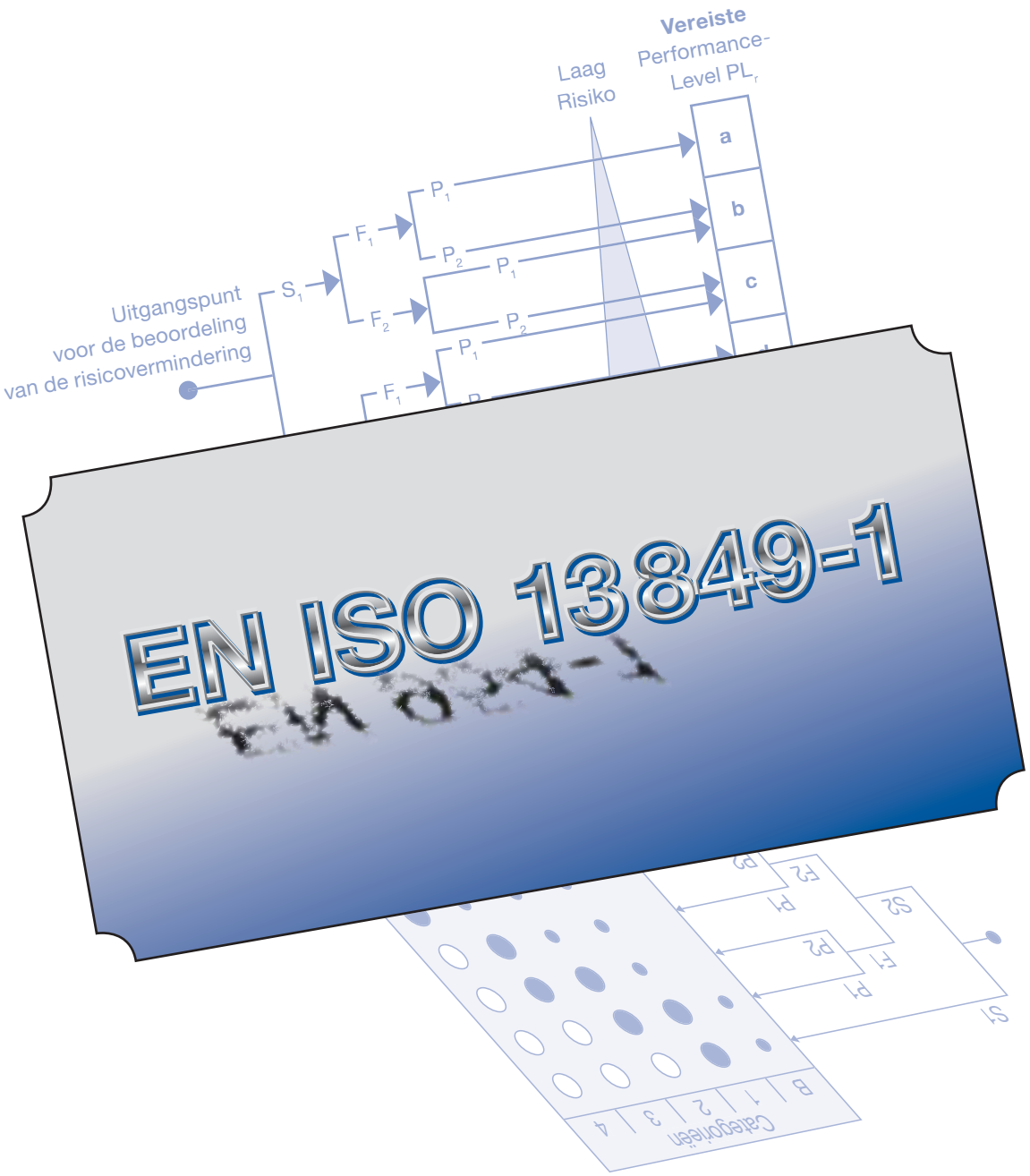
Een nieuwe norm voor de machineveiligheid:

EN ISO 13849-1:2006 – Onderdelen van besturingssystemen met een veiligheidsfunctie



SCHMERSAL

Elan

Update

Wuppertal/Wettenberg, mai 2007

Beste SCHMERSAL klant,
Beste Elan klant,

Na de nodige conflicten en moeilijkheden (zie ook MRL-News 24/02/07, pagina 13 ev., Afschaffing van de EN 954-1: De paradigma-verandering is een feit!) is de ontwerpnorm “Onderdelen van besturingssystemen met een veiligheidsfunctie” nu eindelijk aangenomen en als EN ISO 13849-1:2006 van kracht gewor-den.

In die zin moet de planning voor het inwerking-treden (pagina 46 van onze brochure, uitgave maart 2006) dan ook aangepast worden.
De overgangsperiode voor de nieuwe norm loopt tot november 2009 (tot dat ogenblik mag, maar moet hij echter nog niet toegepast worden).

Eventuele normen die in tegenspraak zijn met de nieuwe norm (met andere woorden: EN 954-1: 1997 of ISO 13849-1:1999) moeten uiterlijk tegen november 2009 teruggetrokken en door de EN ISO 13849-1:2006 vervangen worden. Alle overige informatie in onze brochure met betrekking tot de achtergrond, de toepassing en de praktische omzetting van de nieuwe norm is echter nog altijd actueel en correct.

Met vriendelijke groeten,

Friedrich Adams
K.A. Schmersal Holding GmbH & Co. KG

Vanaf wanneer moet de nieuwe EN ISO 13849-1 toegepast worden?
Zijn er overgangsperiodes?

Wuppertal/Wettenberg, maart 2006

Beste SCHMERSAL klant,
Beste Elan klant,

In deze brochure vindt u een uitvoerige toelichting op de belangrijkste lezing uit de Elan voordrachtenreeks van 2005, namelijk de terugtrekking van de norm EN 954-1 en de nieuwe regels en voorschriften van zijn opvolger, de EN ISO 13849-1:2006. Op deze manier wil de SCHMERSAL Groep haar competentie op het gebied van machineveiligheid onderstrepen. Als leverancier van veiligheidsschakelcomponenten en veiligheidssystemen voor de veiligheid van mens, machine en installatie geven wij onze klanten extra rand- en achtergrondinformatie om zo uw voorkeurspartner te zijn voor alles wat betrekking heeft op het gebruik van veiligheidsonderdelen voor machines en machinebesturingen.

Deze brochure bevat een samenvatting van de desbetreffende toespraak van de heren Ir. Thomas Bömer en Ir. Karl-Heinz Büllesbach, beiden medewerkers van het "Berufsgenossenschaftlichen Instituts für Arbeitsschutz BGIA" , St. Augustin, die door hun werk bij de afdeling "Elektronica" van het vakgebied "Machineveiligheid & Besturingstechniek" nauw bij het onderwerp betrokken zijn.

De afbeeldingen in deze bijdrage zijn gebaseerd op de PowerPoint presentatie van deze heren. Eventuele auteursrechten voor deze afbeeldingen berusten bij hen.

Het BGIA en diverse beroepsorganisaties die zich op machinebouw toespitsen, hebben zich in hoge mate geëngageerd voor het ontwerp van de norm EN ISO 13849-1:2006, met als doel de klanten van de kleine en middelgrote machine- en besturingsbouwers een eenvoudige en toch substantiële leidraad te bieden voor het ontwerpen van de veiligheidsgerichte machinebesturingen in de toekomst.

Er is zwaar gediscuteerd over de opvolging van de EN 954-1. Aan de ene zijde door de voorstanders van de IEC 62061 en aan de andere zijde door de voorstanders van de EN 13849-1:2006. De uitkomst van deze discussie is dat beide normen geharmoniseerd zijn en dat u de keuze heeft volgens welke norm u gaat werken.

Het productgamma van de SCHMERSAL Groep is vandaag reeds conform met de vereisten en specificaties van beide normen. Als u vragen over dit onderwerp heeft, aarzel dan niet om ons te benaderen.

Voor een duidelijk overzicht hebben wij het onderwerp "EN ISO 13849-1: De nieuwe standaard voor machineveiligheid" in afzonderlijke hoofdstukken opgesplitst, die op zich verder onderverdeeld zijn – u kunt dus zelf kiezen hoe grondig u zich in de materie wil verdiepen. Wij vragen u om uw begrip voor het gebruik van de vele afkortingen en Engelse woorden in de tekst, die wegens gebrek aan een officiële vertaling echter onvermijdelijk zijn. Het overzicht (uitklapbare pagina) tracht echter enige duidelijkheid te verschaffen en de leesbaarheid te vergroten.

Hoewel wij ons best gedaan hebben deze samenvatting zo overzichtelijk en begrijpelijk mogelijk te houden, zijn we hier, wegens de complexiteit van het onderwerp, niet altijd even goed in geslaagd. Wij excuseren ons indien bepaalde vragen onbeantwoord blijven of zelfs nieuwe vragen oproepen.

Wij wensen u veel leesplezier en verheugen ons op een prettige samenwerking.

Met vriendelijke groeten,

Heinz Schmersal
Algemeen Directeur
K.A. Schmersal Holding GmbH & Co. KG

Friedrich Adams
K.A. Schmersal Holding GmbH & Co. KG

1) Beroepsorganisatie voor Arbeidsbescherming

Een nieuwe norm voor de machineveiligheid:
EN ISO 13849-1:2006 –
Onderdelen van besturingssystemen met een veiligheidsfunctie

Inhoudsopgave

Uitgever
Elan Schaltelemente GmbH & Co. KG
Im Ostpark 2
35435 Wettenberg
Telefoon +49 (0)641 9848-0
Fax +49 (0)641 9848-420
E-Mail: info@elan.schmersal.com
Internet: www.elan.de

Redactie en lay-out
Friedrich Adams
c/o SCHMERSAL Holding GmbH & Co. KG
Möddinghofe 30
42279 Wuppertal
E-Mail: fadams@schmersal.com

Samenstelling en realisatie
Werbe-Grafik Heinz Flick, 35075 Gladenbach/
Druckteam Peter Bork, 35435 Wettenberg

Een nieuwe norm voor de machineveiligheid:

EN ISO 13849-1:2006 – Onderdelen van besturingssystemen met een veiligheidsfunctie

Inleiding

Binnen afzienbare tijd zal de norm EN 954-1[1] vervangen worden. De afschaffing van deze norm zal voor de machinebouwer een totaal andere manier van denken met zich meebrengen. De deterministische aanpak zal plaats moeten maken voor een meer probabilistische benadering van de veiligheidsrelevante componenten.

Momenteel zijn twee nieuwe normen in de running als opvolger van de EN 954-1: enerzijds de EN ISO 13849-1:2006[2], die rechtstreeks voortvloeit uit de revisie van de EN 954-1 en anderzijds de IEC EN 62061[3], een zogeheten sectornorm die zich specifiek tot de machinebouwer richt en van de IEC EN 61508 afgeleid is.

In tegenstelling tot de EN 954-1, die zich uitsluitend baseert op de analyse van de structuur ('deterministische aanpak'), vereisen de nieuwe normen een analyse van de betrouwbaarheid en de uitvalwaarschijnlijkheid van de onderdelen van besturingssystemen met een veiligheidsfunctie ('probabilistische aanpak'). In de IEC EN 61508 en de IEC EN 62061 weegt de probabilistische aanpak nog zwaarder door in de vorm van wiskundige waarschijnlijkheidsberekeningen en modellen. De normalisatiecommissie van de EN ISO 13849-1:2006 heeft echter getracht een evenwicht te vinden tussen de deterministische en de probabilistische aanpak. De veiligheidsvoorschriften en richtlijnen voor het ontwerpen en evalueren van de onderdelen van besturingssystemen met een veiligheidsfunctie werd in een praktische en uitvoerbare vorm gegoten om de "doorsneegebruikers" van de norm het leven iets te vergemakkelijken (zie figuur 1).

1) EN 954-1:1997-03: Veiligheid van machines – Onderdelen van besturingssystemen met een veiligheidsfunctie – Deel 1: Algemene ontwerpbeginselen (stemt overeen met ISO 13849-1:1999-11)

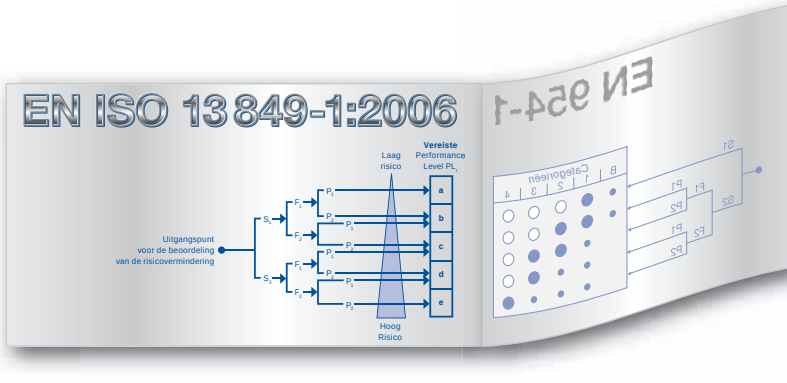
2) EN ISO 13849-1:2007-02: Veiligheid van machines – Onderdelen van besturingssystemen met een veiligheidsfunctie – Deel 1: Algemene ontwerpbeginselen

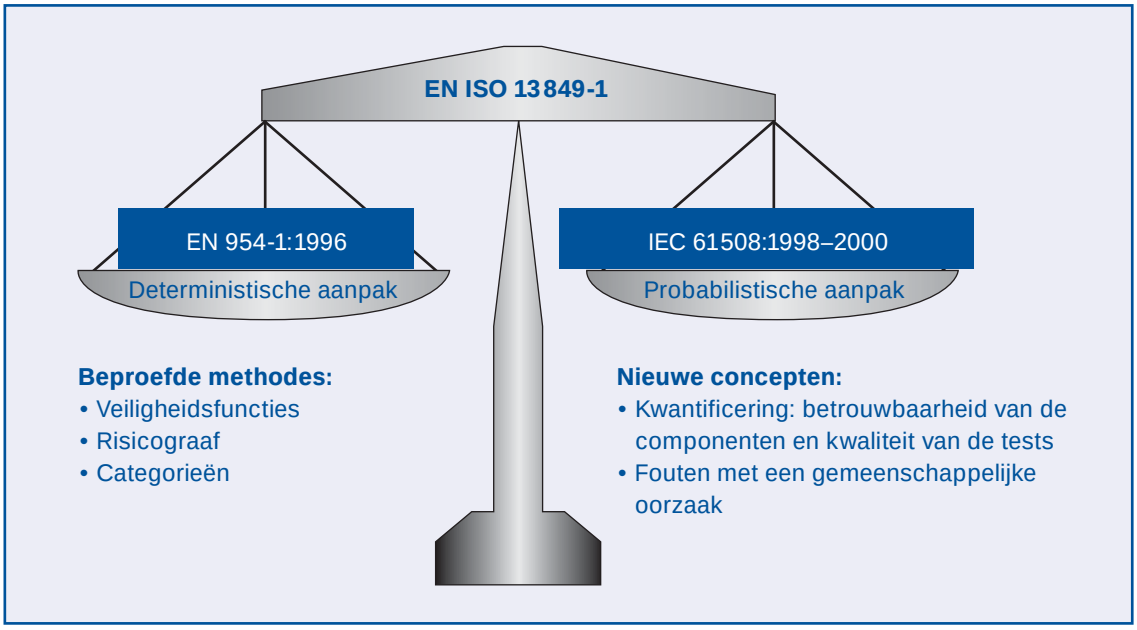
3) IEC EN 62061:2005-10: Veiligheid van machines – Functionele veiligheid van elektrische/elektronische/programmeerbare elektronische veiligheidssystemen

4) IEC EN 61508:2002-11: Functionele veiligheid van elektrische/elektronische/programmeerbare elektronische systemen

- Deel 1: Algemene richtlijnen
- Deel 2: Vereisten voor elektrische/elektronische/programmeerbare elektronische veiligheidssystemen
- Deel 3: Softwarevereisten
- Deel 4: Begrippen en afkortingen
- Deel 5: Voorbeelden voor het bepalen van het veiligheidintegriteitsniveau (SIL, Safety Integrity Level)
- Deel 6: Richtlijnen voor het toepassen van de IEC 61508-2 en de IEC 61508-3
- Deel 7: Richtlijnen voor het toepassen van processen en maatregelen

Referentiebron: Beuth Verlag GmbH, 10772 Berlin; www.beuth.de





Figuur 1: Evenwichtsoefening tussen de deterministische en de probabilistische aanpak

Zonder afbreuk te willen doen aan de inspanningen van de normalisatiecommissie van de EN ISO 13849-1:2006, zouden we kunnen zeggen dat deze norm een “light” versie is van de IEC EN 61508. “Light” in die zin dat de EN ISO 13849-1:2006 de belangen van de meerderheid van zijn klanten, namelijk de kleine en middelgrote bouwers van machines, installaties en besturingssystemen, ter harte probeert te nemen door vereenvoudigingen en veralgemeniseringen toe te laten die aan de doelgroep aangepast en op veiligheidstechnisch gebied verantwoord zijn.

Deze maatregel werd duidelijk getroffen om de extra kosten en inspanningen die de probabilistische aanpak met zich meebrengt, binnen de perken te houden.

Voor uiterst complexe universele besturingssystemen zoals een veiligheids-PLC, veiligheidsbussysteem of veiligheidslaserscanner is eerder het gebruik van andere normen zoals de IEC EN 61508 aangewezen.

Achterliggende reden voor de revisie van de EN 954-1

De ware reden voor de revisie van de EN 954-1 ligt niet in het feit dat ongevallen aan en met machines te wijten zijn aan de onvolkomenheden en de hiaten van de EN 954-1.

Wel is er vanaf het begin al veel kritiek op de EN 954-1. Zo zou de norm niet altijd eenduidig zijn, waardoor heel veel discussie ontstaan is over de praktische uitvoering ervan.

De normcommissie die zich bezighoudt met de verbetering van de EN 954-1 heeft uiteindelijk geconcludeerd dat het beter was een totaal nieuwe norm te schrijven dan de huidige norm verder aan te passen. Dit heeft dus geresulteerd in de EN ISO 13849-1:2006.

De juistheid van de aanpak en de vereisten van de EN 954-1 werd vaak bekritiseerd door Duitsland en de andere lidstaten van de Europese Gemeenschap.

- Vanuit theoretisch standpunt beschouwd baseert deze kritiek zich hoofdzakelijk op het feit dat de EN 954-1 “alleen maar” maatregelen voor de risicovermindering voorziet, die voor alle categorieën tot eenzelfde restrisico leiden. In theorie blijft het risico waaraan de operator blootgesteld wordt, altijd hetzelfde, ongeacht of de SRP/CS aan de vereisten van categorie 1, 2, 3 of 4 beantwoordt en het risico een lichte (omkeerbare) dan wel ernstige (onomkeerbare) verwonding inhoudt.

  De critici zijn bovendien van mening dat een hoger risico ook bijkomende maatregelen ter vermindering van het restrisico vereist.

- Een tweede punt van kritiek is dat de vereisten van de EN 954-1 te weinig rekening houden met de toenemende complexiteit van de industriële automatisering. In het geval van gecoördineerd samenwerkende machines die aan elkaar gekoppeld zijn, houdt de EN 954-1 er bijvoorbeeld geen rekening mee of de SRP/CS in een individuele machine, een complexe installatie of een geïntegreerd productiesysteem geïntegreerd is. Met andere woorden: hoe hoger de complexiteit -> hoe groter het restrisico -> hoe meer bijkomende maatregelen ter beheersing van het restrisico!

- Het feit dat er te weinig rekening gehouden wordt met de complexiteit van een SRP/CS, kan dus niet ontkend worden.

- Het staat echter vast dat de EN 954-1 de huidige stand van de techniek niet langer accuraat weerspiegelt. Zo voorziet zij bijvoorbeeld geen vereisten voor hoogcomplexe besturingssystemen met veiligheidsfunctie, hoewel zij het gebruik van deze systemen niet per definitie uitsluit.

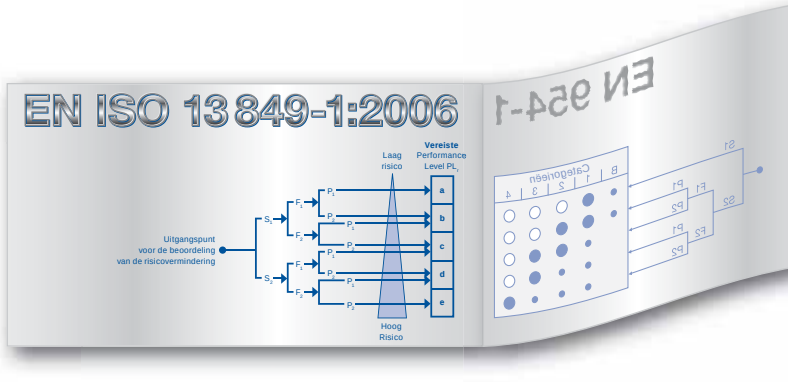
- We geven hier een (niet-beperkende) lijst met kritiekpunten, zodat de lezer een beter inzicht krijgt in de achterliggende redenen, die tot de revisie van de EN 954-1 geleid hebben, zonder dat we dieper op dit onderwerp moeten ingaan (zie ook figuur 2).

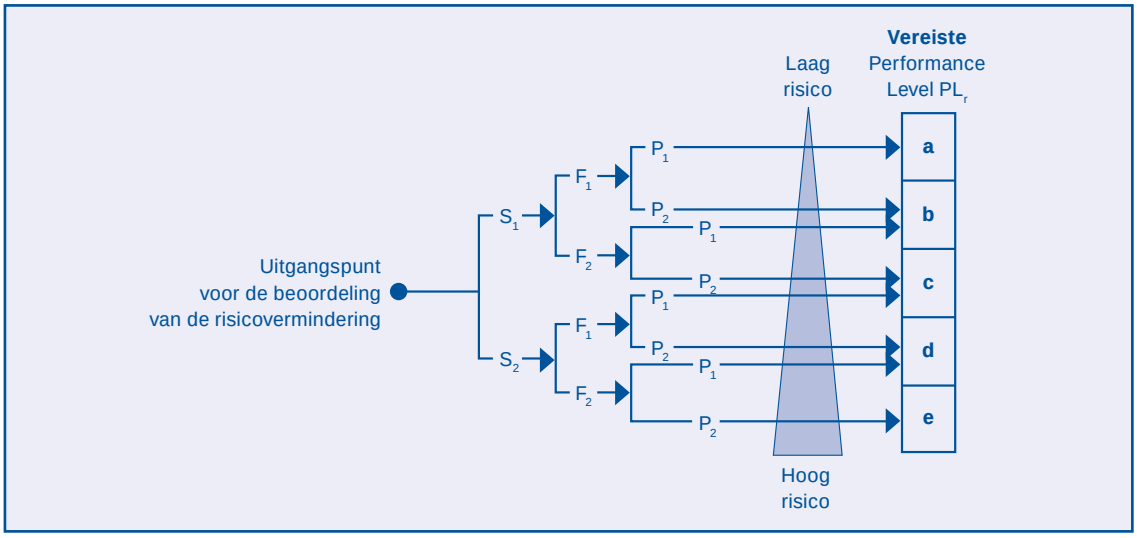
Kritiek:

- Ontbreken van gedetailleerde vereisten, ondanks de integratie van complexe programmeerbare elektronische systemen in de norm
- Onvoldoende vereisten voor het beoordelen van de betrouwbaarheid
- Door de uitsluiting van fouten in categorie 1 ontbreekt een hiërarchie voor de beoordeling van de risicovermindering
- Risicograaf: geen rechtstreeks verband tussen de risicovermindering en de categorie, de complexiteit blijft buiten beschouwing

Figuur 2: Enkele punten van kritiek op de bestaande norm EN 954-1

1) Zie ook CR 954-100: Richtlijnen voor het gebruik en de toepassing van de EN 954-1
2) **OPGELET!** Vanaf dit punt worden de onderdelen van besturingssystemen met een veiligheidsfunctie aangeduid door de afkorting “SRP/CS“, naar analogie met de Engelse term “Safety Related Part/Control System”!





Figuur 3: Vereiste risicovermindering en Performance Level: S = ernst van de verwonding; F = frequentie en/of duur van blootstelling aan het gevaar, P = mogelijkheden voor gevaarafwending

Nieuwe risicograaf

Theorie

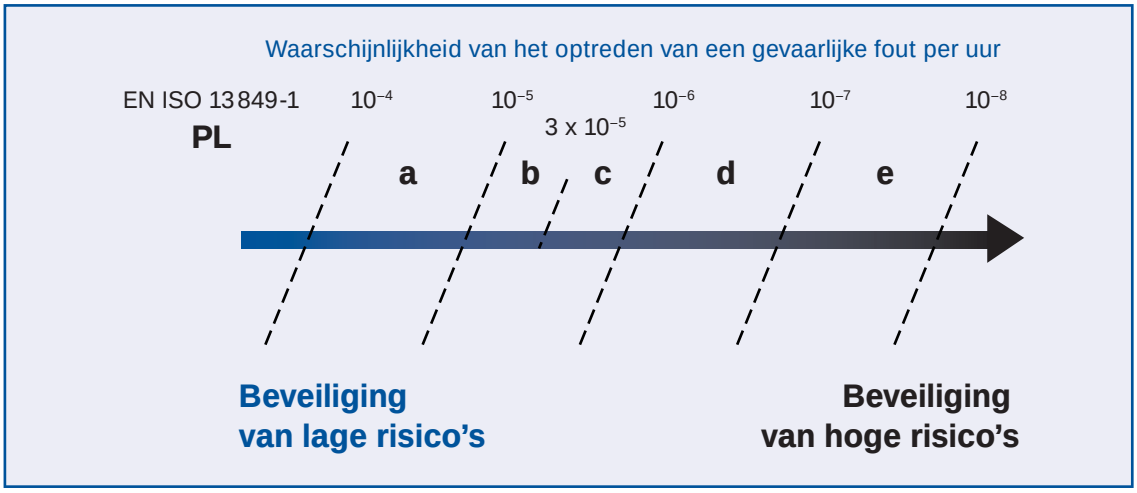
De EN ISO 13849-1: 2006 maakt nog altijd gebruik van het diagram voor het selecteren van de categorieën, de 'risicograaf' (zie figuur 3). Als eindresultaat moet men echter niet langer een categorie toekennen, zoals bij de EN 954-1, maar een "Performance Level" (PL) van "a" (laag) tot "e" (hoog). Het PL vertegenwoordigt het vermogen van een SRP/CS om een veiligheidsfunctie uit te voeren, zodat de verwachte risicovermindering bereikt wordt. De norm specificeert verder de parameters die een rol spelen bij het bepalen van dit Performance Level, zoals de betrouwbaarheid van het materiaal (de MTTF), de structuur van het systeem en de bewaking (DC, Diagnostic Coverage of foutendekking), de CCF (Common Cause Failures of fouten met een gemeenschappelijke oorzaak) en de categorie evenals de kwalitatieve en kwantificeerbare aspecten die het gedrag van de SRP/CS beïnvloeden zoals de systematische fouten.

De individuele risicoparameters S (ernst van de verwonding), F (frequentie en/of duur van blootstelling aan het gevaar) en P (mogelijkheid tot gevaarafwending) van EN ISO 13849-1: 2006 blijven ongewijzigd ten opzichte van EN 954-1.

Toepassing

De waarschijnlijkheid van een gevaarlijke uitval van het systeem, vertegenwoordigd door de waarde PFH_d (zie ook figuur 4) is afhankelijk van diverse factoren, waaronder de systeemstructuur, de foutendekking (Diagnostic Coverage DC), de betrouwbaarheid van de componenten ('Mean Time to Dangerous Failure', $MTTF_d$), de CCF (Common Cause Failures of fouten met een gemeenschappelijke oorzaak), het ontwerpproces, de belasting, de omgevingsvoorwaarden en de bedrijfsmodi. De analyse van de waarschijnlijkheid van restfouten is de nieuwe aanpak van de norm, en ontstaat door het toepassen van betrouwbare engineering en de combinatie van de deterministische en probabilistische benadering. De PL classificaties zijn zo gekozen dat zij met de zogeheten Safety Integrity Levels (SIL's) van de IEC EN 61 508 overeenstemmen en een verwijzing naar de sturingscategorieën van de EN 954-1 toelaten; bijvoorbeeld, sturingscategorie 1 stemt overeen met (is echter niet gelijkgesteld aan) PL "b", sturingscategorie 2 met PL "c" enz.

1) PFH = Probability of Failure per Hour: waarschijnlijkheid van het optreden van een fout per uur

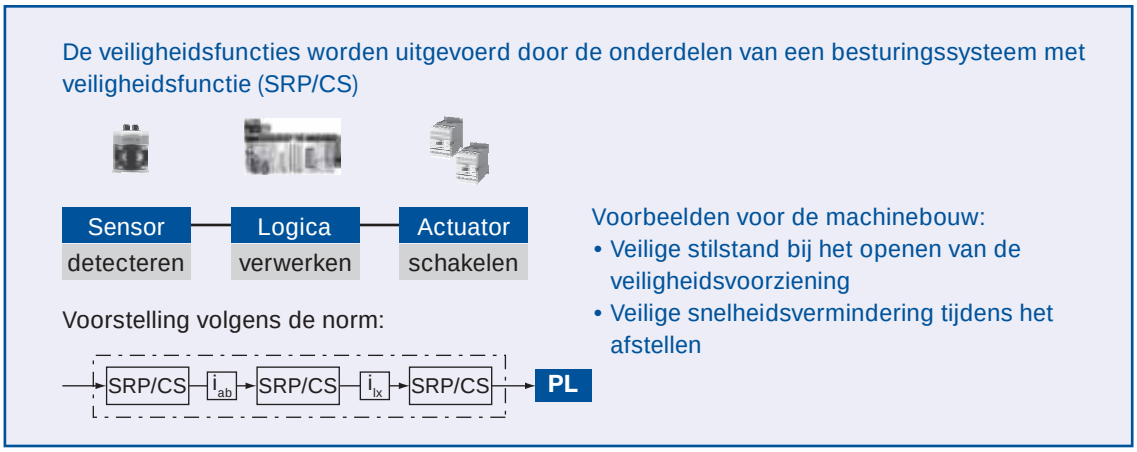


Figuur 4: Definitie van het Performance Level PL als veiligheidsrelevante betrouwbaarheidsfactor

Toepassing

- De ontwerper moet alle veiligheidsfuncties die vereist zijn voor het uitvoeren van de veiligheidsmaatregelen van het besturingssysteem voor de toepassing beoordelen en analyseren, bijvoorbeeld stilzetten in noodgeval (noodstop), het vergrendelen van beweegbare veiligheidsvoorzieningen, enz. Voor iedere geselecteerde veiligheidsfunctie moet een vereist Performance Level PL_r ("r" = "required") bepaald en gedocumenteerd worden.

- Het bepalen van het Performance Level PL is een beoordeling van de globale architectuur van de veiligheidsrelevante functies, die in subsystemen zoals sensoren (detecteren), de logica (verwerken) en de actuatoren (schakelen) onderverdeeld zijn.



Figuur 5: Veiligheidsfuncties en SRP/CS

1) De norm maakt systematisch een onderscheid tussen de PL_r en de PL. PL_r vertegenwoordigt het vereiste Performance Level (in feite de gewenste of doelwaarde) die uit de risicobeoordeling voortvloeit. Het PL is het resultaat van de analyse van de risicovermindering (in feite de werkelijke waarde).

Nieuwe aspecten voor de beoordeling
Door de combinatie van de deterministische en probabilistische aanpak wordt de PL van de SRP/CS door verschillende aspecten (zie figuur 6) bepaald, zoals:

1. De categorie (min of meer), waarvoor de norm zogeheten Designated Architectures voorschrijft, die een vereenvoudigde aanpak voor het kwantificeren van de berekende waarden bevatten;

2. De betrouwbaarheid van de componenten in de vorm van de "$MTTF_d$" waarde ("Mean Time to dangerous Failure" – *gemiddelde kans op gevaarlijke fout*);

3. De foutendekking = kans op detectie van fouten of 'Diagnostic Coverage' (DC);

4. De maatregelen ter vermijding van fouten met een gemeenschappelijke oorzaak ("Common Cause Failure" of CCF).

Hier worden verder nog maatregelen ter vermijding van systematische fouten aan toegevoegd, een vereiste die ook nu al van toepassing is. Deze maatregelen worden besproken in Bijlage G van de EN ISO 13849-1: 2006. De norm maakt een onderscheid tussen toevallige fouten (zie $MTTF_d$) en systematische fouten (zie figuur 7).

Systematische fouten hebben deterministische, niet toevallige of incidentele oorzaken en kunnen alleen door het aanbrengen van wijzigingen aan het ontwerp, het productieproces, de gebruiksprocedures, de documentatie of andere gepaste factoren geëlimineerd worden.

Bijlage G stelt maatregelen voor:

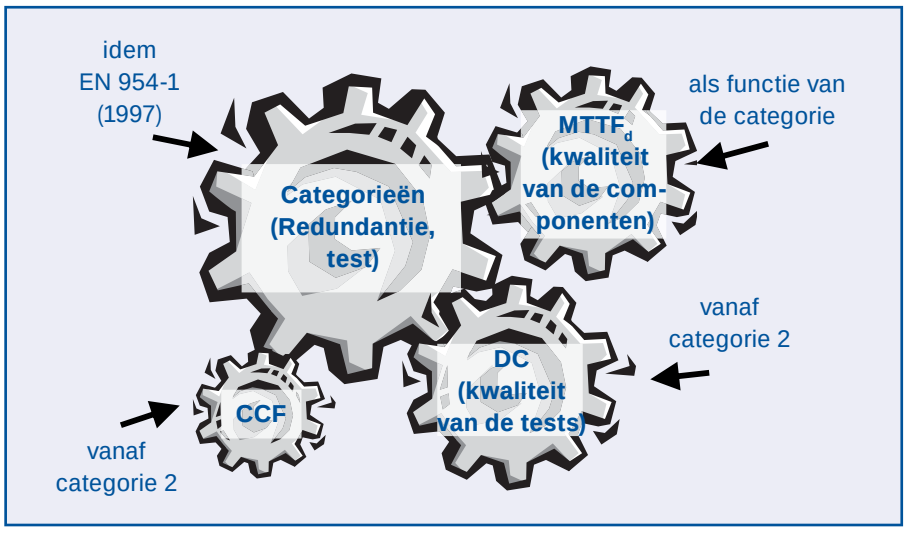
- Energie-uitschakeling, zie EN ISO 13849-2
- Beheersing of verbetering van de omgevingsinvloeden
- Maatregelen op informaticagebied: bewaking van de programma-afloop van de SRP/CS met software
- Beveiliging en beheersing van de datacommunicatie

Figuur 7: Systematische fouten vermijden en beheersen

Toepassing

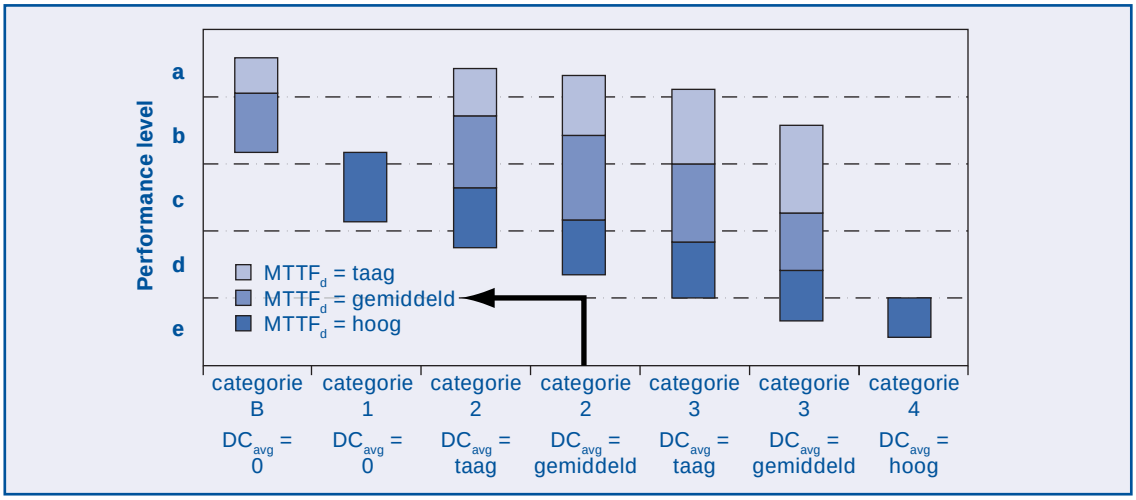
- De ontwerper moet alle veiligheidsfuncties die vereist zijn voor het uitvoeren van de veiligheidsmaatregelen van het besturingssysteem voor de toepassing beoordelen en analyseren, bijvoorbeeld stilzetten in noodgeval (noodstop), het vergrendelen van bewegende veiligheidsvoorzieningen, enz. Voor iedere geselecteerde veiligheidsfunctie moet een vereist Performance Level PL_r ("r" = "required") bepaald en gedocumenteerd worden.

- Het bepalen van het Performance Level PL is een beoordeling van de globale architectuur van de veiligheidsrelevante functies, die in subsystemen zoals sensoren (detecteren), de logica (verwerken) en de actuatoren (schakelen) onderverdeeld zijn. (zie figuur 5)



Figuur 6: Uitbreiding van het begrip "categorie"

1) De norm maakt systematisch een onderscheid tussen de PL_r en de PL. PL_r vertegenwoordigt het vereiste Performance Level (in feite de gewenste of doelwaarde) die uit de risicobeoordeling voortvloeit. Het PL is het resultaat van de analyse van de risicovermindering (in feite de werkelijke waarde).



Figuur 8: Vereenvoudigde methode voor het bepalen van het Performance Level PL

Performance Level in plaats van een categorie

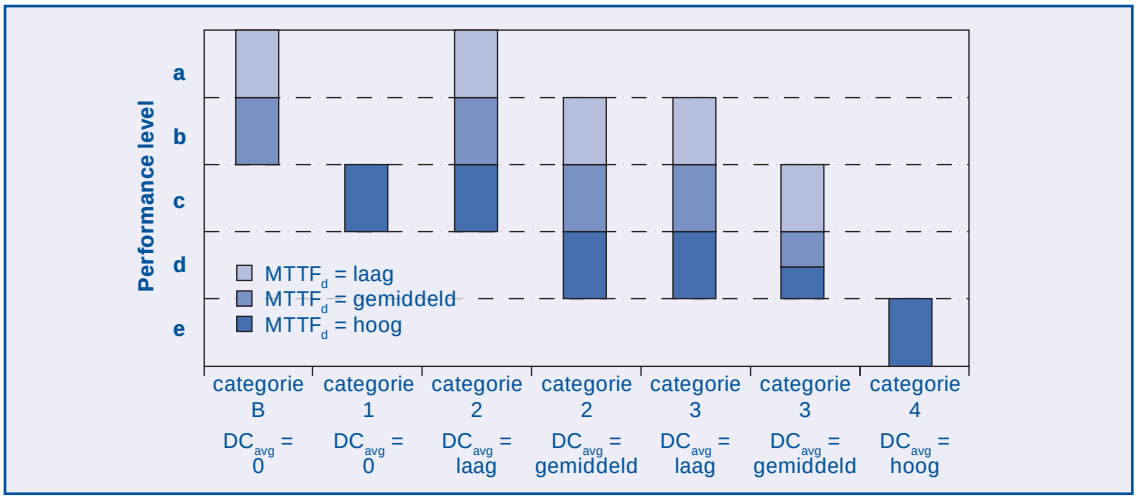
De resultaten van de beoordeling van de betrouwbaarheidswaarden (dus de evaluatie van de Designated architectures, de $MTTF_d$, de DC en de CCF) wordt vervolgens in een staafdiagram geplaatst om het Performance Level (zie figuur 8) te kunnen bepalen.

Dit betekent dat Performance Level “e“ een structuur vereist die overeenstemt met categorie 4, met een “hoge” $MTTF_d$ waarde per kanaal en een “hoge” DC (uitleg van de DC_{avg}: zie verder).

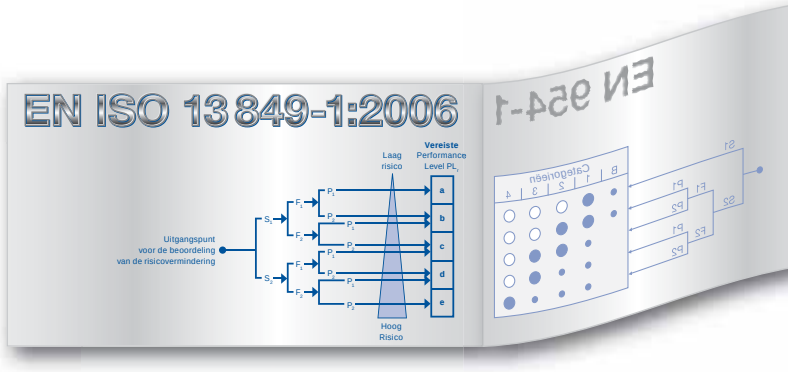
Wil men een Performance Level “c“ of “d“ bereiken voor de vereiste risicovermindering, dan kunnen diverse ontwerpmogelijkheden gekozen worden, bijvoorbeeld: voor een Performance Level “d“ een structuur volgens categorie 2, met $MTTF_d$ “hoog“ en DC “gemiddeld”. Vanaf categorie 2 moeten de CCF altijd in de beoordeling opgenomen worden.

Omwille van de vage afbakening van de grenszones van de diverse PL in het diagram is het gebruik van een vereenvoudigde methode toegestaan (de norm vermeldt hiervoor een tabel in plaats van een grafiek, zie figuur 9).

Tot zover een korte beschrijving van de grote lijnen van de EN ISO 13849-1.



Figuur 9: Performance Level PL: Alternatieve bepaling met behulp van een tabel



Designated Architectures

Theorie
De EN 13849-1 maakt nog altijd gebruik van de “oude“ categorieën van de EN 954-1 om de SRP/CS op basis van hun foutbestendigheid en hun gedrag ten gevolge van fouten in te delen. De EN ISO 13849-1: 2006 voorziet echter het gebruik van Designated architectures voor het bepalen van de categorieën, typische architecturen die aan de vereisten van de bijbehorende categorie beantwoorden. De bijdrage van deze structuren aan de risicovermindering werd op voorhand berekend met behulp van Markov-modellen (cf. IEC EN 61508). De gebruiker van EN ISO 13 849-1: 2006 moet dus geen ingewikkelde wiskundige berekeningen uitvoeren.

De inachtneming van de Designated Architecture van een SRP/CS borduurt verder op de deterministische aanpak van de EN 954-1 maar is slechts een van de vele aspecten van het Performance Level PL.

De Designated architectures zijn in feite de gekende en beproefde structuren van de SRP/CS die reeds jaren model staan voor de verschillende categorieën van de EN 954-1. Categorie 2 vormt echter een uitzondering.

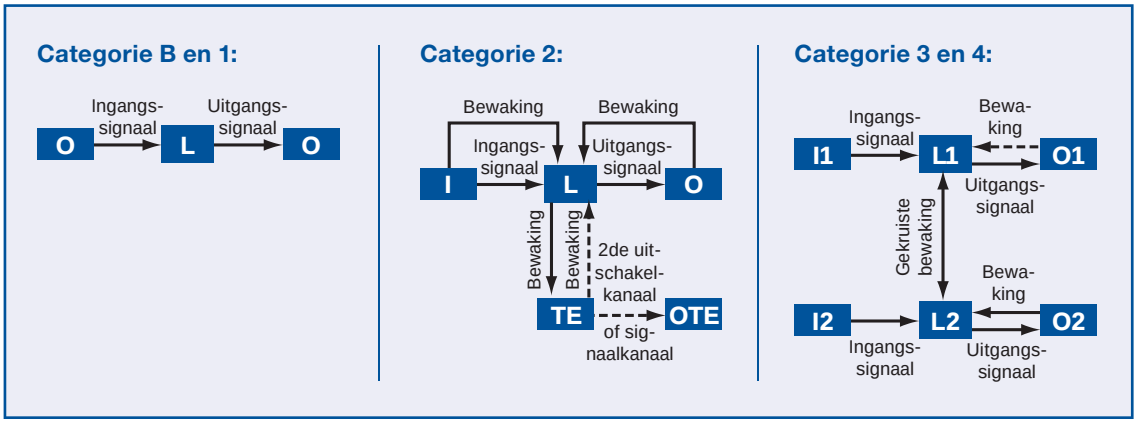
Uitvoering
Figuur 10 toont de Designated architectures die in de EN ISO 13849-1:2006 gebruikt worden.

Toepassing
Het gebruik van de Designated architectures is een onderdeel van de vereenvoudigde aanpak van de EN ISO 13894-1. Net als bij de interpretatie van de EN 954-1 blijven ook nu weer bepaalde vragen onbeantwoord.

Nemen we als voorbeeld de uitvoering van de 2-kanaligheid van sensoren en actuatoren voor de categorieën 3 en 4: moeten in dit geval twee sensoren of actuatoren gebruikt worden voor de positiebewaking van bewegende veiligheidsvoorzieningen? En wat te doen als men van de Designated architectures wil afwijken?

De gebruiker heeft vele mogelijkheden:

Een eerste mogelijkheid is gebaseerd op de C-norm (productnorm) die concrete voorstellen voor de uitvoering formuleert. Voor de positiebewaking van bewegende veiligheidsvoorzieningen aan print- en drukmachines bijvoorbeeld volstaat een gewone veiligheidsschakelaar met 2 elektrische kanalen.



Figuur 10: Inleiding tot de Designated architectures

Een tweede mogelijkheid is het gebruikmaken van de foutuitsluiting (zie figuur 11). Hier moet het foutweerstandsvermogen van de SRP/CS geëvalueerd worden. Bij enkele componenten kunnen in uitzonderlijke gevallen bepaalde fouten uitgesloten worden tijdens de levensduur van de SRP/CS. Onder deze omstandigheden hoeft men bij de bepaling van het Permance Level geen rekening te houden met deze fouten. Indien gebruik wordt gemaakt van foutuitsluiting moet in de documentatie een uitvoerige rechtvaardiging worden opgenomen.

Bijlagen A tot D van de EN ISO 13849-2 (de vroegere EN 954-2) bevatten lijsten met de belangrijkste fouten voor de verschillende technologieën. Deze foutlijsten zijn niet beperkend en indien nodig, moeten eventuele bijkomende fouten beoordeeld en vermeld worden onder de strikte toepassing van paragraaf 3.3 van de EN ISO 13849-2. Ook in dit geval moet de gebruikte evaluatiemethode duidelijk beschreven worden.

Wanneer mag ik fouten uitsluiten?

Bij de evaluatie van een SRP/CS mogen soms bepaalde fouten uitgesloten worden. Voor meer details over foutuitsluiting verwijzen we naar de EN ISO 13849-2. …

De fouten kunnen uitgesloten worden op basis van:

- de technische onwaarschijnlijkheid dat een fout zich voordoet
- de algemeen aanvaarde technische ervaring, onafhankelijk van de toepassing
- de technische vereisten van de toepassing en de speciale risico's en gevaren

In geval van foutuitsluiting moet de documentatie een uitvoerige rechtvaardiging bevatten.

Figuur 11: Foutuitsluiting

Als derde mogelijkheid kan men de vereenvoudigingen van de EN ISO 13849-1: 2006 overboord gooien en met behulp van Markov-modellen, Petrinetwerken (GSPN) of betrouwbaarheidsdiagrammen zelf de nodige wiskundige berekeningen (laten) uitvoeren (zie figuur 12).

Is het gebruik van de Designated architectures verplicht?

4.5.1 … Er bestaan diverse methodes om het Performance Level PL voor ieder type systeem (bijvoorbeeld een complexe structuur) te berekenen, zoals Markov-modellen, Generalised Stochastic Petri Nets (GSPN), betrouwbaarheidsblokdiagrammen [zie bijvoorbeeld de série EN 61 508 (IEC 61 508)].

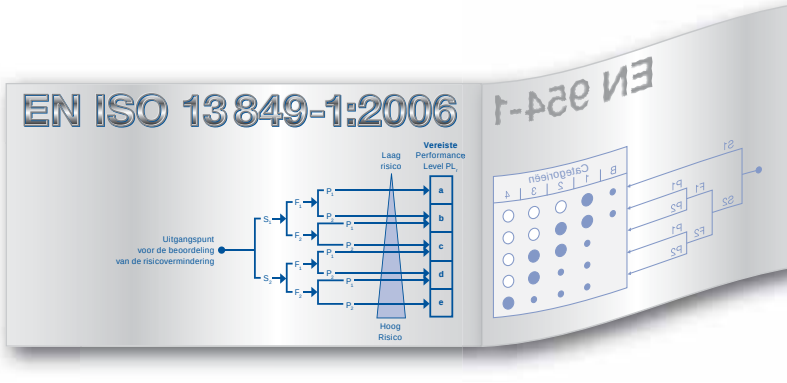
Om de beoordeling van de kwantitatieve aspecten van het Performance Level PL te vergemakkelijken biedt deze norm een vereenvoudigde methode voor het berekenen van het PL, beperkt tot vijf Designated architectures, die aan speciale ontwerpcriteria en een specifiek gedrag in geval van een fout beantwoorden)

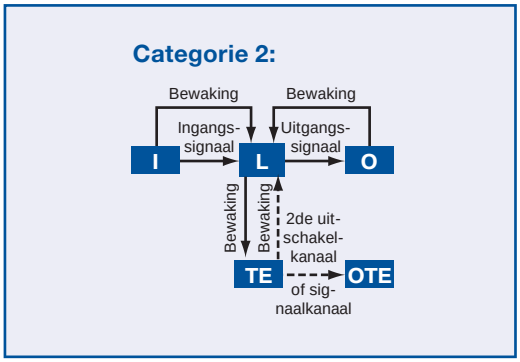
Figuur 12: "Geen regels zonder uitzonderingen"

OPGELET bij het gebruik van de Designated architectures voor categorie 2!

De aanbevolen structuur voor categorie 2 vormt een uitzondering op de gekende Designated architectures.

De SPR/CS van categorie 2 die 1-kanalig uitgevoerd zijn, moeten zodanig ontworpen zijn dat hun functies op gepaste tijdstippen met een testfrequentie die 100 maal hoger ligt dan de geschatte belasting van de veiligheidsfunctie gecontroleerd worden door de machinebesturing; daarnaast moet een tweede uitgang aanwezig zijn. (zie figuur 13, pagina 15).





Figuur 13: Nieuwe vereisten voor categorie 2

In feite kan deze Designated architecture als een 'light' versie van categorie 3 beschouwd worden. Wij raden u met aandrang aan SRP/CS met sturingscategorie 2 te testen met het oog op de conformiteit met de toekomstige gewijzigde vereisten.

$MTTF_d$ waarden

Theorie

Bij het berekenen van de $MTTF_d$ waarden in het kader van de EN ISO 13849-1: 2006, moet men er rekening mee houden dat SRP/CS altijd een zeker percentage restrisico's inhouden, die de veiligheidsfunctie kunnen beïnvloeden (namelijk de waarschijnlijkheid van toevallige gevaarlijke fouten). Het komt er dus op aan deze restrisico's te beheersen en tot een aanvaardbaar niveau terug te dringen.

Een schakelcontact kan bijvoorbeeld niet openen of sluiten. Gewoonlijk veroorzaakt deze toestand in de machinebesturing een gevaarlijke situatie bij gebrek aan een gepast redundant systeem of een geschikte bewaking. Alle contacten zijn echter niet hetzelfde: er bestaan kwaliteitsverschillen op het gebied van hun ontwerp, het gebruikte materiaal, enz.

Deze "kwaliteitsverschillen" kunnen de waarschijnlijkheid van het optreden van toevallige fouten beïnvloeden.

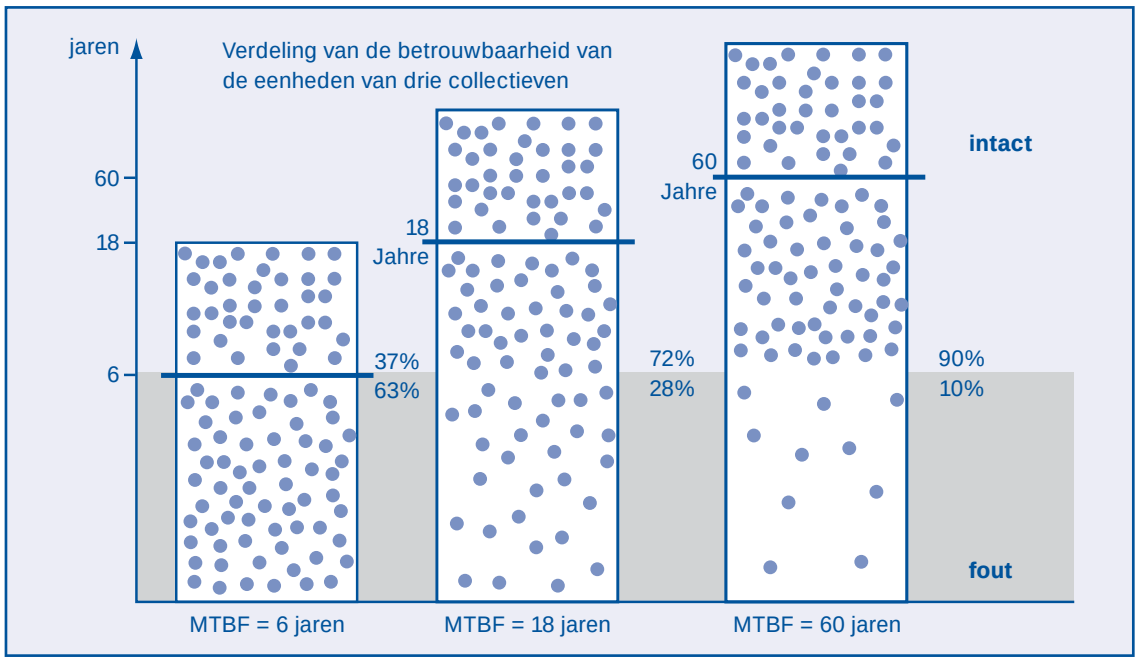
De $MTTF_d$ waarde is dus een beoordeling van de kwaliteit van de betrouwbaarheid op veiligheidsgebied van de componenten en systemen die in een SRP/CS gebruikt worden.

$MTTF_d$ is een statistische gemiddelde waarde die de verwachte werkduur zonder fout of storing in jaren uitdrukt (= $MTTF_d$, Mean Time To Dangerous Failure). Een fout wordt gedefinieerd als het verdwijnen van het vermogen van een entiteit om de vereiste functie te vervullen. De fouten die alleen de beschikbaarheid van het aangestuurde proces beïnvloeden, maken geen deel uit van het toepassingsgebied van de EN ISO 13849-1: 2006. Omdat niet alle fouten invloed hebben op de veiligheid, is de MTTFd waarde altijd > de MTTF waarde. De waarde wordt uitgedrukt in jaren (= y).

De $MTTF_d$ waarde is altijd de reciproque van de PFH_d waarde en omgekeerd. Een $MTTF_d$ waarde van 10 jaar [= 1 × 8.760 uur] is bijvoorbeeld het equivalent van een PFH_d waarde van $1{,}14 \times 10^{-5}$ [1/(10 × 8.760)]. Voor het toepassen van de EN ISO 13849-1 is het van essentieel belang dat de $MTTF_d$ altijd beschouwd wordt voor ieder kanaal van een SRP/CS.

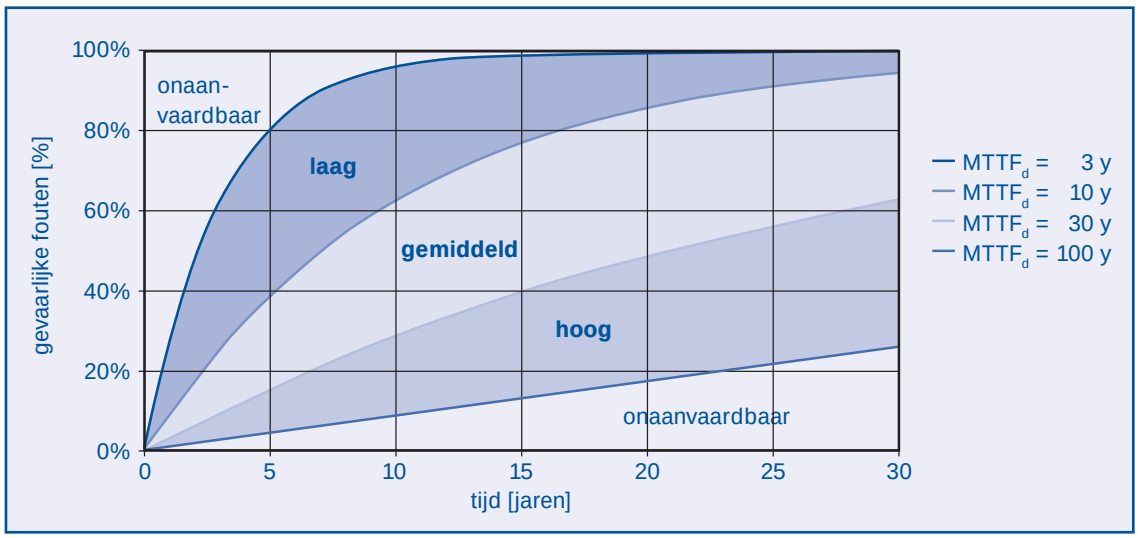
De berekeningen van de MTTF of $MTTF_d$ waarden gaan altijd uit van een exponentiële verdeling van de toevallige fouten. Na het verstrijken van de MTTF of $MTTF_d$, is een (gevaarlijke) fout opgetreden aan 63% van alle eenheden of, anders gezegd: de overlevingswaarschijnlijkheid van de betroffen eenheden na het verstrijken van de MTTF of $MTTF_d$ bedraagt nog slechts 37% (zie figuur 14 en 15).

1) PFH waarden die volgens IEC EN 61508 berekend werden, mogen in de berekeningen volgens EN ISO 13849-1 opgenomen worden, mits inachtneming van de SIL vermeldingen. Dit is een zeer vereenvoudigde berekeningsmethode, vooral voor 2-kanalige structuren, die echter een te rooskleurige voorstelling van de toestand vermijdt.

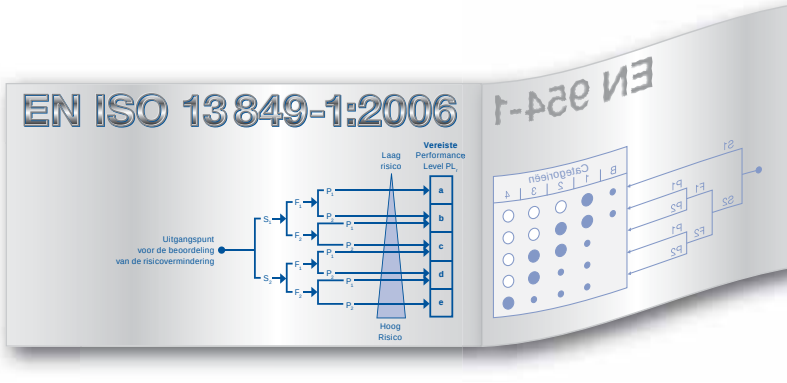


Figuur 14: Aanschouwelijke voorstelling van een gemiddelde levensduur. De drie getoonde collectieven hebben verschillende betrouwbaarheidsniveaus. Hun eenheden (voorgesteld door puntjes) gaan op toevallige momenten in storing. De tijdstippen waarop de fout optreedt, worden door de verticale coördinaten vertegenwoordigd. De fouten zijn verspreid over een tamelijk lange periode; bepaalde afzonderlijke eenheden hebben een levensduur van 18 jaar, terwijl aan anderen al na één jaar een fout optreedt. Na 6 jaar heeft zich een fout voorgedaan aan 63% van de eenheden. (Bron: Inleiding tot de methodes voor betrouwbaarheidsanalyse, SIEMENS AG, I&S IS ICS IT2).

Anders gezegd:



Figuur 15: Wat betekent MTTF$_d$



OPGELET! Slijtagegevoelige componenten hebben een verschillende levensduur en worden uitgesloten uit deze veronderstelling van exponentiële verdeling, die typisch is voor elektrische componenten. De EN ISO 13849-1: 2006 houdt rekening met dit soort componenten via de uitkomst van de berekening van de B_{10d} waarde.

Uitvoering
Volgens de EN ISO 13849-1:2006 moeten de berekeningen van de $MTTF_d$ en de PFH_d gedifferentieerd worden op basis daarvan of zij gebruikt worden:

- voor een veiligheidscomponent
  of
- een kanaal van een SRP/CS
  of
- een volledige SRP/CS

Deze differentiatie is alleen maar zinvol als het merendeel van de gebruikers van EN ISO 13849-1: 2006 hun componenten en andere veiligheidsrelevante systemen die in de SRP/CS geïntegreerd worden, niet zelf fabriceert, maar aankoopt.

De gebruikers van EN ISO 13849-1: 2006 die gebruiksklare veiligheidscomponenten kopen bij firma's zoals de Schmersal Groep, zullen zich voortaan in een bevoorrechte positie bevinden. Het is immers logisch dat alle bekende fabrikanten van veiligheidscomponenten op de situatie zullen inspelen en zo snel mogelijk de volgens de EN ISO 13849-1: 2006 vereiste waarden in hun productspecificaties zullen opnemen (zie ook paragraaf "Inwerkingtreden van de EN ISO 13849-1: 2006").

Deze waarden moeten eveneens meegedeeld worden voor componenten, apparaten en systemen die volgens de Europese Machinerichtlijn strikt genomen geen veiligheidscomponenten, maar eerder "dual use" producten zijn, dit wil zeggen componenten en toestellen voor dubbel gebruik, dus voor veiligheidsgerichte en "gewone" toepassingen.

OPGELET! In geval van een foutuitsluiting voor een bepaalde component, moet de MTTFd waarde voor deze component in de formule gelijkgesteld worden aan ∞ (zie verder).

Toepassing: $MTTF_d$ voor een kanaal
In dit geval moet de gebruiker met behulp van een formule de $MTTF_d$ waarde van ieder kanaal afzonderlijk berekenen volgens de zogeheten "Parts Count Method". Deze berekening maakt gebruik van de $MTTF_d$ waarden van alle afzonderlijke componenten van het bijbehorende kanaal – zie berekeningsvoorbeeld pagina 18.

$$\frac{1}{MTTF_d} = \sum_{i=1}^{N} \frac{1}{MTTF_{di}}$$

Figuur 16: $MTTF_d$ van een kanaal (volgens de "Parts Count Method")

Vervolgens moet hij het resultaat vergelijken met de waarden uit de tabel (figuur 17) om de veiligheidsrelevante kwaliteit van één kanaal van de SRP/CS te bepalen.

1) Gebrauchsfertige Sicherheitsbauteile im MRL-Sinne und Dual-Use-Produkte (wie vor) in einem SRP/CS werden nachfolgend pauschal auch als „sicherheitsgerichtete Geräte" bezeichnet.

Beschrijving van de kwaliteit	$MTTF_d$ waarde
laag	3 jaar ≤ $MTTF_d$ < 10 jaar
gemiddeld	10 jaar ≤ $MTTF_d$ < 30 jaar
hoog	30 jaar ≤ $MTTF_d$ ≤ 100 jaar

$MTTF_d$ is een gemiddelde statistische waarde en vertegenwoordigt in geen geval de gegarandeerde levensduur!

Figuur 17: $MTTF_d$ – Gemiddelde waarde voor de bedrijfsduur zonder gevaarlijke fout in een kanaal van het besturingssysteem

Berekeningsvoorbeeld

j	Component	eenheden (n_j)	$MTTF_{d,j}$ worst case [y]	$1/MTTF_{d,j}$ worst case [1/y]	$nj/MTTF_{d,j}$ worst case [1/y]
1	Transistor bipolair, laag vermogen	2	1142	0,000876	0,001752
2	Weerstand, carbonfilm	5	11416	0,000088	0,000438
3	Condensator, standaard geen vermogen	4	5708	0,000175	0,000701
4	Relais (gegevens volgens de fabrikant)	4	1256	0,000796	0,003185
5	Contact	1	32	0,031250	0,031250
$\Sigma(n_j/MTTF_{d,j})$					0,037325
$MTTF_d = 1/\Sigma(n_j/MTTF_{d,j})$ [y]		**26.79**			

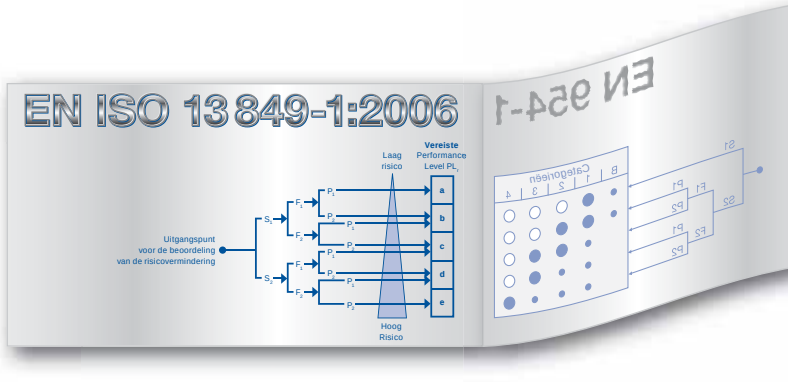
De uitkomst van dit voorbeeld, een $MTTF_d$ van 26,8 jaar, stemt volgens figuur 17 overeen met de classificatie “gemiddeld”. In dit voorbeeld oefent het contact de grootste invloed uit. Het resultaat is gewoonlijk beter, d.w.z. levert een hogere $MTTF_d$ op.

Hierbij moeten de volgende “spelregels“ in acht genomen worden:

- De $MTTF_d$ waarden gelden altijd voor een kanaal, ongeacht de Designated architecture (1 of 2 kanalen), behalve als de kanalen diversitair opgebouwd zijn. In dat geval moet een symmetrieformule gebruikt worden (zie figuur 18).

- Volgens de Europese Machinerichtlijn is de machinebouwer of –verkoper verantwoordelijk voor het (laten) berekenen van de $MTTF_d$ waarde van een kanaal.

- **OPGELET!** Als de uitkomst van de $MTTF_d$ voor een kanaal van een SRP/CS >100 jaar wordt het getal boven 100 buiten beschouwing gelaten, omdat de maximale $MTTF_d$ waarde van een kanaal van een SRP/CS beperkt is tot 100 jaar (dit in tegenstelling tot een afzonderlijke [veiligheids]component, die een hogere score kan hebben). Door deze limiet op 100 jaar vast te stellen wil het normalisatiecomité een te rooskleurige voorstelling van de $MTTF_d$ waarden vermijden om zo tot een hoger Performance Level te komen. Deze procedure verhindert eveneens het gebruik van berekeningsmethodes, waardoor uiteindelijk het gebruik van 1-kanalige structuren toegelaten is, als de toepassing in feite 2-kanalige structuren vereist.



- **De Designated architectures gaan ervan uit dat de MTTFd waarden van de verschillende kanalen van een redundante SRP/CS identiek zijn.**
- **Symmetrieformule bij verschillende $MTTF_d$ waarden:**

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right]$$

- **Voorbeeld: $MTTF_{d\,C1}$ = 3 jaar, $MTTF_{d\,C3}$ = 100 jaar, daaruit volgt $MTTF_d$ = 66 jaar**

Figuur 18: Symmetreren van de $MTTF_d$ voor verschillende kanalen

- **OPGELET!** Het combineren van afzonderlijke veiligheidsrelevante componenten van een SRP/CS gaat ervan uit dat:
  - de toepassing plaats vindt onder strikte inachtneming van de eventuele opmerkingen en instructies uit de bedieningshandleidingen en
  - toegepaste foutuitsluitingen volgens de ISO 13849-2 gegarandeerd zijn, vooral wat de bekabeling betreft
- de speciale vereisten van de EN ISO 13849-1:2006 (zie paragraaf 4.6) van toepassing zijn op eventueel gebruikte software
- Als de twee kanalen van een SRP/CS een diversitaire structuur hebben, moet de symmetrieformule toegepast worden (zie figuur 18).

Opmerkingen

- Fabrikanten die individuele componenten voor een SRP/CS leveren, die aan de vereisten van de IEC EN 61508 (of IEC EN 62061) moeten beantwoorden, zijn verplicht een “lambda“ waarde (λ) te vermelden.

  Wil of moet men voor de veiligheidsgerichte componenten gegevens uit de twee “werelden“ van de EN ISO 13849-1:2006 en de IEC EN 61508 (of IEC EN 62061) gebruiken, dan wordt aanbevolen het SIL niveau om te zetten naar Performance Level PL of het Performance Level PL in een SIL niveau (zie ook pagina 44). Het is ongewenst de twee begrippen door elkaar te gebruiken.
- Is alleen de MTTF waarde beschikbaar is (en dus geen $MTTF_d$ waarde), dan mag de MTTF waarde verdubbeld worden om de $MTTF_d$ waarde te bepalen, mits het evenwicht tussen de gevaarlijke en ongevaarlijke fouten min of meer behouden blijft. In geval van twijfel raadt de EN ISO 13849-1:2006 aan slechts een gedeelte (voorstel: 10%) in de berekening op te nemen.
- Als alleen de MTBF waarde (Mean Time Between Failure, gemiddelde tijd tussen fouten) beschikbaar is, mag deze, om de procedure te vereenvoudigen, zoals een MTTF waarde behandeld worden.

Toepassing: $MTTF_d$ berekening voor een afzonderlijke veiligheidsrelevante component

Dit voorbeeld is bedoeld voor personen die veiligheidsgerichte componenten, systemen en ‘dual use’ producten voor eigen gebruik bouwen. Zij moeten de veiligheidsgerichte apparatuur volledig opdelen in afzonderlijke functionele componenten en de $MTTF_d$ waarde met behulp van de Parts Count Method berekenen.

In dit geval verstrekt de EN ISO 13849-1:2006 eveneens hulpmiddelen die gebruikt kunnen worden als de MTTF of $MTTF_d$ waarden ontbreken of niet beschikbaar zijn. Bijlage C van de norm bevat tabellen met de typische gemiddelde $MTTF_d$ waarden van afzonderlijke elektrische en elektronische componenten (zie figuur 19). Andere naslagwerken zijn bijvoorbeeld de norm SN 29500 of de MIL handboeken.

Tabellen C.2 tot C.7 vermelden de typische gemiddelde $MTTF_d$ waarden voor elektrische componenten van de SN 29500, bijvoorbeeld

Component	Voorbeeld	MTTF [y] component	$MTTF_d$ [y] typisch	$MTTF_d$ [y] worst case	Gevaarlijke fouten
Transistor, bipolair	TO18, TO92, SOT23	34.247	68.493	6.849	50%
Zenerdiode		15.981	31.963	3.196	50%
Condensator	KS, KP, MKT, MKC …	57.078	114.155	11.416	50%
Weerstand, carbonfilm		114.155	228.311	22.831	50%
Opto-koppler met bipolaire uitgang	SFH 610	7.648	14.840	1.484	50%

Figuur 19: $MTTF_d$ voor elektrische componenten (uittreksel/voorbeelden)

EN ISO 13849-1: 2006 besteedt speciale aandacht aan de slijtagegevoelige componenten van een SRP/CS, omdat de belasting (de frequentie waarmee een veiligheidsrelevante functie van de SRP/CS geactiveerd wordt) van doorslaggevend belang is voor hun $MTTF_d$ waarde.

Een directe $MTTF_d$ waarde is alleen beschikbaar voor elektronische en veiligheidsgerichte componenten, omdat de zogenaamde badkuipcurve als indicator voor slijtageonafhankelijke fouten dient. De linkerkant (sleutelwoord: vroegtijdige fouten) van de U-curve wordt niet in rekening genomen, omdat de fabrikant aangepaste maatregelen zoals kunstmatige veroudering kan treffen om vroegtijdige fouten uit te sluiten. De rechterkant wordt eveneens uitgesloten omdat deze de werkelijke levensduur ruimschoots overschrijdt.

B_{10d} waarden
Bij het berekenen van de $MTTF_d$ waarde voor slijtagegevoelige (mechanische, elektromechanische of vloeistof) componenten moet een tussengrootte, de zogeheten B_{10d} waarde, gebruikt worden. Deze stemt min of meer overeen met het aantal schakelingen waarvoor de veiligheidsgerichte functie, volgens de Weibull benadering, als aanvaardbaar beschouwd wordt.

De B_{10d} waarde wordt omgezet in een $MTTF_d$ waarde met inachtneming van de toepassingsvoorwaarden, namelijk de levensduur en de gemiddelde belastingsgraad van de veiligheidsfunctie van de betroffen component (zie figuur 20).

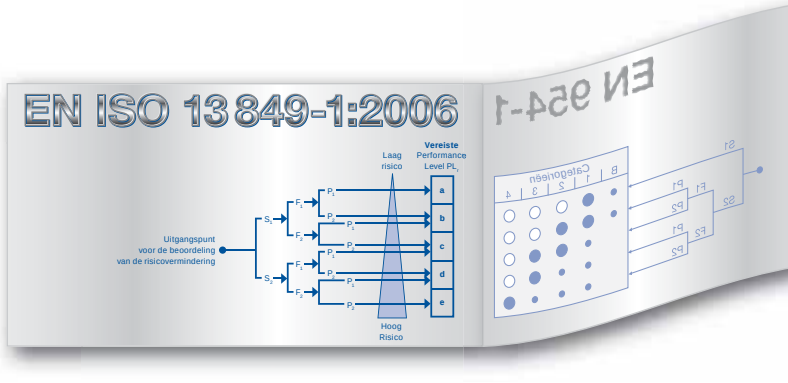
- **De fabrikant vermeldt de B_{10d} waarde van de component** (in de vorm van het aantal schakelingen, waarbij 10% van de geteste prototypes statistisch gezien een gevaarlijke fout vertonen).
- **Vervolgens moet de gemiddelde schakelfrequentie van de toepassing bepaald worden, bijvoorbeeld 0,2 Hz = > interval t_{cycle} = 5 s.**
- **Omzetting van B_{10d} (schakelingen) in $MTTF_d$ (jaren):**

$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3.600 \frac{s}{h}}{t_{cycle}}$$

d_{op}= gemiddeld aantal bedrijfsdagen per jaar
h_{op} = gemiddeld aantal bedrijfsuren per dag
n_{op}: gemiddeld aantal schakelingen per jaar
t_{cycle} = gemiddelde belasting van de veiligheidsfunctie in s (bijvoorbeeld 4 × per uur = 1 × per 15 min. = 900 s)

Figuur 20: Berekening van de $MTTF_d$ waarde voor slijtagegevoelige componenten



$MTTF_d$ mechanische componenten	150 jaar
$MTTF_d$ hydraulische componenten	150 jaar
B_{10d} pneumatische componenten	20.000.000
Relais/contact (lage belasting) B_{10d}	20.000.000
Relais/contact (maximale belasting) B_{10d}	400.000
Hoofdschakelaar (lage belasting) B_{10d}	20.000.000
Hoofdschakelaarcontact (nominale belasting) B_{10d}	2.000.000
Noodstopvoorziening B_{10d}	10.000
Bedienorgaan (drukknop) B_{10d}	100.000

Factor 50

Figuur 21: B_{10d} waarden (uittreksel) volgens de norm

Daarnaast vermeldt EN ISO 13 849-1:2006 aanbevolen B_{10d} waarden (zie figuur 21) voor typische slijtagegevoelige componenten, die de ontwerper van de SRP/CS kan gebruiken bij gebrek aan specificaties van de fabrikant.

Hierbij houdt de norm (bijvoorbeeld voor contactgevers en relais) rekening met de belasting van de component. 'Belasting' moet hier niet uitsluitend in de elektrische betekenis gezien worden; de omgevingsvoorwaarden en de bedrijfsomstandigheden moeten in hun geheel bekeken worden.

De norm stelt 20% voorop als maatstaf voor een lage belasting, hoewel tussenwaarden (echter niet lineair) toegestaan zijn. Bijvoorbeeld: (voor 20 miljoen schakelingen en 20%) 7,5 miljoen schakelingen bij 40%, 2,5 miljoen schakelingen bij 60% en 1 miljoen schakelingen bij 80%.

t_{cycle} =	24 h	1 h	1 min.	1 sec.
Pneumatische componenten	547.945	22.831	380	6,3
Relais/contact (lage belasting)	547.945	22.831	380	6,3
Relais/contact (maximale belasting)	10.960	457	7,6	0,1
Hoofdschakelaar (lage belasting)	547.945	22.831	380	6,3
Hoofdschakelaar (nominale belasting)	54.794	2.283	38	0,6
Noodstopvoorziening	274	11	0,2	0,003
Bedienorgaan (drukknop)	2.739	114	1,9	0,032

$MTTF_d$ > 100 jaar

Figuur 22: Geconverteerde $MTTF_d$ waarden voor pneumatische en elektromechanische componenten in functie van de belastingsgraad (t_{cycle})

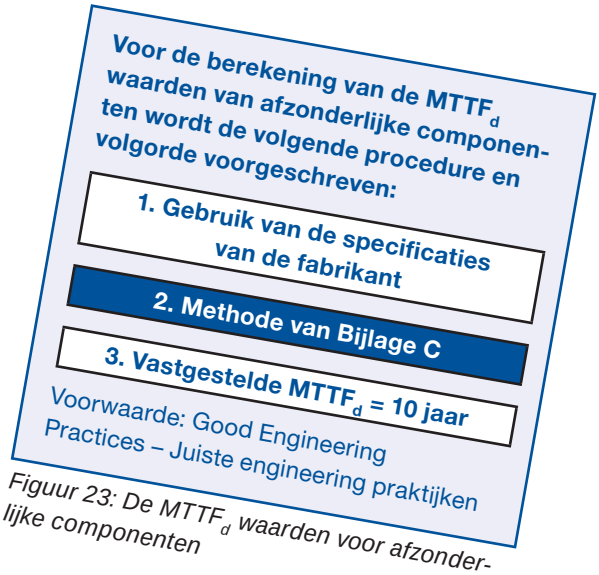
Voor de mechanische en hydraulische componenten die van de norm afwijken, heeft het normalisatiecomité op basis van empirische onderzoeken de $MTTF_d$ waarde vastgesteld op 150 jaar, onafhankelijk van de belastingsgraad.

Figuur 22 toont het voorbeeld van de omrekening van B_{10d} waarden in $MTTF_d$ waarden op basis van verschillende belastingsgraden (1 × alle 24 uur, 1 x per uur, enz.). Het voorbeeld gaat uit van een werking van 24u/dag, 365 dagen per jaar.

T_{10d} waarden
OPGELET! EN ISO 13849-1 voorziet dat uit de berekende B10d waarde vervolgens een T_{10d} waarde afgeleid wordt. Deze stemt overeen met 10% van de berekende $MTTF_d$ waarde. In dit verband wordt dan ook aanbevolen de veiligheidsgerichte componenten te vervangen zodra zij hun T_{10d} waarde bereiken.

Juiste engineering praktijken
EN ISO 13849-1:2006 schrijft voor dat de ontwerper in de $MTTF_d$ berekening bij voorkeur de specificaties van de fabrikant voor de gebruikte componenten gebruikt. De eventueel ontbrekende $MTTF_d$ waarden kunnen vervolgens ingevuld worden met behulp van de hiervoor vermelde vereenvoudigde methodes (= de tabellen).

Tegelijkertijd formuleert de norm kadervoorwaarden die bijkomend in acht genomen moeten worden, vooral bij het gebruik van de tabellen – zie figuur 24.



Figuur 23: De $MTTF_d$ waarden voor afzonderlijke componenten

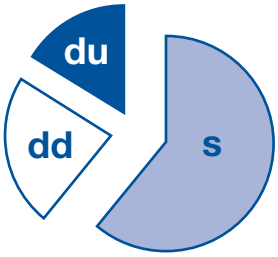
- **Naleving van de essentiële en beproefde veiligheidsprincipes (EN ISO 13849-2) bij het ontwerp van de component**
- **Duidelijke vermelding van de geschikte toepassingen en de toegelaten gebruiksvoorwaarden (fabrikant)**
- **Naleving van de essentiële en beproefde veiligheidsprincipes tijdens de installatie en het gebruik van de component**

➥ **Als deze voorwaarden vervuld zijn, gelden de foutmarges zoals ze in de norm vermeld worden**

➥ **Deze voorwaarden gelden zowel voor de fabrikant, de installateur als de gebruiker van de component**

Figuur 24: Good Engineering Practices – Juiste engineering praktijken

1) BIA rapport 6/04, Onderzoek van de verouderingsprocessen van hydraulische kleppen www.hvbg.de/bgia. Webcode: 1006447



$$DC = \frac{\sum \lambda_{dd}}{\sum \lambda_{dd} + \lambda_{du}}$$

Diagnostic Coverage (foutendekking)

Figuur 25: Diagnostic Coverage DC

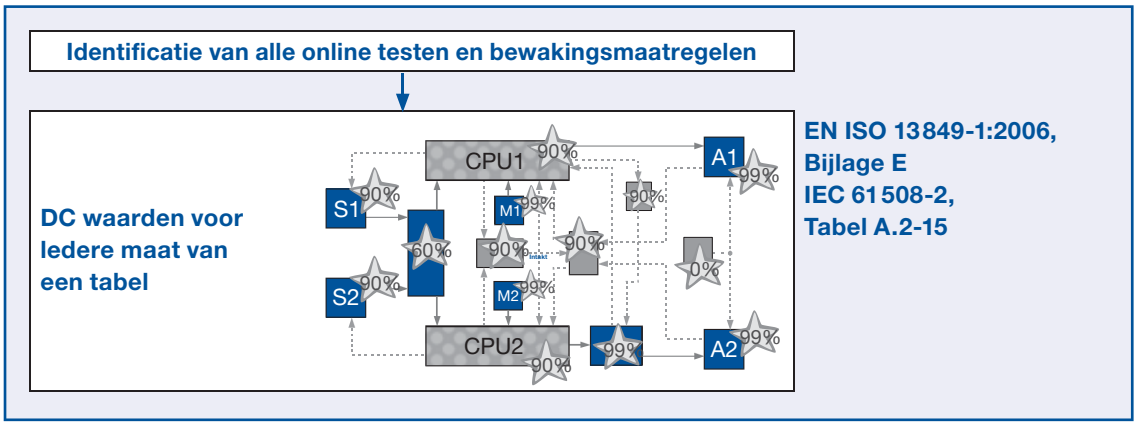
Diagnostic Coverage

Theorie
Hoewel de vereisten van de EN ISO 13849-1: 2006 met betrekking tot de $MTTF_d$ berekeningen tamelijk duidelijk en rechtlijnig zijn, moeten er bij de analyse van de Diagnostic Coverage (= DC) toch concessies gedaan worden.

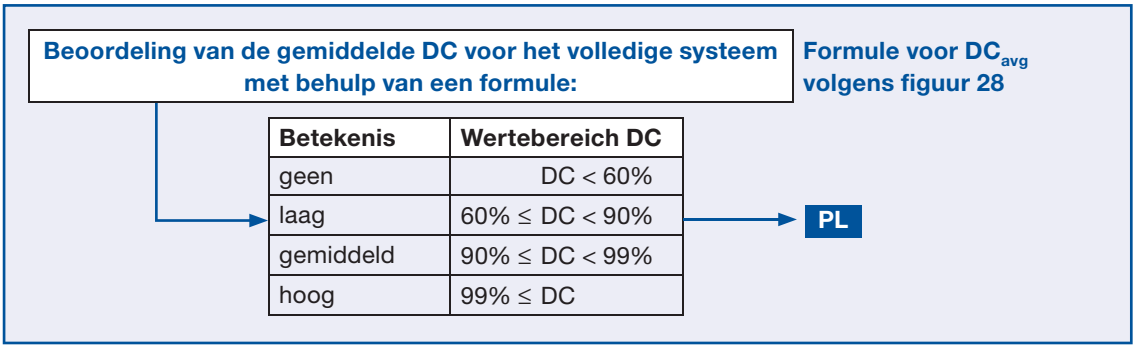
Deze concessies hebben betrekking op de verhouding tussen de waarschijnlijkheid van gedetecteerde gevaarlijke fouten van het betroffen onderdeel tot de waarschijnlijkheid van alle gevaarlijke fouten van het onderdeel, met andere woorden een kwantificering van de efficiëntie van de getroffen maatregelen voor het detecteren van de fouten van een SRP/CS.

Hier veronderstelt de norm dat (a) de waarschijnlijkheid bestaat dat er fouten optreden (zie $MTTF_d$) en (b) de gebruikte methoden voor de foutdetectie een verschillende mate van efficiëntie bezitten en er dus een aantal niet gedetecteerde fouten is.

Deze veronderstelling is relatief, omdat fouten in de SRP/CS niet altijd onmiddellijk gedetecteerd worden. Soms worden zij pas bij de volgende belasting van de veiligheidsfunctie ontdekt, bijvoorbeeld de overbrugging van een elektromechanisch veiligheidscontact of een verkleefd relais tijdens het openen van de bewegende veiligheidsvoorziening.



Figuur 26: Beoordeling van de gemiddelde DC voor het volledige systeem, deel 1



Figuur 27: Beoordeling van de gemiddelde DC voor het volledige systeem, deel 2

Vanuit veiligheidstechnisch standpunt is het onderwerp “foutdetectie” van groot belang om de accumulatie of opeenstapeling van fouten te vermijden, d.w.z. vermijden dat een tweede fout aan de eerste fout, die in de SRP/CS niet gedetecteerd werd, toegevoegd wordt, waardoor de veiligheidsfunctie verloren gaat.

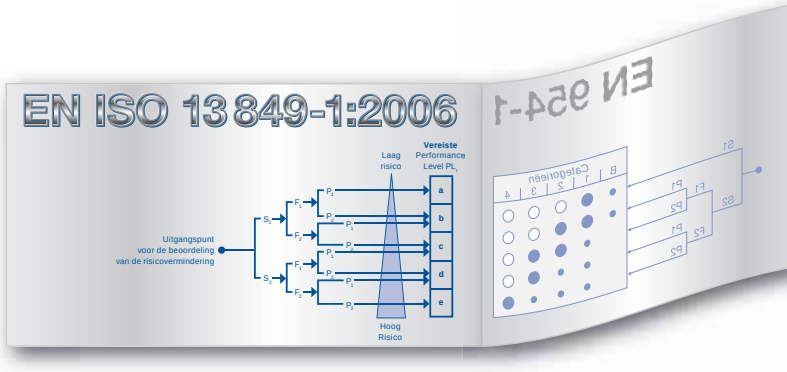
Uit empirische onderzoeken is gebleken dat een eenvoudig redundant systeem met foutdetectie een hoger veiligheidsniveau bereikt dan een complex redundant systeem zonder foutdetectie. Hieruit blijkt duidelijk het belang van de kwaliteit van de Diagnostic Coverage – nog afgezien van het feit dat gewone redundante systemen bovendien goedkoper zijn.

Uitvoering
In de zin van de vereenvoudiging verdeelt deEN ISO 13849-1: 2006 de kwaliteit van de foutendekking of de Diagnostic Coverage DC in verschillende niveaus: none (geen), low (laag), medium (gemiddeld) en high (hoog) – zie figuur 27.

Bijlage E van EN ISO 13849-1:2006 biedt een extra vereenvoudiging (zie pagina 25).

	Maatregel	DC
Relais/contact	Plausibiliteitscontrole, bijvoorbeeld gebruik van gedwongen uitgevoerde maak- en verbreekcontacten	99%
Actuator	Bewakingen van de uitgangen via het 2de kanaal zonder dynamische tests	0–99% afhankelijk van de signaalwissels in de toepassing
Sensor	Bewaking van bepaalde eigenschappen (reactietijd, bereik van de analoge signalen, bijvoorbeeld elektrische weerstand, capaciteit)	60%
Logica	Zelftests door de software	60–90%

Figuur 28: Voorbeelden voor Diagnostic Coverage



- **Het Performance Level PL houdt alleen rekening met de gemiddelde DC (DC_{avg}), d.i. een gewogen waarde van alle tests.**
- **De weegfactor is de $MTTF_d$ van het geteste onderdeel en NIET van de testapparatuur.**

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + ... + \frac{DC_S}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + ... + \frac{1}{MTTF_{dN}}}$$

- **De onderdelen zonder foutdetectie, bijvoorbeeld onderdelen die niet getest werden, hebben een DC = 0. Alle componenten van de SRP/CS, waarvoor geen foutuitsluiting aangetoond kan worden, moeten beoordeeld en opgeteld worden. Er wordt rekening gehouden met de $MTTF_d$ en de DC van iedere component.**

Figuur 29: Gemiddelde Diagnostic Coverage DC_{avg}

Toepassing
De berekende gemiddelde DC, DC_{avg}, vertegenwoordigt de kwaliteit van de Diagnostic Coverage of de foutdetectie van alle SRP/CS die de veiligheidsfunctie uitvoeren.

De $MTTF_d$ waarden van alle SRP/CS die de veiligheidsfunctie uitvoeren, worden in de berekening meegeteld, in die zin dat een combinatie van een “lage” $MTTF_d$ en een “lage” individuele DC zwaarder doorweegt en de DC_{avg} doet dalen (en omgekeerd).

Deze inductieve aanpak voor het berekenen van de gemiddelde foutendekking DC_{avg} is in zekere zin correct, hoewel zij niet onmiddellijk beantwoordt aan het vereenvoudigingsprincipe. Bijlage E van de EN ISO 13849-1:2006 bevat wel een gedetailleerde tabel die de berekening vergemakkelijkt.

Bijlage E somt diverse gekende en beproefde maatregelen voor de Diagnostic Coverage op en geeft een beoordeling van de DC in procenten. Bepaalde maatregelen krijgen echter de beoordeling “0 … 99% afhankelijk van …“. Dit vereist eigenlijk een diepere en grondigere analyse – cf. IEC EN 61508 –, iets dat EN ISO 13849-1:2006 eigenlijk tracht te vermijden.

Maatregelen ter voorkoming van fouten met een gemeenschappelijke oorzaak (CCF)

Theorie
Naast de Designated architectures, de $MTTF_d$ waarde en de DC bepaalt nog een vierde parameter het Performance Level PL, namelijk de fouten met een gemeenschappelijke oorzaak (Common Cause Failures – CCF).

De beoordeling van de invloed van CCF is alleen vereist voor 2-kanalige structuren vanaf categorie 2, omdat EN ISO 13849-1 alleen rekening houdt met de maatregelen ter voorkoming van fouten met een gemeenschappelijke oorzaak van een SRP/CS.

Dit soort fouten kan tot een kritieke veiligheidstoestand van beide kanalen tegelijk leiden. Een voorbeeld: een blikseminslag op de redundante halfgeleideruitgangen (overspanning of "surge" effect) berooft beide kanalen tegelijk van hun in- of uitschakelvermogen.

Voor meerkanalige structuren (categorie 2, 3, 4) zijn maatregelen tegen CCF vereist, die volgens IEC 61508-6, Bijlage D overeenstemmen met een β factor van 2% of minder.

Figuur 30: Fouten met een gemeenschappelijke oorzaak (CCF)

Uitvoering
De effecten van de CCF moeten voor het volledige systeem beoordeeld worden. Iedere component en onderdeel van het besturingssysteem moet afzonderlijk geëvalueerd worden.

EN 13849-1 bevat een tabel met de maatregelen en de bijbehorende waarden die de bijdrage van iedere maatregel aan de vermindering van fouten met een gemeenschappelijke oorzaak (CCF) vertegenwoordigen. Omwille van de motivatie achter de CCF analyse krijgen maatregelen zoals de fysieke scheiding tussen de signaalkanalen, diversiteit of speciale EMV maatregelen een "hoge" score (hetzelfde geldt voor beschermingsmaatregelen tegen overspanning, overdruk of filtreermaatregelen in de vloeistoftechniek).

Om aan de vereisten van de EN ISO 13849-1: 2006 te beantwoorden moet een minimumscore van 65 punten behaald worden. De maximale score bedraagt 100 punten.

Dit is dan het equivalent van de zogeheten β factor van 2% van IEC EN 61508.

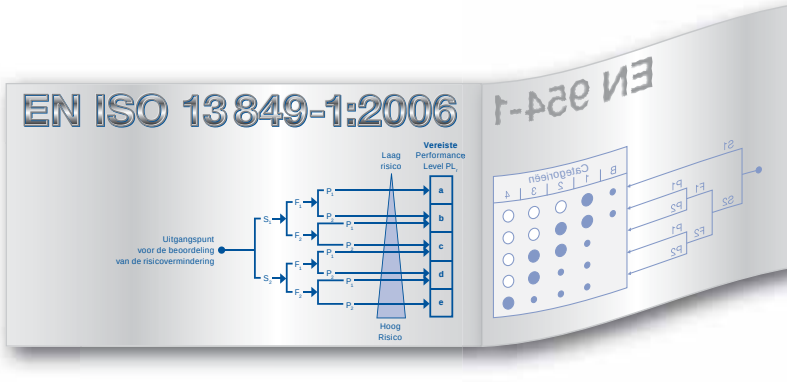
CCF: fouten van verschillende onderdelen/componenten van het systeem door een gemeenschappelijke oorzaak

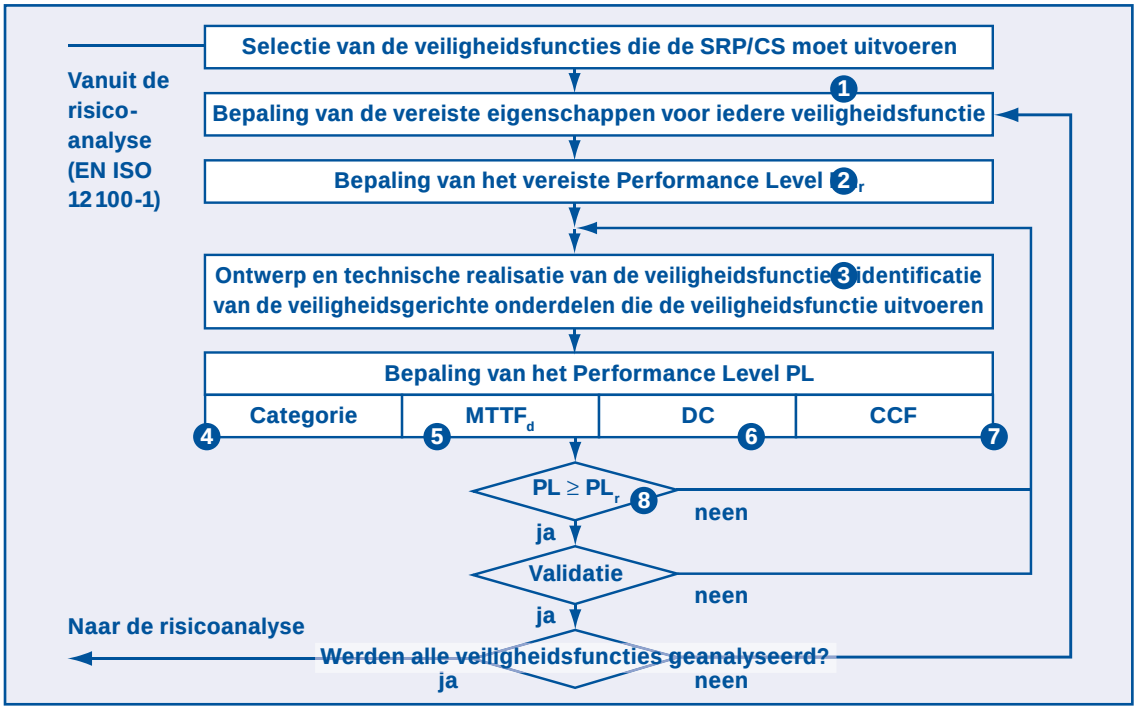
Maatregelen ter voorkoming van CCF
(maximumscore: 100 punten)

• Fysieke scheiding tussen de signaalkanalen	15 punten
• Diversiteit	20 punten
• Beveiliging tegen bijv. overspanning, overdruk, enz.	15 punten
• Bevredigend langdurig gebruik van de componenten, rekening houdend met de omgevingsvoorwaarden	5 punten
• Wordt er rekening gehouden met de resultaten van de analyse van de foutmodi en hun effecten om fouten met een algemene oorzaak bij het ontwerp te vermijden	5 punten
• Competentie/opleiding van de ontwikkelaar	5 punten
• EMV of filteren van het drukmedium en bescherming tegen besmetting	25 punten
• Andere invloeden: temperatuur, vochtigheid, schokken, vibraties, enz.	10 punten

Doel: minstens 65 punten

Figuur 31: Maatregelen tegen CCF





Figuur 32: Iteratief ontwerp- en realisatieproces voor SRP/CS volgens prEN ISO 13849-1:2006

Voorbeeld

EN ISO 13849-1:2006 bevat een aangepaste versie van het iteratieve ontwerpproces voor onderdelen van besturingssystemen met een veiligheidsfunctie (SRP/CS), zoals dit uit de EN ISO 12100-1 bekend is. Het proces wordt hier in 8 theoretische stappen onderverdeeld en begint met de selectie van de veiligheidsfuncties die de SRP/CS moet uitvoeren (stap 1). Het proces eindigt met de conclusie of het vereiste Performance Level PL_r behaald werd (stap 8).

In het voorbeeld (zie figuur 33) wordt de vergrendeling van een bewegende veiligheidsvoorziening besproken: de gevaarlijke beweging stopt zodra de beschermvoorziening geopend wordt, de herstart van de machine wordt verhinderd, enz. (zie EN 1088: Veiligheid van machines – Vergrendelvoorzieningen in combinatie met scheidende beschermvoorzieningen – Grondbeginselen voor het ontwerp en de keuze).

1

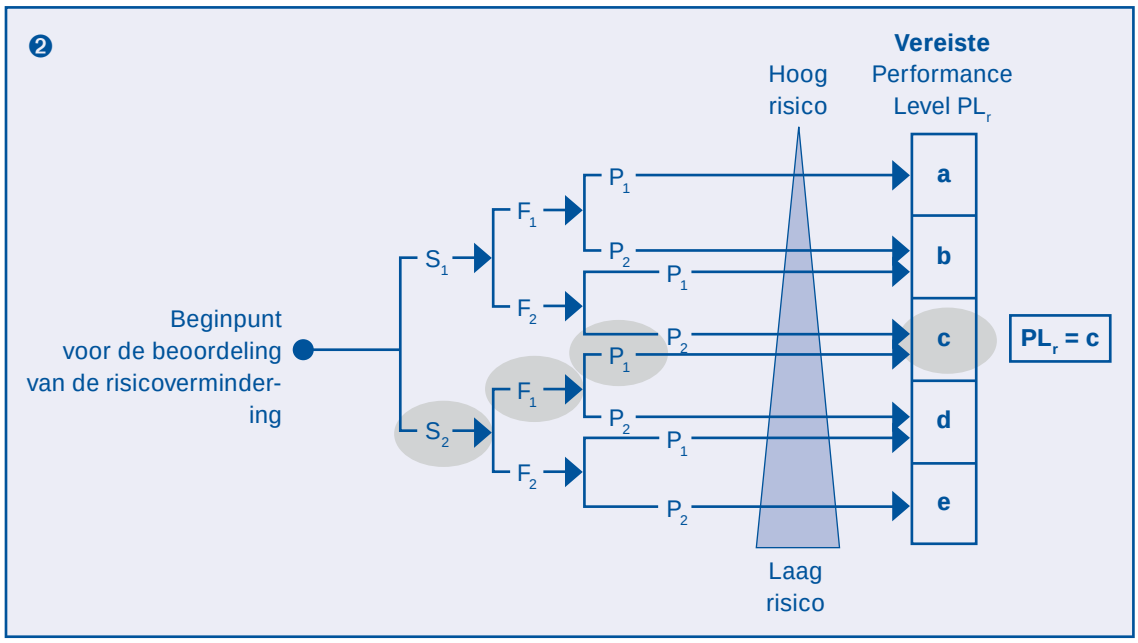
Voorbeeld:

- Vergrendeling van een scheidende veiligheidsvoorziening

Veiligheidsfunctie:

- De gevaarlijke beweging wordt gestopt zodra de deur van de beschermvoorziening geopend wordt

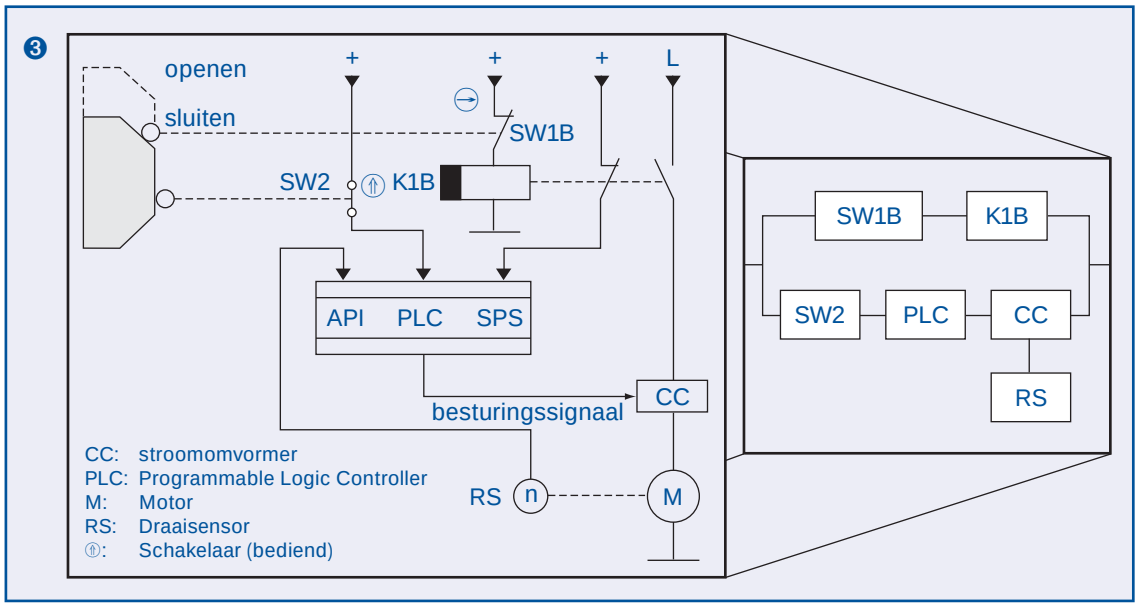
Figuur 33: Selectie en definitie van de vereisten waaraan de veiligheidsfunctie moet voldoen



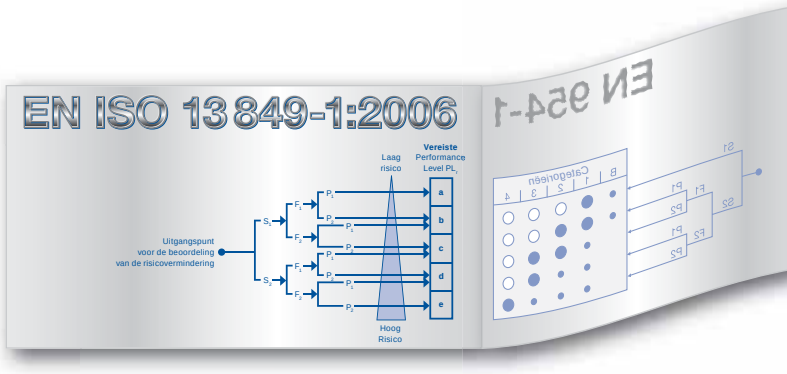
Figuur 34: Bepaling van het vereiste Performance Level PL_r

De beoordeling van het vereiste Performance Level, dus de risicoanalyse met behulp van de nieuwe risicograaf van de EN ISO 13 849-1: 2006, moet uitmonden in een vereist Performance Level PL_r "c" (zie figuur 34).

Figuur 35 bespreekt de structuur van de SRP/CS (Designated architecture).



Figuur 35: Ontwerp en identificatie van de SRP/CS



Op basis van de Designated architecture van figuur 35 betekent dit:

❹

- De vereisten van categorie B zijn vervuld ✔
- Een individuele fout leidt niet tot het verlies van de veiligheidsfunctie? ✔
- Gedeeltelijke foutdetectie ✔
- Een accumulatie van niet-gedetecteerde fouten leidt niet tot het verlies van de veiligheidsfunctie? (niet-gedetecteerde fout in de 1ste PLC, fout in 2de kanaal A) ✔

–> Categorie 3 kan bereikt worden

Figuur 36: Definitie van de categorie voor het PL

Omdat in het voorbeeld de beide kanalen een diversitaire structuur hebben (zie structuur SRP/CS), moeten de verschillende $MTTF_d$ waarden van de kanalen A en B bepaald en op elkaar afgestemd worden (“symmetrie”).

❺

- **SW1B: gedwongen verbrekend contact:** Foutuitsluiting voor het niet-openen van de contacten, het niet bedienen van de schakelaar omwille van een mechanische fout (bijvoorbeeld breuk van de stoter, slijtage van de hefboom, afwijking)
- **K1B: $MTTF_d$ = 30 y specificatie fabrikant)**

$$\frac{1}{MTTF_{d\,C1}} = \frac{1}{MTTF_{d\,K1B}} = \frac{1}{30\ y}$$

Kanaal 1: $MTTF_d$ = 30 y

Figuur 37: Bepalen van het Performance Level PL: $MTTF_d$ voor kanaal A

❺

- **SW2, SPS, CC: $MTTF_d$ = alle 20 y (specificatie fabrikant)**

$$\frac{1}{MTTF_{d\,C2}} = \frac{1}{MTTF_{SW2}} + \frac{1}{MTTF_{PLC}} + \frac{1}{MTTF_{CC}} = \frac{3}{20\ y}$$

Kanaal 2: $MTTF_d$ = 6,7 y

- **Symmetreren $MTTF_d$ voor beide kanalen:**

$$MTTF_d = \frac{2}{3}\left[MTTF_{d\,C1} + MTTF_{d\,C2} - \frac{1}{\frac{1}{MTTF_{d\,C1}} + \frac{1}{MTTF_{d\,C2}}}\right]$$

$MTTF_d$ = 20 y (gemiddeld)

Figuur 38: Bepalen van het Performance Level PL: $MTTF_d$ voor kanaal B en globale $MTTF_d$

Nu wordt de Diagnostic Coverage DC beoordeeld:

❻

- DC_{K1B} 99%, “hoog“ omwille van de gedwongen uitgevoerde elektrische contacten, tabel Bijlage E.1
- DC_{SW2} = 60%, “laag“ omwille van de bewaking van de ingangssignalen zonder dynamische tests
- DC_{PLC} = 30%, “geen“ omwille van de lage efficiëntie van de zelftests
- DC_{CC} = 90%, “gemiddeld“ omwille van de beperkte uitschakelweg met bewaking van de actuator door het besturingssysteem, tabel E.1, Bijlage E.1

$$DC_{avg} = \frac{\frac{DC_1}{MTTF_{d1}} + \frac{DC_2}{MTTF_{d2}} + \ldots + \frac{DC_S}{MTTF_{dN}}}{\frac{1}{MTTF_{d1}} + \frac{1}{MTTF_{d2}} + \ldots + \frac{1}{MTTF_{dN}}}$$

DC_{avg} = 67% (laag)

Figuur 39: Bepalen van het Performance Level PL: DC_{avg}

Aansluitend worden de maatregelen ter voorkoming van fouten met een gemeenschappelijke oorzaak (CCF) beoordeeld:

❼

CCF: fout van diverse componenten door een gemeenschappelijke oorzaak

• Fysieke scheiding tussen de signaalkanalen	15 punten
• Diversiteit	20 punten
• Bescherming tegen overspanning, overdruk, enz.	0 punten
• Gebruik van beproefde componenten	5 punten
• Inachtneming van de resultaten van de analyse van de foutmodi en hun effecten om fouten met een algemene oorzaak bij het ontwerp te vermijden	5 punten
• Competentie/opleiding van de ontwikkelaar	0 punten
• EMV of filtreren van het drukmedium en bescherming tegen besmetting	25 punten
• Temperatuur, vochtigheid, schokken, vibraties, enz.	10 punten

Σ = 80 punten > 65 punten

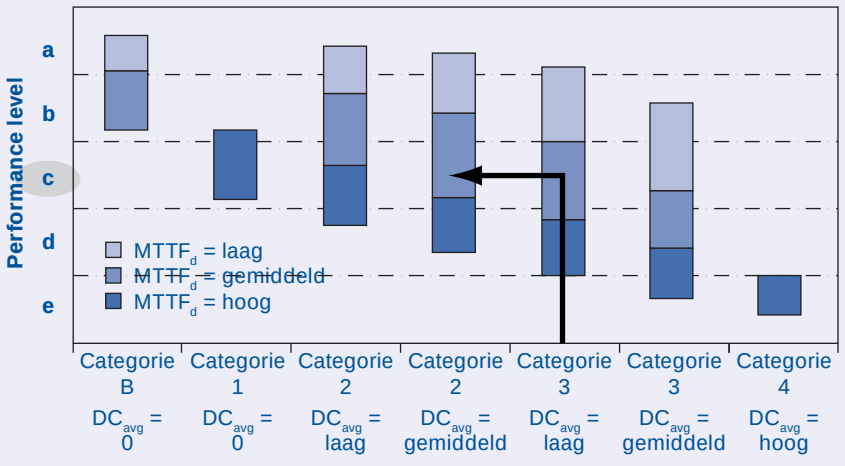
Figuur 40: Bepalen van het Performance Level PL: CCF

… en tot slot worden alle parameters in het blokdiagram ingevoerd ter controle of PL => PL_r (figuur 41).

Opmerking: de nauwkeurige opsplitsing in dit voorbeeld is uiteraard een beetje overdreven. Bovendien bezit het systeem uit het voorbeeld twee kanalen met diversitaire structuur zowel op sensorniveau als op het niveau van het besturingssysteem. Het is dus een beetje ingewikkelder dan de structuren die gewoonlijk gebruikt worden.

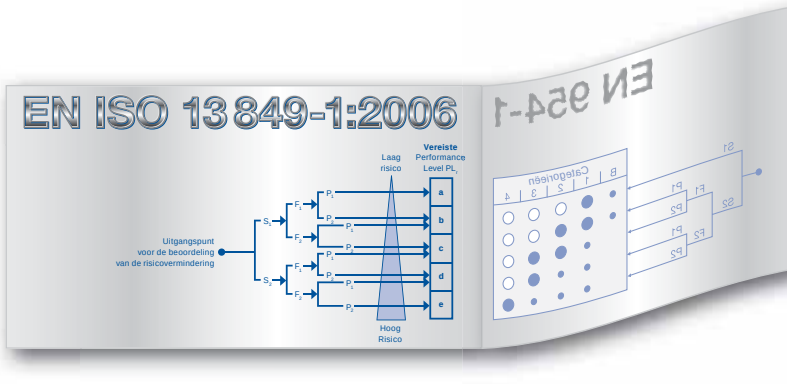
Het voorbeeld illustreert echter perfect de gedachtegang van de EN ISO 13849-1:2006 en haar nieuwe vereisten, hoewel voor de vergrendeling (als elektromechanische component) geen B_{10d} waarde berekend wordt. In dit geval zou het voorbeeld de werkelijkheid nog meer benaderen.

❽



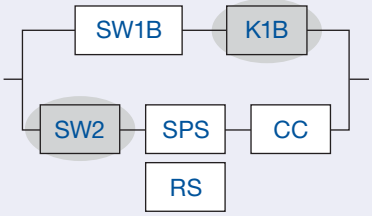
PL = PL_r = c ✔

Figuur 41: Controle of het berekende Performance Level PL ≥ PL_r



Is u niets opgevallen?

Diagram:



$$MTTF_d = \frac{B_{10d}}{0{,}1 \cdot n_{op}}$$

$$n_{op} = \frac{d_{op} \cdot h_{op} \cdot 3.600 \frac{s}{h}}{t_{cycle}}$$

n_{op} = gemiddeld aantal schakelingen per jaar

Figuur 42: Elektromechanische componenten hebben wel degelijk een B_{10d} waarde

Met een B_{10d} waarde zou de $MTTF_d$ voor K_{1B} en SW2 als volgt herberekend moeten worden, als we ervan uitgaan dat de beschermvoorziening 240 dagen per jaar en 16 uur per dag functioneert met een gemiddelde belasting alle 20 s:

Veronderstelling: 240 dagen / 16 uren / toegang alle 20 s

$$n_{op} = \frac{240 \cdot 16 \cdot 3.600}{20} = 691.200 \frac{\text{schakelingen}}{\text{jaar}}$$

$$MTTF_d = \frac{20.000.000}{0{,}1 \cdot 691.200} = 289 \text{ Jahre}$$

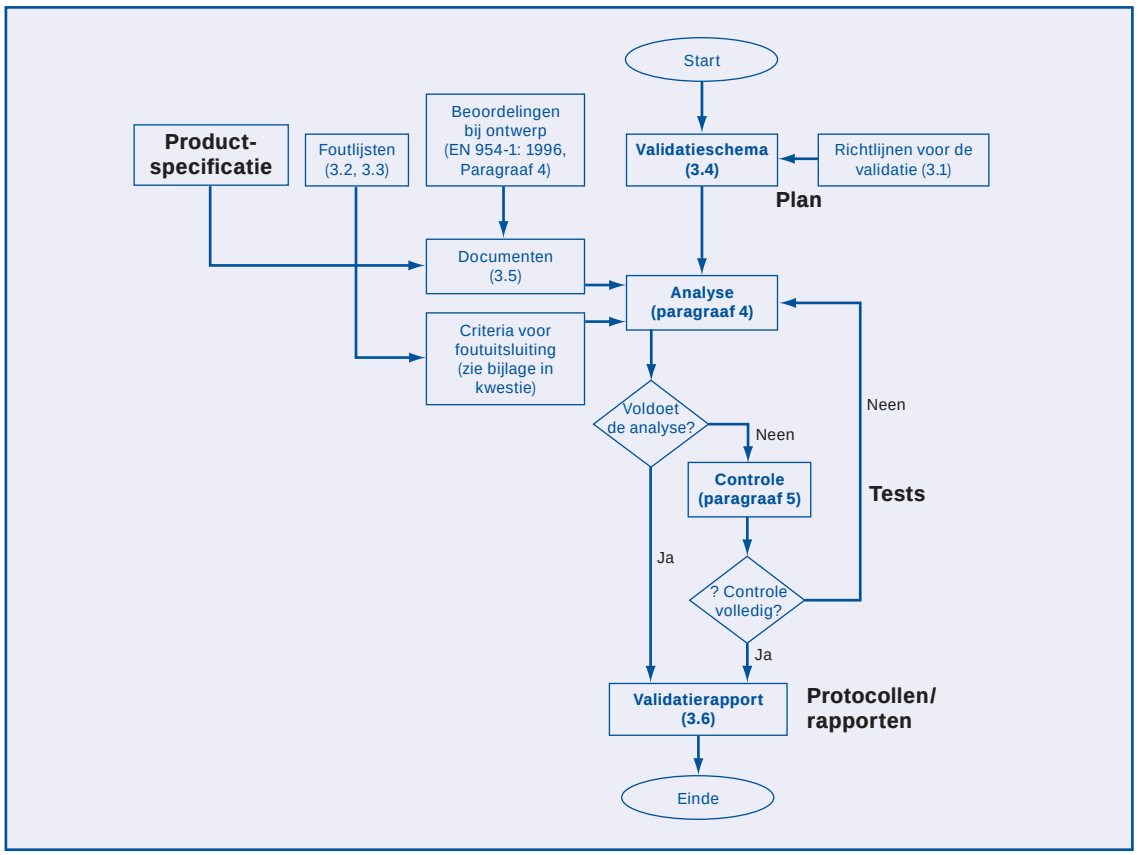
De maximale levensduur die de norm voorziet is: $T_{10d} = B_{10d}/n_{op} = 28{,}9$ jaar

Figuur 43: Berekening van de $MTTF_d$ voor K_{1B} en SW2

In dit voorbeeld zou de parameter F1 van de risicograaf niet langer van toepassing zijn (zie: frequentie en/of duur van blootstelling aan het gevaar: zelden of kort). Hier zou eerder F2 van toepassing zijn, waardoor het vereiste Performance Level PL “d” wordt. Dankzij de gecorrigeerde $MTTF_d$ waarde is het probleem opgelost.

Opmerking van de redacteur

De vereiste correctieprocedure uit het voorbeeld toont aan dat ook het opstellen van normen een iteratief proces is. Het voorbeeld komt immers uit de norm, hoewel het opgesteld werd op een ogenblik waarop de beoordeling van de B_{10d} waarde nog niet opgenomen was. En het zijn juist de beoordelingen van de B_{10d} waarden die voor de gebruiker van de norm van essentieel belang zijn. Zonder deze waarden zou de EN 13849-1 haar specifieke vereisten voor de praktische toepassing niet langer kunnen rechtvaardigen.



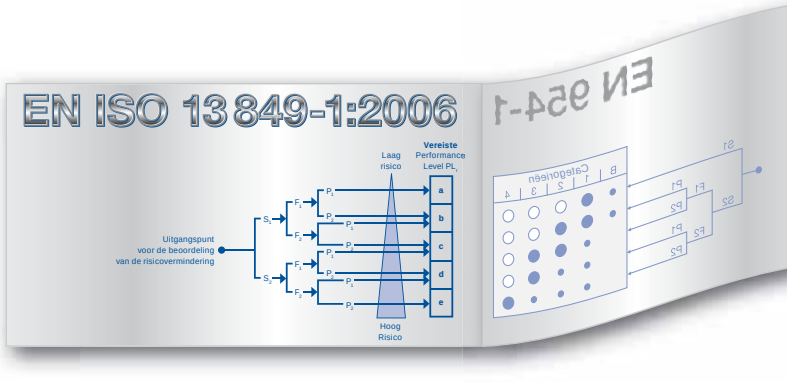
Figuur 44: Validatieschema volgens EN ISO 13849-2

Validatie[1]

Het ontwerp van de SRP/CS moet volgens de EN ISO 13849-2 gevalideerd worden. Aangezien de validatie op dit ogenblik ook al van toepassing is, zullen we hier niet dieper ingaan op dit onderwerp.

De EN ISO 13849-2 heeft betrekking op de inhoud die aanvankelijk voor de norm EN 954-2 voorzien was, die echter na haar aanvaarding rechtstreeks op ISO niveau omgezet werd. Hoogstwaarschijnlijk zal ook deze norm binnenkort een revisie ondergaan om de uitgave van 1998/1999 te updaten en de verwijzingen naar de EN 954-1 aan de huidige norm, de EN ISO 13849-1:2006, aan te passen.

1) We gaan hier niet dieper in op de maatregelen ter beheersing en voorkoming van systematische fouten, omdat deze reeds deel uitmaken van de vereisten voor een SRP/CS. Bijlage G van de EN ISO 13849-1 geeft een gedetailleerde voorstelling.



De meeste ongevallen aan en met machines zijn echter niet aan toevallige fouten toe te schrijven. Zij hangen eerder samen met foutieve specificaties van de veiligheidsvoorschriften en fouten in het ontwerp, de fabricage, de installatie en het gebruik van het materiaal. Daarom is de validatie van het grootste belang voor de veiligheid van een machine.

De informatieve bijlagen van de EN ISO 13849-2 spelen een belangrijke rol voor de EN ISO 13849-1:2006. Zij zijn opgesplitst volgens technologie – mechanische componenten (Bijlage A), pneumatische componenten (Bijlage B), hydraulische componenten (Bijlage C) en elektrische componenten (Bijlage D) en bevatten de volgende lijsten:

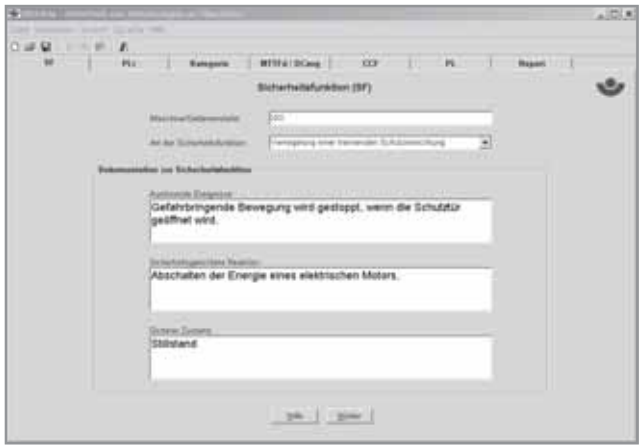
- De essentiële veiligheidsprincipes (belangrijk voor categorie B volgens EN 954-1 of PL “a“),
- De beproefde veiligheidsprincipes (belangrijk voor categorie 1 en volgende volgens EN 954-1 of PL “b“… PL “e“),
- De beproefde veiligheidscomponenten (belangrijk voor categorie 1 volgens EN 954-1 of PL “b“),
- De lijsten met te beschouwen fouten en de toegelaten foutuitsluitingen (belangrijk voor categorie 2, 3 en 4 volgens EN 954-1 of PL “c“ … PL “e“).

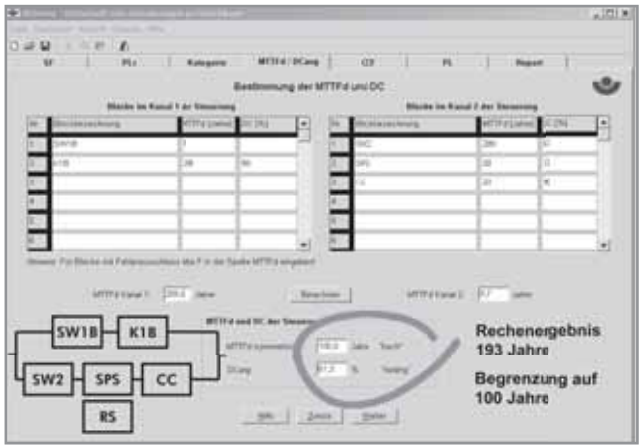
SiSteMa

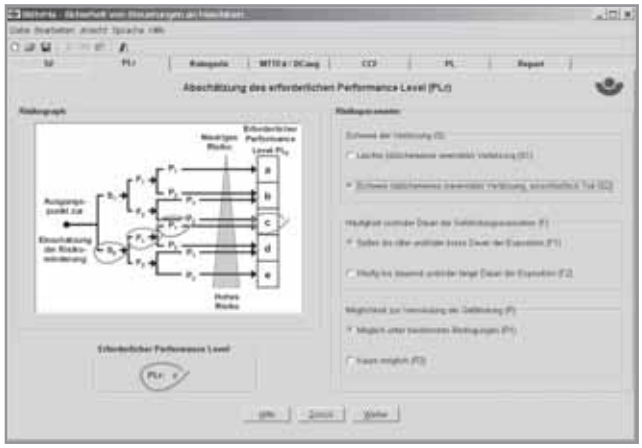
Het zal niet lang duren voor er een software-programma op de markt komt om de hier beschreven voorbeeldprocedures te vereen-voudigen.

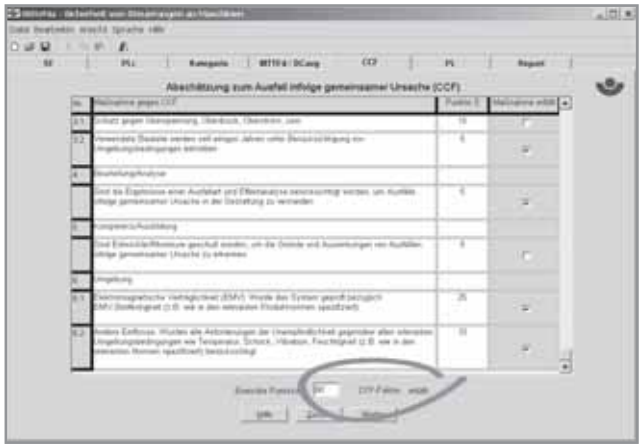
Momenteel bereidt de BGIA een softwarepro-gramma, SiSteMa genaamd (Veiligheid van Machinebesturingen) voor dat binnenkort als freeware beschikbaar gesteld zal worden.

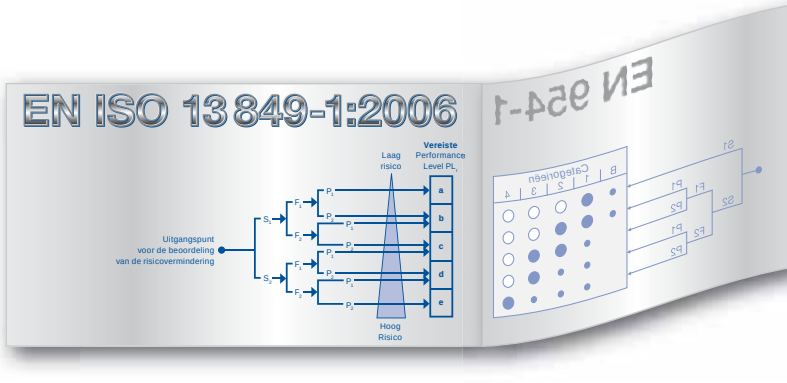
Omdat SiSteMa nog niet beschikbaar is (voorziene releasedatum: half 2006), biedt de beroepsorganisatie al ondersteuning bij het gebruik en de toepassing van de EN ISO

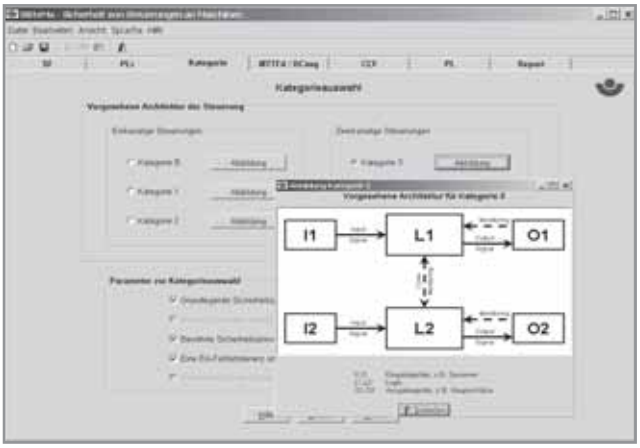


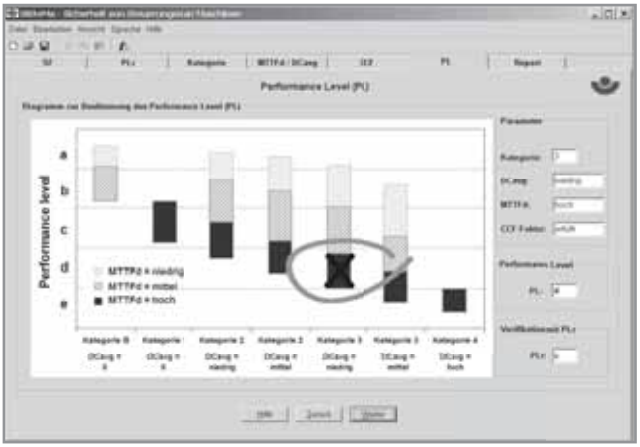


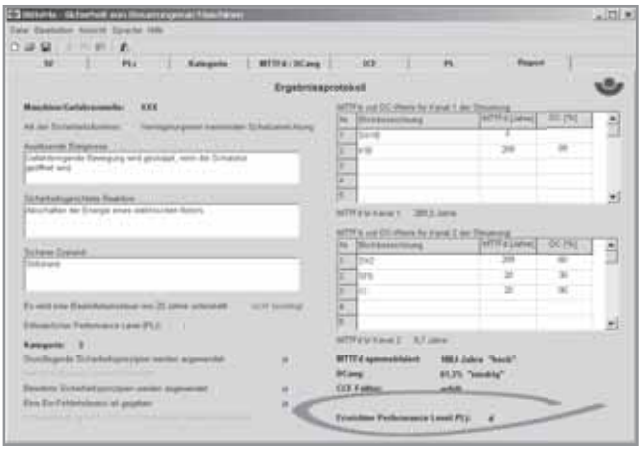












13849-1:2006. In samenwerking met het Zentralverband Elektrotechnik- und Elektronikindustrie (ZVEI – Fachverband Automation – de Duitse centrale beroepsorganisatie voor elektrotechniek, elektrische industrie en automatisering) en het Verband Deutscher Maschinen- und Anlagenbau VDMA – de Duitse associatie van machinebouwers – werd een PLC schijf ontwikkeld, waarmee het Performance Level PL op een eenvoudige en gemakkelijke manier bepaald kan worden.

De methodes van de EN ISO 13849-1: 2006 worden aanschouwelijk gemaakt via twee schijven die ten opzichte van elkaar gedraaid kunnen worden zoals bij een parkeerschijf. Om het Performance Level PL te bepalen moet de eerste schijf gedraaid worden totdat de gewenste $MTTF_d$ (Mean Time to Failure dangerous) waarde in het venster onder aan verschijnt.

Na het kiezen van de gewenste categorie en Diagnostic Coverage (DC), toont het venster bovenaan een cijfer. Dit cijfer moet met de factor uit de legende vermenigvuldigd worden om de gemiddelde waarschijnlijkheid van een gevaarlijke fout van de SRP/CS te kennen. De kleurencode dient om de factor te selecteren en vertegenwoordigt tegelijkertijd het bereikte Performance Level PL.

Bron PLC:
www.hvbg.de/d/bia/pra/drehscheibe.html

EN ISO 13849-1:2006 en overzichtelijke SRP/CS

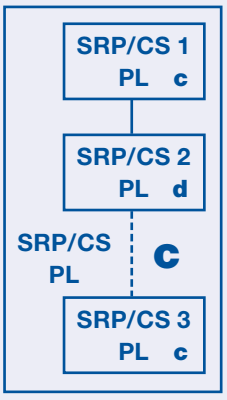
Theorie
Na het bepalen van het Performance Level PL voor ieder onderdeel van het besturingssysteem met een veiligheidsfunctie voorziet de EN ISO 13849-1:2006 een speciale vereenvoudigingsprocedure voor overzichtelijke SRP/CS, d.i. SRP/CS met een lage complexiteit.

Deze procedure geeft ook aan dat het aaneenschakelen van een groot aantal veiligheidsgerichte componenten het globale Performance Level PL kan beïnvloeden. Dit betekent dat het globale Performance Level PL van het volledige besturingssysteem, inclusief diverse aaneengeschakelde SRP/CS, aanzienlijk lager kan uitvallen dan de individuele Performance Levels van de verschillende “schakels” van de ketting. De achterliggende gedachte hiervan is dat een zodanig groot aantal waarschijnlijke restfouten moet opgeteld worden, dat het globale Performance Level PL zonder probleem met een niveau verminderd kan worden.

Uitvoering
De vereenvoudigingsprocedure wordt getoond in de tabel van figuur 45 (de “combinatietabel”). Links wordt het aantal individuele PL van een besturingssysteem vermeld; na het optellen van de laagste Performance Levels PL kan rechts het globale Performance Level PL afgelezen worden.

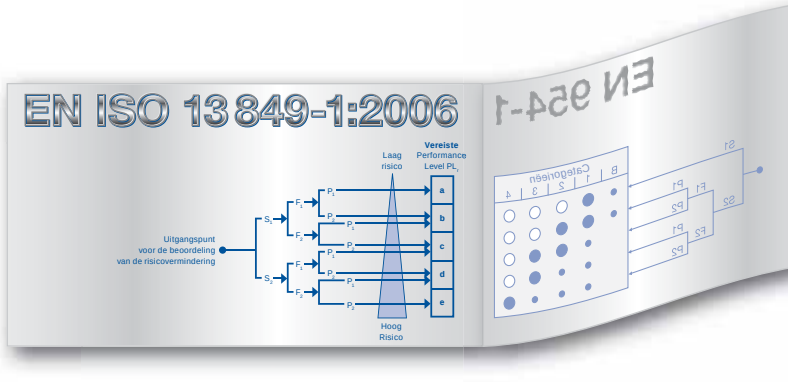
Gewoonlijk mag het globale PL met een niveau verminderd worden, als meer dan drie afzonderlijke PL (voor ‘eenvoudige’ structuren) of meer dan vier afzonderlijke PL (voor beproefde 2-kanalige structuren) hetzelfde zijn. Het resultaat van drie maal een afzonderlijke PL “c“ is dan een globaal Performance Level “b“ of vier maal een individuele PL “e” een globale PL “d”.

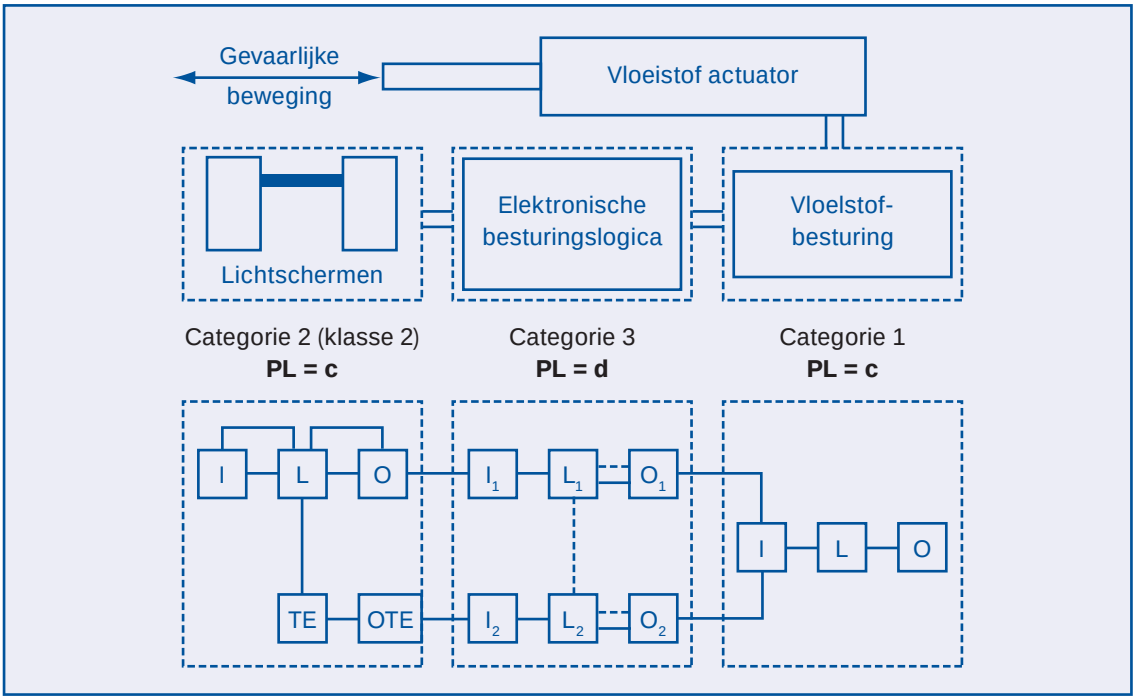
In het onderstaande voorbeeld (figuur 46) betekent dit dat de twee laagste individuele PL opgeteld moeten worden (2 × PL “c“), terwijl de berekening geen rekening houdt met het hogere PL “d“ (vanuit het standpunt van de PFH waarde bekeken is PL "d" een hogere waarde dan PL "c"). 2 × PL “c“ blijft PL “c“. Moest hier ook een PL “c” meegerekend worden in plaats van een PL “d”, dan zou het globale PL (slechts) “b” zijn.



PL low	N low		PL
a	> 3	= >	none
	≤ 3	= >	a
b	> 2	= >	a
	≤ 2	= >	b
c	> 2	= >	b
	≤ 2	= >	c
d	> 3	= >	c
	≤ 3	= >	d
e	> 3	= >	d
	≤ 3	= >	e

Figuur 45: Lineaire combinaties van meerdere SRP/CS





Figuur 46: Verklarend principeschema voor de combinatie van SRP/CS

Toepassing
Als deze beoordeling het vereiste, met behulp van de risicoanalyse berekende Performance Level PL_r oplevert, is het gebruik van deze tabel ongetwijfeld nuttig. In deze beoordeling kunnen echter foutuitsluitingen opgenomen worden, die vervolgens buiten beschouwing gelaten worden.

Als het globale Performance Level, berekend via deze methode, niet overeenstemt met het vereiste Performance Level PL_r, is een meer gedetailleerde analyse vereist. In die zin is het resultaat niet zozeer bepalend, maar eerder te wijten aan de veralgemening van de beoordeling.

De EN ISO 13849-1:2006 biedt ook oplossingen voor dit probleem (zie volgende paragraaf “Serieschakelingen van SRP/CS“).

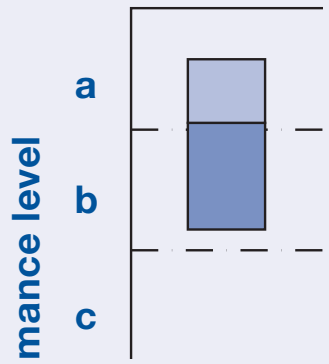
EN ISO 13849-1:2006 en serieschakelingen van SRP/CS

Theorie
De combinatie van onderdelen van een besturingssysteem met een veiligheidsfunctie begint vanaf het punt waar de veiligheidsgerichte signalen gegenereerd worden en eindigt aan de uitgang van de actuatoren. SRP/CS combinaties kunnen echter bestaan uit meerdere onderdelen die lineair met elkaar verbonden zijn (serieschakeling).

Om de gebruiker een hele reeks complexe berekeningen te besparen, voorziet de EN ISO 13849-1:2006 een methode om het PL van alle SRP/CS combinaties te berekenen, als het Performance Level PL voor de individuele onderdelen gekend is.

Uitvoering
De tabel (figuur 47) geeft een beter inzicht in de kwaliteit van de in serie geschakelde SRP/CS combinaties (sleutelwoord: optelsom van de waarschijnlijke restfouten) volgens EN ISO 13849-1:2006.

De tabel in Bijlage K van de EN ISO 13849-1: 2006 toont een gedetailleerde weergave van het centrale blokdiagram (zie figuur 8) om het behaalde PL te bepalen. Hoe correcter de $MTTF_d$ van een kanaal, hoe nauwkeuriger de PFH_d. De waarden die voor de individuele SRP/CS berekend werden, moeten opgeteld worden en aansluitend moet het resultaat van deze optelsom met de maximaal toegestane PFH voor het Performance Level PL in kwestie vergeleken worden (zie figuur 4). Een hogere PFH_d waarde betekent minder kans op fouten.

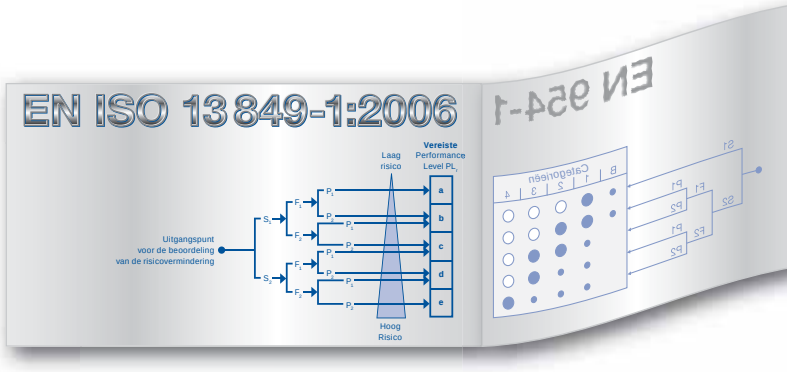


$MTTF_d$ [years]	PFH_d [1/h]	PL
3	$3{,}80 \cdot 10^{-5}$	a
3,3	$3{,}46 \cdot 10^{-5}$	a
3,6	$3{,}17 \cdot 10^{-5}$	a
3,9	$2{,}93 \cdot 10^{-5}$	a
4,3	$2{,}65 \cdot 10^{-5}$	a
4,7	$2{,}43 \cdot 10^{-5}$	a
5,1	$2{,}24 \cdot 10^{-5}$	a
5,6	$2{,}04 \cdot 10^{-5}$	a
6,2	$1{,}84 \cdot 10^{-5}$	a
6,8	$1{,}68 \cdot 10^{-5}$	a
7,5	$1{,}52 \cdot 10^{-5}$	a
8,2	$1{,}39 \cdot 10^{-5}$	a
9,1	$1{,}25 \cdot 10^{-5}$	a
10	$1{,}14 \cdot 10^{-5}$	a
11	$1{,}04 \cdot 10^{-5}$	a
12	$9{,}51 \cdot 10^{-6}$	b
13	...	

+

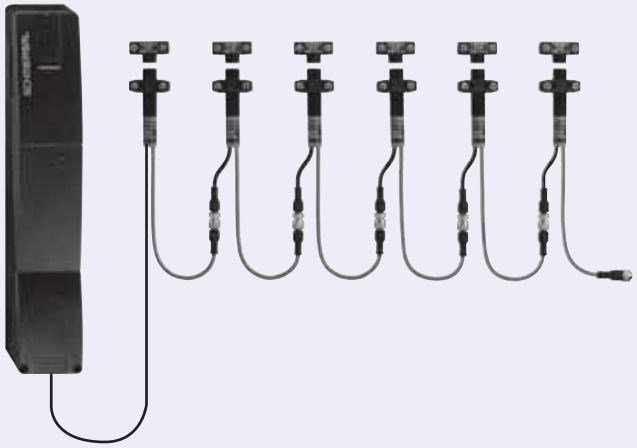
$MTTF_d$ [years]	PFH_d [1/h]	PL
3	$3{,}80 \cdot 10^{-5}$	a
3,3	$3{,}46 \cdot 10^{-5}$	a
3,6	$3{,}17 \cdot 10^{-5}$	a
3,9	$2{,}93 \cdot 10^{-5}$	a
4,3	$2{,}65 \cdot 10^{-5}$	a
4,7	$2{,}43 \cdot 10^{-5}$	a
5,1	$2{,}24 \cdot 10^{-5}$	a
5,6	$2{,}04 \cdot 10^{-5}$	a
6,2	$1{,}84 \cdot 10^{-5}$	a
6,8	$1{,}68 \cdot 10^{-5}$	a
7,5	$1{,}52 \cdot 10^{-5}$	a
8,2	$1{,}39 \cdot 10^{-5}$	a
9,1	$1{,}25 \cdot 10^{-5}$	a
10	$1{,}14 \cdot 10^{-5}$	a
11	$1{,}04 \cdot 10^{-5}$	a
12	$9{,}51 \cdot 10^{-6}$	b
13	...	

Figuur 47: Alternatief: optellen van de PFH_d voor seriegeschakelde SRP/CS combinaties



Serieschakeling zonder verlies van categorie

- De geïntegreerde elektronische logica bewaakt de werking van de schakelaar (zelfbewaking)
- Alle fouten in de serieschakeling worden gedetecteerd (…31 componenten)
- Serieschakeling van de schakelaar (CSS 180 **en/of** AZM 200) **met behoud** van de categorie



Figuur 48: Aanrakingsvrije veiligheidsvergrendelingen met en zonder arrêtering

Complexe serieschakelingen: altijd PL “e“!
De beïnvloeding van het globale PL van een SRP/CS door serieschakeling vormt een groot probleem, vooral bij elektromechanische veiligheidscomponenten.

Hier openen nieuwe, elektronische schakeltechnologieën met veiligheidsfunctie nieuwe perspectieven, omdat zij gewoonlijk permanente dynamische tests van de componenten tolereren. Hierdoor wordt de categorie of het Performance Level PL niet beïnvloed, zelfs niet als meerdere veiligheidscomponenten in serie geschakeld worden.

In het productgamma van SCHMERSAL vinden we ondermeer de CSS 180 veiligheidssensoren en de aanrakingsvrije veiligheidsvergrendelingen van de serie AZM 200, die ook onderling en bovendien serieonafhankelijk aaneengeschakeld kunnen worden (figuur 48).

Meer informatie: www.schmersal.com

Elektronische sensoren en veiligheidsvergrendelingen

De elektronische sensoren en veiligheidsvergrendelingen dienen voor het bewaken van bewegende scheidende veiligheidsvoorzieningen. De machine stopt zodra deze veiligheidsvoorzieningen geopend worden en de herstart van de machine wordt op een veilige manier verhinderd.

Hun belangrijkste voordeel is de aanrakingsvrije positiedetectie van de beschermvoorziening. Zij zijn volledig slijtagevrij en ongevoelig voor afwijkingen van sensor en bediensleutel.

EN ISO 13849-1 en software

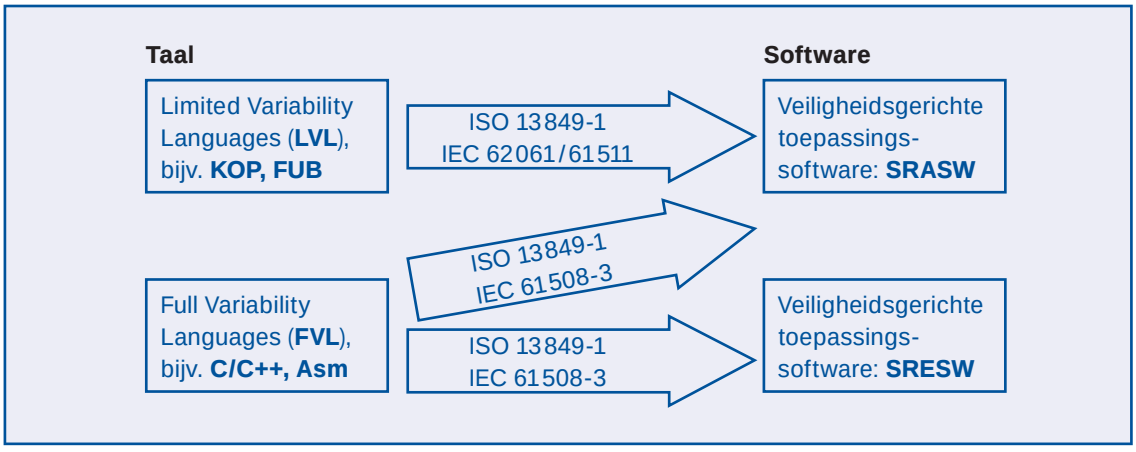
Theorie
In tegenstelling tot de EN 954-1 houdt de EN ISO 13849-1:2006 uitgebreid rekening met elektronische programeerbare systemen met veiligheidsfunctie (= PES systemen) en dus ook met de software. De vereisten van de IEC EN 61508 kunnen echter niet volledig genegeerd worden (bijvoorbeeld voor toepassingen met Performance Level PL "e"). Omdat dit onderwerp alleen van toepassing is voor ontwikkelaars van PES systemen, gaan wij hier niet dieper op dit thema in.

Figuur 49 beschrijft de basisprincipes van de EN ISO 13849-1:2006.

Uitvoering
De vereisten die de EN ISO 13849-1:2006 aan de software stelt, kunnen onderverdeeld worden in algemene vereisten, vereisten voor de veiligheidsgerichte ingebedde software en vereisten voor de veiligheidsgerichte toepassingssoftware met bijkomende onderverdelingen in functie van de gebruikte programmeertaal (LVL[3] of FVL[4]) en het Performance Level PL (zie figuur 50 en 51).

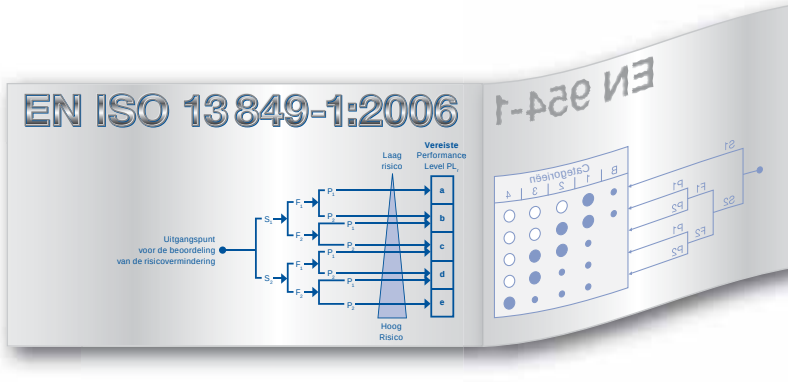
- Voor alle PL en SRESW[1] + SRASW[2]
- In feite: maatregelen ter **voorkoming van fouten en defensief programmeren**
- Fouten zijn te wijten aan fouten in de specificatie en het ontwerp van de software
- Fundamentele veiligheidsnorm IEC 61508-3
- … echter zonder gefundeerde wetenschappelijke basis
- Hoofdzakelijk zonder verwijzingen naar de IEC 61508
- Begrijpelijk, praktijkgericht en gemakkelijk toe te passen

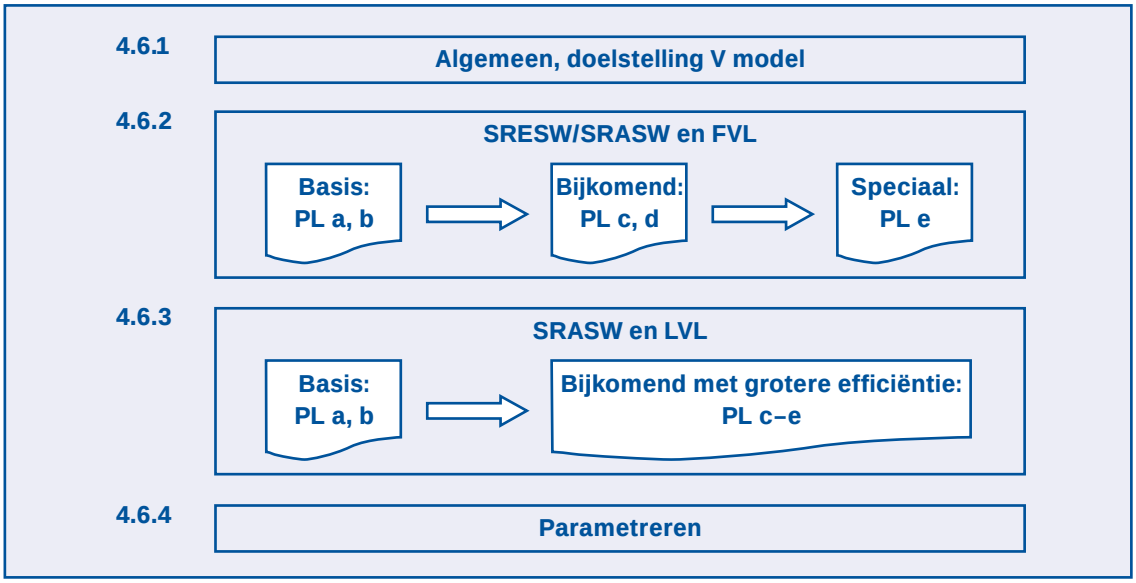
Figuur 49: Basisprincipes voor de softwarevereisten volgens EN ISO 13849-1:2006



Figuur 50: "Netwerken" van veiligheidsgerichte software

1) SRASW (safety-relevant application software) = veiligheidsgerichte toepassingssoftware
2) SRESW (safety-relevant embedded software) = veiligheidsgerichte ingebedde software
3) LVL (Limited Variability Language) – Programmeertaal met beperkt taalbereik : taaltype, dat de mogelijkheid biedt voorgedefinieerde, toepassingsspecifieke en bibliotheekfuncties te combineren om de specificaties van de veiligheidsvereisten uit te voeren.
4) FVL (Full Variability Language) – Programmeertaal met onbeperkt taalbereik: taaltype, dat de mogelijkheid biedt een groot aantal functies en toepassingen uit te voeren



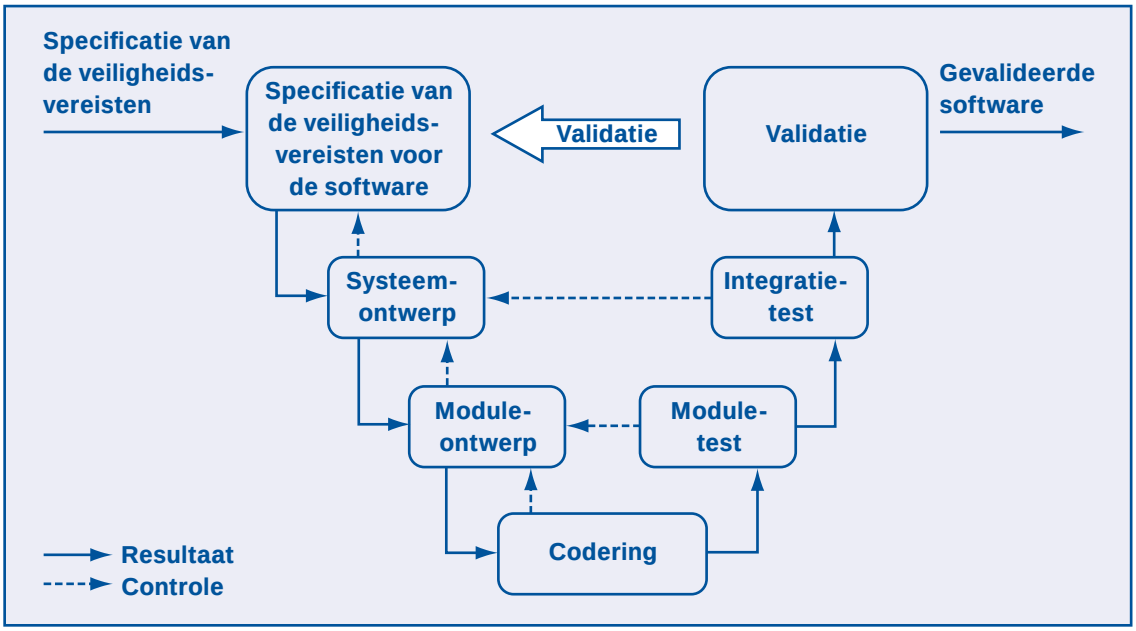


Figuur 51: Structuur van de softwarevereisten volgens paragraaf 4.6 van de EN ISO 13849-1:2006

Toepassing

We gaan hier niet dieper in op de vereisten voor veiligheidsrelevante ingebedde software, omdat deze slechts uitzonderlijk van toepassing zijn voor de gebruikers van EN ISO 13849-1:2006. Het gebruik van toepassingssoftware in de SRP/CS neemt echter toe, hoewel meestal in combinatie met veiligheids-PLC's, veiligheidsbussystemen of andere veiligheidsgerichte aandrijfbesturingen.

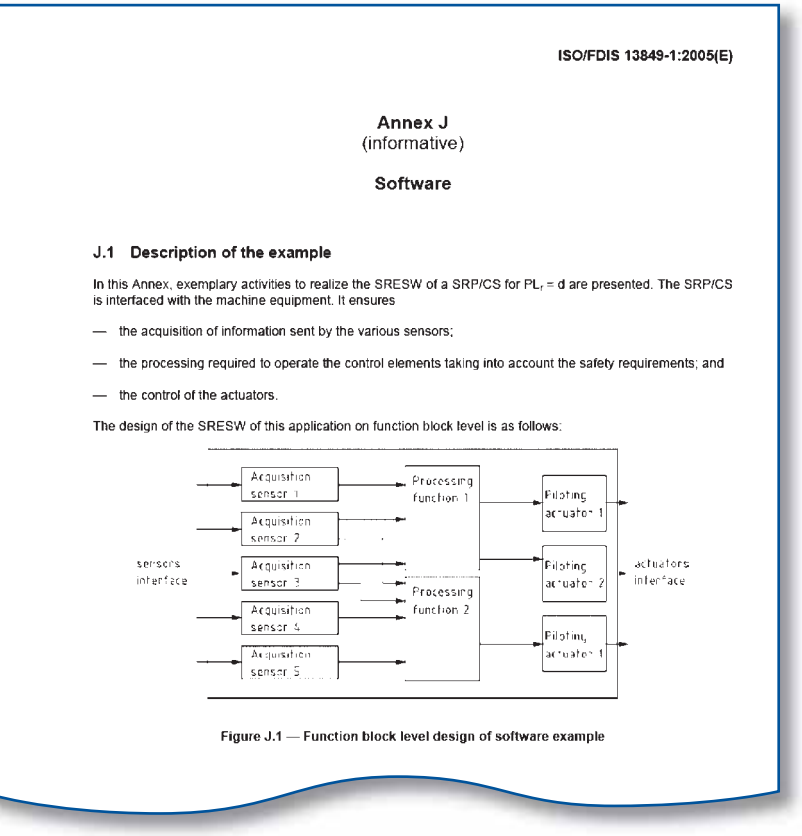
Net zoals voor ingebedde software beveelt EN ISO 13849-1:2006 ook het gebruik van het V model aan, dat in zijn vereenvoudigde vorm algemeen bekend is in de softwaresector.



Afbeelding 52: Vereenvoudigd V model voor SRESW en SRASW in prEN ISO 13849-1:2006

Als de toepassingssoftware uitsluitend uit parameters bestaat (typisch voorbeeld: een veiligheidslaserscanner), zijn andere vereenvoudigingen van toepassing, omdat hier de leverancier al de nodige voorbereidende berekeningen gedaan heeft.

De andere softwarevereisten worden vermeld in Bijlage J van de EN ISO 13849-1:2006 (zie figuur 53).



ISO/FDIS 13849-1:2005(E)

Annex J
(informative)

Software

J.1 Description of the example

In this Annex, exemplary activities to realize the SRESW of a SRP/CS for PL_r = d are presented. The SRP/CS is interfaced with the machine equipment. It ensures

— the acquisition of information sent by the various sensors;

— the processing required to operate the control elements taking into account the safety requirements; and

— the control of the actuators.

The design of the SRESW of this application on function block level is as follows:

Figure J.1 — Function block level design of software example

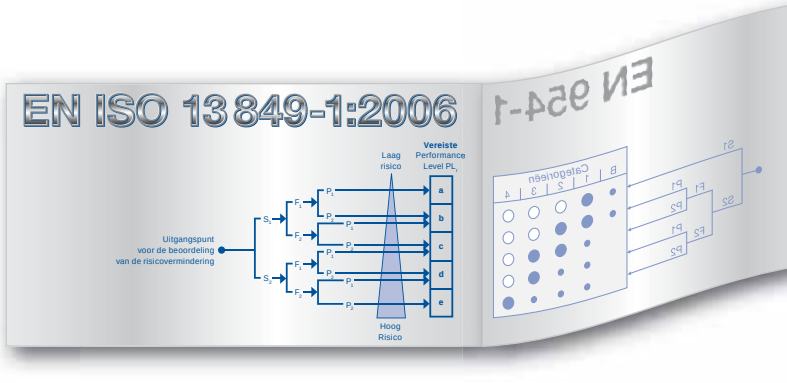
Abbildung 53: Anhang J in EN 13849-1

Vereisten voor de parametersoftware

Basisvereisten voor het parametreren

- Speciale tool van de fabrikant
- Beveiligd tegen ongeoorloofde toegang (bijvoorbeeld via paswoord)
- Plausibiliteitscontroles van de parameters en gegarandeerde gegevensintegriteit tijdens het parametreren
- Beveiligde gegevensoverdracht (met diversitaire weergave)
- Documentatie

Figuur 54: Vereisten voor de parametersoftware



EN ISO 13849-1:2006 versus IEC EN 62061

Theorie

Zoals reeds gezegd komen twee normen – EN ISO 13849-1:2006 en IEC EN 62061 – in aanmerking als opvolger van de EN 954-1. Aanvankelijk was voorzien dat deze normen elkaar zouden aanvullen, om zo tot een eenduidige normenwereld te komen, maar ondertussen is er van “coëxistentie” geen sprake meer.

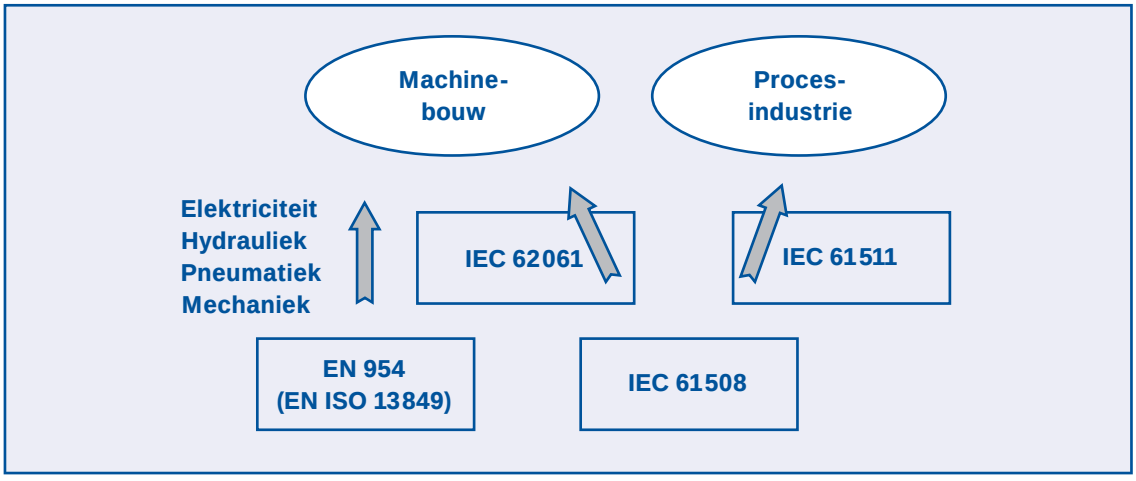
Het staat vast dat de IEC EN 62061, net als de EN ISO 13849-1:2006 en in tegenstelling tot de IEC EN 61508 onder de Machinerichtlijn geharmoniseerd zullen worden. Op die manier zullen beide normen het juridische voordeel van het zogenaamde “vermoeden van overeenstemming met de essentiële vereisten van de Richtlijn” toebedeeld krijgen.

De IEC EN 62061 is een afgeleide van de IEC EN 61508, de specifieke sectornorm voor de machinebouw. Voor de procesindustrie (chemische industrie en procestechnologie) geldt een andere norm, namelijk de IEC EN 61511[1].

De oorspronkelijke bedoeling van de IEC EN 61508 was het opvullen van de hiaten van de EN 954-1, met name vereisten opstellen voor complexe SRP/CS en dan meer bepaald voor elektronische programmeerbare systemen met veiligheidsfunctie (PES systemen), maar het normalisatiecomité van de IEC 61508 heeft het toepassingsgebied van de norm uitgebreid tot discrete elektrische, elektronische en elektronische programmeerbare systemen (E/E/PES).

Op die manier is de IEC EN 61508 uiteindelijk uitgegroeid tot fundamentele overkoepelende norm voor alles wat met veiligheidstechniek te maken heeft. Omdat de IEC EN 61508 tamelijk volumineus is (zij telt meer dan 350 pagina’s en is onderverdeeld in 8 delen), werden sectornormen voor de individuele sectoren uit deze norm afgeleid, zoals de IEC EN 62061[2] voor de machinebouw.

In deze afgeleide normen worden de specifieke vereisten voor de sectoren bepaald; de vereisten en ontwerpprincipes die op andere sectoren van toepassing zijn, worden hierin niet vermeld.



Figuur 55: Overzicht van de concurrerende normen

1) IEC EN 61511-1 (VDE 0810-1:2005-05): Functionele veiligheid – Veiligheidssystemen voor de verwerkende industrie – Deel 1: Algemene begrippen, vereisten voor de systemen, de software en de hardware

2) IEC EN 62061-1 (VDE 0113-50): Veiligheid van machines – Functionele veiligheid van elektrische/elektronische en elektronische programmeerbare systemen met een veiligheidsfunctie

4 Safety Integrity Levels (SIL) en 2 bedrijfsmodi

Safety Integrity Level (veiligheidsintegriteitsniveau)	Lage belasting Gemiddelde waarschijnlijkheid van niet-uitvoering van de verwachte functie op aanvraag PFD	Hoge of continue belasting Gemiddelde waarschijnlijkheid van een gevaarlijke fout per uur PFH
4	$\geq 10^{-5}$ tot $< 10^{-4}$	$\geq 10^{-9}$ tot $< 10^{-8}$
3	$\geq 10^{-4}$ tot $< 10^{-3}$	$\geq 10^{-8}$ tot $< 10^{-7}$
2	$\geq 10^{-3}$ tot $< 10^{-2}$	$\geq 10^{-7}$ tot $< 10^{-6}$
1	$\geq 10^{-2}$ tot $< 10^{-1}$	$\geq 10^{-6}$ tot $< 10^{-5}$

Van toepassing op de machinebouw?

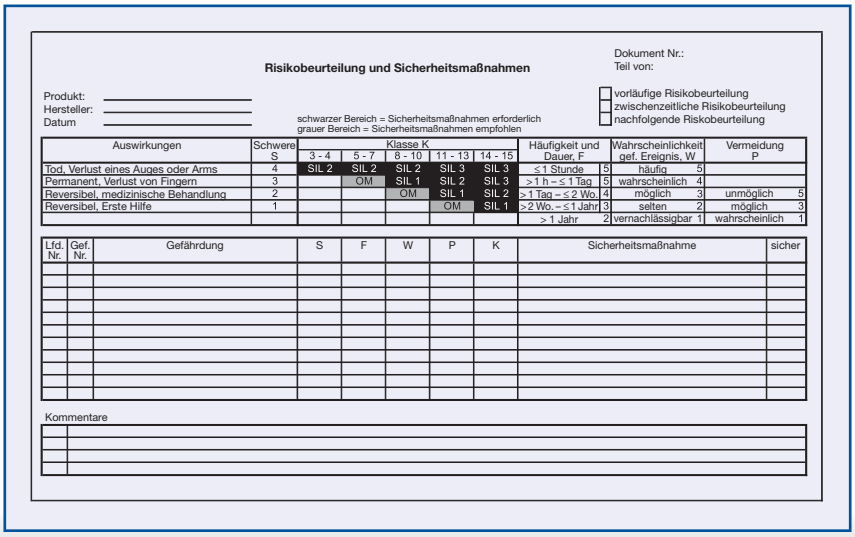
Figuur 56: Safety Integrity Level: IEC 61508 (universele toepassingen) en IEC 62061 (toepassing: machinebouw)

Voor de machinebouw betekent dit dat men zich tot de veiligheidstechnische vereisten beperkt voor hoge of continue belasting (uitgedrukt via de PFH waarde). De lage belasting, waarbij de veiligheidsfunctie minder dan een maal per jaar geactiveerd wordt en niet hoger dan tweemaal de frequentie van de periodieke tests, wordt buiten beschouwing gelaten.

Het Safety Integrity Level SIL 4 (parameter S: dood van meerdere personen, catastrofale uitwerkingen) wordt eveneens uitgesloten.

Toepassing
Verdere details van de IEC EN 62061 worden hier niet besproken. Critici merken op dat deze norm moeilijker in gebruik is dan de EN ISO 13849-1:2006, vooral bij vragen met betrekking tot de risicovermindering aan complexe systemen, die eigen zijn aan de bouw van machines en besturingssystemen. Bij complexe problemen blijkt de IEC EN 61508 toch de meest geschikte norm. Nog een belangrijk verschilpunt tussen de beide normen is dat de EN ISO 13849-1:2006 ook rekening houdt met mechanische, pneumatische en hydraulische componenten. De IEC EN 62061 kent dit onderscheid niet omwille van zijn oorsprong.

Figuur 57: Voorbeeldformulier ter bepaling van het Safety Integrity Level SIL



Risikobeurteilung und Sicherheitsmaßnahmen

Dokument Nr.:
Teil von:

Produkt:
Hersteller:
Datum

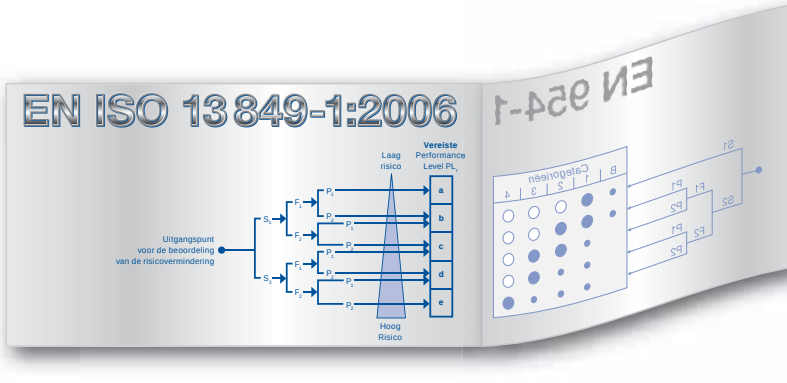
☐ vorläufige Risikobeurteilung
☐ zwischenzeitliche Risikobeurteilung
☐ nachfolgende Risikobeurteilung

schwarzer Bereich = Sicherheitsmaßnahmen erforderlich
grauer Bereich = Sicherheitsmaßnahmen empfohlen

Auswirkungen	Schwere S	Klasse K 3 - 4	5 - 7	8 - 10	11 - 13	14 - 15	Häufigkeit und Dauer, F		Wahrscheinlichkeit gef. Ereignis, W		Vermeidung P	
Tod, Verlust eines Auges oder Arms	4	SIL 2	SIL 2	SIL 2	SIL 3	SIL 3	≤ 1 Stunde	5	häufig	5		
Permanent, Verlust von Fingern	3		OM	SIL 1	SIL 2	SIL 3	> 1 h – ≤ 1 Tag	5	wahrscheinlich	4		
Reversibel, medizinische Behandlung	2			OM	SIL 1	SIL 2	> 1 Tag – ≤ 2 Wo.	4	möglich	3	unmöglich	5
Reversibel, Erste Hilfe	1				OM	SIL 1	> 2 Wo. – ≤ 1 Jahr	3	selten	2	möglich	3
							> 1 Jahr	2	vernachlässigbar	1	wahrscheinlich	1

Lfd. Nr.	Gef. Nr.	Gefährdung	S	F	W	P	K	Sicherheitsmaßnahme	sicher

Kommentare



Voorziene compatibiliteit van de EN ISO 13849-1:2006 en de IEC EN 62061 (IEC EN 61508)

De respectievelijke normalisatiecomités van de IEC EN 62061 en de EN ISO 13849-1:2006 hebben desalniettemin getracht een zekere compatibiliteit tussen de beide normen te bewerkstelligen, door het invoeren van een rechtstreeks verband tussen de Safety Integrity Levels SIL en het Performance Level PL. SIL 1 stemt bijvoorbeeld overeen met Performance Level PL “b” of “c” enz. (zie figuur 58).

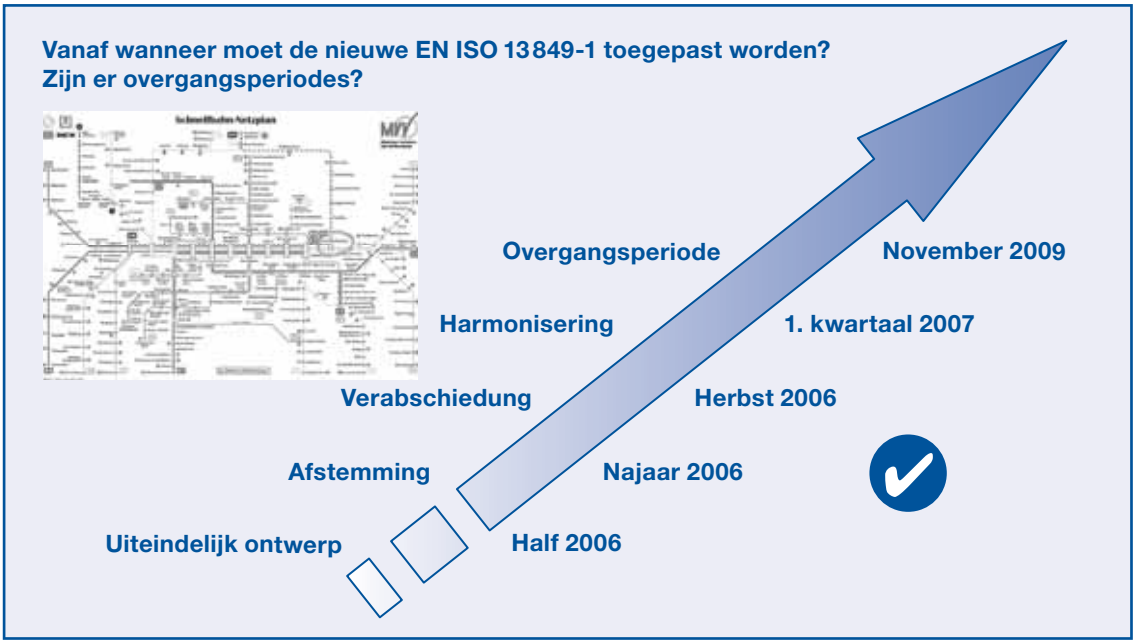
Bovendien zijn de aanbevelingen van beide normen gelijkluidend als het gaat over de meest geschikte norm voor een specifiek probleem. We moeten echter opmerken dat het normalisatiecomité van de EN ISO 13849-1: 2006 van dit compromis afgeweken is voor de wijzigingen die achteraf aangebracht werden, hoewel de toepassingstabel nog altijd in de norm opgenomen is (zie figuur 59).

Figuur 58: Verband tussen het Safety Integrity Level SIL en het Performance Level PL

	Gebruikte technologie voor de veiligheidsgerichte besturingscommando’s	ISO 13849-1 (revisie)	IEC 62061
A	Niet-elektrische, bijvoorbeeld hydraulisch	X	Buiten beschouwing gelaten
B	Elektromechanisch, bijvoorbeeld relais of eenvoudige elektronica	Beperkt tot de Designated architectures[1] en tot PL = e	Alle architecturen en tot SIL 3
C	Complexe elektronica, bijvoorbeeld programmeerbaar	Beperkt tot de Designated architectures[1] en tot PL = d	Alle architecturen en tot SIL 3
D	A gecombineerd met B	Beperkt tot de Designated architectures[1] en tot PL = e	X (EN ISO 13849-1:2006 voor A)
E	C gecombineerd met B	Beperkt tot de Designated architectures[1] en tot PL = d	Alle architecturen en tot SIL 3
F	C gecombineerd met A, of C gecombineerd met A en B	X[2]	X[3]

“X“ betekent dat dit geval besproken wordt in de norm die in de kolomtitel vermeld wordt.
1) De Designated architectures worden gedefinieerd in Bijlage B van de EN ISO 13849-1:2006 (revisie) om een vereenvoudigde aanpak voor de kwantificering van het Performance Level te bieden.
2) Voor complexe elektronica: gebruik van de Designated architectures volgens EN ISO 13849-1:2006 (revisie) tot PL = d of alle architecturen volgens IEC 62061.
3) Voor niet-elektrische technologie: gebruik van de onderdelen als subsysteem volgens EN ISO 13849-1:2006 (revisie).

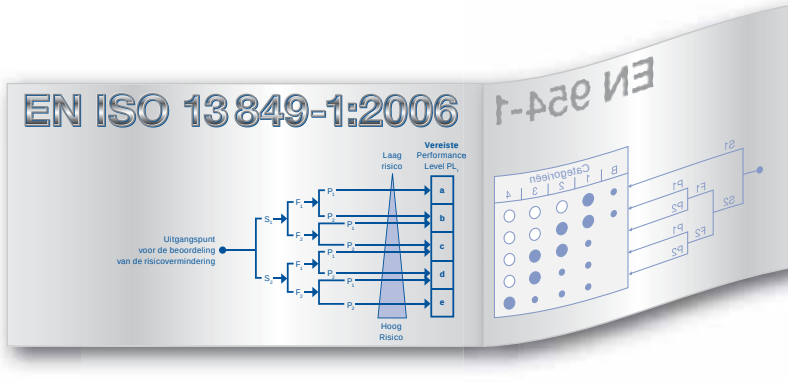
Figuur 59: Aanbevolen toepassing voor de IEC 62061 en de ISO 13849-1 (revisie)



Figuur 60: Planning

Inwerkingtreden van de EN ISO 13849-1: 2006

De IEC EN 62 061 en de EN ISO 13849-1:2006 zijn beiden aangenomen en geharmoniseerd en mogen beiden worden toegepast. Tot november 2009 mag ook de EN-954-1 nog worden toegepast.



Veelgestelde vragen (FAQ)

Wat zijn de essentiële verschillen tussen de huidige versie en de gepubliceerde versie van prEN ISO 13849-1: 2004?

- Aanpassing van de risicograaf
- Specifieke waarden voor de betrouwbaarheid van de veiligheidscomponenten (PFH_d)
- Specifieke $MTTF_d$ en B_{10d} waarden voor hydraulische, pneumatische en elektromechanische componenten
- Softwarevereisten
- Wijziging van het toepassingsgebied
  - Niet beperkt tot de Designated architectures
  - Alleen voor ingebedde software bij PL_e verwijzing naar de IEC 61 508

Figuur 61: Geselecteerde vragen

Een ander verschil vloeit voort uit de interpretatie van categorie 4, waar de beoordeling van een accumulatie van fouten gewoonlijk tot twee fouten beperkt moet blijven.

Hoeveel fouten moet ik combineren in categorie 4?

1. Het optreden van een fout leidt niet tot het verlies van de veiligheidsfunctie
2. De eerste fout wordt …niet gedetecteerd. Als detectie onmogelijk is, mag een accumulatie van fouten niet leiden tot het verlies van de veiligheidsfunctie.

Opmerking: in de praktijk volstaat het dat de combinatie van twee fouten in acht genomen wordt.

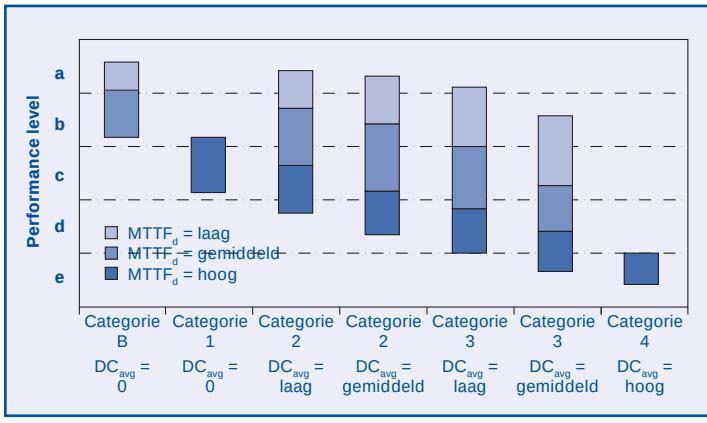
Nieuw: onafhankelijk van de gebruikte technologie voor de toepassing of de foutengraad van de componenten.

Figuur 62: Geselecteerde vragen

EN ISO 13849-1 versus de C-normen
Momenteel bestaan er enkele honderden C-normen of productnormen, bijvoorbeeld voor werktuigmachines, bewerkingscentra, enz. Omdat de huidige C-normen alleen het vermelden van een categorie vereisen, dringen maatregelen ter behoud van de compatibiliteit zich op.

In de komende jaren moeten de ontwikkelaars van de C-normen in actie komen. Zij beschikken over twee mogelijkheden om zich aan de EN ISO 13894-1 aan te passen.

Enerzijds kunnen zij zich ertoe beperken alleen een Performance Level PL voor “hun“ machines te eisen en op die manier hun “klanten” een grotere mate van vrijheid bieden bij het ontwerp, vooral bij een “gemiddeld” Performance Level.



Figuur 63: Diverse mogelijkheden voor de uitvoering

Een andere mogelijkheid bestaat erin, naast het Performance Level ook een categorie te definiëren, vooral als men de invloed op de structuur wil vergroten.

Mijn C-norm vereist een categorie voor de machinebesturing. Kan ik voortaan een Performance Level gebruiken?

- In principe volstaat het als u in de toekomst een Performance Level aangeeft voor de classificatie. De EN ISO 13849-1:2006 voorziet echter dat de gebruikshandleiding van iedere SRP/CS de volgende specificaties vermeldt:

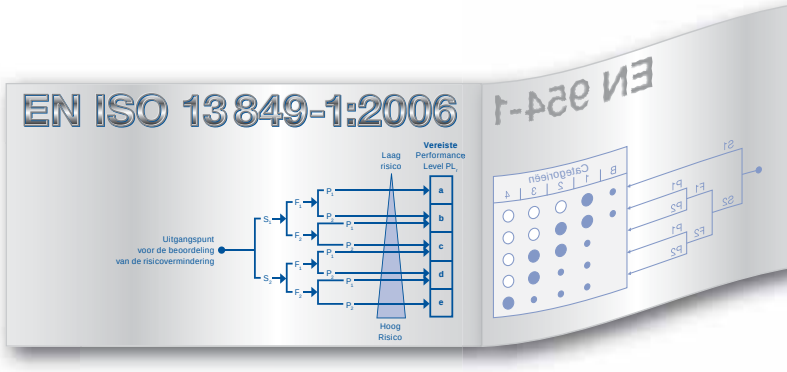
  EN ISO 13849-1:200x
  Categorie X PL Y

Figuur 64: Geselecteerde vragen

De tabel hieronder kan dienen als praktisch hulpmiddel (opgelet bij het realiseren van SRP/CS van categorie 2 met de aangegeven Designated architectures!).

	B	1	2	3	4
Ontwerp in overeenstemming met de relevante normen om het vermogen van de veiligheidsgerichte onderdelen tot het uitvoeren van een veiligheidsfunctie in te voorziene omstandigheden, te garanderen	X	X	X	X	X
Beproefde veiligheidsprincipes		X	X	X	X
Beproefde componenten		X			
Mean Time To dangerous Failure – $MTTF_d$	laag – gemiddeld	hoog	laag – hoog	laag – hoog	hoog
Foutdetectie (tests)			X	X	X
Detectie van een fout				X	X
Inachtneming van de accumulatie van fouten					X
Foutendekking (Diagnostic Coverage) – DC_{avg}			laag – gemiddeld	laag – gemiddeld	hoog
Maatregelen ter voorkoming van fouten met een gemeenschappelijke oorzaak CCF			X	X	X
Hoofdzakelijk gekenmerkt door	Keuze van de component		Structuur		

Figuur 65: Categorieën en bijkomende vereisten



Vooruitblik

Ongetwijfeld blijven er nog een groot aantal vragen in verband met de EN ISO 13849-1: 2006 onbeantwoord. Wij houden u in ieder geval via het MRL News op de hoogte van de laatste ontwikkelingen en verdere verduidelijkingen betreffende dit onderwerp.

De uitwerkingen van de EN ISO 13849-1: 2006 kunnen grofweg in twee groepen onderverdeeld worden: enerzijds de groep met betrekking tot de kwantificering ($MTTF_d$, DC, CCF). Men gaat er van uit dat machines met SRP/CS die beproefde componenten van geschikte kwaliteit integreren, ook aan de vereisten van de nieuwe norm beantwoorden, zonder dat substantiële wijzigingen vereist zijn.

Anderzijds kunnen wijzigingen zich voordoen bij het realiseren van complexe serieschakelingen (“crashgevaar“ voor het Performance Level PL door het optellen van de restrisico’s) en voor het gebruik van de Designated architectures in categorie 2.

Nota's

Overzicht

Uitklappen AUB!

Een nieuwe norm voor de machineveiligheid: **EN ISO 13849-1:2006 – Onderdelen van besturingssystemen met een veiligheidsfunctie**

Overzicht

B10d waarde:
Waarde die het aantal schakelingen vertegenwoordigt, waarbij 10% van de geteste prototypes statistisch gezien een gevaarlijke fout vertonen

CCF:
Fouten met een gemeenschappelijke oorzaak (**C**ommon **C**ause **F**ailure)

Fouten die voortvloeien uit een of meerdere gebeurtenissen, die gelijktijdige fouten veroorzaken van twee of meer gescheiden kanalen in een subsysteem met meerdere kanalen (redundante technologie), waardoor de veiligheidsfunctie verloren gaat

DC:
Foutendekking (**D**iagnostic **C**overage)

Vermindering van de waarschijnlijkheid van een gevaarlijke fout van het materiaal als resultaat van de automatische diagnosetests

DC_{avg}:
Gemiddelde foutendekking (**average D**iagnostic **C**overage)

Designated architecture:
Specifieke configuratie van de materiaal- en software-elementen in een SRPCS

MTBF:
Gemiddelde correcte werkingsduur, gemiddelde tijd voor het optreden van een fout (**M**ean **T**ime **B**etween **F**ailures)

MTTF:
Gemiddelde werking voor het optreden van een fout in een kanaal (**M**ean **T**ime **T**o **F**ailure)

$MTTF_d$:
Gemiddelde werkingsduur voor het optreden van een gevaarlijke fout in een kanaal van een systeem (**M**ean **T**ime **T**o **d**angerous **F**ailure)

PFH:
Waarschijnlijkheid van het optreden van een fout per uur (**P**robability of **F**ailure per **H**our)

PFH_d:
Waarschijnlijkheid van het optreden van een gevaarlijke fout per uur (**P**robability of **d**angerous **F**ailure per **H**our)

PL:
Performance **L**evel

Het vermogen van de veiligheidsgerichte onderdelen om een veiligheidsfunctie uit te voeren onder te voorziene omstandigheden (die in acht genomen moeten worden) om de verwachte risicovermindering te verkrijgen.

PL_r:
Vereiste Performance Level (**P**erformance **L**evel **r**equired)

Performance Level waarmee de vereiste risicovermindering voor iedere veiligheidsfunctie bereikt kan worden.

SIL:
(**S**afety **I**ntegrity **L**evel)

Een van de drie mogelijke discrete niveaus waarmee de vereisten voor de veiligheidsintegriteit van de veiligheidsgerichte besturingscommando's, die aan de SRP/CS toegekend moeten worden, gespecificeerd kunnen worden. SIL 3 vertegenwoordigt de hoogste graad van integriteit, SIL 1 de laagste

SRP/CS:
Onderdelen van een besturingssysteem met veiligheidsfunctie (**S**afety **R**elated **P**arts of a **C**ontrol **S**ystem)

Deel of onderdeel van een besturingssysteem dat op de ingangssignalen reageert en veiligheidsgerichte uitgangssignalen genereert

K.A. Schmersal GmbH
Industrielle Sicherheitsschaltsysteme

Möddinghofe 30
D-42279 Wuppertal
Postfach 240263
D-42232 Wuppertal

Telefon +49 (0)202 6474-0
Fax +49 (0)202 6474-100
E-Mail info@schmersal.com
Internet www.schmersal.com

Elan Schaltelemente GmbH & Co. KG

Im Ostpark 2
D-35435 Wettenberg
Postfach 1109
D-35429 Wettenberg

Telefon +49 (0)641 9848-0
Fax +49 (0)641 9848-420
E-Mail info@elan.schmersal.de
Internet www.elan.de

07/07 X