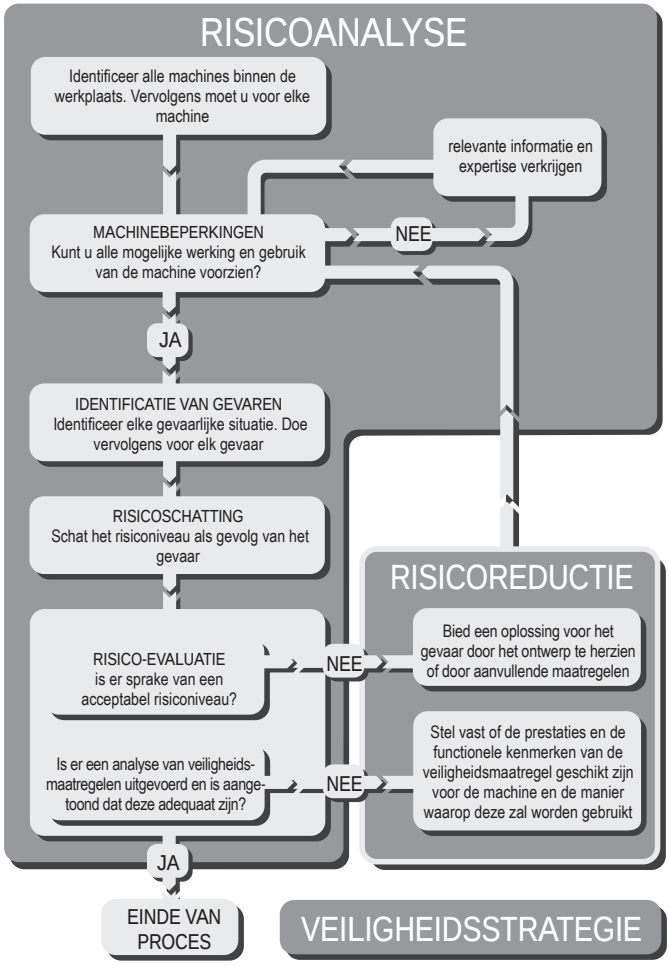
De Standards Council of Canada is het coördinerende orgaan van het National Standards-systeem. Het is een verbond van onafhankelijke en autonome organisaties die op basis van het nationaal belang aan de verdere ontwikkeling en verbetering van de vrijwillige normen werken.

Australische normen

De meeste van deze normen zijn nauw verwant met de vergelijkbare ISO/IEC/EN-normen Standards Australia Limited
286 Sussex Street, Sydney, NSW 2001
Telefoon: +61 2 8206 6000
E-mail:mail@standards.org.au – website: *www.standards.org.au*

Hoofdstuk 3: Veiligheidsstrategie

Vanuit louter functioneel oogpunt geldt dat hoe efficiënter een machine is in het verwerken van materiaal, des te beter de machine is. Om levensvatbaar te zijn dient een machine echter ook veilig te zijn. Veiligheid dient zelfs als een eerste vereiste te worden beschouwd.
Om een doeltreffende veiligheidsstrategie te ontwikkelen dienen er twee belangrijke stappen te worden uitgevoerd, die zoals hieronder aangegeven met elkaar in verband staan.



RISICOANALYSE gebaseerd op de machinefuncties en limieten en op de taken die nodig zijn tijdens de levensduur.

RISICOREDUCTIE wordt uitgevoerd na het risicoanalysestadium. Er worden veiligheidsmaatregelen geselecteerd op basis van de informatie die tijdens de risicoanalyse is verkregen. De manier waarop dit wordt gedaan vormt het uitgangspunt voor de VEILIGHEIDSSTRATEGIE voor de machine.

Het volgen van deze systematische aanpak zorgt ervoor dat er met alle aspecten rekening wordt gehouden, en dat ondanks alle details het belangrijkste principe niet uit het oog wordt verloren. Het hele proces dient te worden gedocumenteerd. Dit zal niet alleen voor grondiger resultaten zorgen, maar maakt deze resultaten ook geschikt voor controle door externe partijen.

Dit gedeelte is van toepassing op zowel de fabrikanten als de gebruikers van machines. De fabrikant dient te waarborgen dat deze machines op veilige wijze kunnen worden gebruikt. De risicoanalyse dient tijdens de machineontwerpfase van start te gaan en dient rekening te houden met alle werkzaamheden die naar alle waarschijnlijkheid op de machine zullen worden uitgevoerd. Deze taakgebaseerde aanpak in het vroegste stadium van de risicoanalyse is van groot belang. Het kan bijvoorbeeld nodig zijn om bewegende onderdelen van de machine regelmatig bij te stellen. Tijdens de ontwerpfase zou het mogelijk moeten zijn om maatregelen in het ontwerp op te nemen die garanderen dat dit proces op veilige wijze verloopt. Als men verzuimt om dergelijke maatregelen in een vroeg stadium te nemen, kan het moeilijk of zelfs onmogelijk zijn om dit in een later stadium te doen. Een mogelijk gevolg hiervan is dat de bewegende onderdelen nog steeds moeten worden bijgesteld, maar op een manier die onveilig of inefficiënt is (of beide). Als voor een machine tijdens het risicoanalysestadium rekening is gehouden met alle werkzaamheden, zal de resulterende machine een veiligere en efficiëntere machine zijn.

De gebruiker (of werkgever) dient ervoor te zorgen dat de machines binnen de werkomgeving veilig zijn. Ook als een machine veilig is verklaard door de fabrikant, dient de gebruiker nog altijd een risicoanalyse uit te voeren om vast te stellen of de apparatuur veilig functioneert binnen de werkomgeving. Machines worden vaak gebruikt onder omstandigheden die de fabrikant niet heeft voorzien. Bijvoorbeeld, voor een frees die in een school wordt gebruikt tijdens handvaardigheidslessen, zullen meer maatregelen moeten worden getroffen dan voor een frees die in een industriële werkplaats wordt gebruikt. Het is ook mogelijk dat afzonderlijke veilige machines worden gecombineerd op een manier die onveilig kan zijn.

Daarnaast dient men er rekening mee te houden dat als een bedrijf twee of meer losse machines aanschaft en deze tot één machine integreert, het bedrijf als de fabrikant van de resulterende gecombineerde machine wordt beschouwd.

Laten we nu ingaan op de essentiële stappen die doorlopen moeten worden om een doeltreffende veiligheidsstrategie te ontwikkelen. De volgende stappen kunnen worden ondernomen voor bestaande fabrieksinstallaties en nieuwe machines.

Risicoanalyse

Risicoanalyse moet niet als een vervelende verplichting worden beschouwd. Het is een nuttig proces dat onmisbare informatie oplevert en gebruikers en ontwerpers in staat stelt om logische beslissingen te nemen met betrekking tot manieren om voor veiligheid te zorgen.

Er zijn verschillende normen van toepassing op dit onderwerp. (EN) ISO 12100 Veiligheid van machines – Algemene principes voor ontwerp – Risicobeoordeling en -reductie vormen de meest wereldwijd gebruikte richtlijnen. Een technisch ISO-rapport: ISO/TR 14121-2 is ook verkrijgbaar. Dit biedt praktische richtlijnen en voorbeelden van methoden voor risicobeoordeling.

Welke techniek er ook wordt gebruikt om een risicoanalyse uit te voeren, een team van mensen uit verschillende functiegebieden zal over het algemeen breder toepasbare en evenwichtigere resultaten opleveren dan slechts één persoon die voor de risicoanalyse zorg draagt.

Risicoanalyse is een herhaaldelijk proces. Het zal in verschillende stadia van de levenscyclus van de machine worden uitgevoerd. De beschikbare informatie zal al naar gelang het stadium van de levenscyclus verschillen. Zo zal een risicoanalyse die door een machinebouwer wordt uitgevoerd informatie opleveren over elk detail van de machinemechanismen en constructiematerialen, maar de uiteindelijke werkomgeving van de machine slechts in grove lijnen aangeven. Een risicoanalyse die door de gebruiker van de machine wordt uitgevoerd hoeft niet per se in te gaan op de technische ins en outs, maar zal wel alle details van de werkomgeving van de machine beslaan. De informatie die tijdens een stadium van het risicoanalyseproces wordt verkregen, zou idealiter de basis moeten vormen voor het volgende risicoanalysestadium.

Bepaling van machinebeperkingen

Dit omvat het verzamelen en analyseren van informatie met betrekking tot de onderdelen, mechanismen en functies van een machine. Daarnaast zal het nodig zijn om rekening te houden met alle vormen van menselijke interactie met de machine en de omgeving waarin de machine zal draaien. Het doel is om een duidelijk begrip te vormen van de machine en het gebruik ervan.

Wanneer afzonderlijke machines op mechanische wijze of met behulp van besturingssystemen met elkaar worden verbonden, dienen deze als één machine te worden beschouwd, tenzij ze worden afgeschermd door de juiste veiligheidsvoorzieningen.

Het is belangrijk om rekening te houden met alle beperkingen en stadia tijdens de levensduur van de machine, met inbegrip van installatie, inbedrijfstelling, onderhoud, ontmanteling, het juiste gebruik en de juiste bediening van de machine en de gevolgen van in alle redelijkheid voorspelbare vormen van verkeerd gebruik of storingen.

Vaststellen van taken en gevaren

Alle gevaren die met het gebruik van de machine gepaard gaan, dienen te worden geïdentificeerd en vermeld op basis van hun aard en locatie. Voorbeelden van gevaren zijn onder meer verbrijzeling, afknelling, verstrikking, uitgeworpen onderdelen, rook, straling, giftige stoffen, hitte, geluid, enz.

De resultaten van de taakanalyse dienen te worden vergeleken met de resultaten van de gevarenidentificatie. Dit zal duidelijk maken waar er sprake is van een mogelijke convergentie van een gevaar en een persoon, oftewel een gevaarlijke situatie. Alle gevaarlijke situaties dienen te worden vermeld. Het is mogelijk dat hetzelfde gevaar tot verschillende typen gevaarlijke situaties kan leiden, afhankelijk van de persoon of taak in kwestie. Zo zal de aanwezigheid van een uiterst ervaren en goed opgeleide onderhoudstechnicus minder gevolgen voor de veiligheid hebben dan de aanwezigheid van een ongeschoolde schoonmaker die geen kennis van de machine heeft. Als elk afzonderlijk scenario wordt beschreven en daar oplossingen voor worden geboden, is het mogelijk dat er andere beschermende maatregelen kunnen worden getroffen voor de onderhoudstechnicus dan voor de schoonmaker. Als de verschillende scenario's niet worden vermeld en er geen afzonderlijke oplossingen voor worden geboden, dient men uit te gaan van het slechtste scenario, en zal dezelfde beschermende maatregel van toepassing moeten zijn op zowel de onderhoudstechnicus als de schoonmaker.

In sommige gevallen zal het nodig zijn om een algemene risicoanalyse uit te voeren voor een bestaande machine die reeds met beschermende voorzieningen is uitgerust (bijvoorbeeld een machine met gevaarlijke bewegende onderdelen die met een vergrendelde deur wordt beschermd). De gevaarlijke bewegende onderdelen vormen een potentieel gevaar dat kan uitgroeien tot een werkelijk gevaar indien er een storing in het vergrendelingssysteem optreedt. Tenzij het vergrendelingssysteem reeds is goedgekeurd (bijvoorbeeld door middel van een risicoanalyse of doordat het ontwerp voldoet aan de eisen van een bepaalde norm) mag de aanwezigheid ervan niet in beschouwing worden genomen.

Risico-inschatting

Risico-inschatting vormt een van de meest fundamentele aspecten van risicoanalyse. Er zijn verschillende manieren om hiermee om te gaan. De basisprincipes worden op de volgende pagina's beschreven.

Elke machine die potentieel gevaarlijke situaties oplevert, vertegenwoordigt het risico van een gevaarlijke gebeurtenis (d.w.z. letsel). Hoe groter het risico, des te groter de noodzaak om er iets aan te doen. Voor bepaalde gevaren kan het risico zo gering zijn dat we dit gevaar tolereren. Voor een ander gevaar kan het risico echter zo groot zijn dat we uiterst scherpe maatregelen moeten treffen om er bescherming tegen te bieden. Om te kunnen beslissen of er iets aan een gevaar moet worden gedaan, en zo ja, wat, moeten we in staat zijn om het risico te kwantificeren.

Bij risico's wordt vaak alleen gedacht aan de ernst van het letsel dat bij een ongeval wordt opgelopen. Zowel met de ernst van het mogelijke letsel als met de waarschijnlijkheid van het optreden ervan moet rekening worden gehouden om de mate van risico te kunnen inschatten.

ISO TR 14121-2 “Risicobeoordeling – Praktische richtlijnen en voorbeelden van methoden” toont verschillende methoden voor de getalsmatige weergave van de risico’s. Er zijn verschillen in de terminologie- en waarderingssystemen, maar alle methoden hebben betrekking op de principes die worden aangestipt in (EN) ISO 12100. De volgende tekst legt de basisprincipes van risicobepaling uit en is bedoeld om hulp te bieden, ongeacht welke methodologie wordt gebruikt. De tekst volgt over het algemeen de parameters die worden gegeven door de Hybrid Tool in clausule 6.5 van ISO TR 14121-2.

Er wordt rekening gehouden met de volgende factoren:
- DE ERNST VAN HET POTENTIËLE LETSEL.
- DE WAARSCHIJNLIJKHEID VAN HET OPTREDEN ERVAN.

De waarschijnlijkheid van het optreden omvat minstens twee factoren:
- REGELMAAT VAN BLOOTSTELLING.
- WAARSCHIJNLIJKHEID VAN LETSEL.

De waarschijnlijkheidsfactor zelf wordt vaak gesplitst in andere factoren, zoals:
- WAARSCHIJNLIJKHEID VAN OPTREDEN.
- MOGELIJKHEID VAN VOORKOMEN.

Maak gebruik van alle informatie en expertise die tot uw beschikking staat. U heeft te maken met alle stadia van de levensduur van de machine. Om te grote complexiteit te vermijden dient u dan ook voor uw beslissingen voor elke factor van het slechtst mogelijke scenario uit te gaan. Daarnaast is het belangrijk om altijd uw gezond verstand te gebruiken. Beslissingen moeten uitgaan van datgene wat mogelijk, realistisch en aannemelijk is. In dit geval zal een team met leden uit verschillende functiegebieden uitkomst bieden.

In deze fase hoeft u meestal geen rekening te houden met bestaande beveiligingssystemen. Als uit de risico-inschatting blijkt dat een veiligheidssysteem is vereist, kunt u gebruikmaken van een aantal methodieken voor het vaststellen van de benodigde kenmerken. Deze methodieken komen later in dit hoofdstuk aan bod.

Ernst van het potentiële letsel

Voor deze beschouwing gaan we ervan uit dat het ongeluk of incident heeft plaatsgevonden. Een grondige evaluatie van het gevaar zal uitwijzen wat het ergst mogelijke letsel is.

Bedenk daarbij: we gaan ervan uit dat het letsel in kwestie onvermijdelijk is, en we houden ons alleen bezig met de ernst ervan. U dient ervan uit te gaan dat de operator wordt blootgesteld aan de gevaarlijke beweging of het gevaarlijke proces. De ernst van het letsel moet worden beoordeeld aan de hand van de factoren die in de gekozen methodologie worden gegeven.

Bijvoorbeeld als volgt:
- Overlijden, verlies van een oog of arm
- Blijvend gevolg, bijv. verlies van vingers.
- Omkeerbaar gevolg, vereist medische zorg
- Omkeerbaar gevolg, vereist eerste hulp

Regelmaat van blootstelling

De regelmaat van blootstelling geeft een antwoord op de vraag hoe vaak de operator of de onderhoudstechnicus aan het gevaar wordt blootgesteld. De regelmaat van blootstelling aan gevaar kan worden geclassificeerd aan de hand van de factoren die worden gegeven in de gekozen methodologie.

Bijvoorbeeld als volgt:
- Meer dan eenmaal per uur
- Tussen eenmaal per uur en eenmaal per dag
- Tussen eenmaal per dag en eenmaal per twee weken
- Tussen eenmaal per twee weken en eenmaal per jaar
- Minder dan eenmaal per jaar

Waarschijnlijkheid van letsel

U dient ervan uit te gaan dat de operator wordt blootgesteld aan de gevaarlijke beweging of het gevaarlijke proces. De waarschijnlijkheid van het optreden van een gevaarlijke gebeurtenis kan worden geclassificeerd aan de hand van de factoren die in de gekozen methodologie worden gegeven. Door de kenmerken van de machine, verwachte menselijke gedragingen en overige factoren te beschouwen, kan de waarschijnlijkheid van het optreden van een gevaarlijke gebeurtenis worden ingedeeld.

Bijvoorbeeld als volgt:
- Verwaarloosbaar
- Zeldzaam
- Mogelijk
- Waarschijnlijk
- Zeer groot

Mogelijkheid van voorkomen

Door te kijken naar hoe mensen samenwerken met de machine en naar andere kenmerken zoals de snelheid waarmee de beweging wordt opgestart, kan de mogelijkheid van het voorkomen van letsel worden ingedeeld aan de hand van de factoren die worden gegeven in de gekozen methodologie.

Bijvoorbeeld als volgt:
- Waarschijnlijk
- Mogelijk
- Onmogelijk

Nadat alle categorieën zijn beoordeeld, worden de resultaten ingevoerd in het diagram of de tabel van de gebruikte risicokwantificering. Dit leidt tot een soort gekwantificeerde schatting van de risico's van de verschillende gevaren van een machine. Deze informatie kan vervolgens worden gebruikt om te besluiten welke risico 's moeten worden gereduceerd om een acceptabel veiligheidsniveau te bereiken.

Risicoreductie

Nu moeten we onze aandacht op elke machine en de risico's ervan richten om voor alle gevaren een oplossing te kunnen bieden.

Hiërarchie van maatregelen voor risicoreductie
Er zijn drie basismethoden die u in overweging moet nemen. Deze methoden dienen in de volgende volgorde te worden gebruikt:

1. De risico's zo ver mogelijk elimineren of reduceren (inherent veilig machineontwerp en -constructie).
2. Beveiligingsmaatregelen en aanvullende beschermende maatregelen treffen met betrekking tot risico's die niet op basis van ontwerp kunnen worden geëlimineerd.
3. Voorzien in informatie voor veilig gebruik met inbegrip van waarschuwingstekens en -signalen. Evenals informatie over resterende risico's en of een bepaalde training of persoonlijke beschermingsmiddelen zijn vereist.

Binnen deze hiërarchie dient elke maatregel te worden overwogen, van boven naar beneden. Waar mogelijk dienen deze maatregelen te worden getroffen. In de meeste gevallen zal dit resulteren in een combinatie van maatregelen.

Eliminatie van risico (inherent veilig ontwerp)

In de machineontwerpfase zal het mogelijk zijn om veel van de mogelijke gevaren op en eenvoudige manier te voorkomen door goed rekening te houden met factoren als materialen, toegangseisen, hete oppervlakken, overdrachtsmethoden, gevarenzones, spanningsniveaus enz.

Als er bijvoorbeeld geen toegang tot een gevaarlijk gebied is vereist, dan is de oplossing om het gebied af te grendelen binnen het frame van de machine, of om gebruik te maken van een bepaald type vergrendelde afscherming.

Beveiligingsmaatregelen en -systemen

Als er wel toegang tot het gevarengebied is vereist, wordt het leven er wat minder gemakkelijk op. Het zal nodig zijn om ervoor te zorgen dat men alleen toegang tot het gevarengebied kan krijgen wanneer de machine zich in een veilige toestand bevindt. Voor dit doel zijn beschermende maatregelen nodig, zoals vergrendelde deuren en/ of uitschakelsystemen. veiligheidssysteem veiligheidsvoorzieningen en -systemen is in hoge mate afhankelijk van de operationele kenmerken van de machine. Dit aspect is van uitermate groot belang, omdat een systeem dat de efficiëntie van de machine in de weg zit naar alle waarschijnlijkheid op ongeoorloofde wijze zal worden verwijderd of omzeild.

Een van de meest directe en complete interacties tussen mensen en machines vindt plaats tijdens onderhoud, probleemoplossing en reparatie. Voor routinematige en kleine interventies is het mogelijk om gebruik te maken van veiligheidsgerelateerde, systeemgebaseerde beschermingsmaatregelen (zie beschrijving verderop) om zorg te dragen voor veiligheid. Maar in alle voorschriften is het volkomen duidelijk dat er voor elk type ingrijpen, zoals groot onderhoud, reparatie, demontage of werk aan stroomcircuits, sprake moet zijn van zowel het voorzien in als het gebruiken van apparatuur die zorgt voor stroomonderbreking en het wegvloeien van energie (in sommige gevallen ook zwaartekracht) op de machine. Op deze manier kan het risico van onverwacht opstarten en blootstelling aan energiebronnen worden geëlimineerd. Dit is opgenomen in veel verschillende veiligheidsvoorschriften en -normen. Zie bijvoorbeeld de voorgaande tekst onder “Amerikaanse voorschriften” waarin de voorschriften en normen inzake “Lockout/tagout” worden beschreven. Europese en ISO-norm EN 1037 en ISO 14118-normen inzake “Voorkomen van onverwacht inschakelen” voorzien ook in vereisten. In termen van elektrische technologie voorzien IEC/EN 60204-1 en NFPA 79 ook in richtlijnen en vereisten.
Het is natuurlijk van het grootste belang dat er sprake is van een correct werkingssysteem dat ervoor zorgt dat alle juiste procedures worden gevolgd.

In het volgende gedeelte worden enkele gangbare implementaties besproken.

Preventie van onverwacht inschakelen van de machine

Op het voorkomen van het onverwacht inschakelen van machines zijn tal van normen van toepassing. Voorbeelden zijn onder meer ISO14118, EN1037, ISO12100, OSHA 1910.147, ANSI Z244-1, CSA Z460-05 en AS 4024.1603. Deze normen hebben een gemeenschappelijk thema: de primaire methode om het onverwacht inschakelen van machines te voorkomen is om de voeding naar het systeem te onderbreken en het systeem in de uit-stand te vergrendelen. Het doel is om mensen de mogelijkheid te bieden om op veilige wijze de gevarenzones van een machine binnen te gaan.

Lockout/tagout

Nieuwe machines moeten worden geconstrueerd met vergrendelbare energieonderbrekende voorzieningen. Deze voorzieningen kunnen worden toegepast op alle vormen van energie, zoals elektrisch, hydraulisch, pneumatisch, zwaartekracht en lasers. Lockout houdt in dit verband in dat een vergrendeling op een energieonderbrekende voorziening wordt aangebracht. De vergrendeling mag alleen worden verwijderd door de eigenaar of door een supervisor, en alleen onder gecontroleerde omstandigheden. Wanneer meerdere personen met de machine moeten werken, dient elke persoon zijn of haar vergrendelingen op de energieonderbrekende apparaten toe te passen. Elke vergrendeling moet kunnen worden herleid naar de overeenkomstige eigenaar.

In de Verenigde Staten vormt tagout een alternatief voor lockout als het gaat om oudere machines waarop nooit een vergrendelbaar apparaat is geïnstalleerd. In dit geval wordt de machine uitgeschakeld, en wordt er een label aangebracht om het personeel te waarschuwen dat zij de machine niet mogen starten wanneer de eigenaar van het label aan de machine werkt. Sinds 1990 moeten machines die worden gewijzigd, opgewaardeerd worden met een vergrendelbare energieonderbrekende voorziening.

Een energieonderbrekende voorziening is een mechanische voorziening die de overdracht of vrijgave van energie op fysieke wijze voorkomt. Deze apparaten kunnen de vorm hebben van een contactverbreker, een uitschakelaar, een handmatig bediende schakelaar, een stekker/stopcontact-combinatie of een handmatig bediende klep. Energieonderbrekingsvoorzieningen dienen alle ongeaarde voedingsgeleiders te schakelen, en geen pool mag afzonderlijk werken.

Het doel van lockout/tagout is om het onverwacht inschakelen van de machine te voorkomen. Onverwacht inschakelen kan verschillende oorzaken hebben: een storing van het bedieningssysteem; een verkeerde bewerking met een startbedieningselement, -sensor, -magneetschakelaar of -klep; het herstel van de stroom na een onderbreking of andere interne of externe invloeden. Na voltooiing van het lockout/tagout proces moet worden gecontroleerd of alle energie is afgesloten.

Veiligheidsisolatiesystemen

Veiligheidsisolatiesystemen zorgen ervoor dat de machine op juiste wijze wordt uitgeschakeld en bieden een eenvoudige manier om de voeding naar de machine te onderbreken. Deze aanpak biedt goede resultaten bij grotere machines en productiesystemen, met name wanneer er zich meerdere voedingen op tussenliggend niveau of op ver afgelegen locaties bevinden.

Voedingsonderbreking (Load Disconnects)

Voor de lokale stroomonderbreking van elektrische apparaten kunnen schakelaars net voor het apparaat worden geplaatst dat moet gelocked out/tagout worden. De lastschakelaars die in Bulletin 194E worden vermeld, zijn voorbeelden van producten die zowel stroomonderbreking als lockout bieden.

Sleutelvergrendelingen

Een andere manier om een vergrendelingssysteem te bieden is om gebruik te maken van sleutelvergrendelingen. Veel sleutelvergrendelingen beginnen met een stroomonderbrekende voorziening. Wanneer de schakelaar wordt uitgeschakeld met behulp van de “primaire” sleutel, wordt de voeding naar de machine onderbroken. De primaire sleutel kan vervolgens verwijderd en meegenomen worden naar een locatie waar toegang tot de machine is vereist. Er kunnen verschillende componenten worden toegevoegd om complexere vergrendelingsconfiguraties mogelijk te maken.

Alternatieve Lockoutmaatregelen (Lockout)

Tijdens het uitvoeren van onderhouds- of reparatiewerkzaamheden op de machine moet gebruik worden gemaakt van lockout/tagout. Ingrepen in de machine tijdens normale productiebewerkingen zijn gedekt door veiligheidsmaatregelen zoals beschermdeurvergrendelingssystemen. Het verschil tussen reparatie/onderhoud en normale productiebewerkingen is niet altijd even duidelijk.

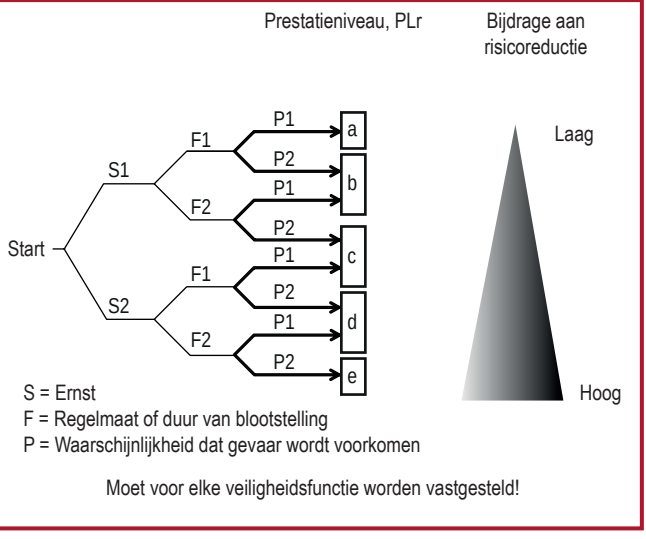
Voor een aantal kleine afstellingen en onderhoudstaken die plaatsvinden tijdens normale productiebewerkingen hoeft de machine niet noodzakelijkerwijze te worden vergrendeld. Voorbeelden zijn het laden en lossen van materialen, kleine wijzigingen en afstellingen van gereedschap, het smeren van de machine en het verwijderen van afvalmateriaal. Deze taken dienen een routinematig en herhalend karakter te hebben en van essentieel belang te zijn voor het gebruik van de machine voor productiedoeleinden. Het werk wordt uitgevoerd met behulp van alternatieve maatregelen, zoals afschermingen, die een effectieve bescherming bieden. Veiligheidsvoorzieningen omvatten onder meer voorzieningen als vergrendelde afschermingen, lichtschermen en veiligheidsmatten. Indien gebruikt in combinatie met de juiste veilige logische modules en uitvoermodules kunnen operators tijdens normale productiewerkzaamheden en kleine onderhouds- en reparatiewerkzaamheden op veilige wijze toegang tot de gevarenzones van de machine krijgen.

In dergelijke gevallen staat of valt de veiligheid van de machine met een juiste toepassing en het correct functioneren van het veiligheidssysteem, zelfs wanneer zich fouten voordoen. Nu zijn we op het punt aangekomen waarop het nodig is om de juiste werking van het systeem te bekijken. Voor elk type systeem is er waarschijnlijk een keur van technologieën beschikbaar die verschillende niveaus van foutbewaking, -detectie en -preventie bieden.

In een ideale wereld zou elk veiligheidssysteem perfect zijn, en zou het ondenkbaar zijn dat storingen een gevaarlijke situatie opleveren. In de werkelijke wereld worden we echter belemmerd door beperkingen op het gebied van kennis en materiaal. Een andere, uiterst tastbare beperking wordt gevormd door de kosten. Op basis van deze factoren wordt duidelijk dat we moeten beschikken over een manier om de mate van veiligheidsmaatregelen te relateren aan het risiconiveau dat in de risicoschattingsfase is verkregen.

Welk type veiligheidsvoorzieningen we ook kiezen, we mogen nooit vergeten dat een “veiligheidsgerelateerd systeem” tal van elementen kan omvatten, zoals veiligheidsinrichtingen, bedrading, een stroomschakelinrichting en, in sommige gevallen, onderdelen van het besturingssysteem van de machine. Al deze systeemelementen (inclusief afschermingen, montagestukken, bedrading enz.) dienen prestatiekenmerken te bezitten die in overeenstemming zijn met hun ontwerpprincipe en technologie. IEC/EN 62061 en (EN) ISO 13849-1 classificeren hiërarchische Performance Level voor veiligheidsgerelateerde onderdelen van besturingssystemen en hun bijlagen bevatten methoden voor risicoanalyse waarmee de integriteitseisen van een veiligheidssysteem kunnen worden vastgesteld.

Bijlage A van (EN) ISO 13849-1:2015 bevat een verbeterd risicodiagram.



In Bijlage A van de norm IEC 62061 wordt eveneens een methode uiteengezet, die de hieronder weergegeven vorm aanneemt.

Risicobeoordeling en veiligheidsmaatregelen

Documentnummer:

Onderdeel van:

☐ Voorafgaande risicobeoordeling
☐ Tussentijdse risicobeoordeling
☐ Vervolgrisicobeoordeling

Product: _____
Afgegeven door: _____
Datum: _____

Zwart gebied = veiligheidsmaatregelen vereist
Grijs gebied = veiligheidsmaatregelen aanbevolen

Gevolg	Ernst Se	Klasse CI					Regelmaat en duur, Fr		Waarschijnlijkheid van gevaarlijke gebeurtenis, Pr		Voorkomen Av	
		3–4	5–7	8–10	11–13	14–15						
Overlijden, verlies van een oog of arm		SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	<= 1 uur	5	Veel voorkomend	5		
Permanent, verlies van vingers			OM	SIL 1	SIL 2	SIL 3	> 1 h – <= dag	5	Waarschijnlijk	4		
Omkeerbaar, medische zorg				OM	SIL 1	SIL 2	> 1 dag – <= 2 weken	4	Mogelijk	3	Onmogelijk	5
Omkeerbaar, eerste hulp					OM	SIL 1	> 2 weken – <= 1 jaar	3	Zelden	2	Mogelijk	3
							> 1 jaar	2	Verwaarloosbaar	1	Waarschijnlijk	1

Se-rienr.	Ge-vaar Nr.	Gevaar	Se	Fr	Pr	Av	Ci	Veiligheidsmaatregel	Veilig

Opmerkingen

Het gebruik van elk van de bovenstaande methoden zou vergelijkbare resultaten moeten opleveren. Elke methode heeft ten doel om rekening te houden met de gedetailleerde inhoud van de norm waartoe deze behoort.

In beide gevallen is het van uitermate groot belang om het advies te volgen dat in de tekst van deze norm wordt geboden. Het risicodiagram of de risicotabel mag niet afzonderlijk of op een al te simplistische manier worden gebruikt.

Evaluatie

Het is belangrijk om de risico-inschatting na het selecteren van een veiligheidsmaatregel te herhalen voordat deze wordt toegepast. Dit is een procedure die vaak achterwege wordt gelaten. Als we een veiligheidsmaatregel toepassen, is het mogelijk dat de operator van een machine daardoor het gevoel krijgt dat hij of zij volledig beschermd is tegen het oorspronkelijk voorziene risico.
Omdat de gebruiker niet langer het gevoel heeft dat er sprake is van een gevaar, zou deze op een andere manier ingrepen op de machine kunnen uitvoeren. Hierdoor zou de gebruiker regelmatiger aan het gevaar kunnen worden blootgesteld, of zou deze zich verder binnen de machine kunnen begeven. Dit houdt in dat het risico, als de veiligheidsmaatregel niet doeltreffend is, groter is dan oorspronkelijk was ingeschat. Dit is het werkelijke risico dat we moeten inschatten. Om deze reden dient de risico-inschatting te worden herhaald. Daarbij moet rekening worden gehouden met voorspelbare veranderingen in de manier waarop mensen met de machine omgaan. De resulterende informatie wordt gebruikt om te controleren of de voorgestelde veiligheidsmaatregelen daadwerkelijk geschikt zijn. Voor meer informatie wordt Bijlage A van IEC/EN 62061 aanbevolen.

Training, persoonlijke beschermingsmiddelen enz.

Het is belangrijk dat de operators van de machine de nodige training volgen met betrekking tot het veilige gebruik van de machine. Dit houdt niet in dat de overige maatregelen terzijde kunnen worden geschoven. Het is niet voldoende om de operators te vertellen dat zij niet in de buurt van gevarengebieden mogen komen (als alternatief voor het afschermen van deze gebieden).

Daarnaast kan het nodig zijn dat de operators gebruikmaken van speciale uitrusting, zoals handschoenen, een veiligheidsbril, ademhalingsmaskers, enz. De machineontwerper dient aan te geven welk type uitrusting is vereist. Het gebruik van persoonlijke beschermingsmiddelen zal normaliter niet de primaire veiligheidsmethode vormen, maar dient als aanvulling op de hierboven beschreven maatregelen. Er is doorgaans ook behoefte aan tekens en markeringen om het besef van overgebleven risico 's te vergroten.

Hoofdstuk 4: Implementatie van beschermende maatregelen

Wanneer uit de risicoanalyse blijkt dat een machine of proces kans op letsel oplevert, dient het gevaar te worden geëlimineerd of ingeperkt. De manier waarop dit wordt bewerkstelligd is afhankelijk van de aard van de machine en van het gevaar. Beschermende maatregelen van veiligheidsbesturingssystemen in combinatie met machineveiligheid voorkomen de toegang tot een gevaar of verhinderen in een gevaarlijke situatie gevaarlijke bewegingen als toegang wel mogelijk is. Typische voorbeelden van beschermende maatregelen van veiligheidsbesturingssystemen worden later besproken en omvatten vergrendelde afschermingen, lichtschermen, veiligheidsmatten, tweehandsbedieningen en activeringsschakelaars.

Noodstopvoorzieningen en -systemen zijn gekoppeld aan veiligheidsgerelateerde besturingssystemen, maar zijn geen directe veiligheidssytemen. Ze moeten uitsluitend beschouwd worden als aanvullende beschermende maatregelen.

Toegang voorkomen met vaste omsluitende afschermingen

Als het gevaar verband houdt met een machineonderdeel waarnaar geen toegang is vereist, dient een permanente afscherming aan de machine te worden bevestigd. Het moet alleen mogelijk zijn om dit type afschermingen met behulp van speciaal gereedschap te verwijderen. De vaste afschermingen moeten 1) bestand zijn tegen hun werkomgeving, 2) waar nodig rondvliegende voorwerpen tegenhouden en 3) zelf geen gevaren opleveren, zoals bijvoorbeeld scherpe randen. Vaste afschermingen kunnen van openingen zijn voorzien op punten waarop de afscherming contact maakt met de machine, dan wel openingen die het gevolg zijn van het gebruik van een gaasbehuizing.

Vensters vormen een handige manier om machineprestaties te bewaken. U dient de nodige zorg in acht nemen bij het selecteren van het gebruikte materiaal, omdat chemische interactie met snijvloeistoffen, ultraviolette stralen en normale slijtage ertoe kunnen bijdragen dat de venstermaterialen na verloop van tijd aan kwaliteit inboeten.

De grootte van de openingen dient te voorkomen dat de operator de gevaarlocatie kan bereiken. Tabel O-10 in U.S. OHSA 1910.217 (f) (4), ISO 13854, tabel D-1 van ANSI B11.19, tabel 3 in CSA Z432 en AS4024.1 bieden aanbevelingen met betrekking tot de afstand die een specifieke opening tot het gevaar dient te hebben.

Toegangsdetectie

Beschermende maatregelen kunnen gebruikt worden om de toegang tot een gevarengebied te detecteren. Wanneer gebruik wordt gemaakt van detectiefunctionaliteit als methode voor risicoreductie, moet de ontwerper er rekening mee houden dat een integraal veiligheidssysteem moet worden gebruikt. De veiligheidsvoorziening zelf biedt onvoldoende risicoreductie. Een dergelijk veiligheidssysteem bestaat normaliter uit drie blokken: 1) een invoermodule die toegang tot het gevaar detecteert, 2) een logisch apparaat dat de signalen van het detectieapparaat verwerkt, de status van het veiligheidssysteem controleert en uitvoermodules in- of uitschakelt, en 3) een uitvoermodule die de actuator bestuurt (bijvoorbeeld een motor).

Detectievoorzieningen

Er zijn tal van alternatieve voorzieningen beschikbaar waarmee de aanwezigheid van een persoon binnen een gevarengebied kan worden gedetecteerd. De beste keuze voor een bepaalde toepassing is afhankelijk van een aantal factoren:

- omgevingsfactoren die van invloed kunnen zijn op de betrouwbaarheid van de detector
- de regelmaat van toegang,
- de stoptijd van het gevaar,
- de noodzaak om de machinecyclus te voltooien en
- insluiten van rondvliegende voorwerpen, vloeistoffen, nevels, dampen enz.

De juiste beweegbare afschermingen kunnen worden vergrendeld om bescherming te bieden tegen rondvliegende voorwerpen, vloeistoffen, nevels en andere soorten gevaren. Deze afschermingen worden vaak gebruikt wanneer er geen sprake is van regelmatige toegang tot het gevarengebied. Vergrendelde afschermingen kunnen ook worden vergrendeld om toegang te voorkomen voordat de machine volledig tot stilstand is gekomen of wanneer het stopzetten van de machine in het midden van een cyclus ongewenst is.

Aanwezigheidsdetectievoorzieningen zoals lichtschermen, matten en laserscanners bieden snelle en eenvoudige toegang tot het gevarengebied. Deze voorzieningen worden vaak gebruikt wanneer de operators regelmatig toegang tot het gevarengebied dienen te hebben. Dergelijke typen voorzieningen bieden geen bescherming tegen rondvliegende voorwerpen, nevels, vloeistoffen of andere soorten gevaren.

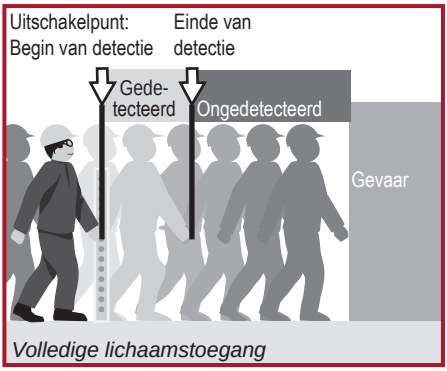
De beste veiligheidsmaatregel is een apparaat of systeem dat maximale bescherming biedt en de normale werking van de machine minimaal belemmert. Alle aspecten van het machinegebruik dienen in overweging te worden genomen. De ervaring leert namelijk dat een veiligheidssysteem dat niet gebruiksvriendelijk genoeg is, sneller wordt verwijderd of omzeild.

Aanwezigheidsdetectievoorzieningen

IEC 62046 voorziet in nuttige richtlijnen inzake de toepassing van aanwezigheidsdetectievoorzieningen. Het gebruik ervan wordt aanbevolen. Bij het bepalen van de manier waarop een zone of gebied moet worden beschermd, is het belangrijk om een duidelijk begrip te hebben van de benodigde veiligheidsfuncties. Over het algemeen zullen er minimaal twee functies zijn:

- het uitschakelen of onderbreken van de stroom wanneer een persoon het gevarengebied betreedt,
- het voorkomen dat de machine wordt ingeschakeld of dat voeding wordt geactiveerd wanneer een persoon zich in het gevarengebied bevindt.

Op het eerste gezicht lijkt het om dezelfde functie te gaan, maar hoewel de functies duidelijk met elkaar verband houden en vaak door dezelfde apparatuur worden ondersteund, is hier in feite sprake van twee verschillende veiligheidsfuncties. Om de eerste functie mogelijk te maken moeten we een bepaald type uitschakelapparaat gebruiken. Anders gezegd: we moeten een apparaat gebruiken dat een lichaamsdeel van een persoon die voorbij een bepaald punt is gegaan kan detecteren en daarop een signaal (opdracht) afgeeft om de stroom uit te schakelen. Als de persoon in kwestie vervolgens in staat is om zich voorbij dit uitschakelpunt te begeven en zijn of haar aanwezigheid niet langer wordt gedetecteerd, kan de tweede functie (het voorkomen van inschakeling) mogelijk niet worden verzorgd.



De afbeelding toont een voorbeeld van volledige lichaamstoegang. Als uitschakelvoorziening wordt gebruikgemaakt van een verticaal gemonteerd lichtscherm. Vergrendelde veiligheidsdeuren kunnen eveneens als uitschakelvoorziening worden beschouwd wanneer er niets is om te verhinderen dat de deur na de toegang tot het gevarengebied wordt gesloten.

Als volledige lichaamstoegang niet mogelijk is, zodat een persoon niet voorbij het uitschakelpunt kan komen, wordt de aanwezigheid van deze persoon altijd gedetecteerd, en wordt de tweede functie (het voorkomen van het inschakelen) verzorgd. Voor toepassingen die betrekking hebben op gedeeltelijke lichaamstoegang draagt hetzelfde type voorzieningen zorg voor het uitschakelen en de aanwezigheidsdetectie. Het enige verschil is het type toepassing.

Aanwezigheidsdetectievoorzieningen worden gebruikt om de aanwezigheid van personen te detecteren. De reeks van voorzieningen omvat veiligheidslichtschermen, veiligheidsbarrières met één lichtstraal, veiligheidslaserscanners en veiligheidsmatten. Voor alle aanwezigheidsdetectievoorzieningen moet bij de omvang van de detectiezone en de plaatsing van de voorziening rekening worden houden met de vereiste veiligheidsafstand.

Veiligheidslichtschermen

Veiligheidslichtschermen kunnen eenvoudig worden omschreven als foto-elektrische aanwezigheidssensoren die specifiek ten doel hebben om personeel te beschermen tegen letsel als gevolg van gevaarlijke machinebewegingen. Lichtschermen, die ook bekend zijn als AOPD's (actieve opto-elektronische beschermende voorzieningen) of ESPE (elektrogevoelige beschermende apparatuur), bieden optimale veiligheid en kunnen toch een grotere productiviteit mogelijk maken. Lichtschermen zijn bij uitstek geschikt voor toepassingen waarbij personeel regelmatig en op eenvoudige wijze toegang tot een gevarengebied binnen dient te hebben. Lichtschermen zijn ontworpen en getest in overeenstemming met de norm IEC 61496-1 en -2.

Veiligheidslaserscanners

Veiligheidslaserscanners maken gebruik van een draaiende spiegel die lichtpulsen met een boog afbuigt, zodat een detectievlak ontstaat. De locatie van het object wordt vastgesteld door de draaiingshoek van de spiegel. Door gebruik te maken van een "looptijd"-techniek voor een gereflecteerde straal van onzichtbaar licht kan de scanner eveneens de afstand van het object tot de scanner detecteren. Aan de hand van de gemeten afstand en de locatie van het object kan de laserscanner de exacte positie van het object vaststellen.

Drukgevoelige veiligheidsmatten

Deze veiligheidsvoorzieningen worden gebruikt om het vloergebied rond een machine te beveiligen. Een serie samengekoppelde matten wordt om het gevarengebied geplaatst. Als een mat onder druk wordt gezet (bijvoorbeeld doordat de operator erop stapt), schakelt de controle-eenheid van de mat de voeding van het gevaar uit. Drukgevoelige matten worden vaak gebruikt binnen een afgesloten gebied dat verschillende machines, flexibele productiesystemen of roboticacellen bevat. Wanneer toegang tot de cel nodig is (bijvoorbeeld voor instellingen of het “instrueren” van een robot), voorkomen ze gevaarlijke bewegingen als de operator het veilige gebied verlaat. Het is belangrijk om bewegen van de mat(ten) te voorkomen door een juiste en veilige bevestiging.

Drukgevoelige boorden

Drukgevoelige boorden zijn flexibele verbindingsstrips die kunnen worden aangebracht op een bewegend onderdeel, zoals een machinetafel of een gemotoriseerde deur, dat een gevaar van verbrijzeling of afknelling oplevert.

Als het bewegende onderdeel in aanraking komt met de operator (of andersom), dan wordt de flexibele gevoelige boord ingedrukt en wordt er een opdracht gegeven om de voeding van het gevaar uit te schakelen. Er kan ook gebruik worden gemaakt van drukgevoelige boorden om machines te beveiligen wanneer de kans bestaat dat de operator in de machine vast komt te zitten. Als een operator in de machine vast komt te zitten, zal de voeding van de machine worden uitgeschakeld als gevolg van het contact met de drukgevoelige boord.

Lichtschermen, scanners, vloermatten en drukgevoelige boorden worden ook geclassificeerd als “uitschakelvoorzieningen”. Ze beperken in feite niet de toegang, maar “detecteren” deze alleen. Het nut van uitschakelvoorzieningen ligt in hun gecombineerde vermogen om toegang te detecteren en de voeding uit te schakelen. Over het algemeen zijn deze veiligheidsvoorzieningen alleen geschikt voor machines die redelijk snel tot stilstand komen nadat de voeding is uitgeschakeld. Aangezien een operator direct in het gevarengebied kan lopen of grijpen, dient de tijd die nodig is om de beweging van de machine stop te zetten minder te bedragen dan de tijd die de operator nodig heeft om het gevaar te bereiken nadat de beveiligingsvoorziening is geactiveerd.

Veiligheidsschakelaars

Wanneer toegang tot de machine onregelmatig is of wanneer er onderdelen kunnen worden uitgeworpen, genieten beweegbare (bedienbare) afschermingen vaak de voorkeur. De afscherming wordt aan de voeding naar het gevaar gekoppeld op een manier die garandeert dat wanneer de veiligheidsdeur niet is gesloten, de voeding naar het gevaar wordt uitgeschakeld.

Voor deze veiligheidsmethode wordt een vergrendelingsschakelaar gebruikt die op de veiligheidsdeur wordt gemonteerd. De regeling van de voeding van het gevaar wordt gerouteerd via het schakelaargedeelte van de eenheid. Hoewel er in de meeste gevallen sprake zal zijn van een elektrische voeding, kan er in sommige gevallen een pneumatische of hydraulische voeding worden gebruikt. Wanneer een beweging van de afschermingsdeur (openen) wordt gedetecteerd, zal de vergrendelingsschakelaar een opdracht geven om de voeding van het gevaar direct te onderbreken met behulp van een elektrische schakelaar (of klep).

Sommige onderbrekingsschakelaars zijn daarnaast voorzien van een vergrendelingsvoorziening die de veiligheidsdeur vergrendelt en deze pas ontgrendelt wanneer de machine zich in een veilige toestand bevindt.

Voor de meeste toepassingen is de combinatie van een beweegbare afscherming en een onderbrekingsschakelaar met of zonder veiligheidsvergrendeling de meest betrouwbare en efficiënte oplossing. (EN) ISO 14119 voorziet in nuttige richtlijnen inzake het selecteren van allerlei typen deurvergrendelingsvoorzieningen. Het gebruik ervan wordt aanbevolen.

Er is een breed scala aan veiligheidsschakelaars beschikbaar, zoals:

- **Tongvergrendelingsschakelaars** – voor deze voorzieningen moet een tongvormige actuator de schakelaar binnengaan en weer verlaten om de machine te kunnen bedienen.

- **Scharniervergrendelingsschakelaars** – deze voorzieningen worden op de scharnierpin van een veiligheidsdeur aangebracht, en gebruiken de openingsactie van de deur om de voeding uit te schakelen.

- **Deurvergrendelingsschakelaars** – bij sommige toepassingen is het nodig om de veiligheidsdeuren te vergrendelen of het openen van de veiligheidsdeur te vertragen. Voorzieningen die hiervoor geschikt zijn, worden deurvergrendelingsschakelaars genoemd. Ze zijn niet alleen geschikt voor machines met uitloopkenmerken, maar kunnen daarnaast voor de meeste typen machines een aanzienlijk hoger beschermingsniveau bieden.

- **Contactloze vergrendelingsschakelaars** – deze voorzieningen vereisen geen fysiek contact om te schakelen, deze kunnen gecodeerd zijn om sabotage te vermijden.

- **Positie(eindschakelaar)vergrendelingen** – nokkengestuurde inschakeling neemt meestal de vorm aan van een positieve modus-begrenzings- (of positie) schakelaar en een lineaire of roterende nok. Deze voorziening wordt meestal gebruikt voor veiligheidsschuifpanelen.

- **Sleutelvergrendelingen** – sleutelvergrendelingen kunnen zowel de bediening vergrendelen als de stroom onderbreken. Met de vergrendeling van de bediening wordt bedoeld dat een vergrendelingsvoorziening een stopopdracht naar een tussenliggend apparaat geeft, dat op zijn beurt een ander apparaat uitschakelt, zodat de voeding van de actuator wordt uitgeschakeld. Met het onderbreken van de stroom wordt bedoeld dat de stopopdracht de voeding naar de actuators van de machine direct onderbreekt.

Veiligheidsvoorzieningen op het bedieningspaneel

Stopfunctie – In de Verenigde Staten, Canada, Europa en op internationaal niveau zijn de normen met betrekking tot de omschrijvingen van stopcategorieën voor machines of productiesystemen geharmoniseerd.
OPMERKING: deze categorieën verschillen van de categorieën van de norm ISO 13849-1. Raadpleeg voor meer informatie de normen NFPA79 en IEC/EN 60204-1. Stopfuncties vallen in drie categorieën uiteen:

Categorie 0 heeft betrekking op het stopzetten van de machine door het direct onderbreken van de voeding naar de actuators van de machine. Dit wordt als ongecontroleerde stopzetting beschouwd. Als de voeding is uitgeschakeld, heeft de rematctie waarvoor stroom is vereist,

geen effect. Op deze manier kunnen motoren vrijelijk draaien en gedurende een lange periode uitlopen tot ze stilstaan. In andere gevallen is het mogelijk dat materiaal wordt losgelaten door houders of grijpers die van stroom moeten zijn voorzien om het materiaal vast te kunnen houden. Mechanische stopzettingsmiddelen (remmen), die geen stroom vereisen, kunnen ook worden gebruikt bij een stopzetting uit categorie 0. De stopzetting uit categorie 0 krijgt voorrang boven stopzettingen uit categorie 1 of 2.

Categorie 1 is een gecontroleerde stopzetting, waarbij de actuatoren van de machine stroom ontvangen om de stopzetting te bewerkstelligen. Wanneer de stopzetting is gerealizeerd, wordt de stroom van de actuators gehaald. Deze categorie stopzetting maakt het mogelijk om met stroom te remmen, zodat gevaarlijke bewegingen snel kunnen worden stopgezet. Vervolgens kan de stroom van de actuators worden gehaald. Dit type stopzetting kan resulteren in een snellere en meer gecontroleerde stopzetting, van waaruit een snellere herstart mogelijk is. OPMERKING: De 2016-versie van IEC/EN 60204-1 bevat meer stopzettingstypen van categorie 1.

Categorie 2 is een gecontroleerde stopzetting waarbij er nog steeds stroom beschikbaar is voor de actuators van de machine. Een normale productiestop wordt beschouwd als stopzetting van categorie 2.

Deze stopcategorieën dienen op elke stopfunctie te worden toegepast. De stopfunctie omvat de actie die de veiligheidsgerelateerde onderdelen van het besturingssysteem moet ondernemen als reactie op een invoer. In dit verband moet categorie 0 of 1 worden gebruikt. Stopfuncties moeten voorrang krijgen boven gerelateerde startfuncties. De selectie van de stopcategorie voor elke stopfunctie moet worden vastgesteld op basis van een risicoanalyse.

Noodstopfunctie

De noodstopfunctie moet functioneren als stopzettingen van categorie 0 of categorie 1, zoals vastgesteld op basis van een risicoanalyse. De noodstopfunctie moet met één menselijke handeling geactiveerd kunnen worden. Wanneer de noodstopfunctie wordt uitgevoerd, dient deze voorrang te krijgen boven alle andere bedrijfsmodi en functies. Het doel is om de stroomvoorziening zo snel mogelijk te onderbreken zonder dat hierdoor nog andere gevaren ontstaan. Wanneer het gevaar bestaat dat een operator van een machine in de problemen komt, dient de operator snelle toegang tot een noodstopvoorziening te hebben. De noodstopvoorziening dient voortdurend te werken en direct toegankelijk te zijn. Bedieningspanelen moet minimaal één noodstopvoorziening hebben. Extra noodstopvoorzieningen kunnen waar nodig op andere locaties worden gebruikt. Noodstopvoorzieningen zijn in tal van vormen verkrijgbaar. Drukknoppen en trekkoordschakelaars zijn voorbeelden van populaire noodstopvoorzieningen

Tot voor kort waren voor noodstopcircuits vastbedrade elektromechanische onderdelen vereist. Als gevolg van recente wijzigingen van normen zoals IEC 60204-1 en NFPA 79 kunnen veiligheids-PLC's en overige vormen van elektronische logica die aan de eisen van normen als IEC 61508 voldoen, in het noodstopcircuit worden gebruikt.

Noodstopvoorzieningen worden als aanvullende veiligheidsapparatuur beschouwd. Ze worden niet als primaire veiligheidsvoorzieningen beschouwd, omdat ze geen toegang tot een gevaar voorkomen en evenmin toegang tot een gevaar detecteren. Ze zijn gebaseerd op menselijke interactie.

Raadpleeg voor meer informatie over noodstopvoorzieningen ISO/EN13850, IEC 60947-5-5, NFPA79 and IEC60204-1, AS4024.1, Z432-94.

Noodstopdrukknoppen

Wanneer een drukknop als een noodstopvoorziening wordt gebruikt, moet de knop de vorm van een paddenstoel hebben, rood van kleur zijn en een gele achtergrond hebben. Wanneer de noodstopvoorziening wordt geactiveerd, moet deze vergrendelen. Het mag niet mogelijk zijn om de stopopdracht te genereren zonder vergrendelen. Het resetten van de noodstopvoorziening mag niet tot een gevaarlijke situatie leiden. Er moet een afzonderlijke en opzettelijke handeling worden uitgevoerd om de machine te herstarten.

Een van de nieuwste technieken die in noodstoppen wordt toegepast, is een zelfbewakingstechniek. Voor dit doel wordt een extra contact aan de achterzijde van de noodstop toegevoegd. Dit contact bewaakt of de achterzijden van de paneelcomponenten nog altijd aanwezig zijn. Deze voorziening staat bekend als een zelfbewakend contactblok. Het gaat om een met een veer geactiveerd contact dat wordt gesloten zodra het contactblok op het bedieningspaneel vastklikt.

Trekkoordschakelaars

Voor machines zoals lopende banden is het vaak handiger en effectiever om een systeem met een trekkoordschakelaar langs het gevarengebied als noodstopvoorziening te gebruiken. Deze voorzieningen maken gebruik van een stalen draad die aan vergrendelbare trekkoordschakelaars is verbonden. Wanneer de draad op een willekeurig punt in een willekeurige richting wordt getrokken, wordt de schakelaar geactiveerd en de voeding naar de machine stopgezet.

De trekkoordschakelaars moeten in staat zijn om te detecteren wanneer er aan de kabel wordt getrokken en wanneer er niet langer aan de kabel wordt getrokken. Kabelontspanningsdetectie is er om te bewaken of de kabel gebruiksklaar is en niet is gebroken.

De kabelafstand is van invloed op de werking van de schakelaar. Voor korte afstanden wordt de veiligheidsschakelaar aan één uiteinde van de kabel gemonteerd, en wordt aan het andere uiteinde van de kabel een spanningsveer aangebracht. Voor langere afstanden moet een veiligheidsschakelaar aan beide uiteinden van de kabel worden aangebracht om ervoor te zorgen dat de operator met één handeling een stopopdracht kan initiëren. Het gebruik van juist geplaatste oogbouten om de kabel te ondersteunen en te leiden is van wezenlijk belang. De vereiste trekkracht mag niet meer bedragen dan 200 N (45 lbs) dan wel een afstand van 400 mm (15,75 in) op een plaats midden tussen twee oogbouten. Het is belangrijk om de aanwijzingen van de fabrikant te volgen voor een juiste werking.

Tweehandsbedieningen

Het gebruik van tweehandsbedieningen (ook wel bimanuele bedieningen genoemd) is een veelgebruikte methode om toegang te voorkomen wanneer een machine zich in een gevaarlijke toestand bevindt. Om de machine te starten moeten twee bedieningsknoppen (binnen 0,5 s van elkaar) tegelijkertijd worden bediend. Op deze wijze wordt gegarandeerd dat beide handen van de operator zich in een veilige positie bevinden (d.w.z. op de bedieningsknoppen) en dat de operator zich dientengevolge niet in het gevarengebied kan bevinden. Tijdens

gevaarlijke omstandigheden moeten de bedieningen voortdurend worden bediend. De werking van de machine moet stoppen zodra een van de bedieningsknoppen wordt losgelaten. Wanneer een knop wordt losgelaten, moet de andere knop eveneens worden losgelaten voordat de machine opnieuw kan worden gestart. Dit voorziet in “anti-vastzetten” en voorkomt dat de tweehandsactie wordt gemanipuleerd tot een eenhandsactie.

Een tweehandsbedieningssysteem is voor het detecteren van fouten sterk afhankelijk van de integriteit van het bedienings- en bewakingssysteem. Het is daarom belangrijk dat dit aspect op basis van de juiste specificatie is ontworpen. De prestatie van het tweehandig veiligheidssysteem wordt ingedeeld in typen door de norm ISO 13851 (EN 574) zoals hieronder afgebeeld. Deze typen zijn gerelateerd aan de categorieën van de norm ISO 13849-1. De typen die het vaakst voor machineveiligheid worden gebruikt zijn IIIB en IIIC. De onderstaande tabel toont de relatie tussen de typen en de veiligheidsprestatiecategorieën.

Eisen	**Typen**				
	I	**II**	**III**		
			A	**B**	**C**
Synchrone schakeling			X	X	X
Gebruik van categorie 1 (van ISO 13849-1)	X		X		
Gebruik van categorie 3 (van ISO 13849-1)		X		X	
Gebruik van categorie 4 (van ISO 13849-1)					X

Tabel met vereisten van ISO 13851

De afstanden binnen het fysieke ontwerp moeten een onjuiste bediening (bijvoorbeeld met hand en elleboog) voorkomen. Dit kan mogelijk worden bewerkstelligd door een bepaalde afstand te creëren of afschermingen aan te brengen. De machine mag niet van de ene cyclus op de andere overgaan zonder dat beide knoppen worden ingedrukt en losgelaten. Dit voorziet in “anti-herhaling” en voorkomt de mogelijkheid dat beide knoppen worden geblokkeerd, zodat de machine ononderbroken blijft lopen. Als een van beide knoppen wordt losgelaten, dient de machine te stoppen.

Gebruik van tweehandsbediening dient zorgvuldig te worden overwogen, omdat dit type voorziening er vaak toe leidt dat de operator aan een vorm van gevaar wordt blootgesteld. De tweehandsbediening beschermt alleen de persoon die er gebruik van maakt. De beschermde operator dient in staat te zijn om alle toegangen tot het gevaar te overzien, omdat het overige personeel mogelijk niet is beschermd.

ISO 13851 (EN574) voorziet in aanvullende richtlijnen inzake de tweehandsbediening.

Inschakelvoorzieningen

Inschakelvoorzieningen zijn bedieningselementen die soms deel uitmaken van een permissieve strategie die een operator in staat stelt om een gevarengebied binnen te gaan terwijl de gevaarlijke motor op een veilig toerental draait, maar alleen zolang de operator de inschakelvoorziening in de geactiveerde stand houdt. Inschakelvoorzieningen maken gebruik van schakelaars met twee of drie standen. Schakelaars met twee standen zijn uitgeschakeld

wanneer de actuator niet wordt bediend, en zijn ingeschakeld wanneer de actuator wordt bediend. Schakelaars met drie standen zijn uitgeschakeld wanneer ze niet worden geactiveerd (positie 1), zijn ingeschakeld wanneer ze in de middelste stand worden gehouden (positie 2) en zijn uitgeschakeld wanneer de actuator voorbij de middelste positie wordt gezet (positie 3). Bij terugkeer van positie 3 naar 1 mag het uitvoercircuit bovendien niet worden gesloten bij het passeren van positie 2.

Inschakelvoorzieningen dienen in combinatie met andere veiligheidsgerelateerde functies te worden gebruikt. Een typisch voorbeeld is de werking met een beweging in een gecontroleerde langzame modus. Tijdens het gebruik van een inschakelvoorziening dient een signaal te worden gegeven dat de inschakelvoorziening actief is.

Logische voorzieningen

Logische voorzieningen vervullen een centrale rol, namelijk die van het veiligheidsgerelateerde onderdeel van het besturingssysteem. Logische voorzieningen dragen zorg voor de controle en bewaking van het veiligheidssysteem, en stellen de machine in staat om te starten of voeren opdrachten uit om de machine stop te zetten.

Er is een reeks logische voorzieningen beschikbaar waarmee een veiligheidsarchitectuur kan worden ontwikkeld die voldoet aan de complexiteit en functionaliteit die voor de machine is vereist. Kleine vastbedrade veiligheidsrelais voor bewakingsdoeleinden vormen de voordeligste oplossing voor kleinere machines waarbij een logisch apparaat speciaal voor het voltooien van de veiligheidsfunctie nodig is. Modulaire en configureerbare veiligheidsrelais genieten de voorkeur wanneer er een groot en uiteenlopend aantal veiligheidsapparaten en de bewaking van een minimale zone zijn vereist. Voor middelgrote tot grote machines en machines met een complexer karakter verdienen programmeerbare veiligheidssystemen met gedistribueerde I/O de voorkeur.

Veiligheidsrelais (MSR)

Veilgheidsrelaismodules spelen binnen tal van veiligheidssystemen een centrale rol. Deze modules bestaan normaliter uit twee of meer positief geleide relais met additionele bedrading die de werking van de veiligheidsfunctie waarborgt.

Positief geleide relais dienen om te voorkomen dat de normaliter gesloten en normaliter geopende contacten tegelijkertijd worden gesloten. Sommige veiligheidsrelais hebben halfgeleideruitgangen met veiligheidskwalificatie.

Veiligheidsrelais voeren tal van controles van het veiligheidssysteem uit. Bij het inschakelen van de stroom voeren ze zelfcontroles van hun interne onderdelen uit. Wanneer de ingangsmodules worden geactiveerd, vergelijkt het veiligheidsrelais de resultaten van redundante ingangen. Als deze acceptabel zijn, controleert het veiligheidsrelais de externe actuatoren die met de uitgangen zijn verbonden. Indien alles naar behoren werkt, wacht het veiligheidsrelais op een resetsignaal om zijn uitgangen van stroom te voorzien. Om deze reden kan een correct geselecteerd en geconfigureerd veiligheidsrelais voorzien in systeemfoutdetectie door de aangesloten invoer- en uitvoermodules te controleren. Het relais kan ook voorzien in een start-/herstartvergrendeling.

De selectie van het juiste veiligheidsrelais is van een aantal factoren afhankelijk: het type apparaat dat door het relais wordt bewaakt, het type reset en het aantal en het type uitgangen, etc.

Ingangstypen voor veiligheidsrelais (MSR)

Verschillende typen beveiligingsvoorzieningen bieden verschillende typen ingangen voor een veiligheidsrelais. Het is daarom belangrijk om te controleren op compatibiliteit. Het volgende is een kort overzicht van de typen ingangen die kunnen worden verwacht en de vereiste dwarsfoutdetectie-eigenschappen.

Elektromechanische vergrendelingen, sommige contactloze vergrendelingen en noodstoppen: Mechanische contacten, enkelkanaals met een normaal gesloten contact of dubbelkanaals, beide normaal gesloten. Het veiligheidsrelais moet zowel ondersteuning voor enkelkanaals als voor dubbelkanaals bieden en de dwarsfoutdetectie voor de dubbelkanaals configuratie verzorgen.

Sommige contactloze vergrendelingen en noodstoppen: Mechanische contacten, tweekanaals, een normaal open en een normaal gesloten contact. Het veiligheidsrelais moet in staat zijn om verschillende vormen van invoer te verwerken.

Modules met halfgeleideruitgangen: Lichtschermen, laserscanners en sommige contactloze afschermingsvergrendelingen hebben twee sourcing-uitgangen en voeren hun eigen dwarsfoutdetectie uit. Het veiligheidsrelais moet in staat zijn om de methode voor dwarsfoutdetectie van de module te negeren.

Drukgevoelige matten: Matten zorgen voor kortsluiting tussen twee kanalen. Het veiligheidsrelais moet speciaal ontworpen of configureerbaar zijn voor deze toepassing.

Drukgevoelige boorden: Sommige boorden zijn ontworpen als vierdraads matten. In sommige gevallen gaat het om voorzieningen met twee draden die voor een wijziging van de weerstand zorgen. Het veiligheidsrelais dient in staat te zijn om een kortsluiting of de wijziging van de weerstand te detecteren.

Motorbewegingsdetectie: Meet de tegen-EMK van een motor tijdens het uitlopen. Het veiligheidsrelais meet de spanning en kan zo stilstand detecteren.

Gestopte beweging: Het veiligheidsrelais telt de pulsen van redundante sensoren en kan zo snelheid en stilstand detecteren.

Tweehandsbediening: Het veiligheidsrelais controleert de twee drukknoppen welke voorzien zijn van een normaal open en een normaal gesloten contact en dit binnen de 0,5 s.

Veiligheidsrelais die voor bewakingsdoeleinden worden gebruikt, moeten specifiek ontworpen of configureerbaar zijn voor communicatie met elk van deze typen apparaten, aangezien deze verschillende elektrische kenmerken hebben. Sommige veiligheidsrelais zijn volledig configureerbaar tot verschillende typen. Sommige veiligheidsrelais kunnen worden aangesloten op verschillende typen ingangen, maar zodra het apparaat is geselecteerd kan het veiligheidsrelais alleen met dat apparaat werken. De ontwerper moet een veiligheidsrelais selecteren of configureren dat compatibel is met de invoermodule.

Ingangsimpedantie

De ingangsimpedantie van het veiligheidsrelais bepaalt hoeveel ingangsmodules op het relais kunnen worden aangesloten, en op welke afstand de ingangsmodules kunnen worden gemonteerd. Een veiligheidsrelais kan bijvoorbeeld een maximaal toegestane ingangsimpedantie van 500 ohm hebben. Wanneer de ingangsimpedantie groter dan 500 ohm is, zullen de relaisuitgangen niet worden ingeschakeld. De gebruiker dient de nodige voorzorg in acht te nemen om ervoor te zorgen dat de ingangsimpedantie onder de maximaal gespecificeerde waarde blijft. De lengte, de grootte en het type van de gebruikte draad zijn van invloed op de ingangsimpedantie.

Aantal ingangsmodules

Het risicobeoordelingsproces moet worden gebruikt om te helpen bepalen hoeveel invoermodules mogen worden aangesloten op een veiligheidsrelais dat voor bewakingsdoeleinden wordt gebruikt, en hoe vaak deze invoermodules moeten worden gecontroleerd. Om ervoor te zorgen dat noodstoppen en deurvergrendelingen operationeel zijn, moeten ze regelmatig op correcte werking worden gecontroleerd, zoals vastgesteld tijdens de risicobeoordeling. Een veiligheidsrelais met dubbelkanaals ingang dat is aangesloten op een vergrendelde deur die gedurende elke machinecyclus moet worden geopend (bijvoorbeeld verschillende malen per dag) hoeft mogelijk niet te worden gecontroleerd. De reden hiervoor is dat het openen van de deur ervoor zorgt dat het veiligheidsrelais zichzelf, zijn ingangen en uitgangen (afhankelijk van de configuratie) op afzonderlijke fouten controleert. Hoe groter de regelmaat waarmee de afscherming wordt geopend, des te groter de integriteit van het controleproces.

Een ander voorbeeld zijn noodstoppen. Omdat noodstoppen normaliter alleen voor noodgevallen zijn bestemd, zullen ze waarschijnlijk zelden worden gebruikt. Om deze reden dient een programma te worden opgesteld om de noodstoppen uit te proberen en de effectiviteit ervan op basis van een planning te bevestigen. Het op deze manier uitproberen van een veiligheidssysteem wordt het uitvoeren van een functionele test genoemd. Een derde voorbeeld zijn toegangsdeuren voor machineafstellingen, die net als noodstoppen waarschijnlijk zelden worden gebruikt. Ook hier moet een programma worden opgezet om de controlefunctie op basis van een planning uit te proberen.

De risicoanalyse zal helpen om vast te stellen of, en met welke regelmaat, de ingangsmodules gecontroleerd moeten worden. Hoe hoger het risiconiveau, des te groter de vereiste integriteit van het controleproces. Hoe lager de regelmaat van de “automatische” controle, des te hoger de regelmaat van de “handmatige” controle.

Dwarsfoutdetectie op de ingang

In dubbelkanaals systemen moeten kortsluitingsfouten tussen de kanalen van de invoermodules, ook wel dwarsfouten genoemd, door het veiligheidssysteem worden gedetecteerd. Deze functie wordt verzorgd door het veiligheidsrelais dat voor de bewakingsdoeleinden wordt gebruikt.

Op microprocessors gebaseerde veiligheidsrelais detecteren, net zoals lichtschermen, laserscanners en geavanceerde contactloze sensoren, deze kortsluitingen op verschillende manieren. Een vaak gebruikte manier om dwarsfouten te detecteren is door gebruik te maken van pulstesten. De signalen die in het veiligheidsrelais worden ingevoerd, worden zeer snel gepulst. Er is een offset tussen de puls van kanaal 1 en de puls van kanaal 2. Als er kortsluiting optreedt, vinden de pulsen tegelijkertijd plaats en worden ze door het apparaat gedetecteerd.

Elektromagnetische veiligheidsrelais voor bewakingsdoeleinden maken gebruik van een andere kortsluitdetectie: een pull up-ingang en een pull down-ingang. Een kortsluiting van kanaal 1 naar kanaal 2 zal ervoor zorgen dat de overstroombeveiligingsvoorziening wordt geactiveerd. Hierop wordt het veiligheidssysteem uitgeschakeld.

Uitgangen

Veiligheidsrelais worden met verschillende hoeveelheden uitgangen geleverd. De typen uitgangen helpen bij het bepalen van het veiligheidsrelais dat voor een bepaalde toepassing moet worden gebruikt.

De meeste veiligheidsrelais hebben minimaal twee direct werkende veiligheidsuitgangen. Veiligheidsrelais voor bewakingsdoeleinden worden gekenmerkt als normaal open. Deze veiligheidsrelais worden als veilig geclassificeerd vanwege de redundantie en interne controle. Een tweede type uitgang omvat vertraagde uitgangen. Vertraagde uitgangen worden normaliter gebruikt in stopzettingen van categorie 1, waarbij de machine tijd nodig heeft om de stopfunctie uit te voeren voordat toegang tot het gevarengebied kan worden geboden. Veiligheidsrelais zijn daarnaast uitgerust met hulpuitgangen. Over het algemeen worden deze beschouwd als normaal gesloten.

Nominale waarden van de uitgangen

De nominale waarden van de uitgangen geven het vermogen van een veiligheidsvoorziening aan om belastingen om te schakelen. Normaliter worden de nominale waarden voor industriële apparaten aangeduid met de term resistief of elektromagnetisch. Een resistieve belasting kan een verwarmend element zijn. Elektromagnetische ladingen zijn normaliter relais, magneetschakelaars of solenoïden waarbij de belasting een sterk inductief karakter heeft. Bijlage A van norm IEC 60947-5-1 beschrijft de nominale waarden voor belastingen.

Letteraanduiding: Een letteraanduiding omvat een letter gevolgd door een getal, bijvoorbeeld A300. De letter is van toepassing op de conventionele besloten thermische stroom en geeft aan of deze stroom een direct of wisselend karakter heeft. De letter A bijvoorbeeld staat voor een wisselstroom van 10 ampère. Het getal staat voor de nominale isolatiespanning. 300 staat bijvoorbeeld voor 300 V.

Gebruik: Het gebruik geeft aan voor welke soorten belastingen het apparaat is ontwikkeld om te schakelen. De gebruiksvormen die relevantie hebben voor de norm IEC 60947-5 worden in de onderstaande tabel weergegeven.

Gebruik	Beschrijving van lading
AC-12	Besturing van resistieve belastingen en halfgeleiderbelastingen met stroomonderbreking door optische koppelaars
AC-13	Besturing van halfgeleiderbelastingen met transformatorisolatie
AC-14	Besturing van kleine elektromagnetische belastingen (minder dan 72 VA)
AC-15	Elektromagnetische belastingen groter dan 72 VA
DC-12	Besturing van resistieve belastingen en halfgeleiderbelastingen met stroomonderbreking door optische koppelaars
DC-13	Besturing van spoelen
DC-14	Besturing van elektromagnetische belastingen met spaarweerstanden in circuit

Thermische stroom, Ith: De thermische stroom is de stroomwaarde die wordt gebruikt voor de temperatuurstijgingstests van de apparatuur wanneer deze in een gespecificeerde behuizing is gemonteerd.

Nominale bedrijfsspanning Ue en nominale bedrijfsstroom Ie: De nominale bedrijfsstroom en de nominale bedrijfsspanning specificeren het inschakel- en uitschakelvermogen van de schakelelementen onder normale bedrijfsomstandigheden. De gangbare nominale waarden voor Allen-Bradley Guardmaster-producten zijn 125 VAC, 250 VAC en 24 VDC.

VA: De nominale VA-waarden (Volt x Ampère) geven de nominale waarden aan van de schakelelementen wanneer het circuit wordt geopend en gesloten.

Voorbeeld 1: Een nominale waarde van A150, AC-15 geeft aan dat de contacten een 7.200 VA-circuit kunnen sluiten. Bij 120 VAC kunnen de contacten een circuit met een aanloopstroomsterkte van 60 ampère sluiten. Omdat de AC-15 een elektromagnetische belasting is, is de 60 ampère slechts van korte duur; de aanloopstroom van de elektromagnetische belasting. De onderbreking van het circuit bedraagt slechts 720 VA, omdat de stationaire stroom van de elektromagnetische belasting 6 A is. Dit is de nominale bedrijfsstroom.

Voorbeeld 2: Een nominale waarde van N150, DC-13 geeft aan dat de contacten een 275 VA-circuit kunnen sluiten. Bij 125 VAC kunnen de contacten een circuit van 2,2 ampère sluiten. Elektromagnetische gelijkstroombelastingen kennen geen aanloopstroom zoals elektromagnetische wisselstroombelastingen. De onderbreking van het circuit bedraagt eveneens 275 VA, omdat de statische stroom van de elektromagnetische belasting 2,2 ampère is. Dit is de nominale bedrijfsstroom.

Herstarten van de machine

Als er bijvoorbeeld een vergrendelde afscherming op een draaiende machine wordt geopend, zal de veiligheidsvergrendelingsschakelaar die machine stopzetten. In de meeste gevallen is het belangrijk dat de machine niet direct opnieuw wordt gestart wanneer de afscherming wordt gesloten. Een veel gebruikte methode om dit te bereiken is het gebruik van een startconfiguratie met een koppelstukmagneetschakelaar.

Als de startknop wordt ingedrukt en losgelaten, wordt de controlespoel van de magneetschakelaar tijdelijk van stroom voorzien. De spoel zal hierop de stroomaansluitingen sluiten. Zolang de stroom door de stroomcontacten loopt, blijft de controlespoel stroom ontvangen (elektrische vergrendeling) via de hulpcontacten van de magneetschakelaar, die mechanisch zijn verbonden met de stroomcontacten. Elke onderbreking van de hoofdstroom of stuurstroom zorgt ervoor dat de stroom van de spoel wordt gehaald en dat de hoofdstroom- en hulpcontacten worden geopend. De vergrendeling van de afscherming is op de stuurstroom van de magneetschakelaar aangesloten. Dit betekent dat de machine alleen opnieuw kan worden gestart door de afscherming te sluiten en de machine vervolgens “AAN” te zetten met de normale startknop, die de magneetschakelaar reset en de machine start.

De vereisten voor normale vergrendelingssituaties worden uiteengezet in ISO 12100 (uittreksel):

“Wanneer de afscherming wordt gesloten, kunnen de gevaarlijke functies die door de afscherming zijn gedekt, functioneren. Het sluiten van de afscherming leidt er echter op zichzelf niet toe dat de werking van deze functies wordt geïnitieerd”.

Veel machines zijn reeds uitgerust met enkele of dubbele magneetschakelaars, die op de hierboven beschreven wijze functioneren (of hebben een veiligheidssysteem dat hetzelfde resultaat bewerkstelligt). Wanneer u een vergrendeling op een bestaande machine aanbrengt, is het nodig om vast te stellen of de vermogensbeveiligingsconfiguratie aan deze eisen voldoet en om indien nodig aanvullende maatregelen te treffen.

Resetfuncties

De veiligheidsrelais van Allen Bradley Guardmaster zijn uitgerust met een bewaakte handmatige reset of automatische/handmatige reset.

Bewaakte handmatige reset

Een bewaakte handmatige reset vereist dat de status van het geresette circuit wordt gewijzigd nadat de afscherming is gesloten of nadat de noodstop is gereset. De mechanisch gekoppelde, normaal gesloten hulpcontacten van de stroomschakelaars zijn in serie geschakeld met een impulsdrukknop. Nadat de afscherming opnieuw is geopend en gesloten, zal het veiligheidsrelais de machine niet toestaan om opnieuw te starten totdat status van de resetknop is gewijzigd. Dit is conform de bedoeling van de eisen voor een aanvullende handmatige reset zoals vermeld in (EN) ISO 13849-1. Dit houdt in dat de resetfunctie waarborgt dat beide schakelaars UITGESCHAKELD zijn, dat beide vergrendelingscircuits

(en bijgevolg de afschermingen) gesloten zijn en tevens dat (omdat een statuswijziging is vereist) de geresette actuator op geen enkele manier is omzeild of geblokkeerd. Als deze controles succesvol zijn, kan de machine vervolgens opnieuw worden gestart met behulp van de normale bedieningselementen. (EN) ISO 13849-1 vermeldt de toestandsverandering van geactiveerd naar gedeactiveerd ('neergaande flank').

De resetschakelaar dient zich op een locatie te bevinden met goed overzicht op de machine, zodat de operator kan controleren of het gebied veilig is alvorens de machine weer in werking te stellen.

Automatische/handmatige reset

Sommige veiligheidsrelais zijn uitgerust met een automatische/handmatige resetfunctie. De handmatige resetmodus wordt niet bewaakt. Wanneer de knop wordt ingedrukt, zal er een reset plaatsvinden. Een kortgesloten of vastgelopen resetschakelaar zal niet worden gedetecteerd. Hierdoor kan mogelijk niet voldaan worden aan de eisen voor een aanvullende handmatige reset zoals vermeld in (EN) ISO 13849-1 indien er geen aanvullende maatregelen worden toegepast.

Als alternatief kan de resetaansluiting worden overbrugd om een automatische reset mogelijk te maken. De gebruiker moet vervolgens zorgen voor een ander mechanisme dat voorkomt dat de machine opstart wanneer de deur wordt gesloten.

Voor een automatische resetvoorziening is geen handmatige schakelactie vereist. Na uitschakeling zal deze voorziening echter altijd een systeemintegriteitscontrole uitvoeren alvorens het systeem te resetten. Een automatisch resetsysteem moet niet worden verward met een apparaat zonder resetfuncties. In het laatste geval zal het veiligheidssysteem direct na uitschakeling worden ingeschakeld, maar zal er geen systeemintegriteitscontrole worden uitgevoerd.

De resetschakelaar dient zich op een locatie te bevinden met goed overzicht op de machine, zodat de operator kan controleren of het gebied veilig is alvorens de machine weer in werking te stellen.

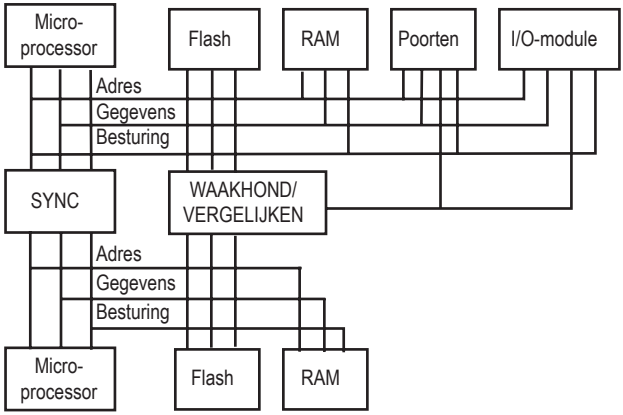
Afschermingen met veiligheidsregelcircuit

Een afscherming met veiligheidsstuurcircuit stopt een machine wanneer de afscherming wordt geopend, en zal de machine direct starten zodra de afscherming wordt gesloten. Het gebruik van afschermingen met veiligheidsregelcircuit is alleen onder strikte voorwaarden toegestaan, omdat het onverwacht opstarten of niet kunnen stopzetten van de machine uitermate gevaarlijk zou kunnen zijn. Het vergrendelingssysteem moet het hoogst mogelijke betrouwbaarheidsniveau bieden. Vaak is het ook aan te raden om gebruik te maken van afschermingsvergrendelingen. Het gebruik van afschermingen met veiligheidsregelcircuit mag ALLEEN worden overwogen voor machines indien er GEEN MOGELIJKHEID bestaat dat een operator of een van diens lichaamsdelen zich in de gevarenzone bevindt of dat de operator in deze gevarenzone grijpt terwijl de afscherming is gesloten. De afscherming met veiligheidsregelcircuit moet de enige toegang tot het gevarengebied vormen.

Veiligheids-PLC's

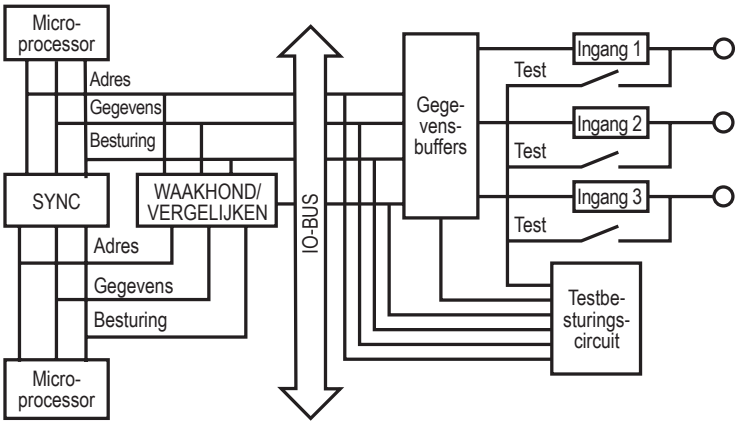
De behoefte aan flexibele en schaalbare veiligheidstoepassingen heeft geresulteerd in de ontwikkeling van veiligheids-PLC's en veiligheidscontrollers. Programmeerbare veiligheidscontrollers bieden gebruikers dezelfde mate van flexibiliteit binnen een veilige toepassing die ze kennen van standaard programmeerbare controllers. Er bestaan echter aanzienlijke verschillen tussen standaard-PLC 's en veiligheids-PLC's. Veiligheids-PLC's zijn voor verschillende platforms beschikbaar om te voorzien in de behoeften van complexere veiligheidssystemen op het gebied van schaalbaarheid, functionaliteit en integratie.

Er worden meerdere microprocessors gebruikt om de I/O, het geheugen en veilige communicatie te verwerken. Bewakingscircuits voeren diagnostische analyses uit. Dit type constructie staat bekend als 1oo2D, omdat elk van beide microprocessors afzonderlijk de veiligheidsfunctie kan uitvoeren, en uitgebreide diagnostische bewerkingen worden uitgevoerd om een synchrone werking van beide microprocessors te garanderen.



1oo2D-architectuur

Daarnaast wordt elk ingangscircuit verschillende malen per seconde getest om een juiste werking te garanderen. U mag de noodstop slechts een keer per maand indrukken. Wanneer u dit doet, is het interne circuit continu getest.



Blokdiagram veiligheidsingangmodule

Veiligheids-PLC-uitgangen zijn elektromechanische of veilige halfgeleideruitgangen. Net zoals de ingangscircuits, worden de uitgangscircuits elke seconde meerdere malen getest om te garanderen dat ze de uitgang kunnen uitschakelen. Als er sprake is van een storing van een van deze drie, zal de uitgang door de andere twee worden uitgeschakeld, en zal de fout door het interne bewakingscircuit worden gerapporteerd.
Als er veiligheidsvoorzieningen met mechanische contacten (noodstoppen, deurschakelaars etc.) worden gebruikt, kan de gebruiker pulstestsignalen gebruiken om dwarsfouten te detecteren.

Software

Veiligheids-PLC's kunnen in grote lijnen als standaard-PLC's worden geprogrammeerd. Alle eerder vermelde additionele diagnostische bewerkingen en foutcontroles worden door het besturingssysteem uitgevoerd. Dit houdt in dat de programmeur zelf niet eens op de hoogte is van hetgeen er gebeurt. De meeste veiligheids-PLC's kennen speciale instructies die kunnen worden gebruikt om het programma voor het veiligheidssysteem te schrijven. Deze instructies weerspiegelen vaak de functie van hun veiligheidsrelaisequivalenten. De noodstopinstructie kent bijvoorbeeld een soortgelijke werking als een veiligheidsrelais. Hoewel de logica achter elk van deze instructies complex is, zien de veiligheidsprogramma 's er relatief eenvoudig uit, omdat de programmeur deze blokken eenvoudig met elkaar verbindt. Deze instructies worden samen met andere logische, wiskundige, gegevensmanipulatie- en andere instructies gecertificeerd door een externe partij om te garanderen dat hun werking voldoet aan de richtlijnen van de toepasselijke normen.

Functieblokken vormen de voornaamste methode die voor het programmeren van veiligheidsfuncties wordt gebruikt. Naast functieblokken en ladderlogica bieden veiligheids-PLC's ook gecertificeerde instructies voor veiligheidstoepassingen. Gecertificeerde veiligheidsinstructies voorzien in toepassingsspecifiek gedrag.

Gecertificeerde functieblokken zijn beschikbaar voor gebruik in combinatie met vrijwel alle veiligheidsvoorzieningen. Een uitzondering hierop is de veilige boord, die gebruikmaakt van weerstandstechnologie.

Veiligheids-PLC's genereren een "handtekening" die de mogelijkheid biedt om eventuele wijzigingen in kaart te brengen. Deze handtekening omvat meestal een combinatie van het programma, de invoer/uitvoer-configuratie en een tijdsstempel. Wanneer het programma is voltooid en gecontroleerd, moet de gebruiker deze handtekening voor naslag opslaan als onderdeel van de controleresultaten. Als het programma moet worden gewijzigd, is een nieuwe controle nodig en moet een nieuwe handtekening worden vastgelegd. Het programma kan tevens met een wachtwoord worden vergrendeld om wijzigingen door onbevoegden te voorkomen.

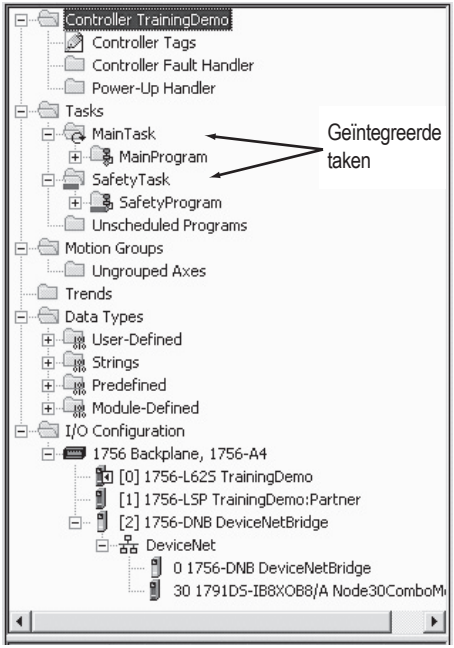
De bedrading van programmeerbare logische systemen is vereenvoudigd ten opzichte van veiligheidsrelais die voor bewakingsdoeleinden worden gebruikt. In tegenstelling tot verbindingen met specifieke aansluitpunten op veiligheidsrelais, worden invoermodules aangesloten op veiligheidsingangsaansluitingen en worden uitvoermodules aangesloten op veiligheidsuitgangsaansluitingen. De aansluitingen worden vervolgens softwarematig toegewezen.

Geïntegreerde veiligheidscontrollers

Veiligheidsbesturingsoplossingen bieden inmiddels volledige integratie binnen één besturingsarchitectuur. De standaardbesturingsfuncties zijn bij elkaar ondergebracht en werken samen. De mogelijkheid om bewegings-, aandrijvings-, proces-, batch-, hogesnelheids-sequentiële en SIL 3-veiligheid in één controller onder te brengen biedt aanzienlijke voordelen. De integratie van veiligheidsbesturingssystemen en standaardbesturingssystemen biedt de mogelijkheid om gebruik te maken van gemeenschappelijke tools en technologie, hetgeen leidt tot verlaging van de kosten die gepaard gaan met het ontwerp, de installatie, de inbedrijfstelling en het onderhoud. Het vermogen om gebruik te maken van gemeenschappelijke besturingshardware, gedistribueerde veiligheids-I/O of apparaten binnen veiligheidsnetwerken en gemeenschappelijke HMI-voorzieningen resulteert in lagere aanschaf- en onderhoudskosten en in een kortere ontwikkelingstijd. Al deze functies verbeteren de productiviteit, verhogen de snelheid van het probleemoplossingsproces en verlagen de trainingskosten vanwege de gemeenschappelijke aard van de functies.

Het volgende diagram toont een voorbeeld van de integratie van de besturing en veiligheid. De standaard niet-veiligheidsgerelateerde besturingsfuncties bevinden zich in de hoofdtaak. De veiligheidsgerelateerde functies bevinden zich in de veiligheidstaak.

Alle veiligheidsgerelateerde en standaardfuncties zijn van elkaar gescheiden. Op deze manier kunnen de veiligheidstags direct door de standaardlogica worden gelezen. Veiligheidstags kunnen tussen GuardLogix-controllers worden uitgewisseld via EtherNet/IP, ControlNet of DeviceNet. De gegevens van veiligheidstags kunnen direct worden gelezen door externe apparaten, human-machine interfaces (HMI's), pc's of andere controllers.



1. Standaardtags en logica gedragen zich op dezelfde manier als ControlLogix.

2. Standaardtaggegevens, door een programma of controller geregelde apparaten en externe apparaten, human-machine-interfaces, pc's, overige controllers, enz..

3. Als geïntegreerde controller biedt GuardLogix de mogelijkheid om de standaardtaggegevens te verplaatsen ('mappen') naar veiligheidstags voor gebruik binnen de veiligheidstaak. Op deze manier wordt aan de gebruikers de mogelijkheid geboden om statusinformatie af te lezen van de standaardzijde van GuardLogix. Deze gegevens mogen niet worden gebruikt om rechtstreeks een veiligheidsuitgang te besturen.

4. Veiligheidstags kunnen rechtstreeks worden gelezen door standaardlogica.

5. Veiligheidstags kunnen door veiligheidslogica worden gelezen of geschreven.

6. Veiligheidstags kunnen tussen GuardLogix-controllers worden uitgewisseld via EtherNet/IP.

7. Door een programma of controller geregelde veiligheidstags kunnen worden gelezen door externe apparaten, HMI's, pc's, overige controllers, enz. Hierbij dient te worden opgemerkt dat deze gegevens, wanneer ze eenmaal buiten de veiligheidstaak zijn gebruikt, worden beschouwd als standaardgegevens, en niet als veiligheidsgegevens.

Veiligheidsnetwerken

Communicatienetwerken op de fabrieksvloer hebben fabrikanten de mogelijkheid geboden om de flexibiliteit te vergroten, meer diagnostische functies te gebruiken, de afstand te vergroten, de installatie- en bedradingskosten te verlagen, het onderhoud te vergemakkelijken en de algehele productiviteit van hun productieprocessen te vergroten. Dezelfde overwegingen hebben geleid tot de implementatie van industriële veiligheidsnetwerken. Deze veiligheidsnetwerken stellen fabrikanten in staat om veiligheids-I/O- en veiligheidsapparaten rond hun machines op te stellen met behulp van één netwerkkabel voor zowel veiligheidscommunicatie als standaard-I/O-communicatie. Hierdoor worden de installatiekosten verlaagd, de diagnostische mogelijkheden verbeterd en complexere veiligheidssystemen mogelijk gemaakt. Daarnaast bieden veiligheidsnetwerken de mogelijkheid van een veilige communicatie tussen veiligheids-PLC's en veiligheidscontrollers, zodat gebruikers de veiligheidsregeling over verschillende intelligente systemen kunnen distribueren.

Veiligheidsnetwerken zijn ontworpen om overdrachtsfouten te detecteren en een geschikte foutreactiefunctie te initiëren. Gedetecteerde communicatiefouten zijn onder meer: het invoegen van berichten, het verloren gaan van berichten, de beschadiging van berichten, de vertraging van berichten, de herhaling van berichten en een onjuiste berichtenvolgorde.

Voor de meeste toepassingen geldt dat het apparaat, wanneer er een storing wordt gedetecteerd, overgaat op een bekende van vermogen afgesloten toestand, die normaliter een "veilige toestand" wordt genoemd. De veiligheidsinvoer- of -uitvoercommunicatiemodule is verantwoordelijk voor de detectie van deze communicatiefouten en, indien wenselijk, voor het overschakelen naar de veilige toestand.

De eerste veiligheidsnetwerken waren gebonden aan een bepaald type media of een mediatoegangsschema, zodat fabrikanten gebruik moesten maken van specifieke kabels, netwerkkaarten, routers, bruggen en dergelijke, die eveneens onderdeel van de veiligheidsfunctie werden. Deze netwerken waren beperkt in die zin dat ze alleen ondersteuning boden voor communicatie tussen veiligheidsvoorzieningen.
Dit hield in dat fabrikanten twee of meer netwerken voor hun machinebedieningsstrategie moesten gebruiken (een netwerk voor de standaardbesturing en een ander netwerk voor de veiligheidsgerelateerde besturing). Dat leidde tot hogere kosten voor de installatie, training en reserveonderdelen.

Moderne veiligheidsnetwerken stellen één netwerkkabel in staat om te communiceren met veiligheids- èn standaardbesturingsapparaten. CIP (Common Industrial Protocol) Safety is een protocol op basis van open standaarden dat is gepubliceerd door de ODVA (Open DeviceNet Vendors Association) en veiligheidscommunicatie mogelijk maakt tussen veiligheidsapparaten in DeviceNet-, ControlNet- en EtherNet/IP-netwerken. Aangezien CIP Safety een uitbreiding op het standaard CIP-protocol vormt, kunnen veiligheidsapparaten en standaardapparaten in hetzelfde netwerk worden gebruikt. Gebruikers kunnen tevens een brug creëren tussen netwerken die veiligheidsapparaten bevatten, zodat ze veiligheidsapparaten kunnen onderverdelen om de veiligheidsresponstijden te optimaliseren of eenvoudig om de distributie van veiligheidsapparaten gemakkelijker te maken. Omdat het veiligheidsprotocol louter de verantwoordelijkheid is van eindapparaten (veiligheids-PLC/controller, veiligheids-I/O-module, veiligheidscomponent), worden standaardkabels, -netwerkkaarten, -bruggens en -routers gebruikt. Op deze manier wordt een einde gemaakt aan de noodzaak van speciale netwerkhardware, zodat deze apparaten niet langer aan de veiligheidsfunctie hoeven te deel nemen.

Uitvoermodules

Veiligheidsbesturingsrelais en veiligheidsmagneetschakelaars

Besturingsrelais en magneetschakelaars worden gebruikt om de stroom van de actuator te halen. Aan besturingsrelais en magneetschakelaars worden speciale functies toegevoegd waardoor ze voor veiligheidstoepassingen kunnen worden gebruikt.

Mechanisch verbonden hulpcontacten worden gebruikt om de status van de controlerelais en magneetschakelaars aan een logische bewakingsmodule te rapporteren. Het gebruik van mechanisch gekoppelde contacten garandeert de veiligheidsfunctie. Om te voldoen aan de eisen voor mechanisch gekoppelde contacten mogen de normaal gesloten en normaal geopende contacten zich niet tegelijkertijd in een gesloten staat bevinden. IEC 60947-4-1 definieert de eisen voor mechanisch gekoppelde contacten. Als de normaal geopende contacten zouden versmelten, dan blijven de normaal gesloten contacten minimaal 0,5 mm geopend. Omgekeerd, als de normaal gesloten contacten zouden versmelten, dan blijven de normaal geopende contacten open.

Veiligheidssystemen mogen alleen op specifieke locaties worden gestart. Standaardbesturingsrelais en -magneetschakelaars maken het mogelijk om de armatuur in te drukken, zodat de normaal geopende contacten worden gesloten. Bij veilig bevonden apparaten wordt de armatuur beschermd tegen handmatige bediening om een onverwacht opstarten van de machine te voorkomen.

Op veiligheidscontrolerelais wordt het normaal gesloten contact door de hoofdveer aangedreven. Veiligheidsmagneetschakelaars maken gebruik van een optelschakeling om de mechanisch gekoppelde contacten te kunnen vinden. Als het contactblok van de voet zou vallen, zouden de mechanisch gekoppelde contacten gesloten blijven. De mechanisch gekoppelde contacten zijn permanent bevestigd aan het veiligheidsbesturingsrelais of de veiligheidsmagneetschakelaar. Op de grotere magneetschakelaars is een optelschakeling ontoereikend om de status van de bredere veer op juiste wijze te weerspiegelen. Er worden gespiegelde contacten gebruikt en deze bevinden zich aan weerszijden van de magneetschakelaar.

De drop out-tijd voor besturingsrelais of magneetschakelaars speelt een rol bij het berekenen van de veiligheidsafstand. Vaak wordt er een overspanningsbeveiliging langs de spoel aangebracht ter vergroting van de levensduur van de contacten die de spoel aandrijven. Voor spoelen die op wisselspanning werken, heeft dit geen invloed op de afvaltijd. Bij spoelen die op gelijkspanning werken, wordt de afvaltijd langer. De verlenging van de drop out-tijd is afhankelijk van het type geselecteerde onderdrukking.

Besturingsrelais en magneetschakelaars zijn bedoeld om grote belastingen te schakelen, van 0,5 A tot meer dan 100 A. Het veiligheidssysteem werkt op zwakstroom. Het feedback-signaal dat door het logische apparaat van het veiligheidssysteem wordt gegenereerd, kan variëren van een paar milliampères tot tientallen milliampères, meestal bij een spanning van 24 VDC. De veiligheidsbesturingsrelais en veiligheidsmagneetschakelaars maken gebruik van gevorkte goudcontacten om dit geringe stroom op een betrouwbare wijze te schakelen.

Overbelastingsbeveiliging

De elektrische normen vereisen het gebruik van een overbelastingsbeveiliging voor motoren. De diagnostische functionaliteit die door de overbelastingsbeveiliging wordt geboden, verbetert niet alleen de veiligheid van de apparatuur, maar ook de veiligheid van de operator. De momenteel beschikbare technologie is in staat om foutcondities te detecteren zoals overbelasting, fase-uitval, aardlekken, blokkeringen, onderbelasting, stroomonbalans en oververhitting. De detectie en communicatie van abnormale condities voorafgaand aan uitschakeling zorgen voor een verbetering van de productie-uptime en beschermen operators en onderhoudstechnici tegen onvoorziene gevaarlijke omstandigheden.

Frequentiesturingen en servoaandrijvingen

Frequentiesturingen en servoaandrijvingen kunnen worden gebruikt om te voorkomen dat er energie voor rotatie wordt geleverd, zodat zowel een veiligheidsstop en een noodstop mogelijk zijn.

Frequentiesturingen zorgen dat aan de eisen voor de veiligheidsbeoordeling wordt voldaan door redundante kanalen te bieden om de voeding weg te nemen die het deurcontrole circuit beheert. De redundante kanalen worden bewaakt door externe of geïntegreerde logica, al naar gelang het type aandrijving. Deze redundante aanpak maakt het mogelijk om de frequentiesturing in noodstopcircuits toe te passen zonder de noodzaak van een magneetschakelaar.

De servoaandrijving bereikt het doel op een vergelijkbare manier als de wisselstroomaandrijvingen door redundante veiligheidssignalen te gebruiken om de veiligheidsfunctie “safe torque-off” te bewerkstelligen.

Aansluitsystemen

Aansluitsystemen bieden toegevoegde waarde door de installatie- en onderhoudskosten van veiligheidssystemen te verlagen. De ontwerpen dienen rekening te houden met enkelkanaals en tweekanaals apparaten, tweekanaals apparaten met indicatie en het gebruik van verschillende typen apparaten.

Wanneer een serieschakeling van tweekanaals vergrendelingen is vereist, kan een distributieblok de installatie vereenvoudigen. Met een IP67-waarde kunnen deze typen modules op externe locaties op de machine worden gemonteerd. Wanneer een uiteenlopende reeks van apparaten nodig is, kan een ArmorBlock Guard I/O-module worden gebruikt. De ingangen kunnen softwarematig worden geconfigureerd om ondersteuning voor verschillende typen apparaten te bieden.

Hoofdstuk 5: Berekening van de veiligheidsafstand

Gevaren moeten in een veilige situatie worden omgezet voordat een operator het gevaar kan bereiken. Voor het berekenen van de veiligheidsafstand zijn er twee groepen normen. In dit hoofdstuk worden deze normen als volgt onderverdeeld:

ISO EN: (EN ISO 13855)

US CAN (ANSI B11.19, ANSI RIA R15.06 en CAN/CSA Z434-03)

Formule

De minimale veiligheidsafstand hangt af van de tijd die nodig is om de stopopdracht te verwerken en hoe ver de operator de detectiezone kan binnendringen alvorens hij door het systeem wordt gedetecteerd. De formule die overal ter wereld wordt gebruikt heeft dezelfde vorm en eisen. Het verschil zit hem in de symbolen die de variabelen en meeteenheden vertegenwoordigen.

De formules zien er als volgt uit:

ISO EN: $S = K \times T + C$

US CAN: $Ds = K \times (Ts + Tc + Tr + Tbm) + Dpf$

Waarbij: Ds en S de minimale veiligheidsafstand van de gevarenzone tot het dichtstbijzijnde detectiepunt vertegenwoordigen

Naderingsrichtingen

Bij het berekenen van de veiligheidsafstand bij gebruik van lichtschermen of een gebiedsscanner, moet rekening worden gehouden met de naderingshoek tot de detectievoorziening. Er zijn drie typen naderingen mogelijk:

Normaal – nadering loodrecht op het detectievlak

Horizontaal – nadering parallel aan het detectievlak

Onder een hoek – nadering van de detectiezone onder een hoek.

Snelheidsconstante

K is een snelheidsconstante. De waarde van de snelheidsconstante is afhankelijk van de bewegingen van de operator (zoals de snelheid van diens handen, loopsnelheid en staplengte). Deze parameter is gebaseerd op onderzoeksgegevens die aantonen

dat het redelijk is om uit te gaan van een handsnelheid van de operator van 1.600 mm/sec indien zijn of haar lichaam stationair blijft. Er dient rekening te worden gehouden met de omstandigheden van de desbetreffende toepassing. Als algemeen uitgangspunt zal de naderingssnelheid variëren van 1.600 mm/s tot 2.500 mm/sec. De juiste snelheidsconstante dient door de risicoanalyse te worden vastgesteld.

Stoptijd

T is de algehele stoptijd van het systeem. De totale tijd in seconden loopt van de initiatie van het stopsignaal tot het verdwijnen van het gevaar. Deze tijd kan worden onderverdeeld in deelstappen (Ts, Tc, Tr en Tbm) om de analyse te vereenvoudigen. Ts is de slechtst mogelijke stoptijd van de machine/apparatuur. Tc is de slechtste mogelijke stoptijd van het besturingssysteem. Tr is de reactietijd van de veiligheidsvoorziening, met inbegrip van de interface. Tbm is een aanvullende stoptijd die door de rembewaking wordt toegestaan voordat deze een verslechtering van de stoptijd detecteert die buiten de door de eindgebruiker ingestelde grenzen ligt. Tbm wordt gebruikt voor mechanische drukpersen met draaiende onderdelen. De waarden van Ts + Tc + Tr worden meestal gemeten met behulp van een meetapparaat voor de stoptijd.

Dieptepenetratiefactoren

De dieptepenetratiefactoren worden weergegeven door de symbolen C en Dpf. Deze omvatten de maximale afstand die naar het gevaar moet worden afgelegd voordat het veiligheidsapparaat tot detectie overgaat. De dieptepenetratiefactoren zullen al naar gelang het type apparaat en toepassing verschillen. Controleer de relevante norm om vast te stellen wat de beste dieptepenetratiefactor is. Voor een normale nadering tot een lichtscherm of gebiedsscanner waarvan de objectgevoeligheid minder dan 64 mm is, gaan de ANSI-normen en Canadese normen uit van:

Dpf = 3,4 x (objectgevoeligheid – 6,875 mm), maar niet minder dan nul.

Voor een normale nadering tot een lichtscherm of gebiedsscanner waarvan de objectgevoeligheid minder dan 40 mm is, gaan de ISO-normen en EN-normen uit van:

C = 8 x (objectgevoeligheid – 14 mm), maar niet minder dan nul.

Deze twee formules kennen een overlappingspunt op 19,3 mm. Voor een objectgevoeligheid die minder dan 19 mm is, houdt de nadering volgens US CAN meer beperkingen in, omdat het lichtscherm of de gebiedsscanner verder van het gevaar dient te worden opgesteld. Voor objectgevoeligheden die meer dan 19,3 mm zijn, is de ISO EN-norm beperkender. Machinebouwers die een machine willen bouwen die overal ter wereld kan worden gebruikt, dienen voor beide berekeningen uit te gaan van de slechtst mogelijke omstandigheden.

Doorreiktoepassingen

Wanneer er grotere objectgevoeligheden worden gebruikt, is er een klein verschil tussen de US CAN- en ISO EN-normen wat betreft de dieptepenetratiefactor en de objectgevoeligheid. De ISO EN-waarde bedraagt 850 mm, terwijl de US CAN-waarde 900 mm bedraagt. De normen verschillen eveneens qua objectgevoeligheid.

Overreiktoepassingen

Beide normen zijn het erover eens dat de minimale hoogte van de laagste straal 300 mm moet zijn, maar wijken af als het gaat om de minimale hoogte van de hoogste straal. De ISO EN-norm schrijft 900 mm voor, terwijl de US CAN-norm 1.200 mm vereist. De waarde voor de hoogste straal lijkt discutabel. In het geval van een doorreiktoepassing moet de hoogte van de hoogste straal veel hoger zijn om ruimte te bieden voor een operator in een staande positie. Als de operator over het detectievlak kan reiken, zijn de overreikcriteria van toepassing.

Enkele of meerdere stralen

Het gebruik van enkele of meerdere stralen wordt verder door de ISO EN-normen gedefinieerd. De onderstaande afbeeldingen tonen de “praktische” hoogten van meerdere stralen boven de vloer. De dieptepenetratiefactor is in de meeste gevallen 850 mm en 1.200 mm bij het gebruik van een enkele straal. De US CAN-norm houdt hiermee rekening in de doorreikeisen. Er dient altijd rekening te worden gehouden met de mogelijkheid dat de gebruiker zich over, onder en rond de enkele of meerdere stralen begeeft.

Aantal stralen	Hoogte boven de vloer – mm (inch)	C – mm (inch)
1	750 (29.5)	1200 (47.2)
2	400 (5.7), 900 (35.4)	850 (33.4)
3	300 (11.8), 700 (27.5), 1100 (43.3)	850 (33.4)
4	300 (11.8), 600 (23.6), 900 (35.4), 1200 (47.2)	850 (33.4)

Afstandsberekeningen

Voor de normale aanpak op het gebied van lichtschermen liggen de berekeningen van de veiligheidsafstand van de ISO EN- en US CAN-normen dicht bij elkaar. Er zijn echter verschillen. Voor de normale nadering tot verticale lichtschermen bij een objectgevoeligheid van maximaal 40 mm moeten volgens de ISO EN-aanpak twee stappen worden uitgevoerd. Ten eerste moet S worden berekend, uitgaande van een snelheidsconstante van 2.000.

$S = 2.000 \times T + 8 \times (d - 1\ 4)$

De minimale afstand voor S is 100 mm.

Wanneer de afstand meer dan 500 mm bedraagt, kan een tweede stap worden gebruikt. Vervolgens kan de waarde K worden verlaagd tot 1.600. Bij een K van 1.600 bedraagt de minimumwaarde voor S 500 mm.

De US CAN-nadering maakt gebruik van een nadering die uit één stap bestaat:
Ds = 1.600 x T * Dpf

Als de responstijd minder dan 560 ms bedraagt, resulteert dit in een verschil tussen de normen van meer dan 5%.

Naderingen onder een hoek

De meeste toepassingen van lichtschermen en scanners worden verticaal (normale nadering) of horizontaal (parallelle nadering) gemonteerd. Dergelijke configuraties worden niet als nadering onder een hoek beschouwd als de voorzieningen zich binnen ±5° van het bedoelde ontwerp bevinden. Wanneer de hoek groter is dan ±5°, dient men rekening te houden met de potentiële gevaren (bijv. de kortste afstand) van voorspelbare naderingen. Wanneer de hoek met het referentievlak (bijv. de vloer) groter is dan 30°, dient deze als normaal te worden beschouwd. Een hoek van minder dan 30 dient als parallel te worden beschouwd.

Veiligheidsmatten

Bij veiligheidsmatten dient er voor de veiligheidsafstand rekening te worden gehouden met de snelheid en staplengte van de operator. Hierbij wordt er vanuit gegaan dat de operator loopt en dat de veiligheidsmatten op de vloer zijn aangebracht. De eerste stap van de operator op de mat vertegenwoordigt een dieptepenetratiefactor van 1.200 mm of 48 inch. Als de operator op een platform moet stappen, kan de dieptepenetratiefactor worden verminderd met 40% van de hoogte van de stap. Het is belangrijk om de mat(ten) goed vast te maken zodat elke beweging wordt voorkomen.

Voorbeeld

Voorbeeld: Een operator volgt een normale nadering van een lichtscherm van 14 mm, dat via een veiligheidsrelais is verbonden met een magneetschakelaar die op gelijkstroom werkt en is uitgerust met een diodeblokje. De reactietijd van het veiligheidssysteem (Tr) bedraagt 20 + 15 + 95 = 130 ms. De stoptijd van de machine, Ts+Tc, bedraagt 170 ms. Er wordt geen gebruik gemaakt van rembewaking. De Dpf-waarde bedraagt 1 inch; de C-waarde bedraagt nul. De berekening zou er als volgt uitzien:

Dpf = 3,4 (14 – 6,875) = 1 in (24,2 mm)

Ds = K x (Ts + Tc + Tr + Tbm) + Dpf
Ds = 63 x (0,17 + 0,13 + 0) + 1
Ds = 63 x (0,3) + 1
Ds = 18,9 + 1
Ds = 19,9 inch (505 mm)

C = 8 (14-14) = 0

S = K x T + C
S = 1600 x (0,3) + 0
S = 480 mm (18,9 inch)

Om deze reden dient de minimale veiligheidsafstand tussen het veiligheidslichtscherm en het gevaar 20 inch of 508 mm te bedragen om de machine overal ter wereld te mogen gebruiken.

Hoofdstuk 6: Veiligheidsgerelateerde besturingssystemen

Inleiding

Wat is een veiligheidsgerelateerd besturingssysteem (vaak afgekort tot SRCS)? Het is een onderdeel van het besturingssysteem van een machine dat voorkomt dat een gevaarlijke situatie optreedt. Het kan gaan om een afzonderlijk, speciaal systeem of een systeem dat is geïntegreerd in het normale besturingssysteem van de machine.

De complexiteit van het systeem kan variëren van een eenvoudig systeem, zoals een vergrendelingsschakelaar voor een afscherming en een noodstopschakelaar die in serie is geschakeld met de bedieningsspoel van een stroommagneetschakelaar, tot een samengesteld systeem dat zowel eenvoudige als complexe apparaten omvat, die softwarematig en hardwarematig met elkaar communiceren.

Veiligheidsgerelateerde besturingssystemen zijn ontworpen om veiligheidsfuncties uit te voeren. Het veiligheidsgerelateerde besturingssysteem moet onder alle voorspelbare omstandigheden op de juiste wijze blijven werken. Wat is nu precies een veiligheidsfunctie, en hoe kunnen we een systeem ontwerpen om deze functie te bieden? En wanneer we dit gedaan hebben, hoe kunnen we dit aantonen?

Veiligheidsfunctie

Een veiligheidsfunctie wordt geïmplementeerd door de veiligheidsgerelateerde onderdelen van het machinebesturingssysteem, die de veiligheid van de apparatuur met betrekking tot een bepaald gevaar of een aantal gevaren garanderen. Een storing van de veiligheidsfunctie kan resulteren in een directe toename van de risico's die gepaard gaan met het gebruik van de apparatuur, oftewel een gevaarlijke toestand.

Van een "gevaarlijke toestand" is sprake wanneer een persoon aan een gevaar kan worden blootgesteld. Een gevaarlijke toestand houdt niet in dat de persoon letsel oploopt. De persoon die aan het gevaar wordt blootgesteld is mogelijk in staat om het gevaar te onderkennen en letsel te voorkomen. De persoon die aan het gevaar wordt blootgesteld is mogelijk niet in staat om het gevaar te herkennen, of het gevaar kan door een onverwacht inschakelen van de machine worden veroorzaakt. De belangrijkste taak van de ontwerper van het veiligheidssysteem is om gevaarlijke toestanden en het onverwacht inschakelen van de machine te voorkomen.

De veiligheidsfunctie kan vaak worden beschreven op basis van eisen met meerdere onderdelen. Zo bestaat de veiligheidsfunctie die door een vergrendelingsveiligheid wordt geïnitieerd uit drie onderdelen:

1. de gevaren waartegen de afscherming bescherming biedt kunnen pas worden geactiveerd wanneer de afscherming wordt gesloten;

2. het openen van de afscherming zal ertoe leiden dat het gevaar wordt opgeheven indien dit ten tijde van het openen van de afscherming actief was; en

3. het sluiten van de afscherming leidt niet tot het herstarten van het gevaar waartegen de afscherming bescherming biedt.

Wanneer een veiligheidsfunctie voor een specifieke toepassing wordt gespecificeerd, dient het woord “gevaar” te worden vervangen door het specifieke gevaar. De bron van het gevaar mag niet worden verward met de resultaten van het gevaar. Verbrijzeling, snijwonden en brandwonden zijn mogelijke resultaten van een gevaar. Een voorbeeld van een gevarenbron is een motor, plunjer, mes, lasbrander, pomp, laser, robot, eindeffector, solenoïde, klep, een ander type actuator of een mechanisch gevaar waarbij de zwaartekracht een rol speelt.

Voor de bespreking van veiligheidssystemen wordt de zin “wanneer of voor een beroep op de veiligheidsfunctie wordt gedaan” gebruikt. Wat wordt nu precies bedoeld met beroep op de veiligheidsfunctie? Voorbeelden van beroepen die op de veiligheidsfunctie worden gedaan zijn het openen van een vergrendelde afscherming, het doorbreken van een lichtscherm, het stappen op een veiligheidsmat of het indrukken van een noodstop. Een operator wil dat het gevaar wordt stopgezet of dat het niet langer van stroom wordt voorzien indien het gevaar reeds is gestopt.

De veiligheidsgerelateerde onderdelen van het machinebesturingssysteem dragen zorg voor de veiligheidsfunctie. De veiligheidsfunctie wordt niet slechts door één apparaat uitgevoerd, bijvoorbeeld alleen door de afscherming. De vergrendeling op de afscherming verzendt een opdracht naar een logisch apparaat dat op zijn beurt een actuator deactiveert. De veiligheidsfunctie begint met de opdracht en eindigt met de uitvoering van deze opdracht.

Het ontwerp van het veiligheidssysteem moet een integriteitsniveau bieden dat in verhouding tot het machinerisico’s staat. Voor grotere risico’s zijn hogere integriteitsniveaus vereist om de werking van de veiligheidsfunctie te garanderen. Machineveiligheidssystemen kunnen worden ingedeeld in niveaus die aangeven hoe goed ze in staat zijn de prestaties van hun veiligheidsfunctie of, met andere woorden, het functionele veiligheidsintegriteitsniveau te waarborgen.

Functionele veiligheid van besturingssystemen

Wat is functionele veiligheid?

Functionele veiligheid is het deel van de algehele veiligheidsvereisten dat afhankelijk is van het juist functioneren van het proces of de apparatuur als reactie op de erdoor ontvangen invoer. IEC TR 61508-0 biedt het volgende voorbeeld om de betekenis van functionele veiligheid te verhelderen. “Een voorbeeld van functionele veiligheid is een oververhittingsbeveiliging die gebruikmaakt van een thermische sensor in de wikkelingen van een elektromotor om de voeding van de motor te onderbreken voordat deze oververhit kan raken. Het bieden van een speciale stroomonderbrekingsvoorziening om tegen hoge temperaturen bestand te zijn is echter geen vorm van functionele veiligheid (hoewel het nog steeds een vorm van veiligheid is en bescherming tegen exact hetzelfde gevaar kan bieden).”

Nog een voorbeeld: laten we een vaste afscherming vergelijken met een vergrendelde afscherming. De vaste afscherming wordt niet beschouwd als vorm van “functionele veiligheid”, hoewel de afscherming bescherming kan bieden tegen hetzelfde gevaar als een vergrendelde afscherming. De vergrendelde afscherming is een vorm van functionele veiligheid. Wanneer de afscherming wordt geopend, dient de vergrendeling als “invoer” naar een systeem dat een veilige toestand teweeg brengt. Op vergelijkbare wijze worden persoonlijke beschermingsmiddelen gebruikt als beschermende maatregel om de veiligheid van het personeel te verbeteren. Persoonlijke beschermingsmiddelen vallen niet onder functionele veiligheid.

Veiligheidsgerelateerde machinebesturingssystemen

Functionele veiligheid is een term die werd geïntroduceerd in IEC 61508:1998. Sindsdien wordt de term soms alleen in verband gebracht met programmeerbare veiligheidssystemen. Dit is echter een misvatting. De functionele veiligheid omvat een brede reeks apparaten die worden gebruikt om veiligheidssystemen te ontwikkelen. Voorzieningen als vergrendelingen, lichtschermen, veiligheidsrelais, veiligheids-PLC's, veiligheidsmagneetschakelaars en veiligheidsaandrijvingen worden geschakeld tot een veiligheidssysteem dat een specifieke veiligheidsgerelateerde functie verzorgt. Dit wordt functionele veiligheid genoemd.

Om deze reden is de functionele veiligheid van een elektrisch besturingssysteem van uiterst groot belang voor de detectie van gevaren die worden veroorzaakt door bewegende onderdelen van machines.

Er zijn twee typen eisen nodig om functionele veiligheid te bewerkstelligen:

- de veiligheidsfunctie en
- de veiligheidsintegriteit.

Risicoanalyse speelt een belangrijke rol tijdens de ontwikkeling van eisen voor functionele veiligheid. Taak- en gevarenanalyse leidt tot de functionele vereisten voor veiligheid (d.w.z. de veiligheidsfunctie). Het kwantificeren van de risico's levert de veiligheidsintegriteitseisen (d.w.z. de veiligheidsintegriteit of het Performance Level) op.

Vier van de belangrijkste normen op het gebied van functionele veiligheid voor besturingssystemen zijn:

1. IEC/EN 61508 "Functionele veiligheid van veiligheidsgerelateerde elektrische, elektronische en programmeerbare elektronische besturingssystemen"

   De norm beschrijft de eisen en bepalingen die van toepassing zijn op het ontwerp van complexe elektronische en programmeerbare systemen en subsystemen. De norm is generiek van aard en beperkt zich dientengevolge niet tot de machinebouwsector.

2. IEC/EN 62061 "Machineveiligheid – Functionele veiligheid van veiligheidsgerelateerde elektrische, elektronische en programmeerbare elektronische besturingssystemen"

   Deze norm omvat een machinespecifieke toepassing van IEC/EN 61508. De norm beschrijft de eisen die van toepassing zijn op het ontwerp op systeemniveau van alle typen veiligheidsgerelateerde elektrische besturingssystemen en op het ontwerp van niet-complexe subsystemen of apparaten. Een vereiste is dat complexe en programmeerbare subsystemen voldoen aan de richtlijnen van de norm IEC/EN 61508

3. (EN) ISO 13849-1 “Machineveiligheid – Veiligheidsgerelateerde onderdelen van besturingssystemen”

   Deze norm heeft ten doel om een direct overgangstraject vanuit de categorieën van de vorige EN 954-1 te bieden.

4. IEC 61511 “Functionele veiligheid – Veiligheidsinstrumentensystemen voor de procesindustrie”

   Deze norm is de op de procesindustrie gerichte implementatie van IEC/EN 61508

De functionele veiligheidsnormen houden een belangrijke verandering in ten opzichte van de bestaande eisen, zoals Control Reliable en het categorieënsysteem van de voorgaande ISO 13849-1:1999 (EN 954-1:1996).

Categorieën zijn niet volledig verdwenen; ze worden nog steeds gebruikt in de huidige (EN) ISO 13849-1.

IEC/EN 62061 en (EN) ISO 13849-1

IEC/EN 62061 en (EN) ISO 13849-1 zijn beide van toepassing op veiligheidsgerelateerde elektrische besturingssystemen. Deze normen zouden uiteindelijk kunnen worden gecombineerd tot één norm waarin een en dezelfde terminologie wordt gebruikt. Beide normen leveren dezelfde resultaten op, maar maken gebruik van verschillende methoden. Ze hebben ten doel om gebruikers de mogelijkheid te bieden om de meest geschikte methode voor hun situatie te kiezen. Gebruikers kunnen ervoor kiezen om een van beide normen te gebruiken. Beide normen zijn geharmoniseerd onder de Europese Machinerichtlijn.
Beide normen bieden vergelijkbare niveaus van veiligheid en integriteit. De methodieken van de twee normen worden gekenmerkt door onderlinge verschillen die op de beoogde gebruikers zijn afgestemd.
De methodiek in IEC/EN 62061 heeft ten doel om ruimte te bieden voor complexe veiligheidsfunctionaliteit die geïmplementeerd kan worden door systeemarchitecturen die voorheen als onconventioneel werden beschouwd. De methodiek van (EN) ISO 13849-1 is bedoeld om een directer en minder gecompliceerd traject te bieden voor meer conventionele veiligheidsfunctionaliteit die door conventionele systeemarchitecturen wordt geïmplementeerd.

Een belangrijk onderscheid tussen deze twee normen is de toepasbaarheid van verschillende technologieën. IEC/EN 62061 is geschikter voor elektrische systemen. (EN) ISO 13849-1 kan worden toegepast op pneumatische, hydraulische, mechanische en elektrische systemen.

Gezamenlijke technisch rapport inzake IEC/EN 62061 en (EN) ISO 13849-1

IEC en ISO hebben een gezamenlijk rapport opgesteld voor gebruikers van beide normen.

In dit rapport wordt de relatie tussen beide normen beschreven en wordt uitgelegd hoe er zowel op systeem- als op subsysteemniveau een parallel getrokken kan worden tussen PL (Performance Level ofwel prestatieniveau) van (EN) ISO 13849-1 en SIL (Safety Integrity Level ofwel veiligheidsintegriteitsniveau) van IEC/EN 62061.

Om aan te tonen dat beide normen gelijkwaardige resultaten opleveren, wordt er in het rapport een voorbeeld van een veiligheidssysteem gegeven dat volgens de methodologieën van beide normen is berekend. Daarnaast wordt in het rapport een aantal zaken verduidelijkt die op verschillende manieren zijn geïnterpreteerd. Een van de belangrijkste thema's is misschien wel het aspect van foutuitsluiting.

Over het algemeen geldt dat als er voor een veiligheidsfunctie PLe moet worden geïmplementeerd door een veiligheidsgerelateerd besturingssysteem, er doorgaans niet alleen vertrouwd kan worden op foutuitsluitingen om dit Performance Level te realiseren. Dit is afhankelijk van de gebruikte technologie en de bedoelde werkomgeving. Het is daarom van essentieel belang dat de ontwerper extra aandacht besteedt aan het gebruik van foutuitsluitingen in het geval er een hoger PL wordt vereist.

Over het algemeen wordt het gebruik van foutuitsluitingen niet toegepast op de mechanische aspecten van elektromechanische positieschakelaars om te kunnen voldoen aan PLe bij het ontwerpen van een veiligheidsgerelateerd besturingssysteem. De foutuitsluitingen die toegepast kunnen worden op specifieke mechanische storingscondities (bijv. slijtage/corrosie, breuken) worden omschreven in tabel A.4 van ISO 13849-2.

Een deurvergrendelingssysteem bijvoorbeeld dat dient te voldoen aan PLe, moet een minimale fouttolerantie van 1 (d.w.z. twee conventionele mechanische positieschakelaars) hebben om dit prestatieniveau te halen. Normaal gesproken is het namelijk niet te rechtvaardigen om fouten zoals gebroken schakelactuatoren uit te sluiten. Het kan echter acceptabel zijn storingen uit te sluiten zoals kortsluiting in de bedrading van een bedieningspaneel dat ontworpen is in overeenstemming met de toepasselijke normen.

SIL en IEC/EN 62061

IEC/EN 62061 beschrijft zowel de mate waarin het risico moet worden gereduceerd als het vermogen van een besturingssysteem om dat risico in termen van SIL (Safety Integrity Level) te reduceren. Binnen de machinebouwsector worden er drie SIL's gehanteerd, waarvan SIL 1 het laagste en SIL 3 het hoogste niveau is.

Omdat de term "SIL" op dezelfde wijze wordt toegepast in andere bedrijfstakken, zoals de petrochemie, de energiesector en de spoorwegsector, is IEC/EN 62061 erg handig als machines in deze sectoren worden gebruikt. Risico's van grotere omvang kunnen zich voordoen in andere sectoren, zoals de procesindustrie. Om

deze reden is SIL 4 opgenomen in de norm IEC 61508 en de norm IEC 615114 die specifiek van toepassing is op de procesindustrie.

Een SIL is van toepassing op een veiligheidsfunctie. De subsystemen waaruit het systeem dat de veiligheidsfunctie verzorgt is opgebouwd, moeten aan de eisen voor de juiste SIL voldoen. Dit wordt soms wel de SIL Claim Limit (SIL CL) genoemd. Een volledige en gedetailleerde evaluatie van IEC/EN 62061 is vereist voordat deze norm op de juiste wijze kan worden toegepast.

PL en (EN) ISO 13849-1

(EN) ISO 13849-1 maakt geen gebruik van de term SIL. In plaats daarvan wordt gebruik gemaakt van de term PL (Performance Level ofwel prestatieniveau). PL kan in veel opzichten worden vergeleken met SIL. Er zijn vijf Performance Level, waarvan PLa het laagste en PLe het hoogste niveau is.

Vergelijking van PL en SIL

Deze tabel toont in grote lijnen de relatie tussen PL en SIL indien toegepast op typische circuitstructuren.

PL (Prestatieniveau)	PFH_D (Waarschijnlijkheid van een gevaarlijke storing per uur)	SIL (Veiligheidsintegriteits-niveau)
a	$\geq 10^{-5}$ tot $<10^{-4}$	Geen
b	$\geq 3 \times 10^{-6}$ tot $<10^{-5}$	1
c	$\geq 10^{-6}$ tot $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ tot $<10^{-6}$	2
e	$\geq 10^{-8}$ tot $<10^{-7}$	3

Overeenkomsten tussen PL en SIL (bij benadering)

BELANGRIJK: De bovenstaande tabel dient louter ter algemene informatie en mag NIET voor conversiedoeleinden worden gebruikt. U dient rekening te houden met de volledige eisen van de normen. De tabellen in Bijlage K bieden meer gedetailleerde informatie.

Hoofdstuk 7: Systeemontwerp volgens (EN) ISO 13849

Een volledige en gedetailleerde evaluatie van (EN) ISO 13849-1 is vereist voordat deze norm op de juiste wijze kan worden toegepast. Hier volgt een korte samenvatting:

Deze norm beschrijft eisen met betrekking tot het ontwerp en de integratie van veiligheidsgerelateerde onderdelen van besturingssystemen, met inbegrip van een aantal softwarematige aspecten. De norm is van toepassing op veiligheidsgerelateerde systemen, maar kan tevens worden toegepast op systeemonderdelen.

SISTEMA-berekeningstool voor het Performance Level

SISTEMA is een softwaretool voor de implementatie van (EN) ISO 13849-1. Het gebruik van SISTEMA zal de kwantificerings- en berekeningsaspecten van de implementatie van de norm enorm vereenvoudigen.

SISTEMA staat voor “Safety Integrity Software Tool for the Evaluation of Machine Applications” ofwel veiligheidsintegratiesoftwaretool voor de evaluatie van machinetoepassingen en wordt voortdurend herzien en geactualiseerd door IFA. Zoals verderop in dit gedeelte wordt beschreven, moeten er verschillende typen gegevens met betrekking tot functionele veiligheid worden ingevoerd. De gegevens kunnen handmatig of automatisch worden ingevoerd met behulp van de SISTEMA-gegevensbibliotheek van de fabrikant.

De SISTEMA-gegevensbibliotheek van Rockwell Automation kan gedownload worden via (hier vindt u tevens een link naar de SISTEMA-downloadsite): *www.rockwellautomation.com, onder Solutions & Services > Safety Solutions.*

Overzicht van (EN) ISO 13849-1

Het volgende algemene overzicht is bedoeld om een overzicht te geven van de basisbepalingen van (EN) ISO 13849-1. Daarnaast wordt nog melding gemaakt van de revisie die begin 2016 is gepubliceerd. Het is essentieel dat de norm zelf tot in de details wordt bestudeerd.
Deze norm kent een breed toepassingsgebied, omdat deze van toepassing is op alle technologieën, met inbegrip van elektrische, hydraulische, pneumatische en mechanische technologie. Hoewel ISO 13849-1 toepasbaar is op complexe systemen, wordt de lezer voor complexe, met software ingebedde onderdelen verwezen naar IEC 61508.

De uitvoer van ISO 13849-1 bestaat uit prestatieniveaus [PL a, b, c, d of e]. Het oorspronkelijke concept van categorieën is gebleven, maar er moet aan aanvullende eisen voldaan worden voordat een prestatieniveau (PL) aan een systeem kan worden toegekend.

Deze eisen kunnen in hoofdlijnen als volgt worden geformuleerd:

- De architectuur van het systeem. In essentie betreft dit de al bekende categorieën;
- Voor de samenstellende onderdelen van het systeem zijn betrouwbaarheidsgegevens vereist;

- De Diagnostic Coverage (DC) van het systeem is vereist. Dit vertegenwoordigt de effectiviteit van de foutbewaking in het systeem
- Bescherming tegen gemeenschappelijk falen
- Bescherming tegen systematische storingen
- Indien van toepassing specifieke software-eisen

Voordat verderop dieper op deze factoren wordt ingegaan, is het zinvol de bedoeling en het principe van de norm als zodanig te behandelen. In dit stadium is duidelijk dat de norm wijzigingen heeft ondergaan, maar de details krijgen pas echt betekenis als we begrijpen wat de norm wil bereiken en waarom.

De eerste vraag luidt dan ook waarom de norm eigenlijk nodig is. Het spreekt voor zich dat de technologie die in machineveiligheidssystemen wordt toegepast, de afgelopen tien jaar grote ontwikkelingen en veranderingen heeft doorgemaakt. Tot vrij recentelijk waren veiligheidssystemen afhankelijk van “eenvoudige” apparatuur met uiterst voorspelbare storingsmodi. Nu worden er in veiligheidssystemen echter in toenemende mate complexere elektronische en programmeerbare elektronische apparaten gebruikt. Dit heeft geleid tot voordelen op het gebied van kosten, flexibiliteit en compatibiliteit, maar het betekent bovendien dat de al bestaande normen niet meer voldoen. Om te weten of een veiligheidssysteem goed genoeg is, moeten we er meer over weten. Daarom vragen de functionele veiligheidsnormen om meer informatie. Omdat veiligheidssystemen gebruik maken van een meer “zwarte doos”-achtige benadering door vooraf gekwalificeerde subsystemen te integreren, verlaten we ons in sterkere mate op hun overeenstemming met normen. Daarom moet met deze normen de technologie adequaat kunnen worden beoordeeld. Hiertoe moeten de normen ingaan op de kernfactoren van betrouwbaarheid, foutdetectie, architectuur- en systeemintegriteit. Dit is de bedoeling van (EN) ISO 13849-1.

Voor een logische behandeling van de norm moeten twee fundamenteel verschillende gebruikerstypen worden onderscheiden: de ontwerper van veiligheidsgerelateerde subsystemen en de ontwerper van veiligheidsgerelateerde systemen. Over het algemeen is de subsysteemontwerper (doorgaans een fabrikant van veiligheidscomponenten) onderworpen aan een hogere mate van striktheid. Hij moet de vereiste gegevens leveren zodat de systeemontwerper kan waarborgen dat de integriteit van het subsysteem overeenstemt met die van het systeem. Hiertoe zijn meestal testen, analyses en berekeningen vereist. De resultaten hiervan worden vastgelegd in de gegevens die door de norm worden voorgeschreven.

De systeemontwerper (doorgaans een machineontwerper of integrator) gebruikt de subsysteemgegevens om relatief eenvoudige berekeningen uit te voeren als deel van de bepaling van het algehele prestatieniveau (PL) van het systeem.

Bepaling van de veiligheidsfunctie

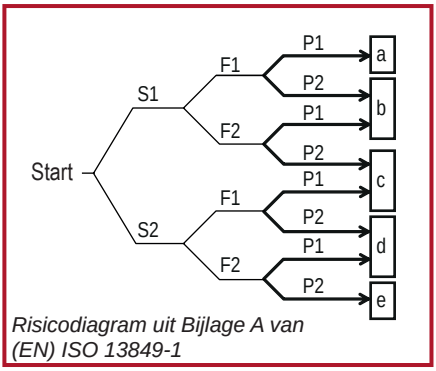
We moeten vaststellen wat de veiligheidsfunctie is. De veiligheidsfunctie moet uiteraard geschikt zijn voor de vereist taak. Hoe kan de norm ons hierbij helpen? We moeten ons realiseren dat de vereiste functionaliteit alleen vastgesteld kan worden door de typische kenmerken van het desbetreffende systeem in ogenschouw te nemen. Dit kan beschouwd worden als het stadium waarin het veiligheidsconcept wordt opgesteld. Het kan niet volledig worden afgedekt door de norm, omdat deze niet alle kenmerken van een specifieke toepassing kent. Vaak geldt dit ook voor de machinebouwer die de machine produceert, maar niet noodzakelijkerwijs de precieze condities kent waaronder deze wordt gebruikt.

De norm biedt hierbij enige hulp door een groot aantal veelgebruikte veiligheidsfuncties op te sommen (bijv. een veiligheidsgerelateerde stopfunctie die geactiveerd wordt door een veiligheidsvoorziening, onderdrukkingsfunctie, start-/herstartfunctie) en door te voorzien in een aantal eisen die hier doorgaans mee in verband staan. Een studie van (EN) ISO 12100: ‘Basic design principles and Risk assessment’ (Basale ontwerpprincipes en risicobeoordeling)wordt aanbevolen voor gebruik in deze fase. ISO TR 22100-2 voorziet in nuttige richtlijnen inzake de relatie tussen het machinerisicobeoordelingsproces van ISO 12100 en het PL-toewijzingsproces van (EN) ISO 13849-1. Daarnaast is er een grote diversiteit aan machinespecifieke normen die voorzien in veiligheidsfunctievereisten voor specifieke machines. Door de Europese EN-normen worden ze aangeduid als type C-normen. Sommige van deze normen hebben een exact ISO-equivalent. ISO TR 22100-1 biedt nadere informatie over de relatie tussen ISO 12100 en C-normen.

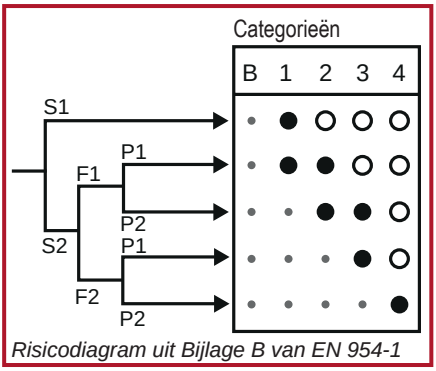
Het is duidelijk dat het stadium waarin het veiligheidsconcept wordt opgesteld, afhankelijk is van het type machine én van de kenmerken van de toepassing en omgeving waarin ze wordt gebruikt. De machinebouwer moet met deze factoren rekening houden zodat hij een geschikt veiligheidsconcept kan opstellen. De bedoelde (voorziene) gebruiksomstandigheden moeten in de gebruikershandleiding vermeld worden. De gebruiker van de machine moet controleren of deze overeenkomen met de feitelijke gebruiksomstandigheden.

De PLr wordt gebruikt om aan te geven welk prestatieniveau vereist wordt door de veiligheidsfunctie en dit wordt bepaald tijdens de risicobeoordeling. Om de PLr vast te stellen, bevat de norm een risicodiagram waarin de toepassingsfactoren “ernst van het letsel”, “regelmaat van blootstelling” en “mogelijkheid van voorkomen” ingevoerd worden.

De uitkomst is de PLr. Gebruikers van de oude norm EN 954-1 kennen deze benadering, maar binnen (EN) ISO 13849-1 is lijn S1 nu ook opgesplitst. Dit was in het oude risicodiagram niet het geval. De 2015-versie biedt de mogelijkheid om het PLr in bepaalde omstandigheden één niveau te verlagen, afhankelijk van de voorspelbare waarschijnlijkheid van optreden.



Risicodiagram uit Bijlage A van (EN) ISO 13849-1



Risicodiagram uit Bijlage B van EN 954-1

Dus nu hebben we een beschrijving van de veiligheidsfunctionaliteit en het vereiste prestatieniveau [PLr] voor de veiligheidsgerelateerde onderdelen van het besturingssysteem [SRP/CS] dat wordt toegepast om deze functionaliteit te implementeren. Nu moeten we het systeem ontwerpen en ervoor zorgen dat het aan PLr voldoet.

Een van de factoren die een belangrijke rol speelt in de beslissing over welke norm wordt gebruikt [(EN) ISO 13849-1 of EN/IEC 62061], is de complexiteit van de veiligheidsfunctie. Meestal is in het geval van machines de veiligheidsfunctie relatief eenvoudig en is (EN) ISO 13849-1 de geschiktste norm. Met behulp van betrouwbaarheidsgegevens, Diagnostic Coverage (DC), de systeemarchitectuur (categorie), gemeenschappelijk falen en, indien van toepassing, software-eisen wordt het Performance Level beoordeeld.

Deze vereenvoudigde omschrijving is alleen bedoeld om een overzicht te geven. Belangrijk is dat alle bepalingen uit de norm moeten worden toegepast. Er is echter hulp beschikbaar. Het SISTEMA-softwaretool kan helpen bij de documentatie en berekeningen. Bovendien genereert dit tool een technisch dossier.

SISTEMA is beschikbaar in een reeks talen, waaronder Duits en Engels. IFA, de ontwikkelaar van SISTEMA, is een gerespecteerd Duits onderzoeks- en testinstituut. Het houdt zich met name bezig met wetenschappelijke en technische veiligheidsproblemen op het gebied van de wettelijk voorgeschreven ongevallenverzekering en -preventie in Duitsland. Het werkt samen met arbo-instanties in meer dan twintig landen.

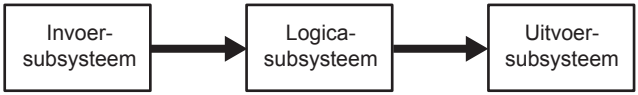
Deskundigen van de IFA en hun collega's van de bedrijfsverenigingen voor de wettelijke ongevallenverzekering hebben een belangrijke bijdrage geleverd aan de tekst van zowel (EN) ISO 13849-1 als IEC/EN 62061.

De "bibliotheek" met gegevens van Rockwell Automation-veiligheidscomponenten die gebruikt kunnen worden in SISTEMA, is beschikbaar op:
www.rockwellautomation.com, onder Solutions & Services > Safety Solutions.

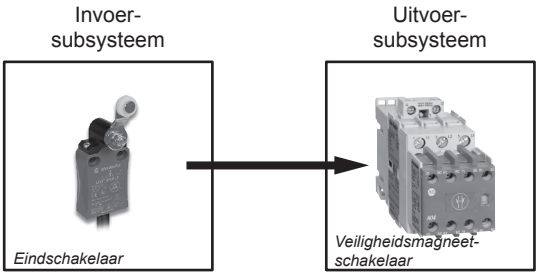
Met welke methode het prestatieniveau (PL) ook wordt berekend, belangrijk is dat de basis klopt. We moeten ons systeem op dezelfde wijze bekijken als de norm. Laten we dan ook hiermee beginnen.

Systeemstructuur

Elk systeem kan in basiscomponenten of “subsystemen” worden onderverdeeld. Elk subsysteem heeft zijn eigen afzonderlijke functie. De meeste systemen kunnen worden onderverdeeld in drie basisfuncties: invoer, logicaoplossing en activering (sommige eenvoudige systemen beschikken mogelijk niet over logicaoplossing).

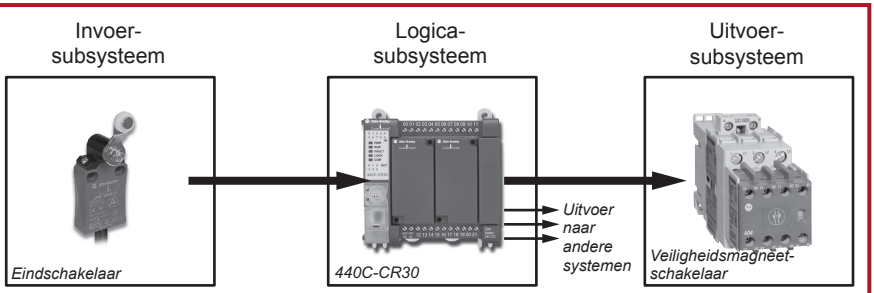


De componentgroepen die deze functies implementeren zijn de subsystemen.



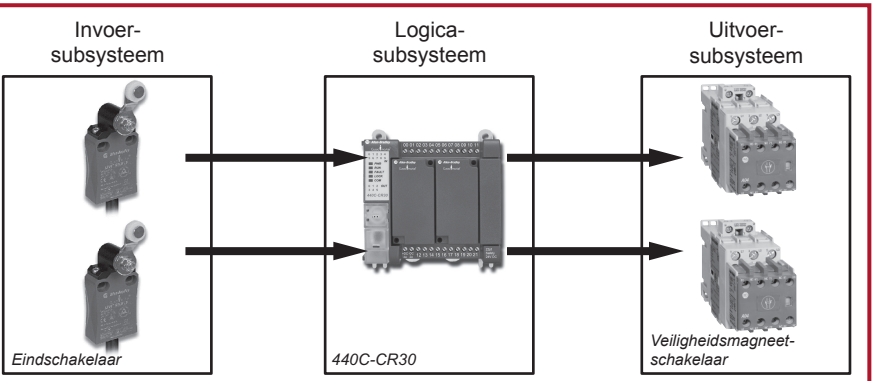
Vergrendelingsschakelaar en veiligheidsmagneetschakelaar

Hierboven wordt een voorbeeld gegeven van een eenvoudig enkelkanaals elektrisch systeem. Het omvat alleen invoer- en uitvoersubsystemen.



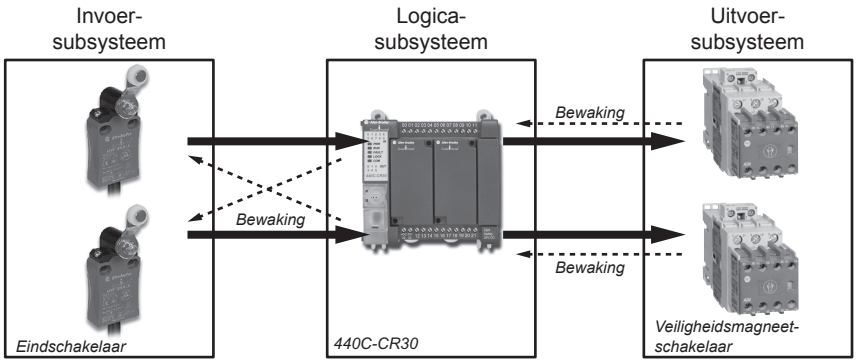
Vergrendelingsschakelaar, veiligheidscontroller en veiligheidsmagneetschakelaar

Het bovengenoemde systeem is iets complexer omdat er ook enige logica is vereist. De veiligheidscontroller zelf is intern fouttolerant (bijv. tweekanaals), maar toch is het complete systeem beperkt tot een enkelkanaals status vanwege de aanwezigheid van subsystemen met één eindschakelaar en één magneetschakelaar. Een enkelkanaals systeem zal uitvallen als een van de enkelkanaals subsystemen uitvalt; het is niet “fouttolerant”.



Tweekanaals veiligheidssysteem

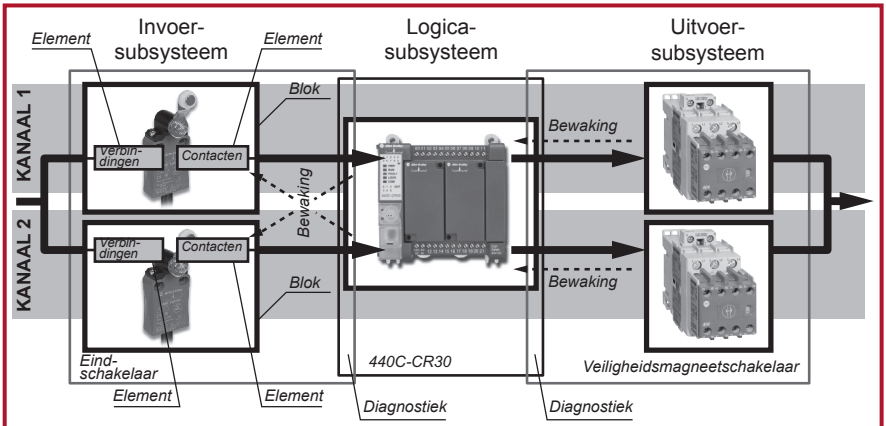
Een tweekanaals [ook wel redundant of “fouttolerant”] systeem wordt hierboven weergegeven. Elk subsysteem heeft twee kanalen en kan een enkele fout tolereren en nog steeds voorzien in de veiligheidsfunctie. Bij deze veiligheidsfunctie zijn er twee storingen nodig, een in elk kanaal, voordat het subsysteem en daarmee het systeem uitvalt. Het is duidelijk dat in het geval van een tweekanaals systeem de kans kleiner is dat een storing een gevaarlijke situatie oplevert dan in het geval van een enkelkanaals systeem. Maar we kunnen het nog betrouwbaarder maken (in termen van zijn veiligheidsfunctie) als we diagnostische maatregelen voor foutdetectie toepassen. Nadat de fout is gedetecteerd, moeten we hier natuurlijk op reageren en het systeem in een veilige toestand zetten. In het volgende schema wordt de toepassing van diagnostische maatregelen op basis van bewakingstechnieken weergegeven.



Diagnostiek met een tweekanaals veiligheidssysteem

Meestal (maar niet altijd) bestaan alle subsystemen van het systeem uit twee kanalen. We zien dus dat in dit geval elk subsysteem twee “subkanalen” heeft. De norm omschrijft deze als “blokken”. Een tweekanaals subsysteem heeft minimaal twee blokken en een enkelkanaals subsysteem heeft minimaal één blok. Het is mogelijk dat sommige systemen uit een combinatie van tweekanaals en enkelkanaals blokken bestaan.

Als we het systeem gedetailleerder willen onderzoeken, moeten we kijken naar de onderdelen van de blokken. Het SISTEMA-tool gebruikt voor deze onderdelen de term “elementen”.



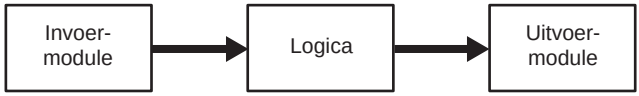
Onderverdeeld systeem met diagnostiek met een tweekanaals veiligheidssysteem

In het schema is het subsysteem van de eindschakelaars onderverdeeld tot elementniveau. Het subsysteem van de uitgangsmagneetschakelaar is onderverdeeld tot op blokniveau. Het logische subsysteem is niet onderverdeeld, omdat het door de fabrikant reeds is gekwalificeerd en gevalideerd tot een bepaald prestatieniveau. De bewakingsfunctie voor zowel de eindschakelaars als de magneetschakelaars wordt uitgevoerd door de logische controller. Daarom overlappen de kaders voor de subsystemen van de eind- en de magneetschakelaars enigszins met het logische subsysteem.

Dit principe van onderverdeling van systemen is terug te vinden in de methodologie van (EN) ISO 13849-1 en in het structuurprincipe van basissystemen in de SISTEMA-tool. Er dient echter opgemerkt te worden dat er wel enige subtiele verschillen zijn. De in de norm gebruikte methodologie is niet restrictief, maar de gebruikelijke eerste stap van de vereenvoudigde methode voor het inschatten van het prestatieniveau (PL) bestaat eruit het complete systeem op te delen in kanalen en de kanalen vervolgens in blokken. Met SISTEMA is het in de meeste gevallen handiger om het systeem in subsystemen te verdelen en vervolgens elk subsysteem in blokken te verdelen. De norm omschrijft niet expliciet het concept van subsystemen, maar de toepassing hiervan in SISTEMA vormt een begrijpelijkere en intuïtievere benadering. Dit heeft vanzelfsprekend geen gevolgen voor de eindberekening. SISTEMA en de norm gebruiken beide dezelfde principes en formules. Daarnaast is vermeldenswaardig dat de benadering van subsystemen ook wordt gebruikt in EN/IEC 62061.

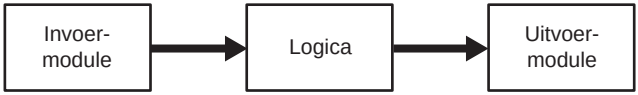
Het systeem dat wij als voorbeeld hebben gebruikt, is slechts een van de vijf basistypen van systeemarchitecturen dat in de norm wordt genoemd. Iedereen die bekend is met het systeem van categorieën, zal ons voorbeeld als representatief beschouwen voor categorie 3 of 4.

De norm maakt gebruik van de vijf oorspronkelijke categorieën van de voormalige norm EN 954. Deze worden Designated Architecture Categories (speciale architectuurcategorieën) genoemd. De eisen voor de categorieën zijn nagenoeg (maar niet helemaal) identiek aan die in EN 954-1. De speciale architectuurcategorieën worden weergegeven in de onderstaande schema's. Belangrijk is dat ze zowel toegepast kunnen worden op een compleet systeem als op een subsysteem. De schema's moeten niet per se opgevat worden als een fysieke structuur, maar ze zijn veeleer bedoeld als grafische weergave van conceptuele eisen.



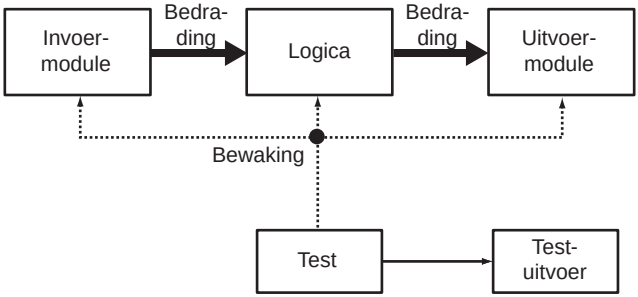
Speciale architectuurcategorie B

Speciale architectuurcategorie B moet gebruikmaken van basisprincipes op het gebied van veiligheid (zie bijlage van (EN) ISO 13849-2). Het systeem of subsysteem kan uitvallen als er één storing optreedt.
Zie (EN) ISO 13849-1 voor alle eisen.



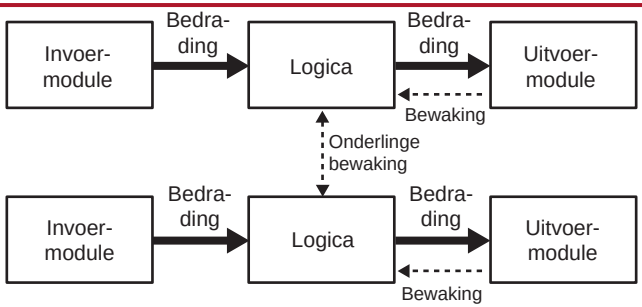
Speciale architectuurcategorie 1

Speciale architectuurcategorie 1 heeft dezelfde structuur als categorie B en kan ook in het geval van één storing uitvallen. Maar omdat categorie 1 ook gebruik moet maken van afdoende geteste veiligheidsprincipes [zie bijlage van (EN) ISO 13849-2], is dit minder waarschijnlijk dan voor categorie B. Zie (EN) ISO 13849-1 voor de volledige vereisten.



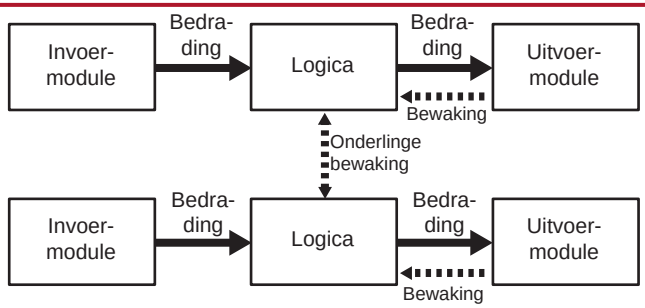
Speciale architectuurcategorie 2

Speciale architectuurcategorie 2 moet de basisprincipes op het gebied van veiligheid toepassen (zie bijlage van (EN) ISO 13849-2). Bovendien moet er diagnostische bewaking plaatsvinden door middel van een functionele test van het systeem of subsysteem. Dit moet gebeuren bij het opstarten en daarna periodiek. De frequentie moet gelijk zijn aan minstens 100 testen voor elke activering van de veiligheidsfunctie. De aanpassing van 2015 bevat een alternatief vereiste waarbij de veiligheidsfunctie naar de veilige toestand moet gaan vóór de procesveiligheidstijd. Het systeem of subsysteem kan nog steeds uitvallen als er een enkele fout optreedt tussen de functionele testen, maar dit is doorgaans minder waarschijnlijk dan voor categorie 1. Hierbij dient te worden opgemerkt dat wanneer categorie 2 gebruikt wordt voor PLd, er sprake moet zijn van twee signaaluitvoermodules, omdat in het geval van een foutdetectie de testuitvoer een veilige toestand moet initiëren. Zie (EN) ISO 13849-1 voor alle eisen.



Speciale architectuurcategorie 3

Speciale architectuurcategorie 3 moet de basisprincipes op het gebied van veiligheid toepassen (zie bijlagen van (EN) ISO 13849-2). Er is bovendien de vereiste dat het systeem of subsysteem niet mag uitvallen als er één storing optreedt. Dit betekent dat het systeem ten aanzien van zijn veiligheidsfunctie één storing moet tolereren. De gebruikelijkste manier om aan deze vereiste te voldoen, is het gebruik van een tweekanaals architectuur zoals hierboven is weergegeven. Bovendien is vereist dat als dat praktisch mogelijk is, één fout dient te worden gedetecteerd. Deze vereiste is identiek aan de oorspronkelijke vereiste voor categorie 3 van EN 954-1. Daar bleek “als dat praktisch mogelijk is” enigszins problematisch te zijn. Het betekende namelijk dat categorie 3 van toepassing was op alles: van een systeem met redundantie maar geen foutdetectie (vaak treffend omschreven als “domme redundantie”) tot een redundant systeem waarin elke afzonderlijke fout wordt gedetecteerd. Dit probleem is in (EN) ISO 13849-1 opgelost met de vereiste dat de kwaliteit van de Diagnostic Coverage (DC) bepaald moet worden. Hoe groter de betrouwbaarheid [$MTTF_D$] van het systeem, hoe lager de DC hoeft te zijn. Maar in alle gevallen moet de DC minimaal 60% bedragen voor architectuur van categorie 3.



Speciale architectuurcategorie 4

Speciale architectuurcategorie 4 moet de basisprincipes op het gebied van veiligheid toepassen (zie bijlagen van (EN) ISO 13849-2). Het schema met eisen is identiek aan dat van categorie 3, maar de bewaking moet strenger zijn, dat wil zeggen een hogere diagnose. Dit wordt weergegeven door de dikkere stippellijnen, die de bewakingsfuncties voorstellen. In wezen is het verschil tussen beide categorieën dat bij categorie 3 de

meeste fouten gedetecteerd moeten worden en dat bij categorie 4 elke afzonderlijke gevaarlijke fout en gevaarlijke combinaties van fouten gedetecteerd moeten worden. In de praktijk wordt dit gewoonlijk gerealiseerd door een hoog niveau van diagnostiek om ervoor te zorgen dat alle relevante fouten worden gedetecteerd voordat er een opeenhoping kan ontstaan. De DC moet ten minste 99% bedragen.

Betrouwbaarheidsgegevens

(EN) ISO 13849-1 maakt bij de berekening van het prestatieniveau (PL) van de veiligheidsgerelateerde onderdelen van een besturingssysteem onder meer gebruik van kwantitatieve betrouwbaarheidsgegevens. De eerste vraag die dit oproept, luidt: “Waar halen we deze gegevens vandaan?” Er kunnen gegevens gebruikt worden uit erkende handboeken met betrouwbaarheidsgegevens, maar in de norm staat expliciet dat de voorkeursbron de fabrikant is. Hiertoe heeft Rockwell Automation de betreffende gegevens beschikbaar gesteld via een gegevensbibliotheek voor SISTEMA.
Voordat we verdergaan, moeten we aan de orde stellen welke typen gegevens vereist zijn en duidelijk maken hoe ze worden verkregen.

Het door de norm (en SISTEMA) meest gewenste gegevenstype dat vereist is om mede het Performance Level te bepalen, is de PFH (de waarschijnlijkheid van een gevaarlijke storing per uur). Dit zijn dezelfde gegevens zoals gebruikt in IEC 61508 en weergegeven door de afkorting PFH_D die wordt gebruikt in IEC/EN 62061.

PL (Prestatieniveau)	PFH_D (Waarschijnlijkheid van een gevaarlijke storing per uur)	SIL (Veiligheidsintegriteits-niveau)
a	$\geq 10^{-5}$ tot $<10^{-4}$	Geen
b	$\geq 3 \times 10^{-6}$ tot $<10^{-5}$	1
c	$\geq 10^{-6}$ tot $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ tot $<10^{-6}$	2
e	$\geq 10^{-8}$ tot $<10^{-7}$	3

In de bovenstaande tabel wordt het verband weergegeven tussen PFH_D en PL en SIL. Voor sommige subsystemen kan de PFH_D beschikbaar zijn gesteld door de fabrikant. Dit maakt de berekening een stuk eenvoudiger. De fabrikant zal hiertoe meestal een aantal relatief complexe berekeningen en/of testen op zijn subsysteem moeten uitvoeren.
Als de PFH niet beschikbaar is, biedt (EN) ISO ISO13849-1 ons een alternatieve, vereenvoudigde methode die gebaseerd is op de $MTTF_D$ (de gemiddelde tijd tot een gevaarlijke storing) van één kanaal. Het PL (en dus de PFH_D) van een systeem of subsysteem kan vervolgens berekend worden met behulp van de methodologie en formules uit de norm. Met SISTEMA is dit zelfs nog gemakkelijker.

OPMERKING: Het is van belang in te zien dat een tweekanaals systeem (met of zonder diagnostiek) niet 1/PFH_D mag toepassen om de $MTTF_D$ te bepalen die vereist wordt door (EN) ISO 13849-1. De norm verlangt de $MTTF_D$ van een enkel kanaal. Dit is een totaal andere waarde dan de $MTTF_D$ die het resultaat is van de combinatie van beide kanalen van een tweekanaals subsysteem. Als de PFH_D van een tweekanaals subsysteem bekend is, kan deze waarde gewoon rechtstreeks in SISTEMA ingevoerd worden.

$MTTF_D$ van een enkel kanaal

Dit is de gemiddelde tijd voordat er een storing optreedt die ertoe zou kunnen leiden dat de veiligheidsfunctie uitvalt. Hij wordt uitgedrukt in jaren. De waarde is een gemiddelde van de $MTTF_D$'s van de "blokken" van elk kanaal en ze kan worden toegepast op een systeem of subsysteem. De norm geeft de volgende formule voor het berekenen van het gemiddelde van alle $MTTF_D$'s van elk element dat in één kanaal of subsysteem wordt gebruikt.

In dit stadium wordt de waarde van SISTEMA duidelijk. Gebruikers besparen tijd omdat taken als het raadplegen van tabellen en het berekenen van formules door de software worden uitgevoerd. Er kan een rapport van meerdere pagina's worden afgedrukt waarin de eindresultaten zijn vastgelegd.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{\tilde{N}} \frac{1}{MTTF_{di}} = \sum_{j=1}^{\tilde{N}} \frac{nj}{MTTF_{dj}}$$

Formule D1 van (EN) ISO 13849-1

In de meeste tweekanaals systemen zijn beide kanalen identiek, waardoor het resultaat van de formule voor beide kanalen geldt.

Als de kanalen van het systeem of subsysteem van elkaar verschillen, beschikt de norm over een formule die hier rekening mee houdt.

$$MTTF_d = \frac{2}{3}\left[MTTF_{dC1} + MTTF_{dC2} - \frac{1}{\frac{1}{MTTF_{dC1}} + \frac{1}{MTTF_{dC2}}} \right]$$

Deze berekent in feite het gemiddelde van twee gemiddelden. Om het eenvoudig te houden is het toegestaan om de "slechtste" kanaalwaarde te gebruiken.

De norm groepeert de $MTTF_D$ als volgt in drie tijdspannes:

Aanduiding van $MTTF_D$ van elk kanaal	**Bereik van $MTTF_D$ van elk kanaal**
Laag	3 jaar <= $MTTF_D$ < 10 jaar
Gemiddeld	10 jaar <= $MTTF_D$ < 30 jaar
Hoog	30 jaar <= $MTTF_D$ < 100 jaar

Niveaus van $MTTF_D$

Er dient in ogenschouw te worden genomen dat (EN) ISO 13849-1 de bruikbare $MTTF_D$ van één kanaal van een subsysteem beperkt tot maximaal 100 jaar, zelfs al zijn de feitelijke afgeleide waarden veel hoger.

Verderop zullen we zien dat het gerealiseerde niveau van het $MTTF_D$-gemiddelde in dat geval gecombineerd wordt met de speciale architectuurcategorie en de Diagnostic Coverage (DC) om tot een voorlopige PL-waarde te komen. De term “voorlopig” wordt gebruikt omdat er in voorkomende gevallen nog aan andere eisen moet worden voldaan, waaronder systeemintegriteit en maatregelen tegen gemeenschappelijk falen.

Methoden van gegevensbepaling

We gaan nu één stap verder en bespreken hoe een fabrikant de gegevens bepaalt via de PFH_D of de $MTTF_D$. Een goed begrip hiervan is essentieel voor de omgang met gegevens van fabrikanten. Componenten kunnen in drie basistypen worden onderverdeeld:

- Mechanisch (elektromechanisch, mechanisch, pneumatisch, hydraulisch enz.)
- Elektronisch (d.w.z. halfgeleider)
- Software

Er is een fundamenteel verschil tussen de mechanismen voor gemeenschappelijk falen van deze drie technologietypen. Elk type kan in algemene zin als volgt worden gekarakteriseerd:

Mechanische technologie:

Falen is evenredig aan zowel de inherente betrouwbaarheid als aan de gebruiksfrequentie. Hoe hoger de gebruiksfrequentie, des te waarschijnlijker dat een van de onderdelen gebreken gaat vertonen en uitvalt. Hierbij dient opgemerkt te worden dat dit niet de enige oorzaak voor falen is, maar het zal wel de belangrijkste zijn als we de bedrijfstijd/-cycli niet beperken. Het spreekt voor zich dat een magneetschakelaar die een schakelcyclus van eens per tien seconden heeft, gedurende een veel kortere periode betrouwbaar werkt dan een identieke magneetschakelaar die eens per dag moet schakelen.

Fysieke technische apparaten bestaan over het algemeen uit componenten die elk afzonderlijk ontworpen zijn voor een bepaalde taak. De onderdelen worden onder meer gevormd, geperst, gegoten en bewerkt en met elkaar verbonden via bijvoorbeeld koppelingen, veren, magneten en elektrische windingen en vormen zo één mechanisme. Omdat de onderdelen doorgaans geen gebruikshistorie in andere toepassingen hebben, kunnen we er geen al bestaande betrouwbaarheidsgegevens van vinden. De bepaling van de PFH_D of $MTTF_D$ voor het mechanisme is normaal gesproken gebaseerd op testen. Zowel EN/IEC 62061 als (EN) ISO 13849-1 bepleit een testproces dat bekend staat als $B10_D$-testen.

In de $B10_D$-test wordt een aantal apparaten (doorgaans minstens tien) onder representatieve omstandigheden getest. Het gemiddeld aantal bedieningscycli dat gerealiseerd wordt voordat bij 10% van de monsters een storing een gevaarlijke situatie oplevert, wordt de B10d-waarde genoemd. In de praktijk is het vaak zo dat bij alle monsters een storing in een veilige situatie resulteert. In dit geval geeft de norm echter aan dat de (gevaarlijke) B10d-waarde gelijk is aan tweemaal de B10-waarde.

Elektronische technologie:

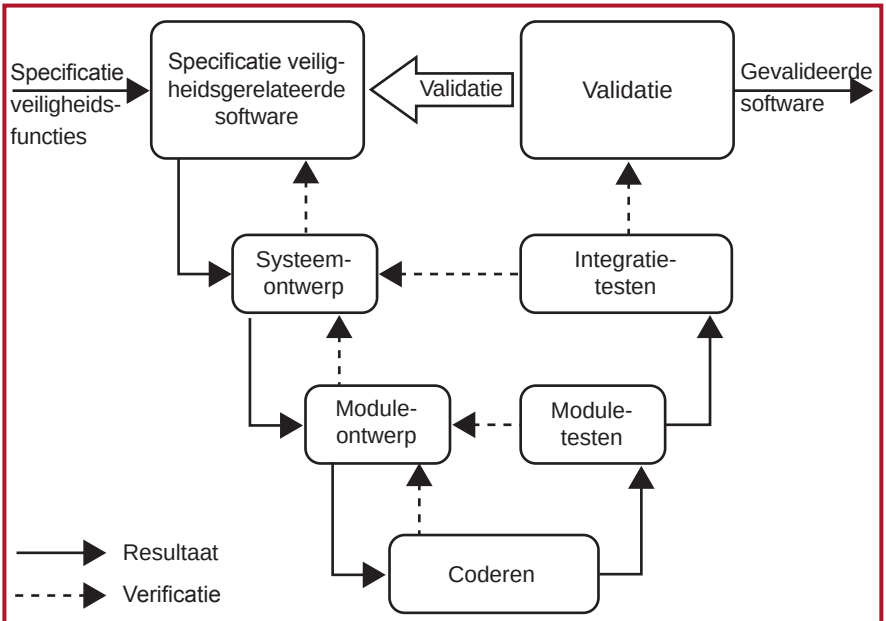
Er is geen fysieke slijtage met betrekking tot bewegende onderdelen. Als ervan uitgegaan wordt dat de werkomgeving geschikt is voor de gespecificeerde elektrische en temperatuurkenmerken, is de belangrijkste storing van een elektronisch circuit evenredig aan de inherente betrouwbaarheid van zijn samenstellende componenten (of het ontbreken daarvan). Er zijn vele redenen waarom een afzonderlijke component uit kan vallen, waaronder productiefouten, bovenmatige vermogenspieken en mechanische verbindingsproblemen. Over het algemeen kunnen storingen in elektronische componenten worden veroorzaakt door belasting, tijd en temperatuur, maar ze zijn moeilijk te voorspellen met analyses en blijken willekeurig van aard te zijn. Daarom worden bij het testen van een elektronisch apparaat onder laboratoriumomstandigheden niet noodzakelijkerwijs kenmerkende patronen voor langetermijnstoringen blootgelegd.

Het is gebruikelijk om de betrouwbaarheid van elektronische apparaten te bepalen aan de hand van analyses en berekeningen. In handboeken met betrouwbaarheidsgegevens zijn geschikte gegevens te vinden voor afzonderlijke componenten. We kunnen met behulp van analyses bepalen welke storingsmodi voor componenten gevaarlijk zijn. Het is aanvaardbaar en gebruikelijk ervan uit te gaan dat 50% van de storingsmodi voor componenten gevaarlijk is en 50% veilig. Dit leidt normaal gesproken tot relatief conservatieve gegevens.

In IEC 61508 zijn formules opgenomen waarmee de algehele waarschijnlijkheid van een gevaarlijke storing (PFH of PFD) van het apparaat (d.w.z. het subsysteem) kan worden berekend. De formules zijn uiterst complex en houden, indien van toepassing, rekening met de betrouwbaarheid van componenten, de kans op gemeenschappelijk falen (bètafactor), de Diagnostic Coverage (DC), het functioneletestinterval en het prooftestinterval. Het goede nieuws is dat deze complexe berekening normaal gesproken gedaan wordt door de fabrikant van het apparaat. Zowel EN/IEC 62061 als (EN) ISO 13849-1 accepteert een subsysteem dat op deze wijze is berekend volgens IEC 61508. De hieruit resulterende PFH_D kan direct gebruikt worden in Bijlage K van (EN) ISO 13849-1 of de SISTEMA-berekeningstool.

Software:

Softwarestoringen zijn van nature systematisch van aard. Storingen worden veroorzaakt door de wijze waarop de software is ontwikkeld, geschreven of gecompileerd. Daarom worden alle storingen veroorzaakt door het systeem op basis waarvan de software is gemaakt en niet door het gebruik ervan. Om de storingen te controleren moeten we dus het systeem controleren. Zowel in IEC 61508 als in (EN) ISO 13849-1 zijn hiervoor eisen en methodologieën opgenomen. We hoeven er op deze plaats niet gedetailleerd op in te gaan. Nu dient alleen opgemerkt te worden dat ze gebruikmaken van het klassieke V-model. Ingebedde software is een zaak van de ontwerper van het apparaat. De gebruikelijke aanpak is dat ingebedde software ontwikkeld wordt volgens de formele methoden die in deel 3 van IEC 61508 uiteengezet worden. Wat betreft de programmacode, de software waarmee een gebruiker taken uitvoert, zijn de meeste programmeerbare veiligheidsvoorzieningen uitgerust met “gecertificeerde” functieblokken of routines. Dit vereenvoudigt de validatietaak voor de programmacode, maar er dient niet vergeten te worden dat het voltooide toepassingsprogramma nog wel gevalideerd moet worden. De wijze waarop de blokken verbonden en geparameteriseerd worden, moet correct en geldig worden bevonden voor de bedoelde taak. Zowel in (EN) ISO 13849-1 als in IEC/EN 62061 zijn voor dit proces richtlijnen opgenomen.



V-model voor softwareontwikkeling

Diagnostic Coverage

We hebben dit onderwerp al kort aangestipt bij de behandeling van de speciale architectuurcategorieën 2, 3 en 4. Deze categorieën vereisen enige vorm van diagnostisch testen om te controleren of de veiligheidsfunctie nog werkt. De term “Diagnostic Coverage” (meestal afgekort tot DC) wordt gebruikt om de effectiviteit van deze test aan te geven. Het is belangrijk te realiseren dat DC niet is gebaseerd op het aantal componenten waarbij een storing tot een gevaarlijke situatie kan leiden. Het betreft de totale frequentie van gevaarlijke storingen. Het symbool λ wordt gebruikt voor “storingsfrequentie”. DC weerspiegelt het verband tussen de frequentie waarin de volgende twee typen gevaarlijke storingen optreden:

Gevaarlijke gedetecteerde storing [λdd]: storingen die het uitvallen van de veiligheidsfunctie hadden kunnen veroorzaken of hiertoe hadden kunnen leiden, maar die zijn gedetecteerd. Na de detectie zorgt een foutreactiefunctie ervoor dat het apparaat of systeem in een veilige toestand overgaat.

Gevaarlijke storing [λd]: alle storingen die het uitvallen van de veiligheidsfunctie zouden kunnen veroorzaken of hiertoe zouden kunnen leiden. Hiertoe behoren zowel de gedetecteerde als de niet-gedetecteerde storingen. Natuurlijk zijn de storingen die echt gevaarlijk zijn, de niet-gedetecteerde gevaarlijke storingen (aangeduid met λdu]

DC wordt uitgedrukt door de formule:
DC = λdd/λd, uitgedrukt als percentage.

De betekenis van de term DC is hetzelfde in (EN) ISO 13849-1 en EN/IEC 62061. De wijze waarop hij wordt afgeleid, kan echter verschillen. De laatstgenoemde norm stelt het gebruik van berekening op basis van storingsmodusanalyse voor, maar staat ook het gebruik toe van de vereenvoudigde methode in de vorm van opzoektabellen zoals voorzien in (EN) ISO 13849-1. Er worden verschillende kenmerkende diagnostische technieken genoemd en het DC-percentage dat hiermee moet worden gerealiseerd. In sommige gevallen is nog steeds een gefundeerd oordeel vereist. Bij bepaalde technieken is de gerealiseerde DC bijvoorbeeld evenredig aan de frequentie waarmee de test wordt uitgevoerd. Er wordt soms gesteld dat deze benadering te vaag is. De berekening van de DC kan echter afhangen van veel verschillende variabelen. En welke techniek er ook wordt gebruikt, het resultaat is doorgaans niet meer dan een benadering.

Het is belangrijk te beseffen dat de tabellen in EN ISO 13849-1 gebaseerd zijn op uitgebreid onderzoek dat door het IFA is uitgevoerd naar de resultaten die door welbekende, feitelijke diagnostische technieken behaald zijn in echte toepassingen. Om het eenvoudig te houden verdeelt de norm de DC onder in vier basisniveaus:

<60 % = geen
60 % to <90 % = laag
90 % to <99 % = gemiddeld
≥99 % = hoog

Deze benadering met niveaus in plaats van met afzonderlijke percentages kan ook als realistischer beschouwd worden als gekeken wordt naar de te realiseren nauwkeurigheid. De SISTEMA-tool gebruikt dezelfde opzoektabellen als de norm. Omdat het gebruik van complexe elektronica in veiligheidsgerelateerde apparaten toeneemt, wordt de DC steeds belangrijker. Waarschijnlijk zal dit thema in toekomstige versies van de normen verder uitgediept worden. Ondertussen moeten een technisch oordeel en gezond verstand voldoende zijn om het correcte DC-niveau te kiezen.

Gemeenschappelijk falen

In de meeste tweekanaals (d.w.z. tolerantie van één fout) systemen of subsystemen is het diagnostisch principe gebaseerd op de vooronderstelling dat gevaarlijke storingen niet tegelijkertijd in beide kanalen kunnen optreden. De term “tegelijkertijd” kan nauwkeuriger uitgedrukt worden als “binnen het diagnostisch testinterval”. Als het diagnostisch testinterval tamelijk kort is (d.w.z. korter dan acht uur), kan redelijkerwijs aangenomen worden dat het hoogst onwaarschijnlijk is dat twee afzonderlijke en niet-gerelateerde storingen binnen deze tijdsperiode optreden. De norm maakt echter duidelijk dat we zorgvuldig moeten afwegen of de mogelijke storingen echt afzonderlijk en niet-gerelateerd zijn. Als bijvoorbeeld te voorzien is dat een storing in een component kan leiden tot storingen in andere componenten, moet het resulterende totaalaantal storingen als één storing opgevat worden.

Het is tevens mogelijk dat een gebeurtenis die ertoe leidt dat één component uitvalt, er de oorzaak van is dat ook andere componenten uitvallen. Dit wordt aangeduid als “gemeenschappelijk falen”, wat doorgaans wordt afgekort tot CCF. De neiging tot CCF wordt vaak de bètafactor (ß-factor) genoemd. Het is erg belangrijk dat (sub)systeemontwerpers zich bewust zijn van de kans op CCF. Er zijn veel verschillende typen CCF en bijgevolg veel verschillende manieren om het te voorkomen. EN ISO 13849-1 vaart een rationele koers tussen de uitersten ‘complexiteit’ en ‘oversimplificatie’. Net als EN/IEC 62061 hanteert het een benadering die in essentie kwalitatief is. Het geeft een lijst met maatregelen waarvan bekend is dat ze CCF helpen voorkomen.

Nr.	Maatregel tegen gemeenschappelijk falen	Waardering
1	Scheiding/segregatie	15
2	Diversiteit	20
3	Ontwerp/toepassing/ervaring	20
4	Evaluatie/analyse	5
5	Expertise/training	5
6	Omgeving	35

Waarderingsmethode voor gemeenschappelijk falen

In het ontwerp van een systeem of subsysteem moeten voldoende van deze maatregelen geïntegreerd worden. Er kan met enige reden gesteld worden dat het gebruik van alleen deze lijst niet toereikend is om elk mogelijk geval van CCF te voorkomen. Als de intentie van de lijst echter zorgvuldig wordt beschouwd, wordt duidelijk dat het het wezen van deze vereiste is dat de ontwerper de mogelijkheden van CCF analyseert en op basis van het type technologie en de kenmerken van de betreffende toepassing preventieve maatregelen implementeert. Het gebruik van deze lijst dwingt tot nadenken over een aantal van de fundamenteelste en effectiefste technieken, zoals verscheidenheid van storingsmodi en ontwerpcompetenties. Ook de SISTEMA-tool van het IFA vereist de implementatie van de CCF-opzoektabellen uit de norm. De tool stelt ze op een gebruiksvriendelijke manier beschikbaar.

Systematische storingen

De gekwantificeerde betrouwbaarheidsgegevens op het gebied van veiligheid zijn al aan de orde gesteld in de vorm van de $MTTF_D$ en de waarschijnlijkheid van een gevaarlijke storing. Dit is echter niet het hele verhaal. Toen we naar deze termen verwezen, hadden we storingen in gedachten die willekeurig van aard blijken te zijn. IEC/EN 62061 verwijst met de afkorting $PFHd_D$ inderdaad specifiek naar de waarschijnlijkheid van willekeurige hardwarestoringen. Maar er is een aantal typen storingen dat algemeen bekend staat als “systematische storing” die kan worden toegeschreven aan fouten die zijn gemaakt tijdens het ontwerp- of productieproces. Het klassieke voorbeeld is een fout in de softwarecode. In Bijlage G van de norm zijn maatregelen opgenomen om deze fouten (en daarmee de storingen) te voorkomen. Deze maatregelen omvatten bepalingen zoals het gebruik van geschikte materialen en productietechnieken, evaluaties, analyses en computersimulatie. Daarnaast zijn er voorzienbare gebeurtenissen en kenmerken in de werkomgeving die tot storingen kunnen leiden als ze niet beheerst worden. Bijlage G bevat ook hiervoor maatregelen. Het is bijvoorbeeld eenvoudig te voorzien dat er af en toe spanningsverlies optreedt. De uitschakeling van componenten moet dan ook resulteren in een veilige toestand van het systeem. Deze maatregelen lijken de gewoonste zaak van de wereld, en dat zijn ze ook, maar ze zijn desondanks essentieel. Alle overige eisen van de norm zijn zinloos als het beheersen en voorkomen van systematische storingen niet de aandacht krijgen die ze moeten krijgen. Bovendien zal dit soms vereisen dat hetzelfde type maatregelen gebruikt wordt voor de beheersing van willekeurige hardwarestoringen (om de vereiste PFH_D te realiseren), zoals automatische diagnostische testen en redundante hardware.

Foutuitsluiting

Een van de belangrijkste analysehulpmiddelen voor veiligheidssystemen is storingsanalyse. De ontwerper en gebruiker dienen inzicht te hebben in de manier waarop het veiligheidssysteem zal functioneren indien er storingen optreden. Er zijn tal van technieken beschikbaar om deze analyse uit te voeren. Voorbeelden zijn onder meer foutboomanalyse; storingsmodi, gevolg- en kriticiteitsanalyse, gebeurtenisstructuuranalyse en evaluaties van de ladingsterkte.

Tijdens de analyse kunnen bepaalde storingen aan het licht komen die niet kunnen worden gedetecteerd aan de hand van automatische diagnostische tests zonder dat dit met hoge kosten gepaard gaat. Daarnaast kan de waarschijnlijkheid dat deze storingen optreden sterk worden geminimaliseerd vanwege het gebruik van een risicoreducerend ontwerp en risicoreducerende constructies en testmethoden. Onder deze omstandigheden kunnen de fouten van nadere overweging worden uitgesloten. Foutuitsluiting is het uitsluiten van het optreden van een storing omdat de waarschijnlijkheid van deze storing van het veiligheidsgerelateerde besturingssysteem verwaarloosbaar is.

(EN) ISO13849-1 staat foutuitsluiting toe op basis van de technische onwaarschijnlijkheid van het optreden ervan, van algemeen geaccepteerde technische ervaring en van de technische eisen die aan de toepassing zijn verbonden. (EN) ISO13849-2 voorziet in voorbeelden van en rechtvaardigingen voor het uitsluiten van bepaalde fouten voor elektrische, pneumatische, hydraulische en mechanische systemen. Foutuitsluitingen dienen te worden gemeld in combinatie met gedetailleerde rechtvaardigingen die in de technische documentatie zijn opgenomen.

Het is niet altijd mogelijk om een veiligheidsgerelateerd besturingssysteem te evalueren zonder aan te nemen dat bepaalde fouten kunnen worden uitgesloten. Raadpleeg voor gedetailleerde informatie over foutuitsluitingen de norm ISO 13849-2.

Als het risiconiveau toeneemt, worden aan de motivering van een foutuitsluiting strengere eisen gesteld. Over het algemeen geldt dat als er voor een veiligheidsfunctie PLe moet worden geïmplementeerd door een veiligheidsgerelateerd besturingssysteem, er doorgaans niet vertrouwd kan worden op foutuitsluitingen om dit prestatieniveau te realiseren. Dit is afhankelijk van de gebruikte technologie en de bedoelde werkomgeving. Het is daarom van essentieel belang dat de ontwerper extra aandacht besteedt aan het gebruik van foutuitsluitingen in het geval er een hoger PL wordt vereist.

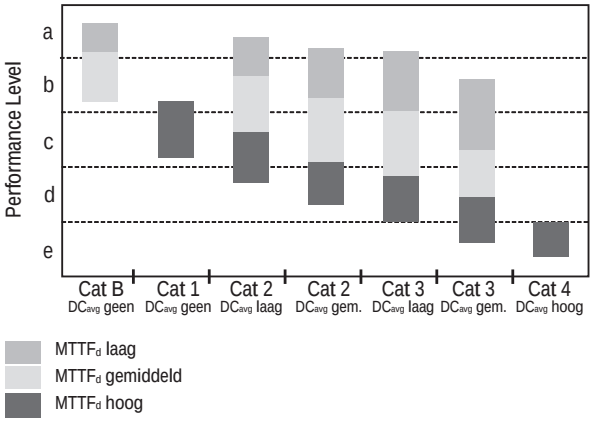
Performance Level, of PL

Het Performance Level is een discreet niveau dat een specificatie biedt van het vermogen van de veiligheidsgerelateerde onderdelen van het besturingssysteem om een veiligheidsfunctie uit te voeren.

Om het Performance Level te evalueren dat door een implementatie van een van de vijf speciale architecturen wordt bereikt, zijn de volgende (sub)systeemgegevens benodigd:

- $MTTF_D$ (gemiddelde tijd tot een gevaarlijke storing van elk kanaal)
- DC (Diagnostic Coverage).
- Architectuur (de categorie)

Het onderstaande diagram toont een grafische methode voor het vaststellen van het Performance Level op basis van een combinatie van deze factoren. De tabel in Bijlage K toont de tabelresultaten voor verschillende Markow-modellen die als basis voor dit diagram hebben gediend. Wanneer u de benodigde waarden nader in detail wilt bepalen, kunt u een beroep op deze tabel doen.



Grafische bepaling van Performance Level

Andere factoren moeten ook gerealiseerd worden om aan het vereiste PL te voldoen. Deze eisen betreffen de bepalingen voor gemeenschappelijk falen, systematische storingen, omgevingscondities en missietijd. Als de PFH_D voor het systeem of subsysteem bekend is, kunnen de tabellen in Bijlage K worden gebruikt om het prestatieniveau (PL) af te leiden.

Ontwerp en combinaties van subsystemen

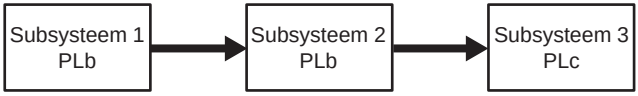
Subsystemen die aan een prestatieniveau (PL) voldoen, kunnen tot een systeem worden gecombineerd aan de hand van de weergegeven tabel.

PL_{laag}	**N_{laag}**	**PL**
a	>3	niet toegestaan
	≤3	a
b	>2	a
	≤2	b
c	>2	b
	≤2	c
d	>3	c
	≤3	d
e	>3	d
	≤3	e

Berekening van het Performance Level voor in serie geschakelde subsystemen

Het gebruik van deze tabel van de norm is niet verplicht; de tabel is alleen bedoeld om te voorzien in een zeer eenvoudige methode als alternatief voor het slechtst mogelijke scenario als de PFHd-waarden niet bekend zijn. Het systeemprestatieniveau (PL) kan worden berekend met andere methoden waaronder SISTEMA. De idee achter deze tabel is duidelijk. Ten eerste kan het systeem nooit beter zijn dan zijn slechtste subsysteem. Ten tweede geldt dat hoe groter het aantal subsystemen, des te groter de kans op storingen.

In het systeem dat in het onderstaande diagram wordt weergegeven, hebben subsysteem 1 en 2 de laagste Performance Level. Beide zijn PLb. Als we dus in de tabel van b (in de kolom PLlaag) naar 2 lezen (in de kolom Nlaag), vinden we het verkregen PL voor het systeem in de vorm van b (in de kolom PL). Als alle drie subsystemen PLb zouden zijn, zou het verkregen Performance Level PLa zijn.



Combinatie van een reeks subsystemen tot een PLb-systeem

Validatie

Validatie van veiligheidsfuncties omvat de verificatie van de gerealiseerde prestatieniveaus, maar gaat verder dan dat. Het is de bedoeling om te valideren dat de geïmplementeerde veiligheidsfunctie in feite de algemene veiligheidsvereisten voor de machines ondersteunt. Validatie speelt een belangrijke rol binnen het gehele ontwikkelings- en inbedrijfstellingsproces voor veiligheidssystemen. In ISO/EN 13849-2:2012 worden de vereisten voor validatie uiteengezet. Hierin wordt de eis van een validatieplan gesteld en validatie wordt besproken op basis van test- en analysetechnieken zoals foutboomanalyse en storingsmodi, en gevolg- en kriticiteitsanalyse. De meeste van deze eisen zullen van toepassing zijn op de fabrikant van het subsysteem, en niet op de gebruiker van het subsysteem.

Inbedrijfstelling van machines

In de fase waarin het systeem of de machine in bedrijf wordt gesteld, dient de controle van de veiligheidsfuncties worden uitgevoerd voor alle bedrijfsmodi, en dient er rekening te worden gehouden met alle normale en voorspelbare abnormale condities. Er dient rekening te worden gehouden met combinaties van ingangen en bewerkingsvolgorden. Deze procedure is van belang omdat het altijd nodig is om te controleren of het systeem geschikt is voor de werkelijke operationele en omgevingskenmerken. Sommige van deze kenmerken kunnen afwijken van de kenmerken die tijdens de ontwerpfase werden voorzien.

Hoofdstuk 8: Systeemontwerp volgens IEC/EN 62061

IEC/EN 62061, “Machineveiligheid – Functionele veiligheid van veiligheidsgerelateerde elektrische, elektronische en programmeerbare elektronische besturingssystemen” is de machinespecifieke toepassing van IEC/EN 61508. Deze norm zet richtlijnen uiteen die van toepassing zijn op het systeemontwerp van alle typen veiligheidsgerelateerde elektrische machinebesturingssystemen en het ontwerp van niet-complexe subsystemen en apparaten.

De risicoanalyse levert een risicoreductiestrategie op die op zijn beurt de noodzaak van veiligheidsgerelateerde besturingsfuncties aangeeft. Deze functies moeten worden gedocumenteerd. De documentatie dient verder te omvatten:

- een specificatie van de functionele eisen en
- een specificatie van de veiligheidsintegriteitseisen.

De functionele eisen omvatten aspecten zoals de regelmaat van bediening, de vereiste responstijd, operationele modi, de inschakelduur, werkomgeving en foutreactiefuncties. De veiligheidsintegriteitseisen worden uitgedrukt in niveaus die safety integrity levels (veiligheidsintegriteitsniveaus; SIL’s) worden genoemd. Afhankelijk van de complexiteit van het systeem dienen sommige of alle elementen in de onderstaande tabel in aanmerking te worden genomen om te kunnen vaststellen of het systeemontwerp aan de voorgeschreven SIL voldoet.

Element voor overweging van SIL	**Symbool**
Waarschijnlijkheid van een gevaarlijke storing per uur	PFH_D
Hardwarefouttolerantie	HFT
Safe Failure Fraction	SFF
Prooftestinterval	T_1
Diagnostisch testinterval	T_2
Vatbaarheid voor gemeenschappelijk falen	β
Diagnostic Coverage	DC

Overwegingen met betrekking tot de SIL

Subsystemen

In IEC/EN 62061 heeft de term “subsysteem” een speciale betekenis. Het is de onderverdeling op het eerste niveau van een systeem in delen die in het geval van storing in uitval van de veiligheidsfunctie zouden resulteren. Als er twee redundante schakelaars binnen een systeem worden gebruikt, zal dus geen van beide schakelaars een subsysteem vormen. Het subsysteem zou in dit geval beide schakelaars en de gerelateerde foutdiagnosefunctie omvatten.

Waarschijnlijkheid van een gevaarlijke storing per uur (PFH_D)

IEC/EN 62061 gebruikt dezelfde basismethoden om storingsfrequenties op componentniveau te bepalen als de methoden die in het gedeelte over (EN) ISO 13849-1 zijn besproken. Voor “mechanische” en elektronische componenten gelden dezelfde bepalingen en methoden. In IEC/EN 62061 speelt $MTTF_D$ al jaren geen rol. De storingsfrequentie per uur (λ) wordt rechtstreeks berekend of op grond van de volgende formule verkregen of afgeleid van de B10-waarde:

λ = 0,1 x C/B10 (C = het aantal bedieningscycli per uur)

Er is een wezenlijk verschil tussen de normen als het gaat om de methodologie voor het bepalen van de totale PFH_D van een (sub)systeem. Er dient een analyse van de onderdelen te worden uitgevoerd om vast te stellen met welke waarschijnlijkheid een storing van de subsystemen zal optreden. Er worden vereenvoudigde formules gegeven voor de berekening van gangbare subsysteemarchitecturen (verderop in de tekst beschreven). Als deze formules niet geschikt zijn, moeten er complexere berekeningsmethoden worden toegepast, zoals Markov-modellen. De waarden voor de waarschijnlijkheid van een gevaarlijke storing (PFH_D) van elk subsysteem worden dan bij elkaar opgeteld om de totale PFH_D van het systeem te bepalen. Tabel 3 van de norm kan vervolgens worden gebruikt om vast te stellen welk veiligheidsintegriteitsniveau (SIL) geschikt is voor dat bereik van PFH_D.

SIL (Veiligheidsintegriteits-niveau)	PFH_D (Waarschijnlijkheid van een gevaarlijke storing per uur)
3	$\geq 10^{-8}$ tot $<10^{-7}$
2	$\geq 10^{-7}$ tot $<10^{-6}$
1	$\geq 10^{-6}$ tot $<10^{-5}$

Waarschijnlijkheid van een gevaarlijke storing voor SIL’s

De PFH_D-gegevens voor een subsysteem worden meestal beschikbaar gesteld door de fabrikant. Gegevens voor veiligheidscomponenten en -systemen van Rockwell Automation zijn beschikbaar op:

www.rockwellautomation.com, onder Solutions & Services > Safety Solutions

IEC/EN 62061 maakt daarnaast duidelijk dat er indien nodig gebruik kan worden gemaakt van handboeken met betrouwbaarheidsgegevens.

Voor elektromagnetische apparaten met een laag complexiteitsniveau is het storingsmechanisme meestal gerelateerd aan het aantal en de frequentie van bewerkingen in plaats van eenvoudig de factor tijd. Om deze reden zullen de gegevens voor deze onderdelen worden afgeleid van bepaalde testen (bijv. de B10-testen die beschreven zijn in het hoofdstuk over (EN) ISO 13849-1). Vervolgens zijn er toepassingsgerelateerde gegevens, zoals het verwachte aantal bewerkingen per jaar, benodigd om de B10d-gegevens of vergelijkbare gegevens om te zetten in PFH_D.

OPMERKING: Over het algemeen geldt het volgende (waarbij jaren omgezet moeten worden in uren):

$PFH_D = 1/MTTF_D$

Het is echter van belang om in te zien dat een tweekanaals systeem (met of zonder diagnostiek) niet $1/PFH_D$ mag toepassen om de $MTTF_D$ te bepalen die vereist wordt door (EN) ISO 13849-1. Deze norm verlangt de $MTTF_D$ van één kanaal. Dit is een totaal andere waarde dan de $MTTF_D$ die het resultaat is van de combinatie van beide kanalen van een tweekanaals subsysteem, met inbegrip van het effect van Diagnostic Coverage.

Architectonische beperkingen

Het wezenlijke kenmerk van IEC/EN 62061 is dat het veiligheidssysteem wordt onderverdeeld in subsystemen. Het veiligheidsintegriteitsniveau van de hardware dat voor een subsysteem kan worden geclaimd wordt niet alleen beperkt door de PFH_D, maar ook door de fouttolerantie van de hardware en de verhouding van het aantal veilige storingen tot het totaal aantal storingen van de subsystemen. Fouttolerantie van de hardware is het vermogen van het systeem om zijn functie in geval van een storing te handhaven. Een fouttolerantie van nul houdt in dat de functie niet wordt uitgevoerd wanneer er één storing optreedt. Een fouttolerantie van één stelt het subsysteem in staat om zijn functie uit te voeren wanneer er één storing optreedt. De verhouding van het aantal veilige storingen tot het totaal aantal storingen van de subsystemen (Safe Failure Fraction oftewel SFF) is het onderdeel van de algehele storingsfrequentie dat niet in een gevaarlijke storing resulteert. De combinatie van deze twee elementen staat bekend als de architectonische beperking en wordt aangeduid als de SIL CL (SIL Claim Limit). De volgende tabel toont de relatie van de architectonische beperkingen met de SIL CL. Een subsysteem (en daarmee het systeem) moet zowel aan de PFH_D-eisen als aan de architectonische beperkingen en andere toepasselijke bepalingen van de norm voldoen.

Verhouding van het aantal veilige storingen tot het totale aantal storingen (SFF)	**Hardwarefouttolerantie**		
	0	**1**	**2**
<60 %	Niet toegestaan, tenzij specifieke uitzonderingen van toepassing zijn	SIL1	SIL2
60 % – <90 %	SIL1	SIL2	SIL3
90 % – <99 %	SIL2	SIL3	SIL3
≥99 %	SIL3	SIL3	SIL3

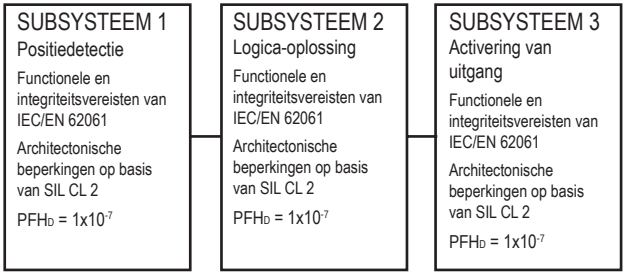
Architectonische beperkingen met betrekking tot SIL

De architectuur van een subsysteem met bijvoorbeeld een enkelvoudige fouttolerantie en een verhouding van het aantal veilige storingen tot het totaal aantal storingen van 75% blijft

beperkt tot maximaal een SIL2-waardering, ongeacht de waarschijnlijkheid van een gevaarlijke storing. Bij het combineren van subsystemen wordt de SIL die door de SRCS wordt bereikt beperkt tot een waarde die kleiner is dan of gelijk is aan de laagste SIL CL van een van de subsystemen die betrokken zijn bij de veiligheidsgerelateerde besturingsfunctie.

Systeemrealisering

Om de waarschijnlijkheid van een gevaarlijke storing te berekenen, dient elke veiligheidsfunctie te worden onderverdeeld in functieblokken, die vervolgens als subsystemen worden gerealiseerd. De implementatie van een systeemontwerp met een typische veiligheidsfunctie zal een detectievoorziening bevatten die is verbonden met een logisch apparaat dat op een magneetschakelaar is aangesloten. Op deze wijze wordt een serieschakeling van subsystemen verkregen. Zoals we al hebben gezien, is het mogelijk om de waarschijnlijkheid van een systeemstoring op eenvoudige wijze te berekenen door de waarschijnlijkheid van storingen van de subsystemen op te tellen, als we de waarschijnlijkheid van een gevaarlijke storing voor elk subsysteem kunnen vaststellen en de SIL CL voor de afzonderlijke subsystemen kennen. Dit concept wordt hieronder uiteengezet.



Als we bijvoorbeeld SIL 2 willen realiseren, dient elk subsysteem een SIL Claim Limit (SIL CL) van ten minste SIL 2 te hebben, en mag de som van de PFH_D voor het systeem niet groter zijn dan de limiet die is toegestaan in de vorige tabel waarin de 'waarschijnlijkheid van gevaarlijke storingen voor SIL 's' wordt weergegeven.

Subsysteemontwerp – IEC/EN 62061

Als een systeemontwerper gebruikmaakt van onderdelen die kant-en-klaar zijn "verpakt" in subsystemen volgens IEC/EN 62061, wordt diens leven er een stuk eenvoudiger op, omdat de specifieke eisen voor het ontwerp van subsystemen in dat geval niet van toepassing zijn. In de meeste gevallen zal de fabrikant van het apparaat (subsysteem) reeds in deze eisen hebben voorzien. Deze eisen hebben een veel complexer karakter dan die voor het ontwerp op systeemniveau.

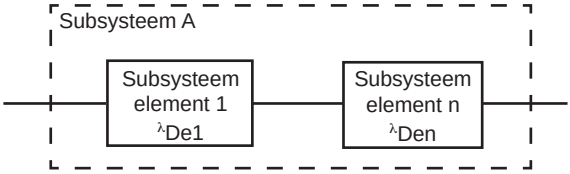
IEC/EN 62061 vereist dat complexe subsystemen zoals veiligheids-PLC's voldoen aan IEC 61508 of andere toepasselijke normen. Dit betekent dat op apparaten die

gebruikmaken van complexe elektronische of programmeerbare onderdelen IEC 61508 integraal van toepassing is. Dit kan een uiterst nauwgezet en intensief proces zijn. Het evalueren van de PFH_D die door een complex subsysteem wordt bereikt, kan een uiterst gecompliceerd proces zijn, waarbij technieken zoals Markov-modellering, betrouwbaarheidsblokdiagrammen en foutboomanalyse moeten worden gebruikt.

IEC/EN 62061 stelt eisen aan het ontwerp van subsystemen met een lager complexiteitsniveau. Normaliter zou dit relatief eenvoudige elektrische onderdelen omvatten, zoals vergrendelingsschakelaars en elektromechanische veiligheidsrelais die voor bewakingsdoeleinden worden gebruikt. De eisen zijn niet zo intensief als die van IEC 61508, maar kunnen nog steeds uiterst gecompliceerd zijn.

IEC/EN 62061 voorziet in vier logische architecturen voor subsystemen met gerelateerde formules die kunnen worden gebruikt om de PFH_D van een subsysteem met een laag complexiteitsniveau te evalueren. Deze architecturen vormen louter logische vertegenwoordigingen en dienen niet als fysieke architecturen te worden beschouwd. De vier logische subsysteemarchitecturen met gerelateerde formules worden in de volgende vier diagrammen weergegeven.

Voor een eenvoudig subsysteemarchitectuur zoals hieronder wordt weergegeven, worden de waarschijnlijkheden van gevaarlijke storingen eenvoudig bij elkaar opgeteld.

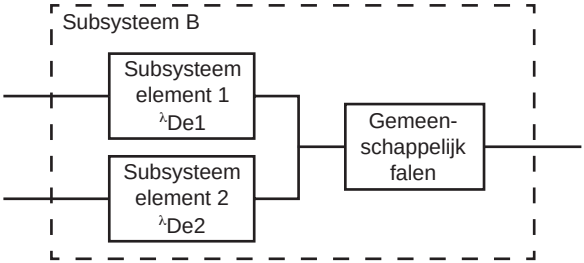


Logische subsysteemarchitectuur A

λDssA = λDe1 + … + λDen
PFHDssA = λDssA

λ lambda vertegenwoordigt de storingsfrequentie. De storingsfrequentie wordt uitgedrukt in storingen per uur. λ_D, lambda sub D, vertegenwoordigt de frequentie van gevaarlijke storingen. λ_{DssA}, lambda sub DssA, vertegenwoordigt de frequentie van gevaarlijke storingen voor subsysteem λ. Lambda sub DssA vertegenwoordigt de som van de storingsfrequenties van de afzonderlijke elementen e1, e2, e3, tot en met en. De waarschijnlijkheid van een gevaarlijke storing wordt vermenigvuldigd met 1 uur om de waarschijnlijkheid van een storing binnen één uur te verkrijgen.

Het volgende diagram toont een enkelvoudig fouttolerant systeem zonder diagnostische functie. Als de architectuur in fouttolerantie voor een enkele storing voorziet, blijft de kans op gemeenschappelijk falen bestaan en dient daar rekening mee te worden gehouden. Het herleiden van de oorzaak van het gemeenschappelijk falen komt later in dit hoofdstuk kort aan bod.



Logische subsysteemarchitectuur B

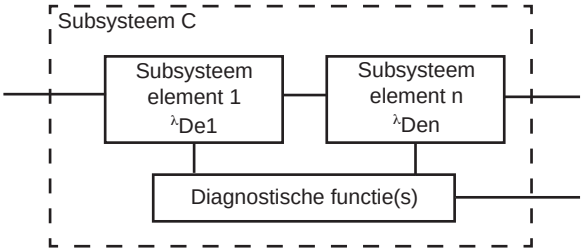
DssB = $(1-\beta)^2$ x λDe1 x λDe2 x T1 + β x (λDe1 + λDe2)/2
PFHDssB = λDssB

De formule voor deze architectuur houdt rekening met de parallelle schakeling van de elementen van de subsystemen en voegt de volgende twee elementen toe uit de vorige tabel 'Overwegingen met betrekking tot de SIL'.

ß – de vatbaarheid voor gemeenschappelijk falen (bèta)

T1 – het prooftestinterval of de levensduur (de kleinste van deze twee waarden). De prooftest heeft ten doel om storingen en een degradatie van het veiligheidssubsysteem te detecteren, zodat het subsysteem naar een werkende toestand kan worden hersteld. Praktisch gezien betekent dit meestal vervanging (zoals het equivalent "missietijd" in (EN) ISO 13849-1).

Het volgende diagram toont de functionele vertegenwoordiging van een systeem met een fouttolerantie van nul met een diagnostische functie. Er wordt gebruikgemaakt van diagnostisch falen om de kans op gevaarlijke hardwarestoringen te verminderen. Het diagnostisch falen worden automatisch uitgevoerd. De definitie van Diagnostic Coverage is hetzelfde als in (EN) ISO 13849-1, dat wil zeggen de verhouding tussen de frequentie van gedetecteerde gevaarlijke storingen en de frequentie van alle gevaarlijke storingen.

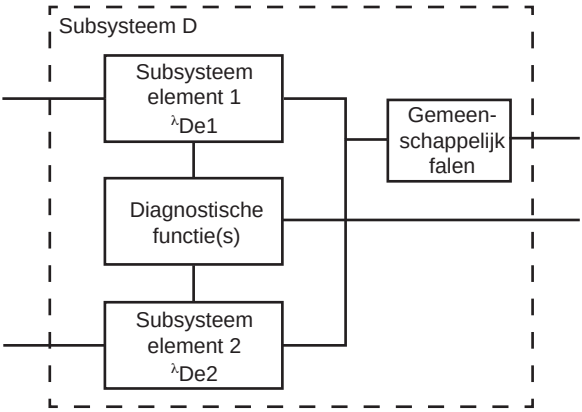


Logische subsysteemarchitectuur C

$\lambda_{DssC} = \lambda_{De1}$ (1-DC1)+ … + λ_{Den} (1-DCn)
PFHDssC = λDssC

Deze formules omvatten de Diagnostic Coverage (DC) voor elk van de elementen van het subsysteem. Van de storingsfrequenties voor elk van de subsystemen wordt telkens de Diagnostic Coverage van het subsysteem afgetrokken.

Hieronder wordt een vierde voorbeeld van een subsysteemarchitectuur gegeven. Dit subsysteem biedt fouttolerantie voor één storing en bevat een diagnostische functie. Bij systemen met een fouttolerantie voor één storing moet eveneens rekening worden gehouden met de kans op gemeenschappelijk falen.



Logische subsysteemarchitectuur D

Als de elementen van het subsysteem niet identiek zijn, worden de volgende formules gebruikt:

λDssD = (1 – β)2 {[λDe1 x λDe2 x (DC1+ DC2)] x T2/2 + [λDe1 x λDe2 x (2- DC1 – DC2)] x T1/2 } + β x (λDe1 + λDe2)/2
PFHDssD = λDssD

Als de elementen van het subsysteem identiek zijn, worden de volgende formules gebruikt:

$A_{DssD} = (1 – \beta)^2$ {[λ_{De^2} x 2 x DC] x $T_2/2$ + [λ_{De^2} x (1-DC)] x T_1 }+ β x λ_{De}
PFHDssD = λDssD

Hierbij dient te worden opgemerkt dat beide formules gebruikmaken van een extra parameter, T2. Deze parameter vertegenwoordigt het diagnostische interval. Dit is slechts een periodieke controle van de functie. Hij is minder uitgebreid dan de prooftest.

Als voorbeeld gaan we uit van de volgende voorbeeldwaarden. In dit voorbeeld is sprake van identieke subsysteemelementen:

β = 0,05
λDe = 1 x 10^{-6} storingen per uur
T1 = 87.600 uur (10 jaar)
T2 = 2 uur
DC = 90 %

PFH_{DssD} = 5,790E-8 gevaarlijke storingen per uur. Dit valt binnen het waardebereik dat vereist is voor SIL3.

Gevolgen van het prooftestinterval

IEC/EN 62061 stelt dat een prooftestinterval (PTI) van 20 jaar de voorkeur verdient (maar niet verplicht is). Wat zijn nu de gevolgen van het prooftestinterval op het systeem? Als we in de formule voor T1 20 jaar invullen, levert dit een PFHDssD van 6,58E-8 op. Dit is nog steeds binnen het bereik dat is vereist voor SIL 3.
De ontwerper moet er rekening mee houden dat dit subsysteem met andere subsystemen moet worden gecombineerd om de totale frequentie van gevaarlijke storingen te berekenen.

Effect van de analyse van gemeenschappelijk falen

Laten we eens kijken naar het effect dat gemeenschappelijk falen voor het systeem zal hebben. Laten we ervan uitgaan dat we extra maatregelen treffen en dat onze ß-waarde (bètawaarde) verbetert tot 1% (0,01), terwijl het prooftestinterval 20 jaar blijft. De frequentie van gevaarlijke storingen verbetert tot 2,71E-8, wat betekent dat het subsysteem nu geschikter is om in een SIL 3-systeem te worden gebruikt.

Gemeenschappelijk falen (CCF)

Er is sprake van gemeenschappelijk falen wanneer meerdere storingen die een en dezelfde oorzaak hebben in een gevaarlijke storing resulteren. Informatie over de CCF zal over het algemeen alleen nodig zijn voor de ontwerper van het subsysteem. In de meeste gevallen is dit de fabrikant. Deze informatie wordt gebruikt als onderdeel van de formules voor de inschatting van de PFH_D van een subsysteem. Het zal normaliter niet worden vereist op systeemontwerpniveau.

Bijlage F van IEC/EN62061 voorziet in een eenvoudige aanpak van de inschatting van de CCF. De volgende tabel geeft een samenvatting van het waarderingsproces.

Nr.	Maatregel tegen gemeenschappelijk falen	Waardering
1	Scheiding/segregatie	25
2	Diversiteit	38
3	Ontwerp/toepassing/ervaring	2
4	Evaluatie/analyse	18
5	Expertise/training	4
6	Omgeving	18

Waardering van maatregelen tegen gemeenschappelijk falen

Er worden punten toegekend voor het gebruik van specifieke maatregelen tegen gemeenschappelijk falen. Deze waardering wordt opgeteld om de CCF vast te stellen, zoals in de volgende tabel weergegeven. De bètafactor wordt gebruikt in de subsysteemmodellen om de storingsfrequentie “bij te stellen”.

Algehele waardering	Factor voor gemeenschappelijk falen (R)
<35	10 % (0,1)
35 – 65	5 % (0,05)
65 – 85	2 % (0,02)
85 – 100	1 % (0,01)

Bètafactor voor gemeenschappelijk falen

Diagnostic Coverage (DC)

Er wordt gebruikgemaakt van automatische diagnostische tests om de kans op gevaarlijke hardwarestoringen te verkleinen. Detectie van alle gevaarlijke hardwarestoringen zou ideaal zijn, maar in de praktijk wordt als maximumwaarde 99% (dit kan ook uitgedrukt worden als 0,99) genomen.

De Diagnostic Coverage is de verhouding tussen de waarschijnlijkheid van het aantal gedetecteerde gevaarlijke storingen en de waarschijnlijkheid van alle gevaarlijke storingen.

$$DC = \frac{\text{De waarschijnlijkheid van het aantal gedetecteerde gevaarlijke storingen, } \lambda_{DD}}{\text{De waarschijnlijkheid van het totaalaantal gevaarlijke storingen, } \lambda_{Dtotal}}$$

De waarde voor de Diagnostic Coverage zal tussen nul en 99% liggen.

Hardwarefouttolerantie

De hardwarefouttolerantie vertegenwoordigt het aantal storingen dat een subsysteem aankan voordat er een gevaarlijke storing optreedt. Een hardwarefouttolerantie van 1 houdt bijvoorbeeld in dat twee storingen kunnen resulteren in het uitvallen van de veiligheidsgerelateerde besturingsfunctie, terwijl één storing dit gevolg niet zou hebben.

Beheer van functionele veiligheid

De norm zet eisen uiteen voor de besturing van technische en beheerwerkzaamheden die moeten worden uitgevoerd om een veiligheidsgerelateerd elektrisch besturingssysteem te realiseren.

Prooftestinterval

Het prooftestinterval vertegenwoordigt de periode waarna een subsysteem volledig moet worden gecontroleerd of vervangen om te garanderen dat het zich in een “zo goed als nieuwe” toestand bevindt. In de praktijk wordt dit in de machinebouwsector bewerkstelligd door subsystemen te vervangen. Het prooftestinterval is dientengevolge meestal gelijk aan de levensduur. (EN) ISO 13849-1 noemt dit de missietijd (mission time oftewel MT).

Een prooftest is een controle die in staat is om storingen en veroudering in een SRCS te detecteren, zodat de SRCS kan worden hersteld naar een toestand die praktisch gezien zo dicht mogelijk bij een “zo goed als nieuwe” toestand komt. De prooftest moet in staat zijn om 100% van alle gevaarlijke storingen te detecteren, met inbegrip van de diagnostische functie (indien van toepassing). Afzonderlijke kanalen dienen afzonderlijk te worden getest.

In tegenstelling tot diagnostische tests, die een automatisch karakter hebben, worden prooftesten meestal handmatig uitgevoerd terwijl de machine offline is. Vanwege het automatische karakter worden diagnostische tests vaker uitgevoerd dan prooftesten, die onregelmatig plaatsvinden. De circuits die met een vergrendelingsschakelaar op een afscherming zijn verbonden, kunnen automatisch worden getest voor korte en open circuitcondities met behulp van diagnostische (bijv. puls)tests.

Het prooftestinterval dient door de fabrikant te worden aangegeven. In sommige gevallen zal de fabrikant een reeks uiteenlopende prooftestintervallen aangeven. Het is gebruikelijker om het subsysteem gewoon door een nieuw subsysteem te vervangen, in plaats van een prooftest uit te voeren.

Verhouding van het aantal veilige storingen tot het totale aantal storingen (SFF)

De verhouding van het aantal veilige storingen tot het totale aantal storingen is vergelijkbaar met de Diagnostic Coverage, maar houdt eveneens rekening met een eventuele inherente neiging tot storingen die in een veilige toestand resulteren. Wanneer er een zekering doorbrandt, is er sprake van een storing. Het is echter hoogst waarschijnlijk deze storing zal plaatsvinden naar een open circuit. In de meeste gevallen zou dan sprake zijn van een “veilige” storing. SFF is (de som van de frequentie van “veilige” storingen plus de frequentie van gedetecteerde gevaarlijke storingen) gedeeld door (de som van de frequentie van “veilige” storingen plus de frequentie van gedetecteerde en niet-gedetecteerde gevaarlijke storingen). Het is belangrijk om op te merken dat de enige typen storingen om rekening mee te houden storingen zijn die enige invloed op de veiligheidsfunctie kunnen hebben.

De SFF-waarde wordt normaliter door de fabrikant aangegeven als deze relevant is.

De Safe Failure Fraction (SFF) kan als volgt worden berekend:

$$SFF = (\sum \lambda_S + (\sum \lambda_{DD})/((\sum \lambda_S + (\sum \lambda_D)$$

waarbij

$\sum_S$ = de frequentie van veilige storingen,
$\sum \lambda_S + \sum \lambda_D$ = de frequentie van alle storingen,
λ_{DD} = de frequentie van gedetecteerde gevaarlijke storingen,
λ_D = de frequentie van alle gevaarlijke storingen.

Systematische fouten

De norm omvat eisen voor de het inperken en voorkomen van systematische fouten. Systematische fouten verschillen van willekeurige hardwarestoringen. Deze laatste zijn storingen die op willekeurige momenten optreden, meestal als gevolg van veroudering van hardwareonderdelen. Typische vormen van mogelijke systematische fouten zijn fouten in het softwareontwerp, fouten in het hardwareontwerp, fouten in specificaties van eisen en operationele procedures. Voorbeelden van maatregelen die moeten worden getroffen om systematische fouten te voorkomen zijn onder meer:

- een juiste selectie, combinatie, plaatsing, montage en installatie van de onderdelen;
- het toepassen van de beste technische werkwijzen;
- het opvolgen van de specificaties en installatie-instructies van de fabrikant;
- het garanderen van onderlinge compatibiliteit van de onderdelen;
- het bestand zijn tegen omgevingscondities;
- het gebruik van geschikte materialen.

Hoofdstuk 9: Veiligheidsgerelateerde besturingssystemen, aanvullende overwegingen

Overzicht

Dit hoofdstuk behandelt algemene structuuroverwegingen en -principes waarmee rekening moet worden gehouden als er een veiligheidsgerelateerd besturingssysteem wordt ontworpen.

Categorieën besturingssystemen

De “categorieën” van besturingssystemen hebben hun oorsprong in de voormalige EN 954-1:1996 (ISO13849-1:1999). Ze worden echter nog vaak gebruikt om de structuur van veiligheidsbesturingssystemen te beschrijven en ze blijven als speciale architecturen integraal onderdeel van (EN) ISO 13849-1. De beschrijving en de vereisten van de categorieën zijn eerder besproken in deze publicatie in “Overzicht van (EN) ISO 13849-1”. Dit gedeelte is bedoeld om te voorzien in een vereenvoudigde, maar praktische leidraad voor de manier waarop u de categoriestructuren implementeert.

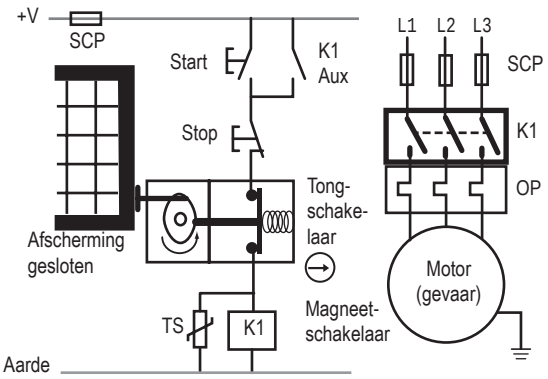
Categorie B

Categorie B moet worden gezien als de basis waarop alle andere categorieën zijn geconstrueerd. Deze categorie bevat geen speciale bepalingen of structuur voor veiligheid die verder reikt dan de basisprincipes op het gebied van veiligheid zoals voorzien in Bijlage A tot en met D van (EN) ISO 13849-2. Deze vertegenwoordigen een algemene goede werkmethode qua ontwerp en keuze van materialen.

Categorie 1

Categorie 1 vereist het gebruik van afdoende geteste onderdelen en afdoende geteste veiligheidsprincipes.

Deze afbeelding toont een gangbaar systeem bedoeld om te voldoen aan de vereisten van Categorie 1. De vergrendeling en de magneetschakelaar spelen een belangrijke rol bij het onderbreken van de voeding naar de motor wanneer er toegang tot het gevarengebied is vereist. De tongvergrendeling voldoet aan de eisen van IEC 60947-5-1 voor direct openende actiecontacten, zoals aangeduid met een symbool in de vorm van een pijltje binnen een cirkel. Door het gebruik van afdoende geteste onderdelen is de waarschijnlijkheid dat de voeding wordt onderbroken groter voor categorie 1 dan voor categorie B. Het gebruik van afdoende geteste onderdelen is bedoeld om het mogelijke uitvallen van de veiligheidsfunctie te minimaliseren, maar hierbij dient te worden opgemerkt dat een enkele fout nog steeds tot het uitvallen van de veiligheidsfunctie kan leiden.

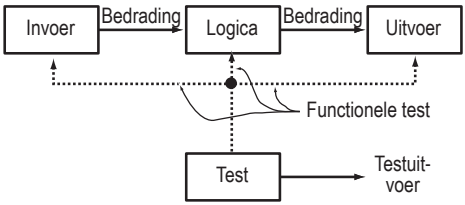


Eenvoudig categorie 1-veiligheidssysteem

Categorie 1 is bedoeld om storing te voorkomen door gebruik te maken van een eenvoudig ontwerp met uiterst betrouwbare onderdelen. Wanneer dit type preventie op zichzelf onvoldoende risicoreductie biedt, moet er foutdetectie worden gebruikt. De categorieën 2, 3 en 4 zijn gebaseerd op storings- of foutdetectie, en stellen steeds hogere eisen om hogere niveaus van risicoreductie te kunnen bewerkstelligen.

Categorie 2

Naast het voldoen aan de eisen van categorie B en het gebruik van afdoende geteste veiligheidsprincipes moet het veiligheidssysteem de nodige tests ondergaan om aan de richtlijnen van categorie 2 te kunnen voldoen. Deze tests moeten ten doel hebben om fouten binnen de veiligheidsgerelateerde onderdelen van het besturingssysteem te detecteren. Als er geen fouten worden gedetecteerd, mag de machine draaien. Als er wel fouten worden gedetecteerd, moet een foutreactiefunctie ervoor zorgen dat de machine in een veilige toestand blijft.



De apparatuur waarmee de test wordt uitgevoerd kan een integraal onderdeel van het veiligheidssysteem of op zichzelf staande apparatuur vormen.

De testprocedure moet worden uitgevoerd:

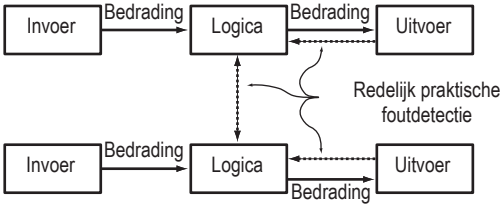
- wanneer de machine wordt ingeschakeld,
- voorafgaande aan het ontstaan van een gevaar, en
- periodiek indien dit op basis van de risicoanalyse wenselijk wordt geacht.

Opmerking: (EN) ISO 138491-1 gaat uit van een verhouding van 100:1 tussen het testen van de veiligheidsfunctie en de activering ervan, of van een test van het beroep op de veiligheidsfunctie met de mogelijkheid een fout te detecteren en de machine tot stilstand te brengen binnen kortere tijd dan nodig is om het gevaar te realiseren.

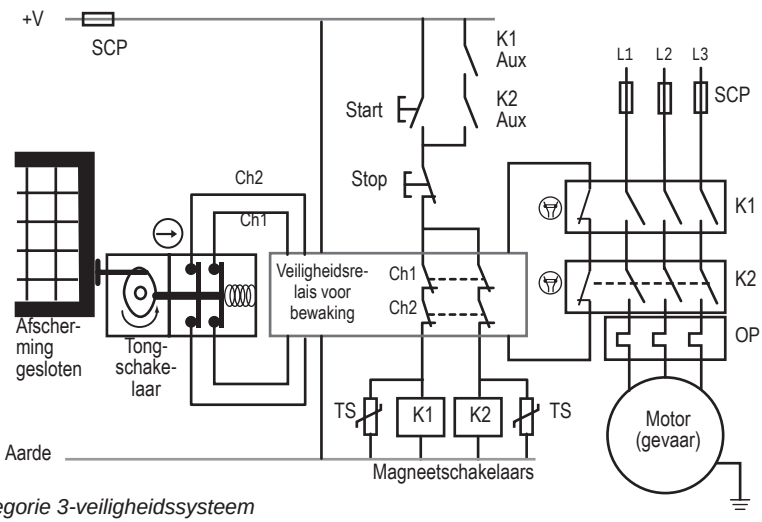
In wezen moet een veiligheidssysteem of -subsysteem volledig worden uitgeprobeerd om te testen of de veiligheidsfunctie nog steeds correct werkt. Dit betekent dat het moeilijk of zelfs onmogelijk kan zijn om te implementeren met technologieën die mechanische eigenschappen hebben. Een aanpak volgens categorie 2 is doorgaans relevanter voor elektronische technologie. Voor PLd moet er sprake zijn van een testuitvoer die in staat is om een veilige toestand te initiëren als er een storing wordt gedetecteerd.

Categorie 3

Naast het feit dat er aan de eisen van categorie B en afdoende geteste veiligheidsprincipes moet worden voldaan, vereist categorie 3 een succesvolle werking van de veiligheidsfunctie indien er één fout optreedt. Deze fout moet worden gedetecteerd voor of tijdens het moment waarop een beroep op de veiligheidsfunctie wordt gedaan, indien dit in alle redelijkheid praktisch toepasbaar is.
Sommige fouten, zoals dwarsfouten, die geen onmiddellijke uitval van de veiligheidsfunctie tot gevolg hebben, worden mogelijk niet gedetecteerd. Dit houdt in dat voor categorie 3 een opeenhoping van ongedetecteerde fouten kan resulteren in de uitval van de veiligheidsfunctie.



In het blokdiagram worden de principes van een categorie 3-systeem uiteengezet. Om de werking van de veiligheidsfunctie te garanderen wordt gebruikt gemaakt van redundantie in combinatie met onderlinge bewaking en bewaking van de uitgang.



Categorie 3-veiligheidssysteem

De afbeelding toont een voorbeeld van een categorie 3-systeem. De tongvergrendelingsschakelaar beschikt over redundante sets contacten. Het veiligheidsrelais dat voor bewakingsdoeleinden wordt gebruikt is intern uitgerust met redundante circuits die elkaar bewaken. Een redundante reeks van magneetschakelaars onderbreekt de voeding naar de motor. De magneetschakelaars worden door het veiligheidsrelais bewaakt via de mechanisch gekoppelde contacten.

Voor elke onderdeel van het veiligheidssysteem moet foutdetectie worden overwogen. Wat zijn de storingsmodi van een tweekanaals tongschakelaar? Wat zijn de storingsmodi van het veiligheidsrelais? Wat zijn de storingsmodi van de magneetschakelaars K1 en K2? Wat zijn de storingsmodi van de bedrading?

Voor categorie 3-circuits is het een veel gebruikte werkwijze om enkele tongvergrendelingsschakelaars met redundante sets elektrische contacten te gebruiken. Dit houdt in dat de mogelijkheid van een fout van een enkele component binnen de bedieningsverbindingen moet worden uitgesloten. Als deze fout niet kan worden uitgesloten, betekent dit dat een enkele fout de uitval van de veiligheidsfunctie kan veroorzaken. Het is van groot belang dat elke foutuitsluiting volledig gemotiveerd is.

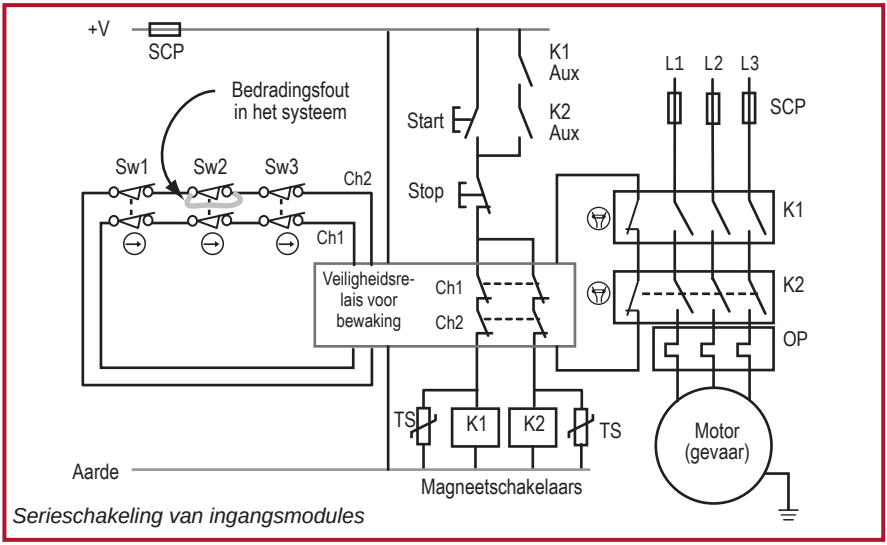
Het veiligheidsrelais (MSR) voorziet in foutdiagnostiek voor de tongvergrendelingsschakelaar en voor de magneetschakelaars. Het veiligheidsrelais kan ook andere functionaliteit, zoals een handmatige reset, mogelijk maken. Op basis van hun interne architectuur voldoen veiligheidsrelais in de meeste gevallen aan PLe of SIL3.

De twee magneetschakelaars moeten zijn uitgerust met overbelastings- en kortsluitbeveiliging. De waarschijnlijkheid dat de magneetschakelaar uitvalt als gevolg van gesmolten contacten is laag, maar niet ondenkbaar. Er kan ook een storing van een magneetscha-

kelaar optreden doordat zijn stroomschakelingscontacten gesloten blijven als gevolg van een vastgelopen anker. Als er een storing van een magneetschakelaar optreedt die in een gevaarlijke toestand resulteert, zal de tweede magneetschakelaar blijven functioneren en de voeding naar de motor onderbreken. Het veiligheidsrelais zal de uitgevallen magneetschakelaar tijdens de volgende machinecyclus detecteren. Wanneer de deur is gesloten en de startknop wordt ingedrukt, zullen de mechanisch gekoppelde contacten van de uitgevallen magneetschakelaar open blijven, en zal het veiligheidsrelais niet in staat zijn om zijn veiligheidscontacten te sluiten, zodat de fout aan het licht zal komen.

Niet-gedetecteerde fouten

Bij een systeemstructuur van categorie 3 kan er sprake zijn van storingen die niet gedetecteerd kunnen worden maar zelf niet tot het uitvallen van de veiligheidsfunctie mogen leiden. In het geval dat storingen gedetecteerd kunnen worden, moeten we weten of ze onder bepaalde omstandigheden verborgen kunnen blijven of onbedoeld opgelost kunnen worden door de andere apparaten in de systeemstructuur.



Serieschakeling van ingangsmodules

Deze afbeelding toont een op brede schaal gebruikte aanpak voor het verbinden van meerdere voorzieningen met een veiligheidsrelais. Elke voorziening bevat twee normaal gesloten, direct openende contacten. Met deze aanpak kan op bedradingskosten worden bezuinigd, omdat de ingangsmodules in een ringnetwerk zijn opgenomen. Stel dat er kortsluiting van een van de contacten optreedt bij Sw2 (zie bovenstaand diagram). Kan deze fout worden gedetecteerd?

Als schakelaar Sw1 (of Sw3) wordt geopend, zijn zowel Ch1 als Ch2 open circuits en onderbreekt het veiligheidsrelais met succes de voeding naar het gevaar. Als Sw3 vervolgens wordt geopend en daarna weer gesloten, dan wordt de storing in de contacten niet gedetec-

teerd, omdat de status van het veiligheidsrelais niet is gewijzigd: zowel Ch1 en Ch2 blijven open. Wanneer Sw1 (of Sw3) dan wordt gesloten, kan het gevaar opnieuw worden gestart door de startknop in te drukken. Onder deze omstandigheden leidde de storing niet tot het uitvallen van de veiligheidsfunctie, maar ze werd niet gedetecteerd. Ze blijft daarom in het systeem aanwezig en een volgende storing (een kortsluiting in het tweede contact van Sw2) zou het uitvallen van de veiligheidsfunctie kunnen betekenen.

Als alleen Sw2 was geopend en gesloten en de andere schakelaars niet zijn geactiveerd, gaat Ch1 open en blijft Ch2 gesloten. Het veiligheidsrelais onderbreekt de voeding naar het gevaar doordat Ch1 wordt geopend. Wanneer Sw2 wordt gesloten, kan de motor niet worden gestart wanneer de startknop wordt ingedrukt, omdat Ch2 niet open is gegaan. De fout is gedetecteerd. Als echter om wat voor reden dan ook Sw1 (of Sw3) vervolgens geopend en gesloten wordt, dan zijn zowel Ch1 en Ch2 eerst een open en daarna een gesloten circuit. Deze volgorde simuleert het oplossen van de storing en resulteert in een onbedoelde reset van het veiligheidsrelais.

Dit werpt de vraag op welke DC kan worden geclaimd voor de afzonderlijke schakelaars in deze structuur bij gebruik van (EN) ISO 13849-1 of IEC 62061? Tot aan de publicatie van ISO TR 24119 (november 2015: Evaluation of fault masking serial connection of interlocking devices associated with guards with potential free contacts (Evaluatie van foutmaskerende seriële aansluiting van vergrendelingsvoorzieningen gekoppeld aan afschermingen met spanningsloze contacten) bestond er hiervoor geen specifieke definitieve richtlijn, maar was het gebruikelijk om uit te gaan van een Diagnostic Coverage van 60% op voorwaarde dat de schakelaars op gepaste tijden afzonderlijk worden getest om eventuele fouten aan het licht te brengen. Als te voorzien was dat een of meerdere schakelaars nooit afzonderlijk zou worden getest, zou gesteld kunnen worden dat de Diagnostic Coverage als nul beschouwd moet worden. ISO TR 24119 voorziet in een gedetailleerde richtlijn voor de bepaling van Diagnostic Coverage voor deurvergrendelingsvoorzieningen die gebruikmaken van seriegeschakelde spanningsloze contacten. De volgende tabel biedt een basaal overzicht. Het is van wezenlijk belang om het document volledig te bestuderen om de feitelijke maximaal toegestane Diagnostic Coverage voor een bepaalde architectuur en toepassing vast te stellen.

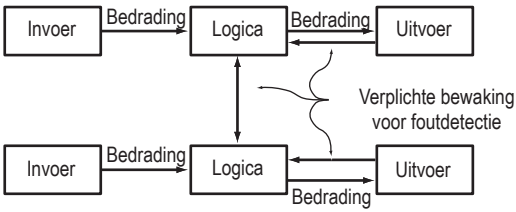
Aantal veelgebruikte beweegbare afschermingen[1]	Aantal aanvullende beweegbare afschermingen	Maskeringswaarschijnlijkheid	Diagnostic Coverage	Maximaal realiseerbare PL
0	2 tot 4	Laag	Gemiddeld	PL d
	5 tot 30	Gemiddeld	Laag	PL d
	>30	Hoog	Geen	PL c
1	1	Laag	Gemiddeld	PL d
	2 tot 4	Gemiddeld	Laag	PL d
	≥5	Hoog	Geen	PL c
>1	--	Hoog	Geen	PL c

[1] Schakelingsfrequentie meer dan eenmaal per uur

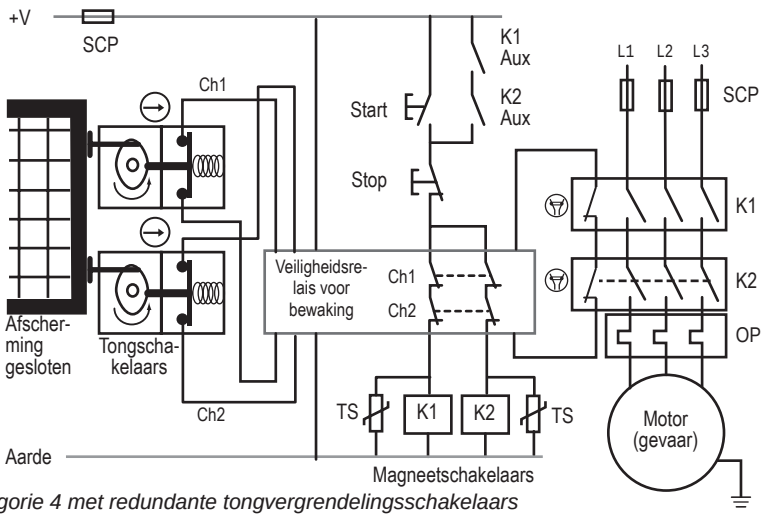
De serieschakeling van elektromechanische contacten is beperkt tot maximaal PLd. In sommige gevallen kan dit worden beperkt tot maximaal PLc. Als in elk geval te voorzien valt dat er foutmaskering zal optreden (er zullen bijv. meerdere beweegbare afschermingen tegelijkertijd geopend zijn als onderdeel van normale werking of normaal bedrijf), is de Diagnostic Coverage beperkt tot nul.
Het is opvallend dat deze kenmerken van een categorie 3-structuur altijd al aandacht hebben gevraagd, maar dat ze door de normen inzake functionele veiligheid sterk aan belang hebben gewonnen.

Categorie 4

Evenals categorie 3 vereist categorie 4 dat het veiligheidssysteem voldoet aan de eisen van categorie B, dat het gebruikmaakt van beproefde veiligheidsprincipes en dat het de veiligheidsfunctie uitvoert indien er één fout optreedt. In tegenstelling tot categorie 3, waarbij een opeenstapeling van fouten kan resulteren in het uitvallen van de veiligheidsfunctie, vereist categorie 4 dat de veiligheidsfunctie wordt gehandhaafd wanneer er een opeenstapeling van fouten optreedt. In de praktijk wordt dit gewoonlijk gerealiseerd door een hoog niveau van diagnostiek om ervoor te zorgen dat alle relevante fouten worden gedetecteerd voordat er een opeenhoping kan ontstaan. Bij het in aanmerking nemen van een theoretische opeenstapeling van fouten kunnen twee fouten voldoende zijn, hoewel er bij sommige ontwerpen drie fouten nodig kunnen zijn.

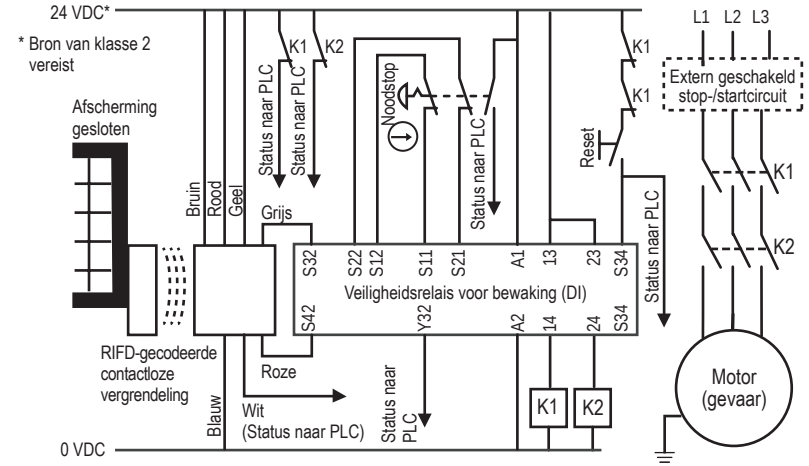


Deze afbeelding toont het blokdiagram voor categorie 4. Bewaking van beide uitvoerapparaten en onderlinge bewaking zijn vereist. Categorie 4 heeft een hogere Diagnostic Coverage dan categorie 3.



Categorie 4 met redundante tongvergrendelingsschakelaars

Tot relatief kort geleden werd overwogen om enkele, met een tong bediende vergrendelingsschakelaars met twee elektrische kanalen te gebruiken in categorie 4 circuits. Om in een tweekanaals circuit gebruik te kunnen maken van een enkele tongvergrendeling, is het nodig om de mogelijke enkele-foutpunten op de mechanische bedieningstong en de schakelaarverbindingen uit te sluiten. Het Joint Technical Report (Gezamenlijk technisch rapport) ISO TR 23849 heeft echter duidelijk gemaakt dat dit type foutuitsluiting niet mag worden gebruikt in PLe- of SIL 3-systemen. Als de ontwerper van het veiligheidssysteem het gebruik van tongvergrendelingen prefereert, dan kunnen er twee afzonderlijke schakelaars worden gebruikt om te voldoen aan de eisen van categorie 4.



Categorie 4 met RFID-geactiveerde elektronische contactloze vergrendeling

Moderne technologie kent een andere benadering om een categorie 4-architectuur (en PLe/SIL 3) te realiseren. Het gebruik van complexe elektronica heeft de kostenbesparende integratie van fouttolerantie en een hoge mate van Diagnostic Coverage in één apparaat mogelijk gemaakt. De afgebeelde vergrendelingsvoorziening voldoet niet alleen aan categorie 4, maar biedt tevens een zeer hoge mate van weerstand tegen sabotage (omzeiling) door het gebruik van RFID-codering. Deze voorziening kan ook in serie worden aangesloten op andere, soortgelijke voorzieningen zonder verlaging van categorie of Diagnostic Coverage.

PL (prestatieniveau) voor kwalificaties van onderdelen en systemen

De speciale architecturen (categorieën) van (EN) ISO 13849 kunnen worden gebruikt als onderdeel van PL-kwalificaties van veiligheidscomponenten (-voorzieningen) evenals PL-kwalificaties van systemen. Dit kan leiden tot een bepaalde mate van verwarring. Deze situatie kan worden opgehelderd door een begrip van de componenten en hun mogelijkheden. Als we de voorgaande voorbeelden bestuderen zien we dat een onderdeel zoals een vergrendelingsschakelaar die aan de vereisten voor categorie 1 voldoet, op zichzelf kan worden gebruikt in een categorie 1-systeem.
Bovendien kan het deel uitmaken van een categorie 3- of een categorie 4-systeem als twee van de componenten gezamenlijk gebruikt worden in combinatie met een diagnostische functie die uitgevoerd wordt door een veiligheidsrelais.

Bepaalde componenten, zoals veiligheidsrelais en programmeerbare veiligheidscontrollers, hebben hun eigen interne diagnostiek en controleren zichzelf op een correcte werking. Daarom kunnen ze gewaardeerd worden als veiligheidscomponenten die zonder aanvullende maatregelen voldoen aan categorie 2, 3 of 4.

Foutoverwegingen en -uitzonderingen

Voor de veiligheidsanalyse is een uitgebreide analyse van fouten vereist, alsmede een diepgaand begrip van de prestatie van het veiligheidssysteem indien er fouten optreden. ISO 13849-1 en ISO 13849-2 bieden nadere informatie over foutoverwegingen en -uitzonderingen.

Als een fout leidt tot een storing van een volgend onderdeel, worden de eerste fout en alle daaropvolgende fouten als een enkele fout beschouwd.

Als er twee of meer fouten optreden als gevolg van een en dezelfde oorzaak, worden de fouten als één fout beschouwd. Dit staat bekend als een fout met een gemeenschappelijke oorzaak.

Het tegelijkertijd optreden van twee of meer onafhankelijke fouten wordt als zeer onwaarschijnlijk gezien, en wordt in deze analyse buiten beschouwing gelaten.

Foutuitsluitingen

(EN) ISO 13849-1 en IEC 62061 staan het gebruik van foutuitsluitingen toe bij het vaststellen van de classificatie van een veiligheidssystemen, indien kan worden aangetoond dat het optreden van de fout uiterst onwaarschijnlijk is. Het is belangrijk dat foutuitsluitingen goed worden gemotiveerd en geldig zijn voor de bedoelde levensduur van het veiligheidssysteem. Hoe hoger het risiconiveau dat door het veiligheidssysteem wordt afgedekt, des te strenger de eisen die worden gesteld aan de motivering van de foutuitsluiting. Dit heeft altijd tot enige verwarring geleid over het wanneer wel en het wanneer niet gebruiken van bepaalde typen foutuitsluiting. Zoals we eerder in dit hoofdstuk hebben gezien, maken nieuwe normen en richtlijnen bepaalde aspecten van deze kwestie duidelijk.

Als er PLe of SIL3 wordt voorgeschreven voor een veiligheidsfunctie die door een veiligheidssysteem wordt geïmplementeerd, maakt ISO TR 23849 duidelijk dat het niet normaal is om op foutuitsluitingen te vertrouwen om dit prestatieniveau te realiseren. Dit is afhankelijk van de gebruikte technologie en de bedoelde werkomgeving. Het is daarom van essentieel belang dat de ontwerper extra aandacht besteedt aan het gebruik van foutuitsluitingen zodat het PL of SIL toeneemt. Foutuitsluiting is bijvoorbeeld niet van toepassing op de mechanische aspecten van elektromechanische positieschakelaars en handmatig bediende schakelaars (bijv. een noodstopvoorziening) om een PLe- of SIL3-systeem te realiseren. De foutuitsluitingen die toegepast kunnen worden op specifieke mechanische storingscondities (bijv. slijtage/corrosie, breuken) worden omschreven in tabel A.4 van ISO 13849-2. Een deurvergrendelingssysteem dat dient te voldoen aan PLe, moet daarom een minimale fouttolerantie van SIL3 1 (d.w.z. twee conventionele mechanische positieschakelaars) hebben om dit Performance Level te halen. Normaal gesproken kan namelijk op geen enkele wijze gemotiveerd worden dat fouten zoals gebroken schakelactuators uitgesloten worden. Het kan echter acceptabel zijn storingen uit te sluiten zoals kortsluiting in de bedrading van een bedieningspaneel dat ontworpen is in overeenstemming met de toepasselijke normen.

Stopcategorieën volgens IEC/EN 60204-1 en NFPA 79

Het is zowel ongelukkig als verwarrend dat de term “categorie” in het kader van veiligheidsgerelateerde besturingssystemen verschillende betekenissen heeft. Tot dusverre hebben we de categorieën uit EN 954-1 besproken. Deze vormen een classificatie van de prestaties van een veiligheidssysteem onder storingscondities.

Er is ook een classificatie die bekend staat als “stopcategorieën”. Deze vinden hun oorsprong in IEC/EN 60204-1 en NFPA 79. Er zijn drie stopcategorieën.

Stopcategorie 0 vereist dat de voeding naar de actuators onmiddellijk onderbroken wordt. Dit wordt soms opgevat als een ongecontroleerde stopzetting, omdat het in bepaalde omstandigheden enige tijd kan duren voordat de motor is uitgelopen en de beweging tot stilstand is gekomen.

Stopcategorie 1 vereist dat de voeding behouden blijft voor de remactie totdat de stopzetting is gerealiseerd, en onderbreekt vervolgens de voeding naar de actuator. Opmerking: Zie IEC 60204-1 voor informatie over stopcategorieën 1a en 1b.

Bij **Stopcategorie 2** is een gecontroleerde stopzetting waarbij er nog steeds stroom beschikbaar is voor de actuators van de machine. Een normale productiestop wordt beschouwd als stopzetting van categorie 2.

Alleen stopcategorieën 0 of 1 kunnen als noodstop gebruikt worden. Welke van beide categorieën gebruikt moet worden, moet vastgesteld worden op basis van een risicoanalyse.

Alle voorbeelden van circuits die tot nu toe in dit hoofdstuk zijn gegeven, maken gebruik van stopcategorie 0. Stopcategorie 1 wordt bewerkstelligd door met een tijdvertraagde uitgang de voeding definitief te onderbreken. Vaak zijn categorie 1-stopsystemen uitgerust met een vergrendelde afscherming. Op deze manier wordt de afscherming in een gesloten positie vergrendeld totdat de machine een veilige (d.w.z. gestopte) toestand heeft bereikt.

Het stopzetten van een machine zonder voldoende rekening te houden met de programmeerbare controller kan van invloed zijn op het opnieuw starten van de machine, en kan schade aan gereedschap of de machine tot gevolg hebben. Voor een veiligheidsgerelateerde stoptaak kan niet worden voldaan met een standaard (niet-veiligheids-)PLC. Om deze reden dienen er andere methoden te worden overwogen. Hieronder worden twee mogelijke oplossingen voor stopzettingen van categorie 1 gegeven:

1. Veiligheidsrelais met een tijdvertraagde uitschakelopdracht

Er wordt gebruikgemaakt van een veiligheidsrelais met zowel direct werkende als vertraagd werkende uitgangen. De direct werkende uitgangen zijn verbonden met ingangen op het programmeerbare apparaat (bijvoorbeeld PLC of de “inschakeling” van de aandrijving). De uitgangen met een vertraagde werking zijn op een hoofdmagneetschakelaar aangesloten. Wanneer de vergrendelingsschakelaar van de afscherming wordt geactiveerd, zullen de directe uitgangen op het veiligheidsrelais omschakelen. Hierdoor ontvangt het programmeerbare systeem het signaal om op de juiste wijze een stopzetting uit te voeren. Nadat er korte maar voldoende tijd is verstreken om dit proces te laten uitvoeren, zal de vertraagde uitgang

op het veiligheidsrelais omschakelen en de stroom naar de hoofdmagneetschakelaar onderbreken.

Opmerking: Elke berekening van de algehele stoptijd dient rekening te houden met de vertragingsperiode van de uitgang van het veiligheidsrelais. Dit is met name van belang wanneer deze factor wordt gebruikt om de plaatsing van de voorzieningen op basis van een berekening van de veiligheidsafstand vast te stellen.

2. Veiligheids-PLC's

De vereiste logica- en timingsfuncties kunnen makkelijk worden geïmplementeerd door gebruik te maken van een veiligheids-PLC zoals GuardLogix.

Amerikaanse vereisen voor veiligheidsbesturingssystemen

Control Reliable

Het hoogste niveau van risicoreductie binnen de Amerikaanse en Canadese robotnormen wordt geboden door veiligheidsgerelateerde besturingssystemen die voldoen aan de eisen van de Control Reliable-norm. Veiligheidsgerelateerde besturingssystemen die aan de Control Reliable-norm voldoen omvatten tweekanaals architecturen met bewakingsfunctionaliteit. De stopfunctie van de robot mag niet worden gehinderd door een storing van een afzonderlijk onderdeel, met inbegrip van de bewakingsfunctie.

De bewakingsfunctie dient een stopopdracht te geven indien er een fout wordt gedetecteerd. Als een gevaarlijke toestand in stand blijft nadat de beweging is gestopt, dient er een waarschuwingssignaal te worden gegeven. Het veiligheidssysteem moet in een veilige toestand blijven totdat de fout is verholpen. De fout dient bij voorkeur op het moment van de storing te worden gedetecteerd. Als dit niet mogelijk is, dient de fout te worden gedetecteerd wanneer er opnieuw een beroep op het veiligheidssysteem wordt gedaan. Er dient rekening te worden gehouden met vaak voorkomende storingen van modi indien er een aanzienlijke kans bestaat dat een dergelijke storing optreedt.

De Canadese normen verschillen van de Amerikaanse normen in die zin dat er nog twee extra eisen worden voorgeschreven. Ten eerste moeten de veiligheidsgerelateerde besturingssystemen onafhankelijk functioneren van de normale programmabesturingssystemen. Ten tweede mag het veiligheidssysteem niet op eenvoudige wijze kunnen worden gesaboteerd of omzeild zonder dat dit wordt gedetecteerd.

Opmerkingen over Control Reliable

Het meest fundamentele aspect van Control Reliable is tolerantie van enkele fouten en bewaking (foutdetectie). De eisen geven aan hoe het veiligheidssysteem dient te reageren indien er "één storing", "om het even welke storing" of "om het even welke storing van een onderdeel" optreedt.

Met betrekking tot storingen dienen drie uiterst belangrijke concepten in aanmerking te worden genomen: (1) niet alle fouten worden gedetecteerd, (2) het toevoegen van het

woord “onderdeel” leidt tot vragen over bedrading, en (3) bedrading vormt een integraal deel van het veiligheidssysteem. Bedradingsfouten kunnen resulteren in het uitvallen van de veiligheidsfunctie.

Control Reliability heeft ten doel om de werking van de veiligheidsfunctie te garanderen indien er een storing optreedt. Als de storing wordt gedetecteerd, dient het veiligheids-systeem een veilige actie uit te voeren, de storing te melden en verdere bediening van de machine te voorkomen totdat de storing is verholpen. Als de storing niet wordt gede-tecteerd, dient de veiligheidsfunctie nog steeds op aanvraag te worden uitgevoerd.

Hoofdstuk 10: Toepassingsvoorbeelden

Overzicht – kant-en-klare veiligheidsfuncties voor machines

Een machineveiligheidsfunctie – of dit nu een noodstop-, beschermings- of aanwezigheidsdetectiefunctie is – vereist meerdere elementen, met inbegrip van een sensor of invoerapparaat, een logisch apparaat en een uitvoerapparaat. Samen voorzien deze elementen in een beschermingsniveau dat wordt berekend aan de hand van een prestatieniveau zoals beschreven in (EN) ISO 13849-1.

In dit hoofdstuk hebben we een van de vele kant-en-klare veiligheidsfuncties voor machines geselecteerd, die door Rockwell Automation zijn ontwikkeld. Deze veiligheidsfunctiedocumenten voorzien elk in een leidraad voor een specifieke veiligheidsfunctie op basis van functionele eisen, apparatuurselectie en prestatieniveau-eisen, met inbegrip van installatie en bedrading, configuratie, verificatie- en valideringsplan en berekening van prestatieniveau.

De kant-en-klare veiligheidsfuncties zijn gratis en zijn beschikbaar om te downloaden op de website van Rockwell Automation.

www.rockwellautomation.com, onder Solutions & Services > Safety Solutions.

De volgende kant-en-klare veiligheidsfunctie is gebaseerd op een vergrendelings-schakelaar voor deurbewaking met een configureerbaar veiligheidsrelais. De gebruikte producten zijn: RFID-gecodeerde, contactloze SensaGuard-veiligheidsvergrendelings-schakelaar die is verbonden met een configureerbaar veiligheidsrelais van het type Guardmaster 440C-CR30. De gebruikte uitvoerapparaten zijn veiligheidsmagneet-schakelaars van het type 100S-C.
De veiligheidsbeoordeling die door deze kant-en-klare veiligheidsfunctie wordt behaald, is: CAT. 4, PLe volgens (EN) ISO 13849-1.

Het publicatienummer van het oorspronkelijke document is: SAFETY-AT133C-EN-P

Beschrijving van functionele veiligheid

Het personeel is tegen de gevaarlijke beweging beveiligd door een vaste afscherming. Toegang tot het gevaarlijke gebied geschiedt, indien nodig, via een klapdeur. De deur

wordt bewaakt door een contactloze SensaGuard-vergrendeling. Deze is verbonden met ingangen van het configureerbare veiligheidsrelais van het type 440C-CR30. Het relais 440C-CR30 stuurt twee veiligheidsmagneetschakelaars van het type 100S-C aan, die, in serie geschakeld, de voeding regelen naar de motor die de gevaarlijke beweging aandrijft. Wanneer deze bewaakte deur wordt geopend, onderbreekt het veiligheidssysteem de stroomtoevoer naar de motor. De motor en de gevaarlijke beweging die door de motor wordt aangedreven, lopen uit tot stilstand (stopcategorie 0). De motor kan niet worden herstart zolang de bewaakte deur is geopend. Zodra de deur is gesloten, kan de motor opnieuw worden gestart door de resetknop in te drukken en los te laten om het relais 440C-CR30 te resetten. Vervolgens wordt de externe start geïnitieerd om de stroomtoevoer naar de motor te herstellen, die wordt geregeld door de 100S-C-magneetschakelaars.

De SensaGuard-schakelaar bewaakt de status (geopend of gesloten) van de deur. De SensaGuard-schakelaar bewaakt ook zijn twee OSSD-uitgangen op fouten. Het relais 440C-CR30 bewaakt de ingangen van de SensaGuard-schakelaar op fouten en bewaakt tevens de status van de reset- en feedbacksignalen vanaf de 100S-C-magneetschakelaars. Het relais bewaakt tevens zijn eigen uitgangen op fouten. Deze uitgangen sturen de 100S-C-magneetschakelaars. Het relais 440C-CR30 schakelt zijn uitgangen uit en onderbreekt de stroomtoevoer naar de motor wanneer er een fout wordt gedetecteerd. Er vindt geen reset plaats voordat de betreffende fout is verholpen.

Stuklijst

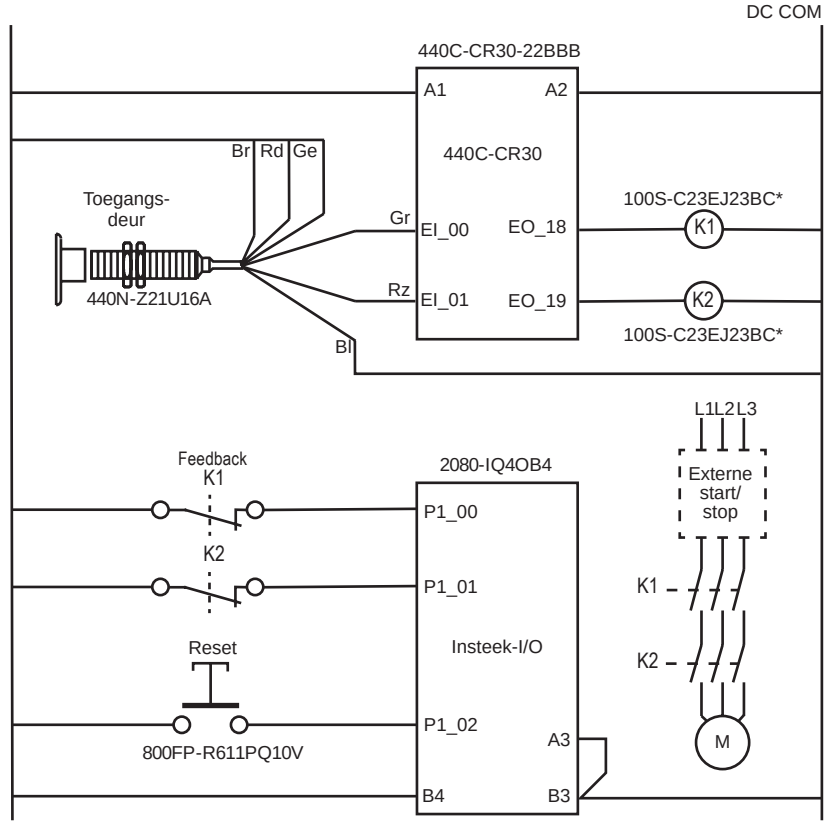
Deze toepassing maakt gebruik van deze producten.

Catalogusnummer	Beschrijving	Aantal
440N-Z21S16B	SensaGuard-schakelaar, 18 mm kunststof, 2 x PNP, 0,2 A max., veiligheidsuitgang, 10 m kabel	1
800FP-R611	800F reset, rond kunststof (type 4/4X/13, IP66), blauw, R, standaardpakket	1
2080-IQ4OB4	4-kanaals digitale invoer-/uitvoercombinatiemodule	1
1761-CBL-PM02	Kabel; configureerbaar veiligheidsrelais 440C-CR30 naar pc, printerkabel	1
440C-CR30-22BBB	Via software geconfigureerd veiligheidsrelais van het type Guardmaster 440C-CR30, PLe SIL 3, 22 veiligheids-I/O, geïntegreerde seriële poort, USB-programmeerpoort, 2 insteeksleuven, 24,0 VDC	1
100S-C23EJ23BC	MCS 100S-C-veiligheidsmagneetschakelaar, 23 A, 24 VDC (met elektrische spoel), gevorkt contact	2

Systeemoverzicht

De SensaGuard-vergrendelingsschakelaar wordt gebruikt om te bevestigen dat de beschermde deur zich in de veilige en gesloten toestand bevindt. De gevaarlijke

beweging wordt gestopt of voorkomen wanneer deze deur niet is gesloten. Naast het bewaken van de status van de beschermde deur, bewaakt de SensaGuard-schakelaar zijn uitgangen op alle foutcondities. Het configureerbare veiligheidsrelais 440C-CR30 detecteert ook een open-draadfout, een enkelkanaalsfout of een kortsluiting naar 0 V op zijn SensaGuard-schakelaaringangen.
Het configureerbare veiligheidsrelais 440C-CR30 bewaakt de pulsgeteste uitgangen die de spoelen van de veiligheidsschakelaar aansturen, op alle foutcondities. De juiste, veilige toestand van de veiligheidsmagneetschakelaars K1 en K2 wordt bevestigd door het configureerbare veiligheidsrelais 440C-CR30 dat de feedbacksignalen op SMF2 bewaakt bij het opstarten.



**ISO 13849-2 vereist bescherming tegen overspanning over de belasting als basisveiligheidsprincipe. De elektronische spoel 'EJ' biedt geschikte bescherming.*

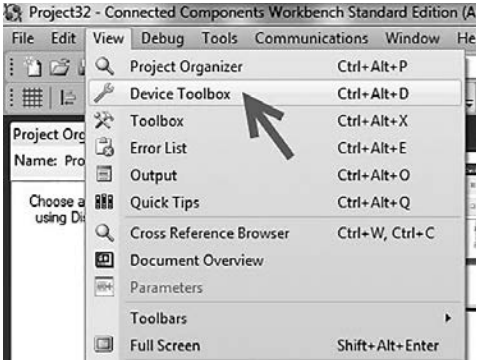
Configuratie

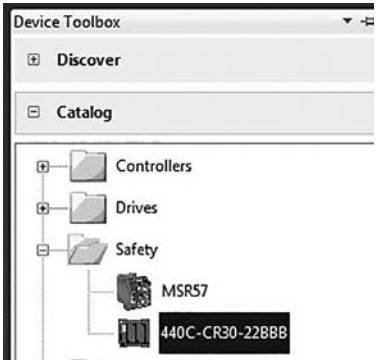
Het relais 440C-CR30 wordt geconfigureerd door gebruik te maken van Connected Components Workbench™-software, versie 6.01 of hoger. Een gedetailleerde beschrijving van elke stap valt buiten het bestek van dit document. Kennis van de Connected Components Workbench-software wordt verondersteld.

Configureren van het relais 440C-CR30

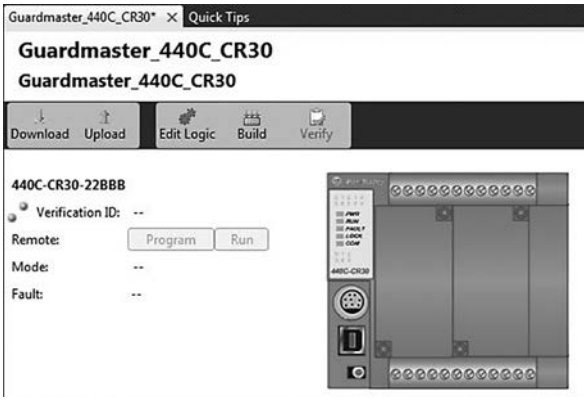
Volg deze stappen voor het configureren van het Guardmaster-relais 440C-CR30 in Connected Components Workbench-software.

1. Kies In Connected Components Workbench-software de optie View en vervolgens Device Toolbox. Selecteer in Device Toolbox de optie 440C-CR30-22BBB.

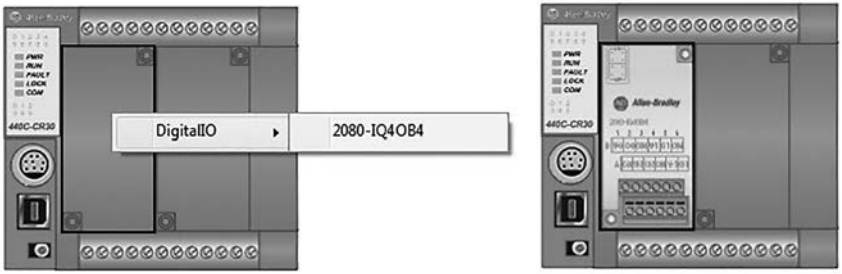




2. Dubbelklik in de Project Organizer op Guardmaster_400C_CR30 *.

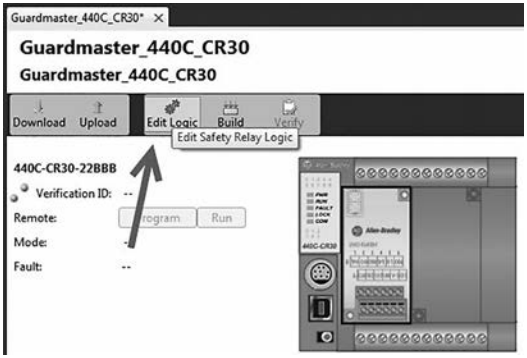


3. Om de insteek-I/O-module toe te voegen die voor dit circuit benodigd is, klikt u met de rechtermuisknop op de ruimte van de linkerinsteekmodule en kiest u de module 2080-IQ4OB4.

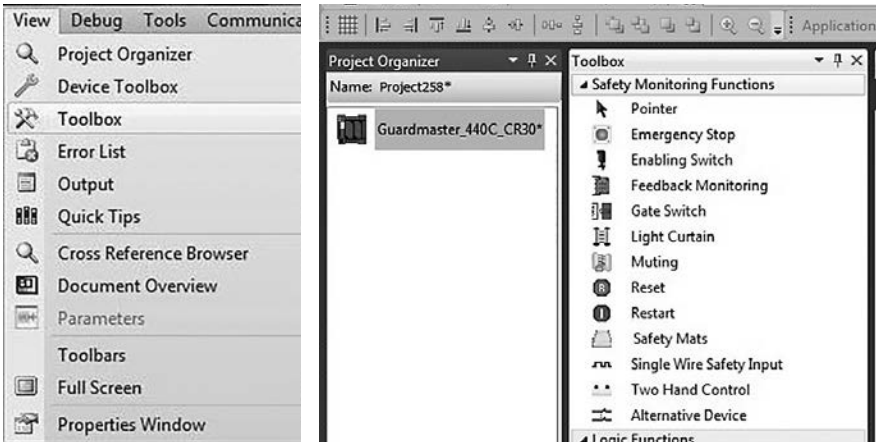


TIP: De I/O-module wordt standaardgrijs weergegeven omdat het geen veiligheids-I/O-module is. Dat is toegestaan in deze toepassing omdat deze niet wordt gebruikt voor het aansluiten van veiligheidssignalen. Ingangen zoals de knoppen Feedback en Reset worden niet beschouwd als pure veiligheidssignalen. Het gebruik van de standaard-I/O voor deze niet-veiligheidssignalen kan het beperkte aantal veiligheidsingangen en -uitgangen reserveren voor werkelijke veiligheidssignalen.

4. Klik op de knop Edit Logic om te werkruimte van Connected Components Workbench te openen. Er wordt een lege werkruimte weergegeven.



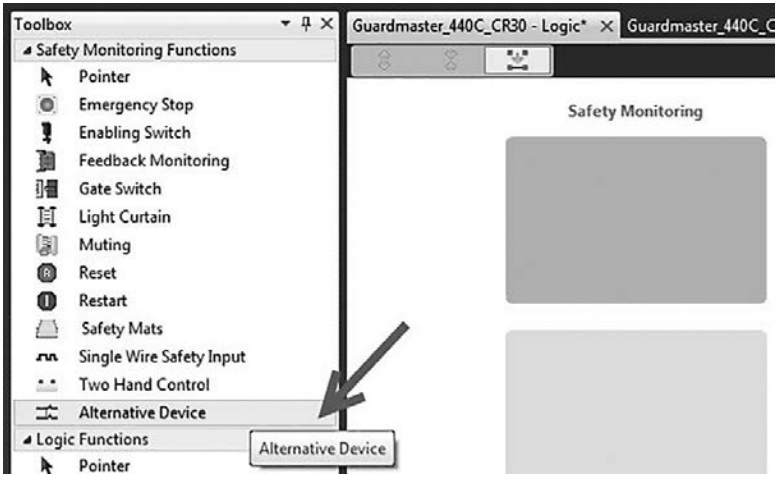
5. Kies in het vervolgkeuzemenu View de optie Toolbox. De Toolbox wordt weergegeven.



Configureren van de ingangen

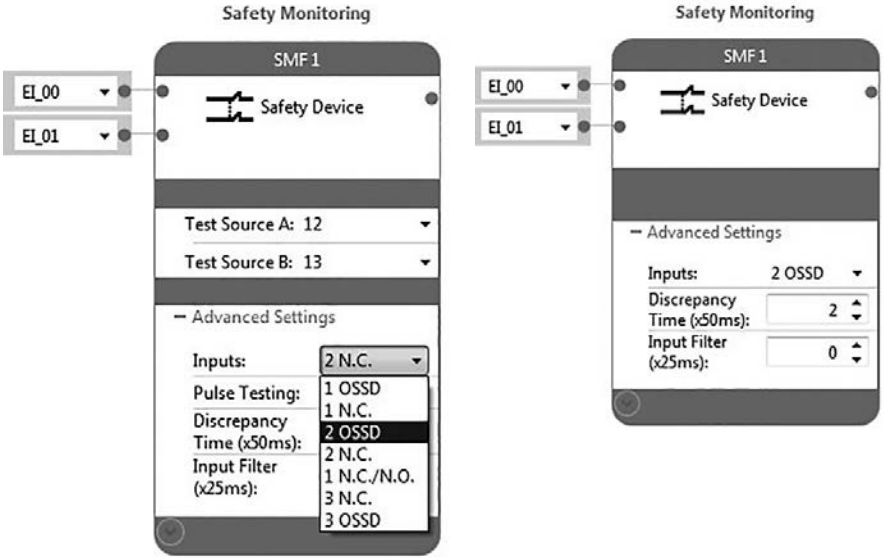
De Toolbox vermeldt geen SensaGuard Safety Monitoring Function. Volg deze stappen om een dergelijke functie te configureren.

1. Selecteer Alternative Device. Sleep dit naar het groene blok in de kolom Safety Monitoring en zet het neer.

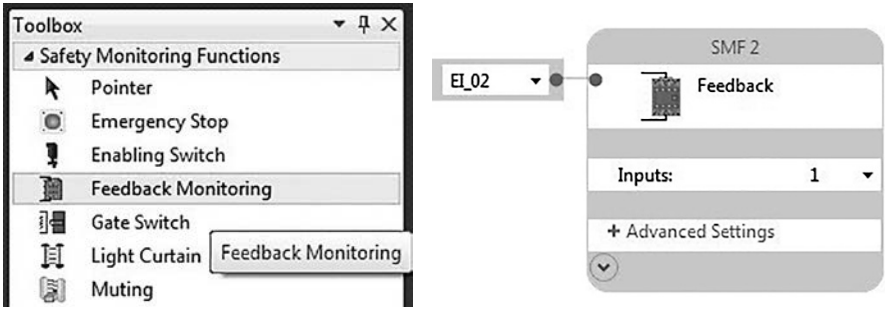


De Connected Components Workbench-software wijst de eerste twee beschikbare ingangen,EI_00 en EI_01, automatisch toe aan het apparaat. Laat deze toegewezen zijn. De Connected Components Workbench-software wijst automatisch de functienaam SMF 1 toe aan dit blok. De software gaat automatisch uit van een elektromechanisch apparaat en wijst Test Sources toe. De SensaGuard-schakelaar heeft twee OSSD-uitgangen en heeft geen Test Sources nodig.

2. Om het blok goed te configureren, opent u Advanced Settings en selecteert u 2 OSSD in het vervolgkeuzemenu Inputs. Het resulterende blok wordt weergegeven zoals getoond.

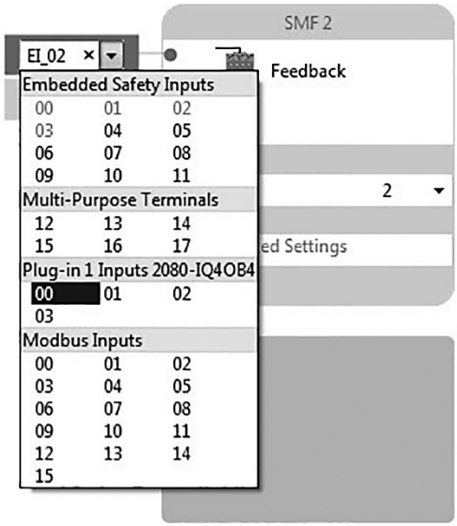


3. Klik op de Safety Monitoring-functie Feedback Monitoring, sleep deze naar het blok Safety Monitoring onder het blok SensaGuard in de werkruimte en zet deze neer.

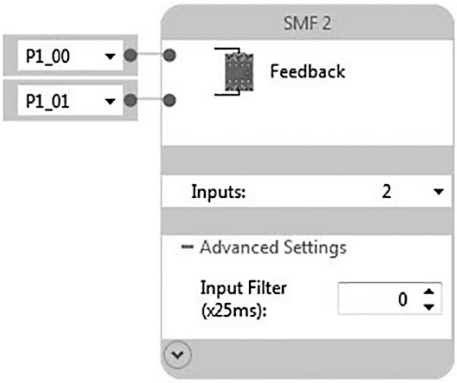


U ziet dat de Connected Components Workbench-software dit toewijst aan ingangsaansluiting EI_02, de eerst beschikbare Safety Input-aansluiting. De software gaat er vanuit dat dit een enkele ingang is en wijst automatisch de functienaam SMF 2 toe aan dit blok.

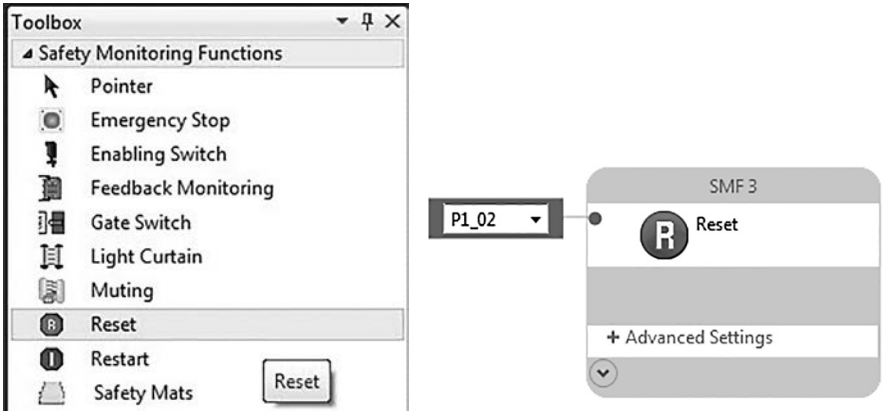
4. Omdat het circuit twee ingangen vereist, één van elke magneetschakelaar, wijzigt u het aantal ingangen naar 2, één voor het N.C.-contact van elke 100S-magneetschakelaar.



5. Wijs de ingangen toe aan Plug-In-aansluitingen PI_00 en PI_01. Dit voorkomt het onnodig gebruik van Safety Inputs voor feedbacksignalen.



6. Klik op de Safety Monitoring-functie Reset, sleep deze naar het blok Safety Monitoring onder het blok Feedback Monitoring in de werkruimte en zet deze neer.

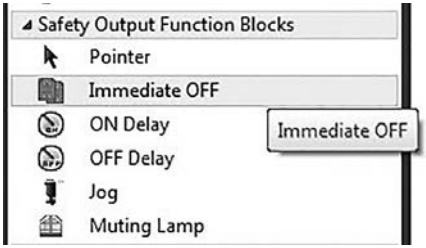


De Connected Components Workbench-software wijst automatisch de functienaam SMF 3 toe aan dit blok. Wijs de Reset-ingang opnieuw toe aan Plug-In-aansluiting PI_02.

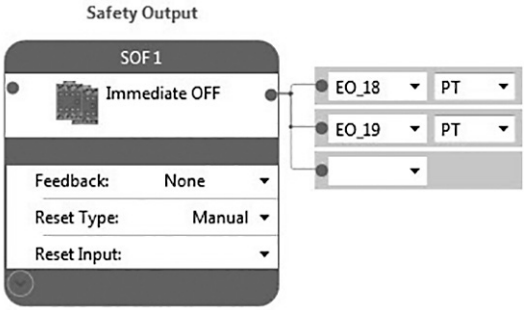
Configureren van de uitgangen

Volg deze stappen voor het configureren van de uitgangen.

1. Klik op Immediate OFF en sleep dit vanuit het gedeelte Safety Output Function Blocks van de Toolbox.

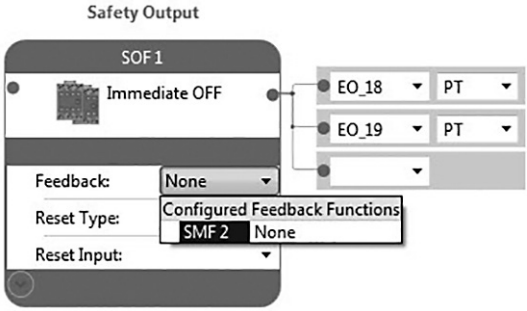


2. Zet het neer op het bovenste blok van de kolom Safety Output in de werkruimte.

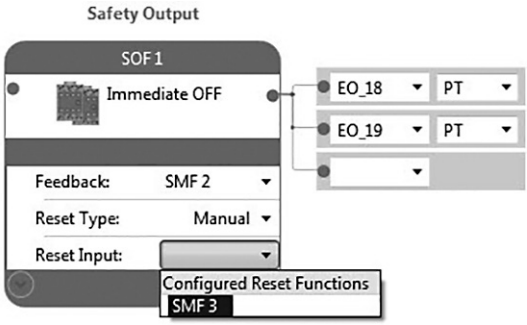


De Connected Components Workbench-software wijst automatisch uitgangsaansluitingen EO_18 en EO_19 toe. Pulse Testing is standaard voor deze aansluitingen. De standaardwaarde voor Reset Type is Manual. Laat deze instellingen op hun standaardwaarden staan.

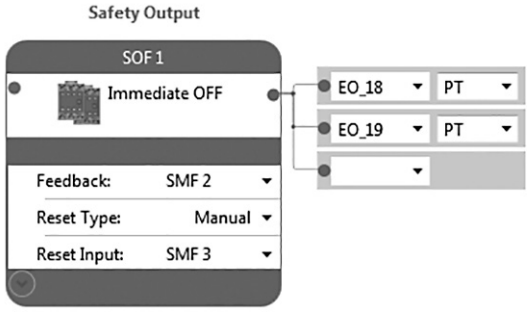
3. Kies SMF 2 in het vervolgkeuzemenu Feedback.



4. Kies SMF 3 in het vervolgkeuzemenu Reset Input.



De veiligheidsuitgangsconfiguratie is voltooid.

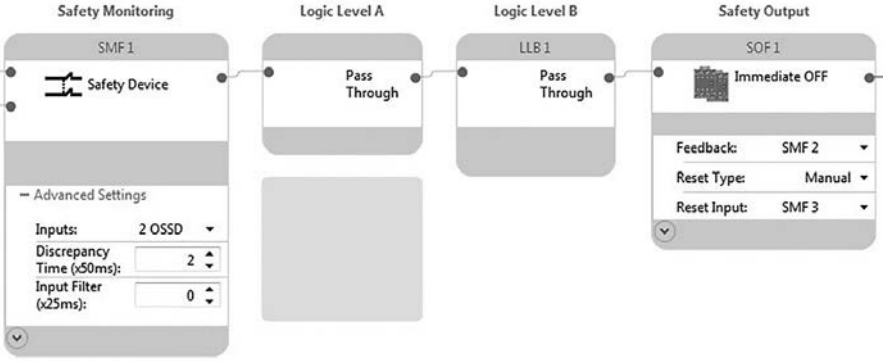


Configureren van de logica

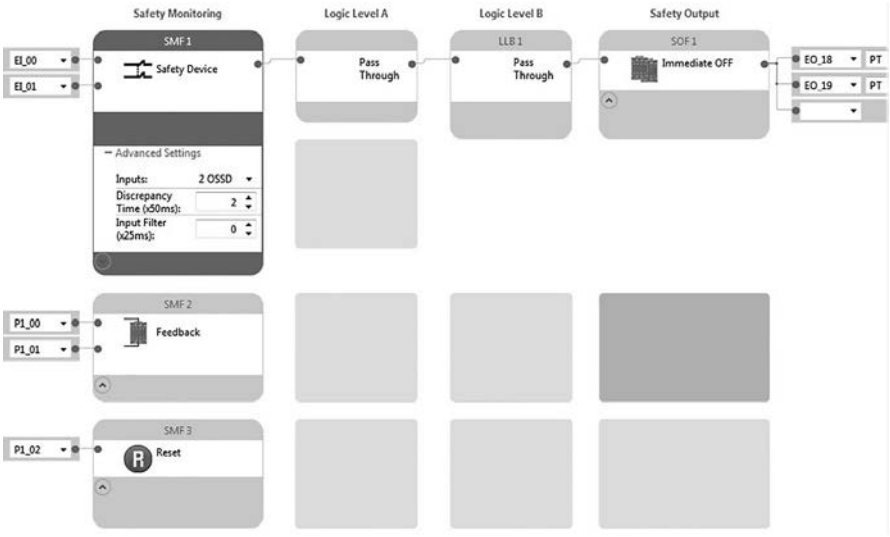
De sectie Logica bepaalt hoe de veiligheidsuitgangen reageren op de veiligheidsbewakingsingangen. In dit geval volgt de veiligheidsuitgang de veiligheidsbewakingsingang direct.

1. Klik op de blauwe punt aan de rechterzijde van het blok SensaGuard Safety Monitoring-ingangen. Deze punt wordt grijs.

2. Klik op de blauwe punt aan de linkerzijde van het blok Safety Output om de logica aan te sluiten.

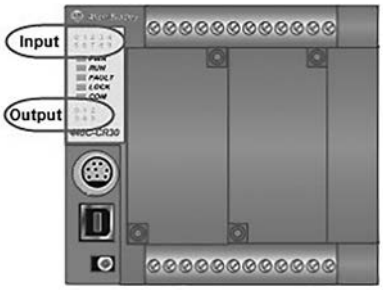


De voltooide logica zier er als volgt uit.



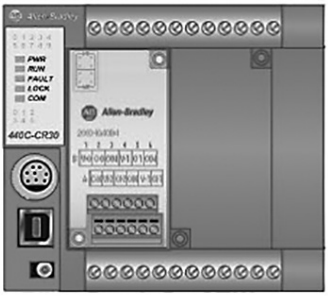
Configureren van de statusindicators

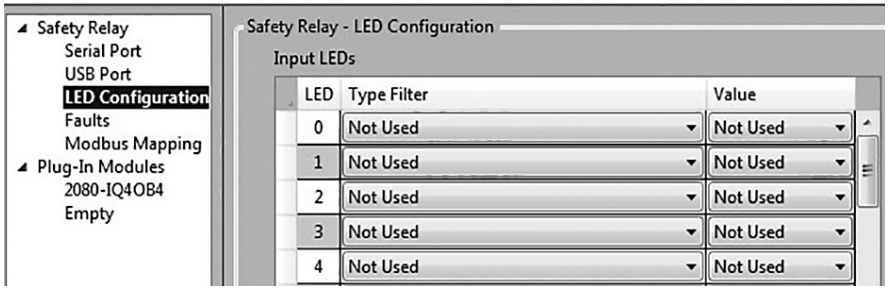
Het configureerbare veiligheidsrelais 440C-CR30 voorziet in tien door de gebruiker te configureren indicatieleds voor de ingangsstatus en zes door de gebruiker te configureren indicatieleds voor de uitgangsstatus. In veel gevallen zijn deze zeer nuttig bij de installatie, inbedrijfstelling, bewaking en probleemoplossing van een systeem met een configureerbaar veiligheidsrelais 440C-CR30. Ze hebben geen enkele invloed op de werking van het systeem en het is niet noodzakelijk om ze te configureren. Ze zijn echter gemakkelijk te configureren en het wordt aanbevolen om ze te gebruiken.



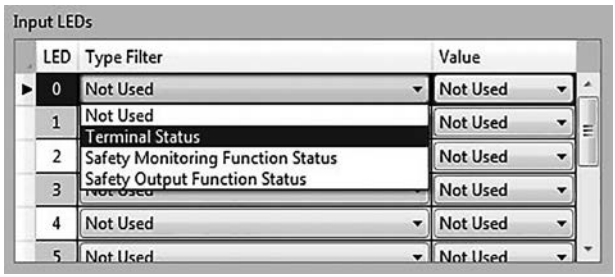
1. Klik op Guardmaster_440C_CR30*.

2. Selecteer LED Configuration.

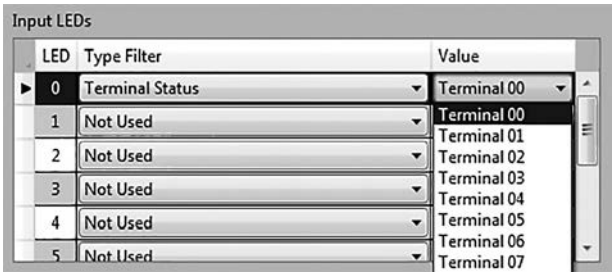




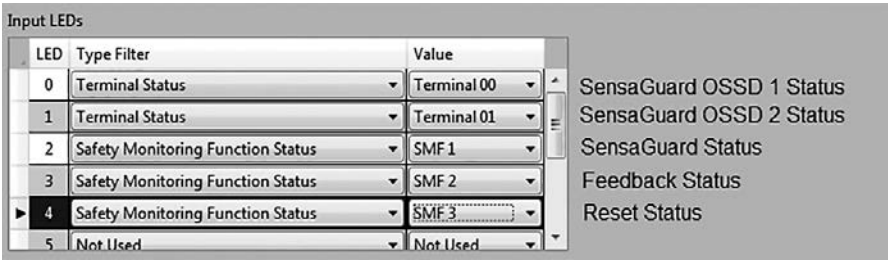
3. Kies bij Type Filter de optie Terminal Status voor LED 0.



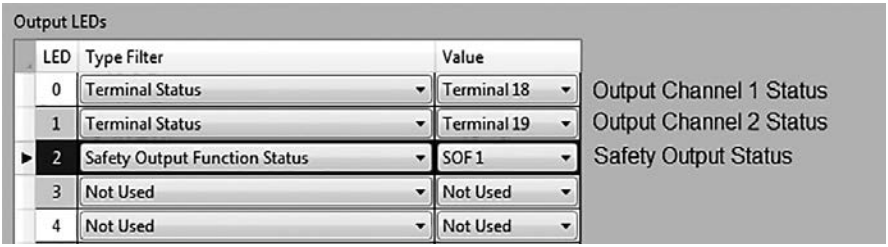
4. Kies voor LED 0 de optie Terminal 00 in het vervolgkeuzemenu Value. De statusindicator LED 0 is nu geconfigureerd om de status van terminal 00 weer te geven.



5. Wijs de volgende vier ingangsleds (1 … 4) op dezelfde manier toe. De indicatieleds voor de ingangsstatus zijn nu geconfigureerd.



6. Wijs de drie uitgangsleds als volgt toe.

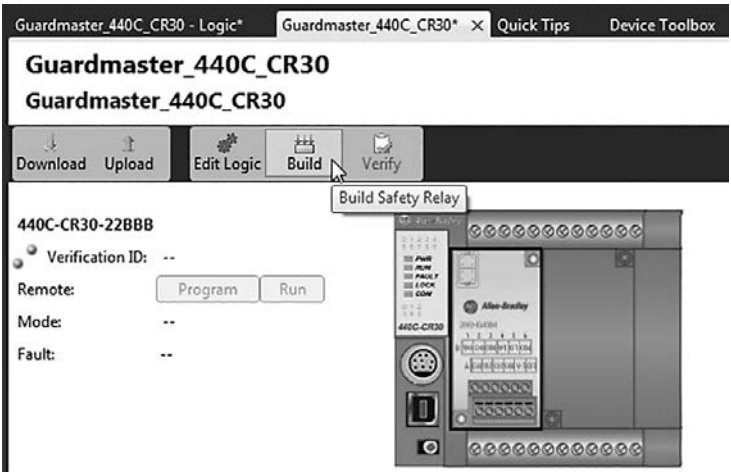


De validiteit van de build

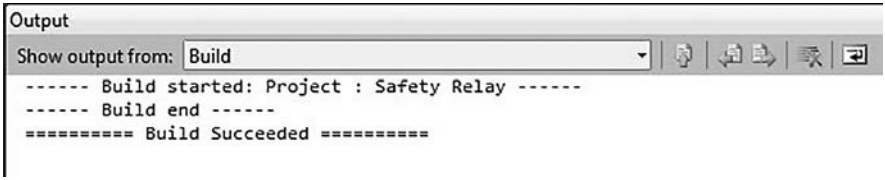
Volg deze stappen om de validiteit van de logica te bevestigen met behulp van de functie Build in de Connected Components Workbench-software.

1. Klik op Guardmaster_440C_CR30 in de balk boven de werkruimte.

2. Klik op Build.



Het bericht Build Succeeded bevestigt dat de configuratie geldig is.



Als er een fout of omissie wordt ontdekt tijdens een build, wordt een bericht weergegeven met detailinformatie over de fout zodat deze kan worden verholpen. Nadat u de fout hebt verholpen, moet u de build opnieuw uitvoeren.

Het project opslaan en downloaden

Volg deze stappen om het project op te slaan en te downloaden.

1. Kies in het menu File de optie Save as om het project op te slaan.

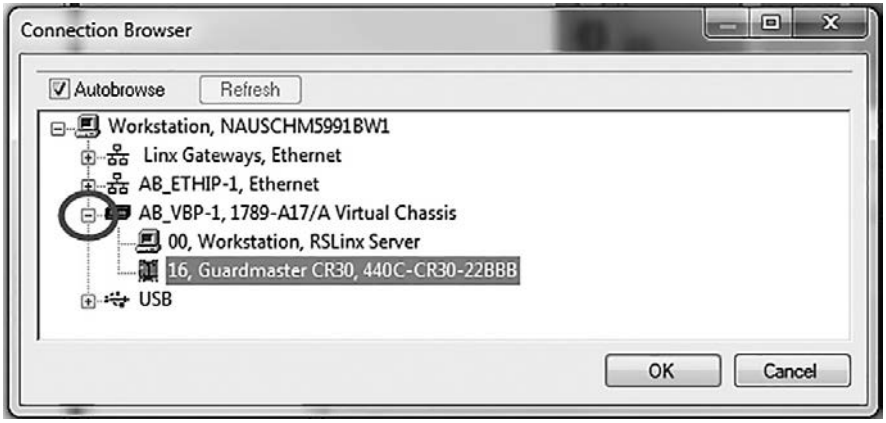
2. Dubbelklik in het venster Project Organizer op Guardmaster_440C_CR30 om de werkruimte te openen.

3. Zet spanning op het veiligheidsrelais 440C-CR30.

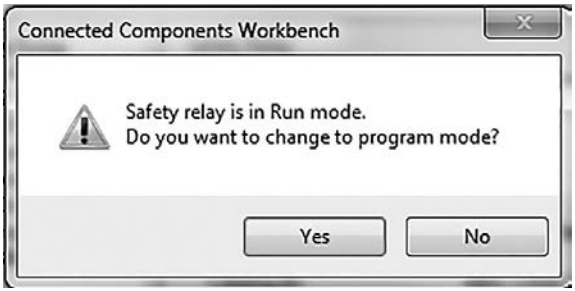
4. Verbind de USB-kabel met het relais 440C-CR30.

5. Klik op Download.

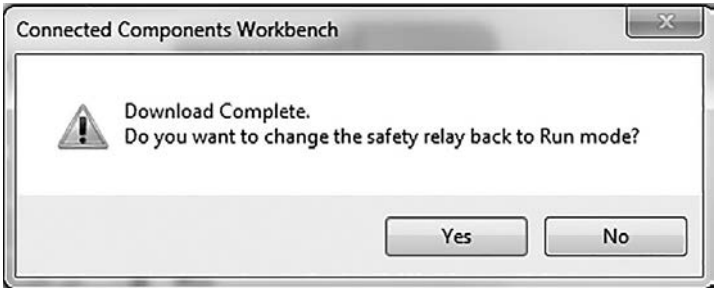
6. Breid in de Connection Browser het AB_VBP-1 Virtual Chassis uit en selecteer de Guardmaster 440C-CR30-22BBB. Klik op OK.



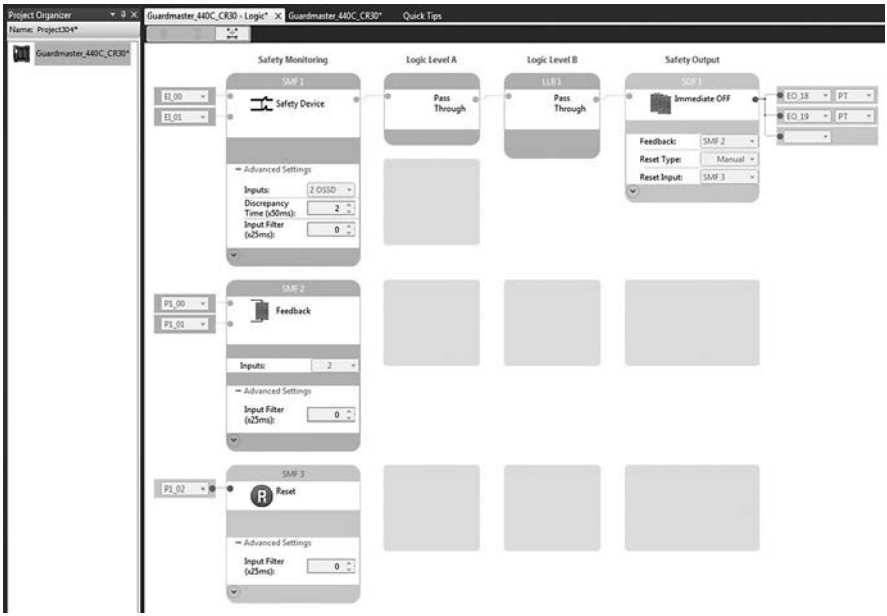
7. Klik op Yes om over te schakelen van de modus Run naar de modus Program.



8. Wanneer de download is voltooid, klikt u op Yes om over te schakelen van de modus Program naar de modus Run.



9. Klik op Edit Logic om de online diagnostiek te bekijken.

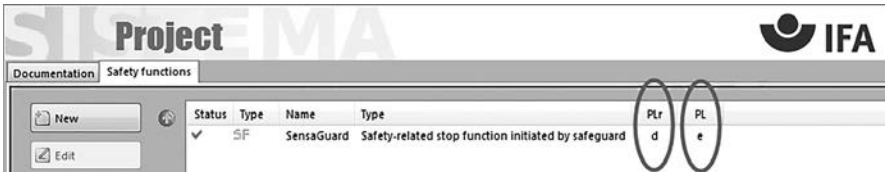


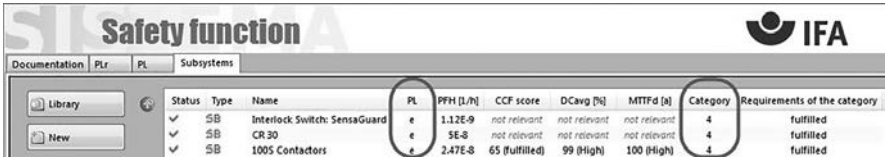
Groen geeft aan dat een blok Waar is of dat een ingangs- of uitgangsaansluiting AAN is. Knipperend groen geeft aan dat een Safety Output-functie klaar is voor Reset.
De online diagnostische modus van het relais 440C-CR30 kan zeer nuttig zijn tijdens het verificatieproces.

10. Bekijk de informatie in Berekening van het prestatieniveau (PL) en Verificatie- en validatieplan voordat u verdergaat met de verificatie van de configuratie.

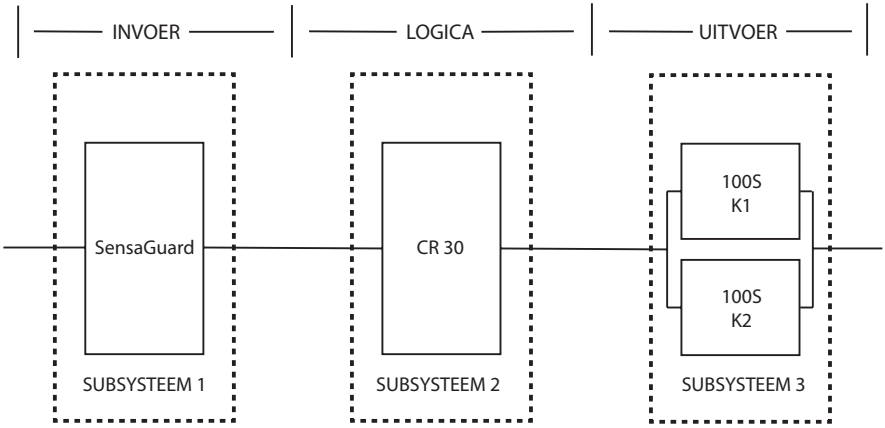
Berekening van het prestatieniveau (PL)

Wanneer deze veiligheidsgerelateerde stopfunctie goed is geïmplementeerd, kan deze een veiligheidskwalificatie krijgen van Categorie 4, Performance Level e (Cat. 4, PLe), volgens ISO 13849-1: 2008, zoals berekend met behulp van de PL-berekeningstool van de SISTEMA-software.
Het minimaal vereiste prestatieniveau (PLr) van de risicobeoordeling voor deze veiligheidsfunctie is PLd.





Deze veiligheidsgerelateerde stop die door de veiligheidsfunctie van een afscherming wordt geïnitieerd, kan als volgt worden gemodelleerd:



Omdat dit elektromagnetische apparaten zijn, bevatten de gegevens van de veiligheidsmagneetschakelaars het volgende:

- Gemiddelde tijd tot storing, gevaarlijk ($MTTF_D$)
- Diagnostic Coverage (DCavg)
- Gemeenschappelijk falen (CCF)

Evaluaties van de functionele veiligheid van elektromagnetische apparaten bevatten het volgende:

- Hoe vaak ze worden bediend
- Of ze effectief worden bewaakt op fouten
- Of ze zijn correct zijn gespecificeerd en geïnstalleerd

SISTEMA berekent de MTTFd door gebruik te maken van B10d-gegevens die voor de magneetschakelaars worden geleverd, samen met de geschatte gebruiksfrequentie die wordt ingevoerd tijdens de aanmaak van het SISTEMA-project.

De DCavg (99%) voor de magneetschakelaars is geselecteerd in de tabel Output Device van ISO 13849-1 Bijlage E, Direct Monitoring.

De CCF-waarde wordt gegenereerd door gebruik te maken van het waarderingsproces dat wordt beschreven in Bijlage F van ISO 13849-1. Het volledige CCF-waarderingsproces moet worden uitgevoerd wanneer een toepassing fysiek wordt geïmplementeerd. Er moet een minimumscore van 65 worden behaald.

Verificatie- en validatieplan

Verificatie en validatie spelen een belangrijke rol bij het voorkomen van fouten gedurende het ontwerp- en ontwikkelingsproces van het veiligheidssysteem. ISO 13849-2 stelt de vereisten voor verificatie en validatie. De norm vraagt om een gedocumenteerd plan om te bevestigen dat aan alle functionele veiligheidseisen is voldaan.

Verificatie is een analyse van het resulterende veiligheidsbesturingssysteem. Het prestatieniveau (PL) van het veiligheidsbesturingssysteem wordt berekend om te bevestigen dat het systeem voldoet aan het gespecificeerde, vereiste prestatieniveau (PLr). De SISTEMA-software wordt doorgaans gebruikt om de berekeningen uit te voeren en te helpen bij het voldoen aan de vereisten van ISO 13849-1.

Validatie is een functionele test van het veiligheidsbesturingssysteem die moet aantonen dat het systeem voldoet aan de gespecificeerde vereisten van de veiligheidsfunctie. Het veiligheidsbesturingssysteem is getest om te bevestigen dat alle veiligheidsgerelateerde uitgangen correct reageren op de overeenkomstige veiligheidsgerelateerde ingangen. De functionele test omvat normale bedrijfsomstandigheden naast mogelijke foutinvoer van storingsmodi. Een controlelijst wordt doorgaans gebruikt om de validatie van het veiligheidsbesturingssysteem te documenteren.

Voorafgaand aan de validatie van het systeem moet worden bevestigd dat het configureerbare veiligheidsrelais Guardmaster 440C-CR30 is bedraad en geconfigureerd in overeenstemming met de installatie-instructies.

Controlelijst voor verificatie en validatie

Algemene machine-informatie Beschrijving	
Machinenaam/modelnummer	
Serienummer van machine	
Klantnaam	
Testdatum	
Namen van testers	
Nummer van schematische tekening	
Invoerapparaten	440N-Z21S16B
Configureerbaar veiligheidsrelais	440C-CR30-22BBB
Aandrijving met variabele frequentie	
Veiligheidsmagneetschakelaar	100S-C23EJ23BC

Veiligheidsbedrading en relaisconfiguratie			
Teststap	**Verificatie**	**Geslaagd/ mislukt**	**Wijzigingen/ modificaties**
1	Bevestig dat alle componentspecificaties geschikt zijn voor de toepassing. Zie Basisprincipes op het gebied van veiligheid en Beproefde veiligheidsprincipes van ISO 13849-2.		
2	Voer een visuele inspectie van het veiligheidsrelaiscircuit uit om te bevestigen dat het is bedraad zoals is gedocumenteerd in de diagrammen.		
3	Bevestig dat de configuratie van het configureerbare veiligheidsrelais 440C-CR30 de juiste en bedoelde configuratie is.		

Verificatie van normale werking – Het veiligheidssysteem reageert correct op alle normale start-, stop-, reset-, noodstop- en SensaGuard-schakelaaringangen.			
Teststap	**Verificatie**	**Geslaagd/ mislukt**	**Wijzigingen/ modificaties**
1	Bevestig dat niemand zich in het afgeschermde gebied bevindt.		
2	Bevestig dat de gevaarlijke beweging is gestopt.		
3	Bevestig dat de deur is gesloten.		
4	Schakel de voeding naar veiligheidssysteem in.		
5	Bevestig dat de indicatieleds voor de ingangsstatus van Terminal 00, Terminal 01 en SMF1 van het veiligheidsrelais 440C-CR30 groen branden. Bevestig dat alle indicatieleds voor de uitgangsstatus UIT zijn. Bevestig dat de indicatieleds voor de status van Power en Run groen branden. Controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
6	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Bevestig dat de indicatieleds voor de uitgangsstatus van Terminal 18, Terminal 19 en SOF1 groen branden. Controleer de statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
7	Bevestig dat de gevaarlijke beweging niet begint bij het opstarten.		

8	Druk kort op de knop Start van de aandrijving. Bevestig dat de gevaarlijke beweging begint en dat de machine begint te werken.		
9	Druk op de externe knop Stop. De machine moet stoppen op de normale, geconfigureerde manier. Het veiligheidssysteem mag niet reageren.		
10	Druk kort op de externe knop Start. Bevestig dat de gevaarlijke beweging begint en dat de machine begint te werken.		
11	Open de beschermde deur. Het veiligheidssysteem moet uitschakelen. De gevaarlijke beweging moet binnen minder dan 0,7 seconden stoppen. Controleer de statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
12	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Het configureerbare veiligheidsrelais 440C-CR30 mag niet reageren. Controleer de statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
13	Sluit de beschermde deur. De machine mag niet starten. Het veiligheidsrelais 440C-CR30 mag niet reageren. Controleer de statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
14	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. De SOF1 van het veiligheidsrelais 440C-CR30 moet onder spanning komen. De gevaarlijke beweging mag niet beginnen. Controleer de statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
15	Druk kort op de externe knop Start. Bevestig dat de motor wordt gestart en dat de machine begint te werken.		

Validatie van veilige reactie op abnormale werking – Het veiligheidssysteem reageert goed op alle voorspelbare fouten met overeenkomstige diagnostiek.			
Testen van configureerbare veiligheidsrelais SensaGuard en 440C-CR30			
Teststap	**Verificatie**	**Geslaagd/ mislukt**	**Wijzigingen/ modificaties**
1	Houd de beschermde deur gesloten. Terwijl de gevaarlijke beweging doorgaat, verwijdert u de draad van SensaGuard OSSD1 naar terminal EI_00 van het veiligheidsrelais 440C-CR30. Het veiligheidsrelais 440C-CR30 moet direct uitschakelen. De rode indicatieled voor Fault status op het relais moet knipperen. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
2	Sluit de draad naar E1_00 weer aan. Het veiligheidsrelais 440C-CR30 mag niet reageren. Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Het veiligheidsrelais 440C-CR30 mag niet reageren. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
3	Open en sluit de beschermde deur. De rode foutstatusled moet UIT zijn. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		

4	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. De SOF 1-uitgang op het relais 440C-CR30 relais moet onder spanning komen. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
5	Druk op de externe knop Start. De machine moet beginnen te lopen. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software. Deze stap is optioneel in de volgende SensaGuard-validatietesten (stap 6 tot en met 27).		
6	Terwijl de beschermde deur gesloten is, verbindt u OSSD 1 met 24 VDC. Na ongeveer 40 seconden schakelt de SensaGuard-schakelaar uit. Het veiligheidsrelais 440C-CR30 schakelt uit. De rode indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 moet knipperen. De statusindicatieled op de SensaGuard-schakelaar knippert rood. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
7	Koppel OSSD 1 los van 24 VDC. De SensaGuard-schakelaar noch het veiligheidsrelais 440C-CR30 reageert. Druk kort op de knop Restart op het veiligheidsrelais 440C-CR30. De SensaGuard-schakelaar noch het veiligheidsrelais 440C-CR30 reageert. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
8	Zet spanning op de SensaGuard-schakelaar. Ongeveer vijf seconden nadat de voeding naar de SensaGuard-schakelaar is hersteld, gaat de statusled groen branden. De rood knipperende indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 gaat UIT. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
9	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
10	Verbind OSSD 1 met DC COM. Het veiligheidsrelais 440C-CR30 schakelt direct uit. De rode signaalkolom voor Safe Stop gaat AAN. De oranje signaalkolom voor Gate 1 gaat AAN. De rode indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 moet knipperen. De statusindicatieled op de SensaGuard-schakelaar knippert rood.		
11	Koppel OSSD1 los van DC COM. De SensaGuard-schakelaar noch het veiligheidsrelais 440C-CR30 reageert. Druk kort op de knop Restart op het veiligheidsrelais 440C-CR30. De SensaGuard-schakelaar noch het veiligheidsrelais 440C-CR30 reageert.		
12	Zet spanning op de SensaGuard-schakelaar. Ongeveer vijf seconden nadat de voeding naar de SensaGuard-schakelaar is hersteld, gaat de statusindicatieled groen branden. De oranje signaalkolom voor Gate 1 gaat UIT. De rode signaalkolom voor Safe Off blijft AAN. De rood knipperende indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 gaat UIT.		
13	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. SOF 1 van het veiligheidsrelais 440C-CR30 moet de magneetschakelaars bekrachtigen. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		

14 tot en met 27	Herhaal stap 1 tot en met 13 waarbij u EI_01 gebruikt in plaats van EI_00, en OSSD 2 in plaats van OSSD 1.		
28	Verbind OSSD 1 met OSSD 2 (aansluiting EI_00 naar aansluiting EI_01). Na ongeveer 50 seconden schakelt de SensaGuard-schakelaar uit. Het veiligheidsrelais 440C-CR30 schakelt uit. De statusindicatieled op de SensaGuard-schakelaar knippert rood. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
29	Koppel OSSD 1 los van OSSD 2. De SensaGuard-schakelaar noch het veiligheidsrelais 440C-CR30 reageert. Druk kort op de knop Restart op het veiligheidsrelais 440C-CR30. De SensaGuard-schakelaar noch het veiligheidsrelais 440C-CR30 reageert.		
30	Zet spanning op de SensaGuard-schakelaar. Ongeveer vijf seconden nadat de voeding naar de SensaGuard-schakelaar is hersteld, gaat de statusled groen branden. De rood knipperende indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 gaat UIT. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
31	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. De rode signaalkolom voor Safe Stop moet UIT zijn. De SOF1-uitgang van het veiligheidsrelais 440C-CR30 moet de magneetschakelaars bekrachtigen. Controleer alle statusindicatieleds op een juiste werking en controleer het veiligheidsrelais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		

Validatie van veilige reactie op abnormale werking – Het veiligheidssysteem reageert goed op alle voorspelbare fouten met overeenkomstige diagnostiek.			
Magneetschakelaar – Testen van het configureerbare veiligheidsrelais 440C-CR30			
Teststap	**Verificatie**	**Geslaagd/ mislukt**	**Wijzigingen/ modificaties**
1	Terwijl de machine blijft lopen, verbreekt u de verbinding tussen aansluiting EO_18 van het configureerbare veiligheidsrelais 440C-CR30 en aansluiting A1 van de spoel K1. De gevaarlijke beweging moet uitlopen tot stilstand.		
2	Druk op de externe knop Stop. Herstel de verbinding. Druk op de externe knop Start om de gevaarlijke beweging te hervatten.		
3	Terwijl de gevaarlijke beweging blijft voortduren, verbindt u aansluiting A1 van spoel K1 met 24 VDC. Na circa 18 seconden moet het veiligheidsrelais 440C-CR30 uitschakelen. K2 moet spanningsloos zijn. De gevaarlijke beweging loopt uit tot stilstand. De rode indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 is AAN.		
4	Koppel aansluiting A1 van de spoel K1 los van 24 VDC. Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Het veiligheidsrelais 440C-CR30 mag niet reageren.		
5	Zet spanning op het veiligheidsrelais 440C-CR30. Het relais reageert. De indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 is UIT.		
6	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Druk op de externe knop Start. De gevaarlijke beweging moet worden hervat.		
7	Terwijl de machine blijft lopen, sluit u aansluiting A1 van de spoel K1 kort naar DC COM. Het veiligheidsrelais 440C- CR30 moet uitschakelen. De rode indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 is AAN.		

8	Koppel aansluiting A1 van de spoel K1 los van DC COM. Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Het veiligheidsrelais 440C-CR30 mag niet reageren.		
9	Zet spanning op het veiligheidsrelais 440C-CR30. Het veiligheidsrelais 440C-CR30 reageert. De indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 is UIT.		
10	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Druk op de externe knop Start. De gevaarlijke beweging wordt hervat.		
11 tot en met 21	Herhaal stap 1 tot en met 10, waarbij u EO_19 gebruikt in plaats van EO_18 en K2 in plaats van K1.		
22	Verbind aansluiting A1 van K1 met aansluiting A1 van K2. Na circa 18 seconden moet het veiligheidsrelais 440C-CR30 uitschakelen. De gevaarlijke beweging loopt uit tot stilstand. De rode indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 is AAN.		
23	Koppel aansluiting A1 van K1 los van aansluiting A1 van K2. Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Het veiligheidsrelais 440C-CR30 mag niet reageren.		
24	Zet spanning op het veiligheidsrelais 440C-CR30. Het relais reageert. De indicatieled voor Fault status op het veiligheidsrelais 440C-CR30 is UIT.		
25	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Druk op de externe knop Start. De gevaarlijke beweging moet worden hervat.		

Validatie van veilige reactie op abnormale werking – Het veiligheidssysteem reageert goed op alle voorspelbare fouten met overeenkomstige diagnostiek.

Magneetschakelaarfeedback – Testen van het configureerbare veiligheidsrelais 440C-CR30

Teststap	Verificatie	Geslaagd/ mislukt	Wijzigingen/ modificaties
1	Terwijl de machine blijft lopen, verwijdert u de feedbackverbinding K1 op aansluiting P1_00. De machine moet blijven lopen.		
2	Open de beschermde deur. Het veiligheidssysteem moet uitschakelen. De gevaarlijke beweging moet binnen minder dan 0,7 seconden stoppen. Controleer de statusindicatieleds op een juiste werking en controleer het relais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
3	Sluit de beschermde deur. De machine mag niet starten. Het relais 440C-CR30 mag niet reageren. Controleer de statusindicatieleds op een juiste werking en controleer het relais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
4	Druk kort op de knop Reset op het veiligheidsrelais 440C-CR30. Het relais 440C-CR30 mag niet reageren. Controleer de statusindicatieleds op een juiste werking en controleer het relais 440C-CR30 op de juiste status met behulp van de Connected Components Workbench-software.		
5	Breng de verbinding op P1_00 weer aan. Zet spanning op het relais 440C-CR30. Druk op de knop Reset op het relais 440C-CR30. De uitgangen van het relais 440C-CR30 moeten worden bekrachtigd. Druk kort op de externe knop Start. Bevestig dat de motor wordt gestart en dat de machine begint te werken.		
6	Herhaal stap 1 tot en met 5 waarbij u de feedbackverbinding K2 op aansluiting P1_01 gebruikt.		

Verificatie van de configuratie

Het systeem moet de configuratie van elke afzonderlijke toepassing controleren met behulp van de opdracht Verify. Als de configuratie van het veiligheidsrelais 440C-CR30 niet is geverifieerd, zal het relais na 24 uur in storing vallen.

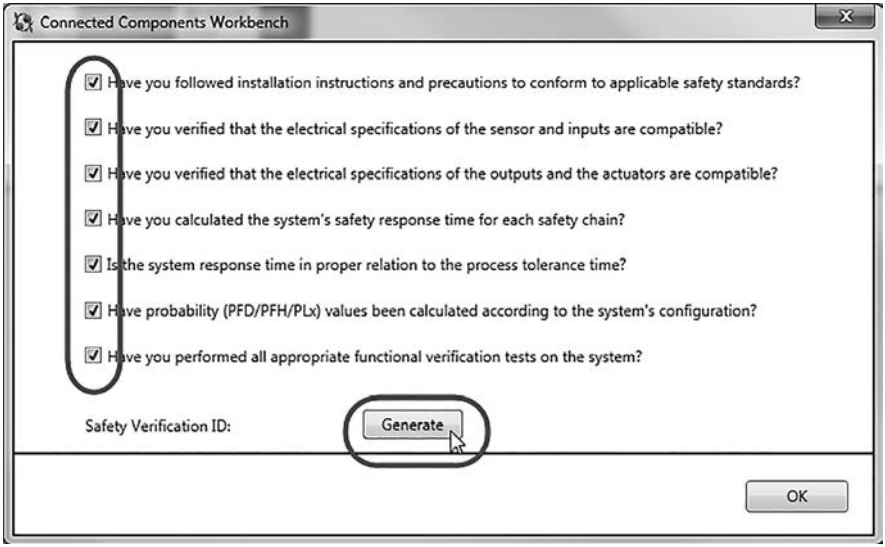
LET OP: Het verificatieproces dient te worden gedocumenteerd in het technisch dossier van het veiligheidssysteem.

Volg deze stappen om de configuratie te downloaden en te verifiëren.

1. Zorg dat het relais 440C-CR30 is bekrachtigd en via de usb-kabel met uw werkstation is verbonden.
2. Bevestig dat in de rechterbovenhoek van het tabblad Project van Connected Components Workbench wordt aangegeven dat het relais 440C-CR30 is aangesloten. Als dat niet zo is, klikt u op Connect to Device om de softwareverbinding tot stand te brengen.

3. Klik op Verify.

4. Beantwoord alle vragen en vink ieder vakje aan als u klaar bent. Klik op Generate.

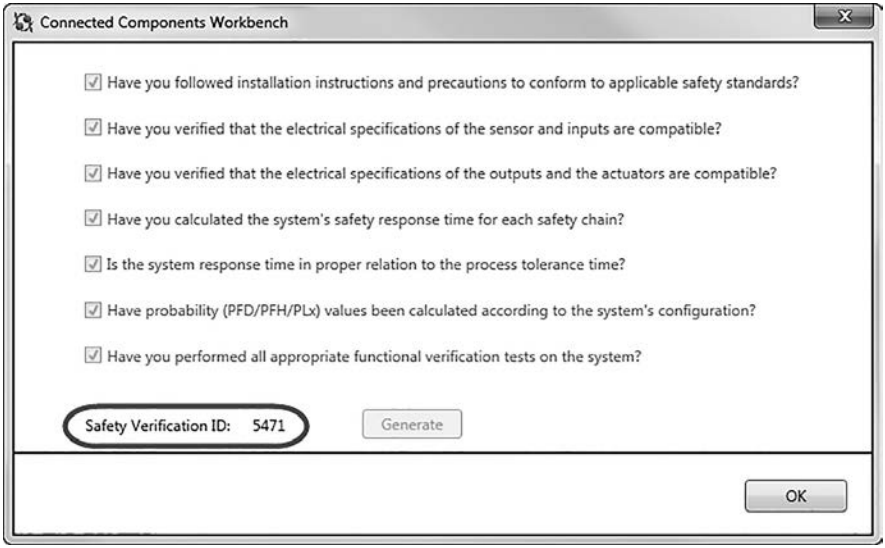


BELANGRIJK: Alle vakjes moet worden gemarkeerd om de Verification ID (verificatie-id) te kunnen genereren.

6. Klik op Yes om door te gaan met de verificatie.

7. Klik op Yes om over te schakelen naar de modus Run.

8. Registreer de Safety Verification ID (veiligheidsverificatie-id) in de documentatie van de machine.



Dit proces is de feedback naar het relais 440C-CR30 dat de systeemverificatie en de functionele testen zijn voltooid. De unieke verificatie-id kan worden gebruikt om te controleren of er wijzigingen zijn uitgevoerd aan een configuratiebestand. Bij elke wijziging aan de configuratie wordt de veiligheidsverificatie-id verwijderd. Bij opvolgende verificatieacties wordt een andere verificatie-id gegenereerd. De veiligheidsverificatie-id wordt alleen in de Connected Components Workbench-software weergegeven wanneer u verbonden bent met het relais 440C-CR30.

Hoofdstuk 11: Producten, tools en diensten

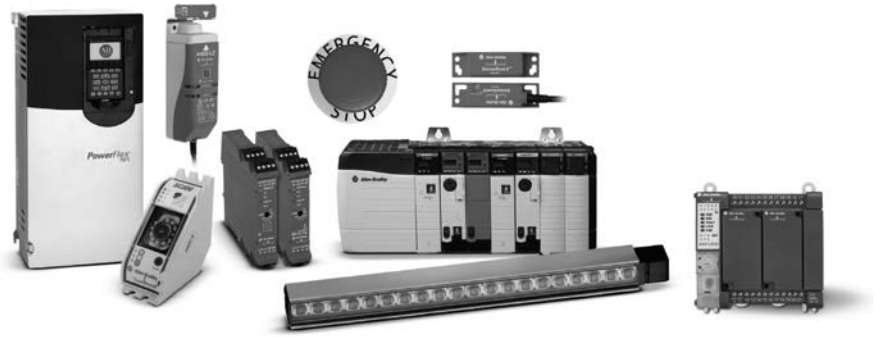
Overzicht

Rockwell Automation is een vooraanstaande wereldwijde leverancier van industriële vermogens-, besturings- en informatieoplossingen en ondersteunt zijn klanten al meer dan 100 jaar in uiteenlopende bedrijfstakken. Veelomvattende technologieën, tools en diensten op het gebied van machineveiligheid zijn onderdeel van het industriële automatiseringsportfolio van Rockwell Automation.

Producten en technologieën voor uw toepassingen

Rockwell Automation heeft de meest uitgebreide portfolio van alle leveranciers van machineveiligheidsoplossingen en kan alle drie de onderdelen van een veiligheidssysteem (invoermodule, logicabesturing en eindvoedingselement) leveren.

De verkrijgbare producten en technologieën zijn onder meer:



Veiligheidsinvoermodules

- **Veiligheidsvoorzieningen met aanwezigheidsdetectie**
  Veiligheidsvoorzieningen met aanwezigheidsdetectie detecteren de locatie van objecten of personeel in de buurt van gevaarlijke omgevingen. Dit zijn onder meer: veiligheidslichtschermen, veiligheidslaserscanners, veiligheidssensoren voor handdetectie, drukgevoelige matten en boorden

- **Veiligheidsvergrendelingsschakelaars**
  Veiligheidsschakelaars zijn ontworpen en gebouwd volgens wereldwijde normen voor hoge betrouwbaarheid, stabiliteit, en kwaliteit. Veiligheidsschakelaars zijn onder meer eind- en vergrendelingsschakelaars en noodstopschakelaars.

- **Noodstop- en uitschakelvoorzieningen**
  Noodstopschakelaars omvatten een assortiment paddenstoelvormige drukknopapparaten met positief geleide contacten. Activeringsschakelaars en trekkoordschakelaars voorzien in de noodfunctie in een toepassing of zijn vastgezet zodat de operator zich kan bewegen binnen de veiligheidstoepassing.

- **Operatorinterface**
  Operatorinterfacevoorzieningen stellen de operator in staat om met de toepassing samen te werken en ze bieden aanvullende, speciale veiligheidsfunctionaliteit.

Controllers met veiligheidslogica

- **Veiligheidsrelais (enkele functie of configureerbaar)**
  Veiligheidsrelais controleren en bewaken een veiligheidssysteem, en stellen de machine in staat om te starten of voeren opdrachten uit om de machine te stoppen. Veiligheidsrelais met een enkele functie vormen de voordeligste oplossing voor kleinere machines waarbij een speciaal logisch apparaat is vereist voor het completeren van de veiligheidsfunctie. Modulaire en configureerbare veiligheidsrelais genieten de voorkeur wanneer er een groot en uiteenlopend aantal veiligheidsapparaten en de bewaking van een minimale zone zijn vereist.

- **Geïntegreerde veiligheidscontrollers**
  Veiligheids-PLC's brengen de voordelen van traditionele PLC-systemen naar veiligheidstoepassingen, en vervangen bekabelde relaissystemen die zijn normaal zijn vereist om geautomatiseerde processen in een veilige toestand te brengen. Met veiligheids-PLC 's kunnen standaard- en veiligheidsgerelateerde programma's worden ondergebracht in een enkel controllerframe. Dit voorziet in flexibele programmering en biedt tevens een vertrouwde en gebruiksvriendelijke omgeving voor programmeurs. Veiligheidscontrolleroplossingen bieden open en geïntegreerde besturing die helpt om voor machineveiligheid en de bescherming van uw bedrijfsmiddelen te zorgen.

- **Veiligheids-I/O-voorzieningen**
  De veiligheidsproducten Guard I/O™ bieden alle voordelen van traditioneel gedistribueerde I/O, maar zijn ontworpen voor veiligheidssystemen. Ze zorgen voor lagere bedradingskosten en een kortere opstarttijd voor machines en cellen en zijn verkrijgbaar met een groot aantal functies voor toepassingen in kasten of op machines.

Veiligheidsactuatoren

- **Veiligheidsmagneetschakelaars en starters**
  Gedistribueerde ArmorStart® motorcontrollers voldoen aan de veiligheidsfunctionaliteit van categorie 4 en voorzien in een veiligheidsoplossing die is geïntegreerd in uw DeviceNet™ On-Machine™-veiligheidsinstallatie. De IEC-veiligheidsmagneetschakelaars en besturingsrelais helpen om personeel te beschermen tegen onbedoeld opstaren van machinestart en uitval van de veiligheidsfunctie.

- **PowerFlex ®-frequentieomvormers**
  PowerFlex-aandrijvingen zijn verkrijgbaar met veiligheidsfuncties. De PowerFlex 525-frequentieomvormers bevatten ingebouwde STO (Safe Torque-Off ofwel veilige koppeluitschakeling) als standaardfunctie. Safe Torque-Off is een optionele functie voor de PowerFlex-frequentieomvormers uit de serie 40P, 70, 700H, 700S en 750, die ook SSM-functionaliteit (Safe Speed Monitor ofwel veiligtoerentalbewaking) ondersteunen.

- **Kinetix ® geïntegreerde beweging**
  De servoaandrijvingen Kinetix 300, 6000, 6200, 6500 en 7000 zijn allemaal voorzien van ingebouwde veiligheidsfunctionaliteit. Met STO wordt een aandrijvingsuitgang uitgeschakeld om het motorkoppel op te heffen zonder de stroomtoevoer naar de gehele machine te onderbreken. Met SSM kunnen gebruikers de snelheid van de toepassing verlagen en bewaken om een operator te helpen om sommige soorten werkzaamheden op veilige wijze uit te voeren zonder de machine volledig tot stilstand te brengen.

Verbindingssystemen/-netwerken

- **‘Quick Connect’-verbindingssystemen**
  T-poorten/-splitters, verdeelkasten en kortsluitpluggen van Guardmaster® Safety zijn onderdelen van een systeem voor snelle ontkoppeling dat is toegespitst op machineveiligheid.

- **GuardLink™**
  GuardLink is een op veiligheid gebaseerd communicatieprotocol dat gebruikmaakt van standaardbekabeling in een topologie van ‘trunk and drop’ met ‘plug and play’-verbindingen. Het maakt communicatie van veiligheidsapparatuur voor diagnostiek en besturing, zoals opdrachten voor resetten op afstand en vergrendeling, mogelijk over een enkele kabel. Er kunnen maximaal 32 apparaten worden verbonden bij een kabellengte van maximaal 1.000 meter. Met Allen-Bradley-veiligheidsap-

paraten met GuardLink-technologie hebt u toegang tot veiligheidssysteeminformatie via EtherNet/IP. GuardLink kan helpen om systeemconfiguratie te vereenvoudigen, bedrading te verminderen en diagnostische informatie voor onderhoud en werking uit te breiden.

- **Veiligheid over EtherNet/IP**
  Het EtherNet/IP™-netwerk biedt fabrieksbrede netwerksystemen met gebruikmaking van open netwerktechnologieën volgens de industrienorm. Het biedt realtimebesturing en -informatie in discrete toepassingen voor continue processen, batches, veiligheid, aandrijving, beweging en hoge beschikbaarheid. EtherNet/IP-netwerken verbinden apparaten zoals motorstarters en sensoren met controllers en HMI-apparaten en met apparatuur verderop in de onderneming. Het biedt ondersteuning voor niet-industriële en industriële communicatie binnen een enkele, gemeenschappelijke netwerkinfrastructuur.

Tools om u te helpen

Een breed assortiment van tools die naleving van veiligheidsnormen ondersteunen, het risico van letsel reduceren en de productiviteit verbeteren.

Safety Automation Builder

Safety Automation Builder is een GRATIS softwaretool die helpt om het ontwerp en de validatie van machineveiligheid te vereenvoudigen, waardoor tijd en kosten worden bespaard. Integratie met RASWin-software voor risicobeoordeling biedt gebruikers een consistent, betrouwbaar en gedocumenteerd beheer van de functionele veiligheidslevensduur. Safety Automation Builder stroomlijnt het ontwerp van een veiligheidssysteem, helpt u om effectiever te voldoen aan de eisen van wet- en regelgeving en om de kosten terug te dringen. Safety Automation Builder begeleidt gebruikers tijdens de ontwikkeling van veiligheidssystemen, van de indeling tot de productselectie en de veiligheidsanalyses die nodig zijn om te voldoen aan de PL-eisen (Performance Level) voor machineveiligheid zoals vastgelegd in de wereldwijde norm (EN) ISO 13849-1.

RASWin

RASWin-software helpt gebruikers met het beheren van de voortgang door de functionele veiligheidslevensduur. RASWin rangschikt informatie uit elke stap van het proces en uit de machinevalidatie. RASWin koppelt de stappen van de veiligheidslevensduur om systematische fouten te voorkomen, met inbegrip van veiligheidsfunctiespecificaties, toewijzing en berekening van PLr (vereist prestatieniveau), veiligheidscircuitvalidatie en documentatie.

SISTEMA-calculator voor prestatieniveau

De SISTEMA-tool, die is ontwikkeld door het instituut voor beroepsveiligheid en -gezondheid van de Duitse sociale ongevallenverzekering (IFA), automatiseert de berekening van het gerealiseerde prestatieniveau uit de veiligheidsgerelateerde onderdelen van een machinebesturingssysteem volgens (EN) ISO 13849-1. Gegevens voor machineveiligheidsproducten van Rockwell Automation zijn beschikbaar in de vorm

van een bibliotheek die kan worden gebruikt met de SISTEMA-calculatietool. De combinatie van beide biedt machine- en systeemontwerpers uitgebreide en tijdbesparende ondersteuning bij het evalueren van veiligheid volgens (EN) ISO 13849-1. Met een exportfunctie van Safety Automation Builder kan het veiligheidssysteemontwerp op eenvoudige wijze in SISTEMA worden geïmporteerd om een verificatie door een externe partij van het vereiste prestatieniveau te ontvangen.

Kant-en-klare veiligheidsfuncties voor machines

Functies voor machineveiligheid vereisen meerdere elementen, met inbegrip van een sensor of invoerapparaat, een logisch apparaat en een uitvoerapparaat. Samen bieden deze elementen een beschermingsniveau dat wordt berekend aan de hand van een prestatieniveau zoals beschreven in (EN) ISO 13849-1. Rockwell Automation heeft veel documenten over veiligheidsfuncties ontwikkeld, en elk document voorziet in richtlijnen voor een specifieke veiligheidsfunctie op basis van functionele eisen, apparatuurselectie en vereist prestatieniveau. Ze omvatten installatie en bedrading, configuratie, een verificatie- en validatieplan en berekening van het prestatieniveau.

De tool Safety Maturity Index

De Safety Maturity Index™ is een uitgebreide meting van prestaties qua veiligheidscultuur, nalevingsprocessen en -procedures en kapitaalinvesteringen in veiligheidstechnologieën. Deze softwareoplossing helpt bedrijven inzicht te krijgen in hun huidige prestatieniveau en in welke stappen zij kunnen zetten om de veiligheid en winstgevendheid te verbeteren.

Services en ervaring om u te ondersteunen

Als grootste leverancier van industriële veiligheid ter wereld helpt Rockwell Automation letsel en kosten terug te brengen terwijl we de productiviteit verbeteren in iedere fase van de veiligheidslevenscyclus.

Veiligheidsservices worden verleend door ervaren personeel met veiligheidskwalificaties, velen met machineveiligheidscertificaten van TÜV Rheinland. Rockwell Automation heeft functionele veiligheidsexperts, constructeurs en technici met TÜV-kwalificaties in dienst om klanten te helpen met hun holistische veiligheidslevenscyclus.

De veiligheidslevenscyclus is een duidelijk gedefinieerd proces dat helpt om de productiviteit te maximaliseren en de veiligheid te verbeteren door de stappen vast te stellen die nodig zijn om machinerisico's te beoordelen en te beperken. De veiligheidslevenscyclus kan in dit document worden bekeken en gedownload.

Enkele van de beschikbare services zijn:

- **Veiligheidsbeoordelingen**
  Services die u helpen om productievestigingsrisico te evalueren en om gefundeerde besluiten te ondersteunen die de veiligheid van werknemers en machines helpen verbeteren.

- **Ontwerpservices**
  Uitgebreid circuitontwerp, de juiste toepassing van apparatuur en ontwerpcontrole om de algehele veiligheid te helpen verbeteren.

- **Installatie- en validatieservices**
  Verificatie dat systemen functioneren binnen gedefinieerde parameters en normen.

- **Veiligheidstraining**
  Uitgebreide opleidingsprogramma's die zijn ontwikkeld door vooraanstaande experts in de bedrijfstak.

- **Service op maat**
  Behandelt klantspecifieke toepassingen, technologieën, toepassingen, platforms en configuraties.

Waarom zou u Rockwell Automation kiezen

Het integreren van veiligheid met automatisering kan zorgen voor productiviteitsverbeteringen in uiteenlopende stadia van het productieproces, van het ontwerpen en testen van apparatuur en de installatie en inbedrijfstelling ervan, tot de bediening en het onderhoud en het aanpassen of uit gebruik nemen van machines. Tijdens al deze stadia kunt u de processen optimaliseren met de juiste inzet van veiligheidsoplossingen.

Als wereldleider in industriële automatisering en veiligheid en als technologisch innovator is Rockwell Automation als geen ander in staat om u te helpen met de ontwikkeling van efficiëntere, veiligere en productievere productieoplossingen.

Met jarenlange ervaring op het gebied van automatisering en veiligheid, kennis van toepassingen en gebruik van geavanceerde richtlijnen van veiligheidsnormen zoals ISO 12000, (EN) ISO 13849-1 en IEC 62061 helpt Rockwell Automation u met de selectie, integratie, training en ondersteuning voor oplossingen voor machineveiligheid, procesveiligheid en elektrische veiligheid.

www.rockwellautomation.com

Hoofdkantoren voor Aandrijvings- Besturings- en Informatieoplossingen.

Noord- Midden- & Zuid-Amerika: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europa, Midden-Oosten & Afrika: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Nederland: Rockwell Automation, Rivium Promenade 160, 2909 LM, Capelle aan de IJssel, The Netherlands, Tel: +31 (0) 10 266 55 55, Fax: +31(0) 10 266 56 57; www.rockwellautomation.nl

Publicatie: SAFEBK-RM002C-NL-P – November 2016