Zijn standaardcomponenten inzetbaar voor veiligheidsfuncties?

>> Met de komst van de nieuwe veiligheidsnormen NEN-EN-ISO 13849-1 en NEN-EN 62061 onder de Machinerichtlijn krijgt SICK van steeds meer machinefabrikanten vragen over het gebruik van standaardsensoren in veiligheidsfuncties.

Sensorproducenten, waaronder SICK, noteren meestal uitsluitend een MTTFd- of MTTF-waarde. Is deze waarde alleen voldoende voor een beslissing om standaardsensoren te gebruiken in een veiligheidsfunctie? En is het sowieso toegestaan om standaard-onderdelen te gebruiken voor veiligheidsfuncties? Waarom geven de producenten geen parameters op voor bijvoorbeeld Performance Level of Safety Integrity Level voor deze standaardonderdelen?

SICK geeft u inzicht in belangrijke aspecten voor het gebruik van standaardsensoren in veiligheidsfuncties. Aan de hand van twee voorbeelden laten we het verschil in gebruik zien tussen standaardcomponenten en veiligheidscomponenten.

Het antwoord luidt: in principe wel

Kun je standaardcomponenten gebruiken in toepassingen voor machineveiligheid? Het antwoord op deze vraag is: in principe wel.

Enerzijds zorgen de nieuwe veiligheidsnormen NEN-EN-ISO 13849-1 en NEN-EN 62061 voor grotere flexibiliteit bij de machine-fabrikant. Deze kan standaardcomponenten gebruiken in veilig-heidscircuits om materiaalkosten te besparen. Anderzijds hebben systeemontwerpers meer werk te verrichten bij de beoordeling van de betrouwbaarheid en de effecten van de optimalisatie-maatregelen.

De betrouwbaarheidswaarde MTTF (Mean Time To Failure: betrouwbaarheid van onderdelen in relatie tot het optreden van een fout) is een van de factoren bij een dergelijke beoordeling. Steeds meer machinefabrikanten vragen om deze waarde, zodat ze standaardcomponenten kunnen gebruiken in veiligheids-functies. Maar: de MTTF-waarde is slechts één onderdeel van de gegevens waarmee rekening moet worden gehouden in veiligheidsfuncties.

NEN-EN 954-1 vs NEN-EN-ISO 13849-1

NEN-EN 954-1 beschrijft de structurele maatregelen (de archi-tecturen) ingedeeld in categorieën; in NEN-EN-ISO 13849-1 zijn dezelfde categorieën opgenomen. Als aanvulling op de structurele criteria ligt de nadruk van de nieuwe normen vooral op betrouwbaarheid van de componenten, diagnose en maat-regelen om fouten te voorkomen. In het kader ‘De termen toegelicht’ wordt dit nader verklaard (zie pagina 14). Deze genoemde items zijn gericht op NEN-EN-ISO 13849-1 met het Performance Level (PL), maar zijn eveneens geldig als NEN-EN 62061 wordt toegepast.

Waaraan moet u denken als u veiligheidsfuncties ontwerpt volgens de nieuwe veiligheidsnormen NEN-EN-ISO 13849-1 en NEN-EN 62061? Een beknopt overzicht:

Een veiligheidsfunctie wordt uitgevoerd door een veiligheidssysteem om een veilige situatie van een machine en/of systeem te bereiken of te behouden. Een fout in de veiligheidsfunctie resulteert onmiddellijk in een verhoging van het risico. De veiligheidsfunctie wordt bepaald in de gevaren- en risicoanalyse. De veiligheidsfunctie moet minimaal de volgende basis items bevatten:

- **Detectie**
- **Logica**
- **Beweging**
- **Tijdslimieten**, indien nodig

Dit wordt weergegeven in de NEN-EN-ISO 13849-1 als 'subsystemen'. Bij het ontwerpen van subsystemen moet u met de volgende criteria rekening houden:

- Hard- en softwarestructuur (architectuur)
- Betrouwbaarheid van de componenten, in verband met veiligheid
- Effectiviteit van foutdetectie-mechanismen
- Maatregelen die worden genomen ter bestrijding van fouten met een gemeenschappelijke oorzaak
- Het ontwerpproces van hardware en software
- Geschiktheid voor de werkbelasting en de omgevingsomstandigheden

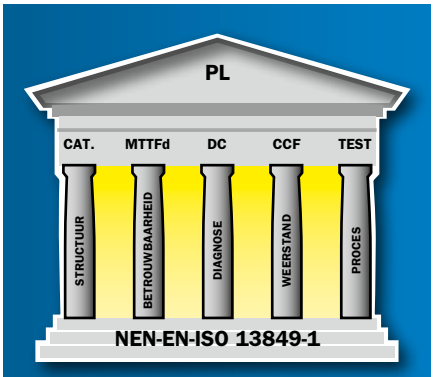


Fig. 1: De pijlers voor het bepalen van de veiligheidsprestaties van een subsysteem volgens NEN-EN-ISO 13849-1

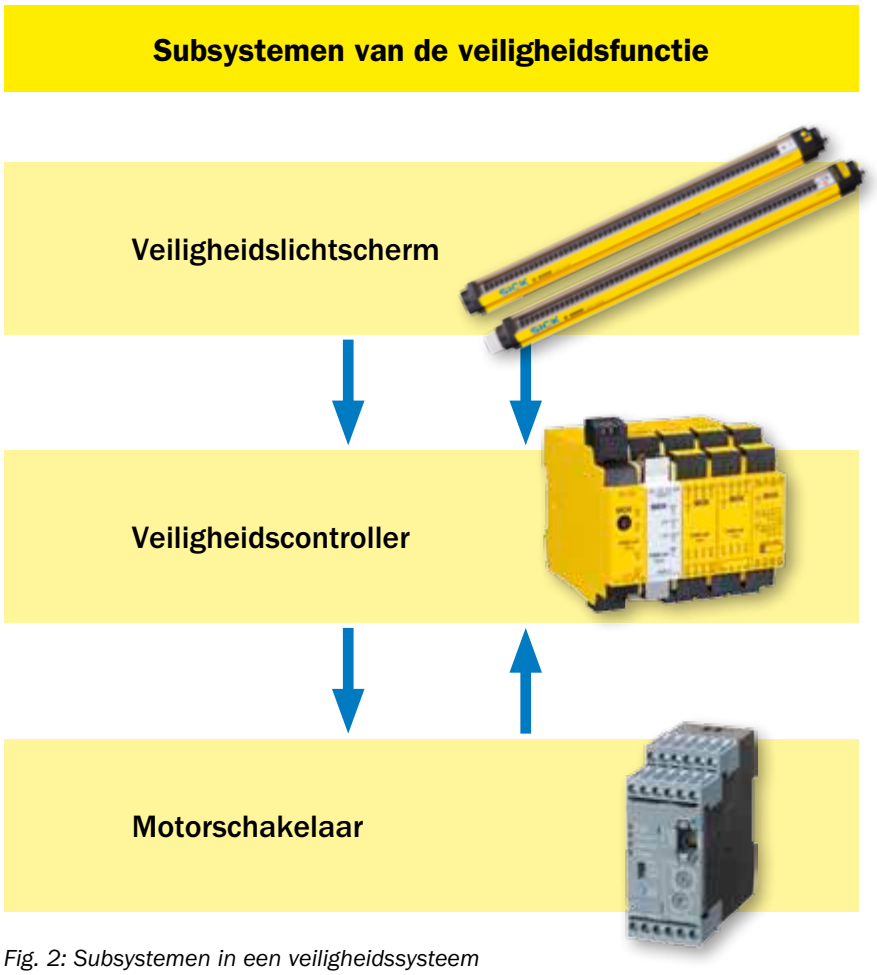


Fig. 2: Subsystemen in een veiligheidssysteem

De subsystemen, bijvoorbeeld veiligheidslichtschermen of veiligheidscontrollers, worden vastgesteld voor de berekening en evaluatie van een veiligheidsfunctie (zie fig. 2).

Voor deze subsystemen wordt de Performance Level (PL) volgens NEN-EN-ISO 13849-1 dan wel het Safety Integrity Level (SILcl) volgens NEN-EN 62061 bepaald.

Voor foutdetectie van vaak elektromechanische componenten in het veiligheidscircuit, zoals motorschakelaars en vergrendelingen maar ook bijvoorbeeld ventielen, zijn aanvullende maatregelen door middel van een overkoepelend besturingssysteem vereist.

Indien optische sensoren worden gebruikt, moet niet alleen rekening worden gehouden met de functionele veiligheidsaspecten, maar ook met de optische kenmerken die de vereiste detectiecapaciteit van de sensor bepalen. Deze kenmerken zijn variabel, afhankelijk van het feit of de veiligheidsfunctie is bedoeld voor de detectie van personen of objecten. De tabel op pagina 11 geeft de aanvullende optische kenmerken voor detectie van personen weer.

SICK
Sensor Intelligence.

Hoe bepaalt u de vereiste Safety Performance Level?

Figuur 3: Zes stappen naar een veilige machine

De 'Guidelines Safe Machinery' van SICK beschrijven in zes stappen welke wetten, normen en regels de gebruiker moet naleven en wat de mogelijke beschermende maatregelen zijn. Een deel van stap 3 is het bepalen van de Safety Performance Level.

In NEN-EN ISO 13849-1 wordt een risicografiek gebruikt om deze vereiste Performance Level (PLr; de r staat voor 'required') te bepalen (zie figuur 4). De systeemontwerper beoordeelt eerst de gevaren van de machine zonder beschermende maatregelen op basis van:

- de ernst van het letsel;
- de frequentie en/of de duur van het gevaar;
- de mogelijkheid om het gevaar te vermijden of de schade/het letsel te beperken.

Dit resulteert in een Performance Level 'PLr = a t/m e' voor de vereiste kwaliteit van de beschermende maatregelen, waarbij 'e' staat voor de grootste risicovermindering. >>

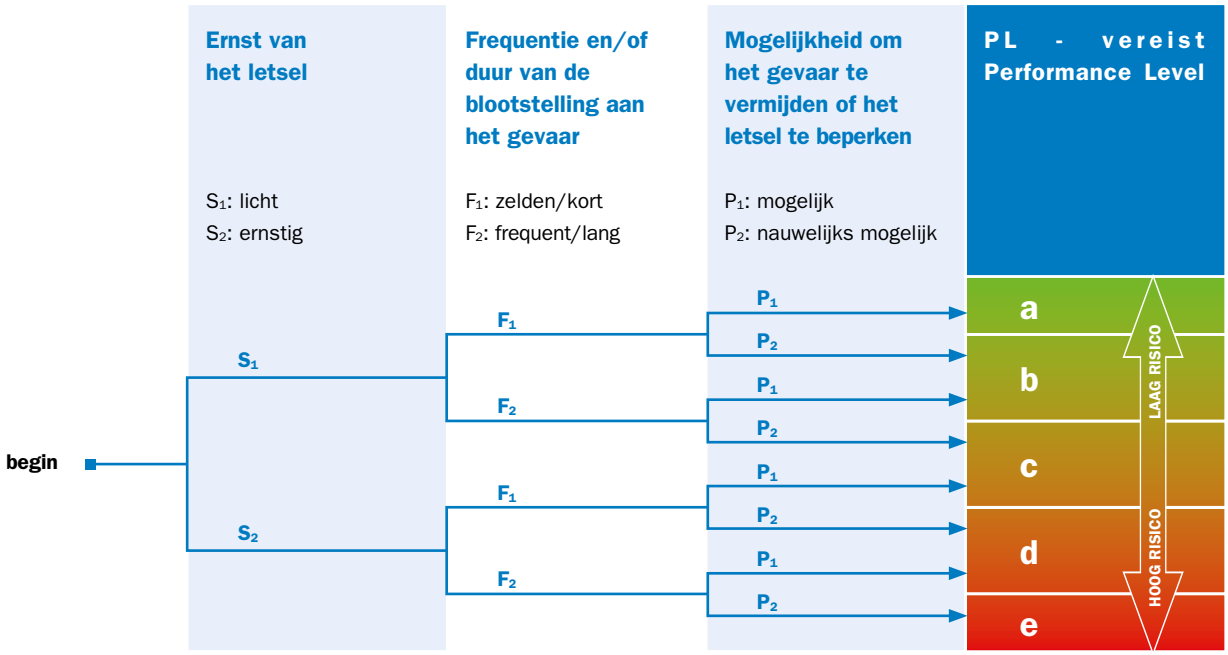
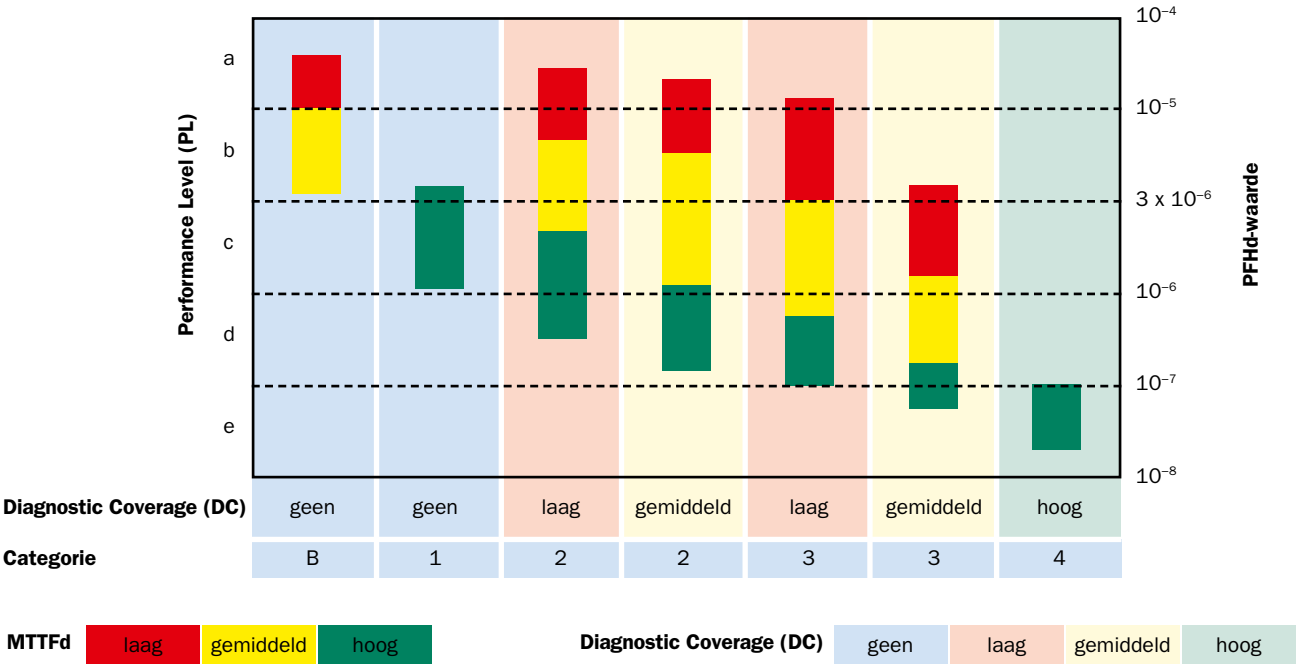


Fig. 4: Het bepalen van het vereiste Performance Level volgens NEN-EN ISO 13849-1 (risicografiek)

SICK
Sensor Intelligence.

Levert de technische beschermingsmaatregel de vereiste veiligheidsprestaties op?

De NEN-EN ISO 13849-1 geeft een leidraad om te bepalen of de technische beschermingsmaatregel het vereiste Safety Performance Level (PLr) kan opleveren. In de norm staat ook een staafdiagram dat een vereenvoudigd overzicht geeft van de vereiste criteria (zie figuur 5). Niet getoond worden: de eisen voor het ontwerpproces, de toepassingsomstandigheden en de maatregelen tegen de systematische fouten (zie het kader 'De termen toegelicht').



Figuur 5: Het bepalen van het PL van een subsysteem volgens de vereenvoudigde methode van de NEN-EN ISO 13849-1.

De beveiligingstaak en de oplossing

Twee voorbeeldsituaties, meerdere beveiligingsoplossingen

Als toelichting op de theorie van hiervoor hier twee praktijkcases. Hierbij wordt aan de hand van verschillende oplossingen het gebruik van standaardsensoren voor veiligheidsfuncties beoordeeld.

SICK
Sensor Intelligence.

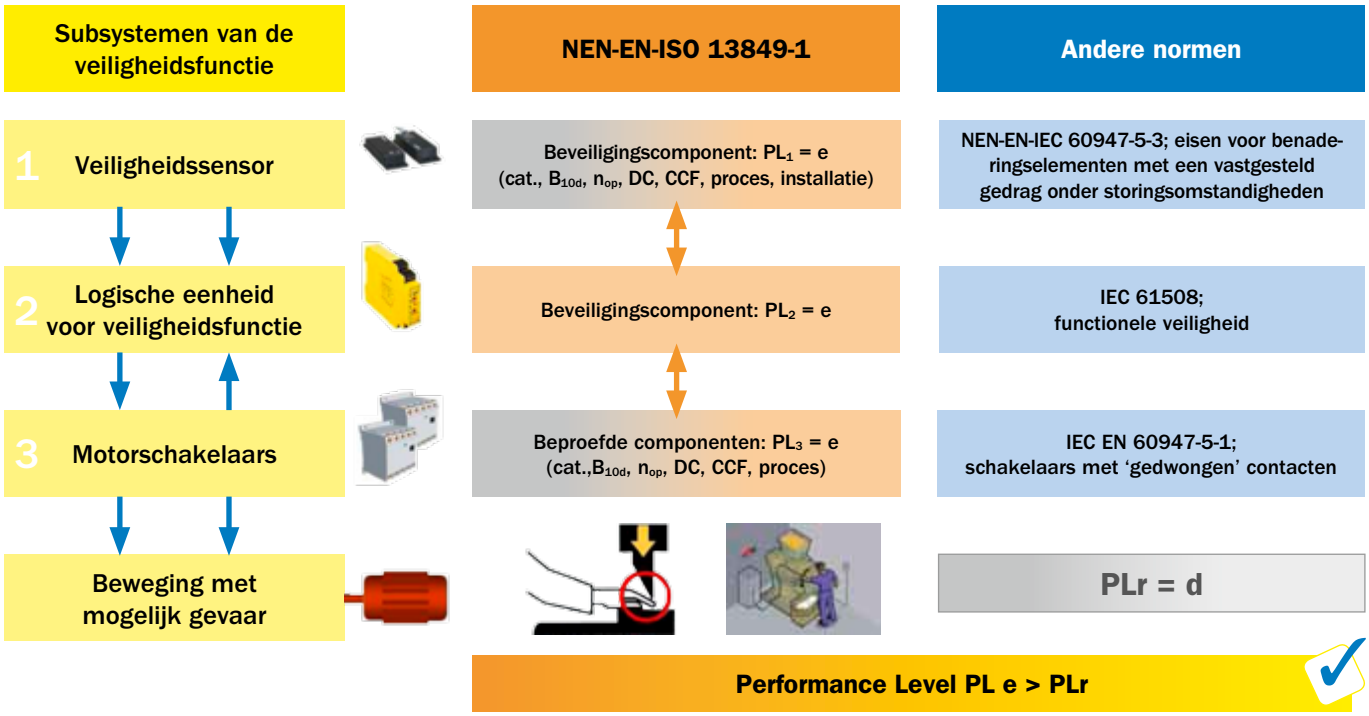
Case 1: bewaken van de veiligheidsdeur op een maalmachine

De veiligheidsdeur van de maalmachine wordt viermaal per uur geopend en gesloten. De veiligheidsfunctie moet ervoor zorgen dat de motor van de maalmachine onmiddellijk uitschakelt als de deur wordt geopend.
De risicobeoordeling heeft geleid tot het vereiste veiligheidsniveau PLr = d.

Figuur 6: Taak 1: een maalmachine beveiligen met veiligheidsdeurdetectie

Oplossing 1.1 – Een veilige magneetschakelaar

>> Een benaderingsschakelaar voor veiligheidsfuncties wordt gebruikt als sensor. Het veiligheidssysteem bestaat uit de veiligheidssensor, een logische eenheid en de motorschakelaars waarmee de gevaarlijke beweging wordt gestopt. Het bereikte PL voor elk van deze subsystemen wordt vastgesteld. De fabrikant van de componenten zorgt voor de benodigde gegevens en de normen zoals toegepast voor de gebruikte componenten, inclusief beveiligingscomponenten (zie figuur 7).



Figuur 7: Veiligheidssysteem met subsystemen voor oplossing 1.1 van Taak 1, de beoordeling ervan conform NEN-EN ISO 13849-1 en de relevante productnormen

Zoals blijkt uit figuur 7 geeft de fabrikant geen Performance Level (PL) voor alle gebruikte componenten. Om de Performance Level vast te stellen, moet de gebruiker een beoordeling uitvoeren van de structuur (de categorie), de diagnose en de testmaatregelen (DC) zoals deze zijn uitgevoerd door de logische eenheid, en de maatregelen die zijn genomen om fouten met een gemeenschappelijke oorzaak (CCF) te bestrijden.

De sensor moet zodanig op de machine worden geplaatst dat niemand de beschermingsmaatregel kan omzeilen (met andere woorden: op een 'sabotagebestendige' plaats). Het bij oplossing 1.1 vastgestelde veiligheidsniveau is PL = e, dat zelfs hoger is dan het vereiste niveau PLr = d.

Resultaat: de veiligheidsfunctie kan voor beschermingsdoeleinden worden gebruikt.

SICK
Sensor Intelligence.

Oplossing 1.2 – Eén standaard inductieve sensor

>> Er wordt één standaard inductieve sensor gebruikt voor de veiligheidsfunctie (figuur 8). De fabrikant geeft een MTTFd van 83 jaar voor de sensor (MTTFd = "Hoog" volgens NEN-EN ISO 13849-1). De sensor is ontwikkeld in overeenstemming met de productnorm NEN-EN-IEC 60947-5-2. Daardoor kan worden aangenomen dat de sensor overeenstemt met de basis-veiligheidsprincipes voor dit specifieke type (zie "De termen toegelicht").

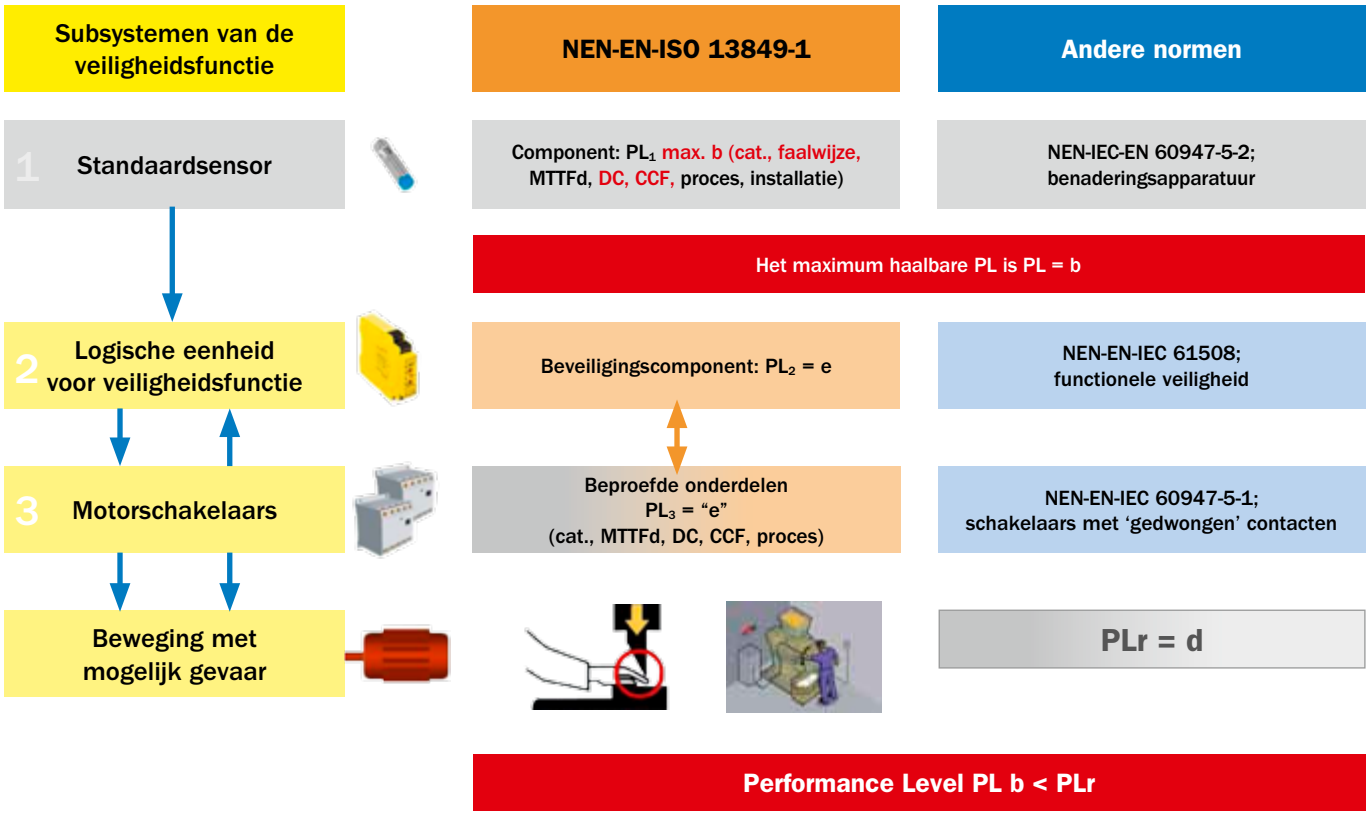
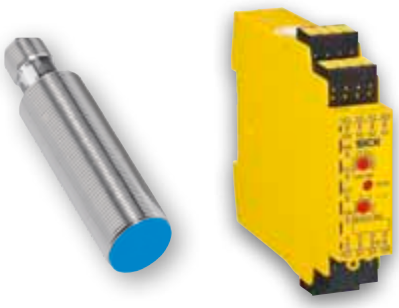


Fig. 8: Veiligheidssysteem met subsystemen voor oplossing 1.2, de beoordeling ervan conform NEN-EN ISO 13849-1 en de relevante productnormen

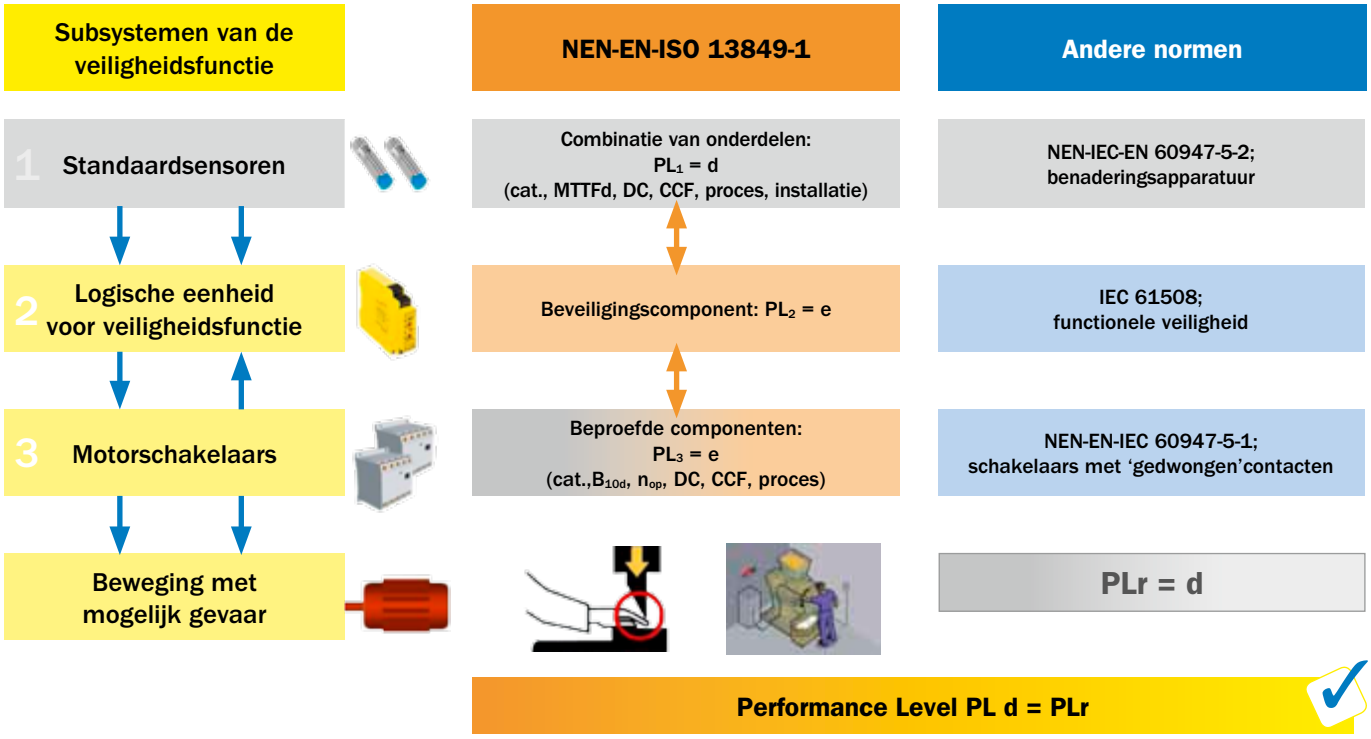
Deze standaardsensor is meestal voorzien van complexe elektronische onderdelen (bijvoorbeeld µC, ASIC, transistorreeksen). De fabrikant specificeert geen faalwijze ingeval van een interne fout. Dit betekent dat deze sensor geen component volgens beproefde veiligheidsprincipes is, zoals gedefinieerd in de NEN-EN ISO 13849-2 – het is gewoon een standaardcomponent (zie 'De termen toegelicht'). Deze beperking houdt in dat de veiligheidsbeoordeling niet hoger kan zijn dan categorie B of Performance Level b, ervan uitgaande dat het component de in de toepassing te verwachten omgevingsinvloeden kan weerstaan (zie 'De termen toegelicht').



Resultaat: met oplossing 1.2 wordt de vereiste Performance Level d niet bereikt, ondanks de hoge MTTFd-waarde van de sensor (zie figuur 5). Met een extra, extern elektrisch testmechanisme kunnen enkele veiligheids-gerelateerde fouten worden gedetecteerd. Het is echter onmogelijk om een complete foutendekking (DC) te krijgen, omdat de interne structuur en faalwijzen in de sensor onbekend zijn. Het testmechanisme zou de veiligheidsbeoordeling dan ook niet veranderen.

Oplossing 1.3 – Twee standaard inductieve sensoren

>> Twee dezelfde sensoren als bij oplossing 1.2, die worden gebruikt als een tweekanaals ingangscircuit. De logische eenheid zorgt voor de diagnose en controleert of de ingangssignalen naar het ingangscircuit plausibel zijn (beide kanalen moet altijd een identiek signaalniveau hebben).



Figuur 9: Twee identieke standaardsensoren in een tweekanaals ingangscircuit voor oplossing 1.3

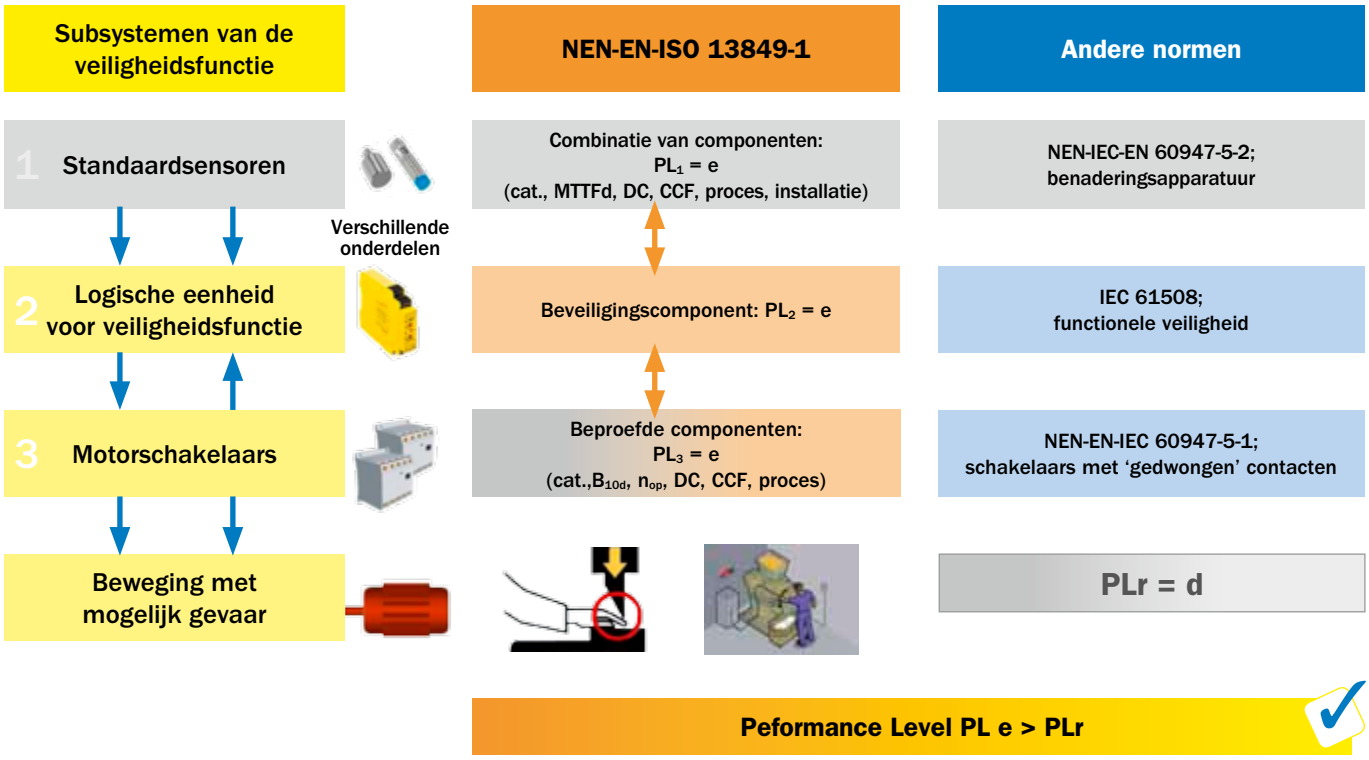
Deze tweekanaals architectuur, met plausibiliteitscontrole door de logische eenheid, biedt een betere foutendekking dan de oplossing met één kanaal. De controle wordt iedere keer uitgevoerd als de veiligheidsdeur wordt geopend en gesloten (ongeveer viermaal per uur). Aangezien er geen dynamische test en geen detectie van kortsluiting tussen de twee ingangskanalen is, bereikt het subsysteem van sensoren samen met de logische eenheid een gemiddelde foutendekking (DC 90%).

Resultaat: met de architectuur uit categorie 3 en de gemiddelde DC kan het mogelijk zijn om PLd te bereiken (zie figuur 5). Er moeten echter maatregelen worden genomen om het optreden van onbekende fouten in beide kanalen van het ingangscircuit op hetzelfde tijdstip te voorkomen. Dat kan namelijk leiden tot het falen van de veiligheidsfunctie (zie 'De termen toegelicht'). Bijvoorbeeld: overspanningspieken op de sensorlijnen als gevolg van hoge inductieve schakelbelastingen in de buurt kunnen een gelijktijdige vernieling van de schakeluitgangen van de sensoren veroorzaken (beide kanalen moeten op 'hoog' niveau blijven).

Als de CCF-maatregelen niet voldoende zijn of als de lokale omstandigheden niet kunnen worden beoordeeld, dan moet de tweekanaals architectuur worden beoordeeld alsof het een eenkanaals architectuur is. In dat geval is, net als voor oplossing 1.2, categorie B de hoogst haalbare, omdat de combinatie van twee standaardsensoren evenmin kan worden beschouwd als beproefd veiligheidsprincipe. Het vereiste Performance Level d kan worden bereikt met oplossing 1.3. Daarbij moet de gebruiker de toepassingsomstandigheden kennen en de effecten van falen beoordelen.

Oplossing 1.4 – Twee verschillende standaardsensoren

>> In tegenstelling tot oplossing 1.3 wordt hier de krachtige techniek van meervoudige redundantie gebruikt. Twee verschillende types standaardsensoren met verschillende interne structuren en met inverse uitgangsniveaus worden door de logische eenheid op basis van twee kanalen gecontroleerd (figuur 10). De MTTFd-waarden van de twee sensoren samen geven een hoge totale MTTFd-waarde.



Figuur 10: Twee verschillende standaardsensoren als een tweekanaals ingangscircuit voor oplossing 1.4

Het ingangscircuit heeft een tweekanaals architectuur met plausibiliteitscontrole en kortsluitdetectie door de logische eenheid. De foutendekking verbetert tot 99% (DC = 'hoog') en de diversiteit draagt sterk bij aan het voorkomen van CCF.

Resultaat: met de categorie 4-architectuur, DC = 'hoog', adequate maatregelen om CCF te voorkomen, en MTTFd = 'hoog', is het zelfs mogelijk om een totaal van PL = e te bereiken (zie figuur 5).

Case 2: bescherming van een gevaarlijk punt bij een batch collector

Een lichtscherm moet zorgen voor de bescherming van een gevaarlijk punt bij een batch collector in de productielijn van een bakkerij. Het vereiste Performance Level, PLr, is c. Andere factoren dan de PL waarmee in de keuze van het lichtscherm rekening moet worden gehouden, zijn de optische omstandigheden, zoals de effecten van omgevingslicht en reflecties, en de gevolgen daarvan voor de detectiebetrouwbaarheid (zie tabel op pagina 11).

Figuur 11: Bescherming voor een batch collector met PLr = c

Oplossing 2.1 – Veiligheidslichtscherm

>> De componenten worden geselecteerd aan de hand van de vereiste Safety Performance Level (figuur 12).

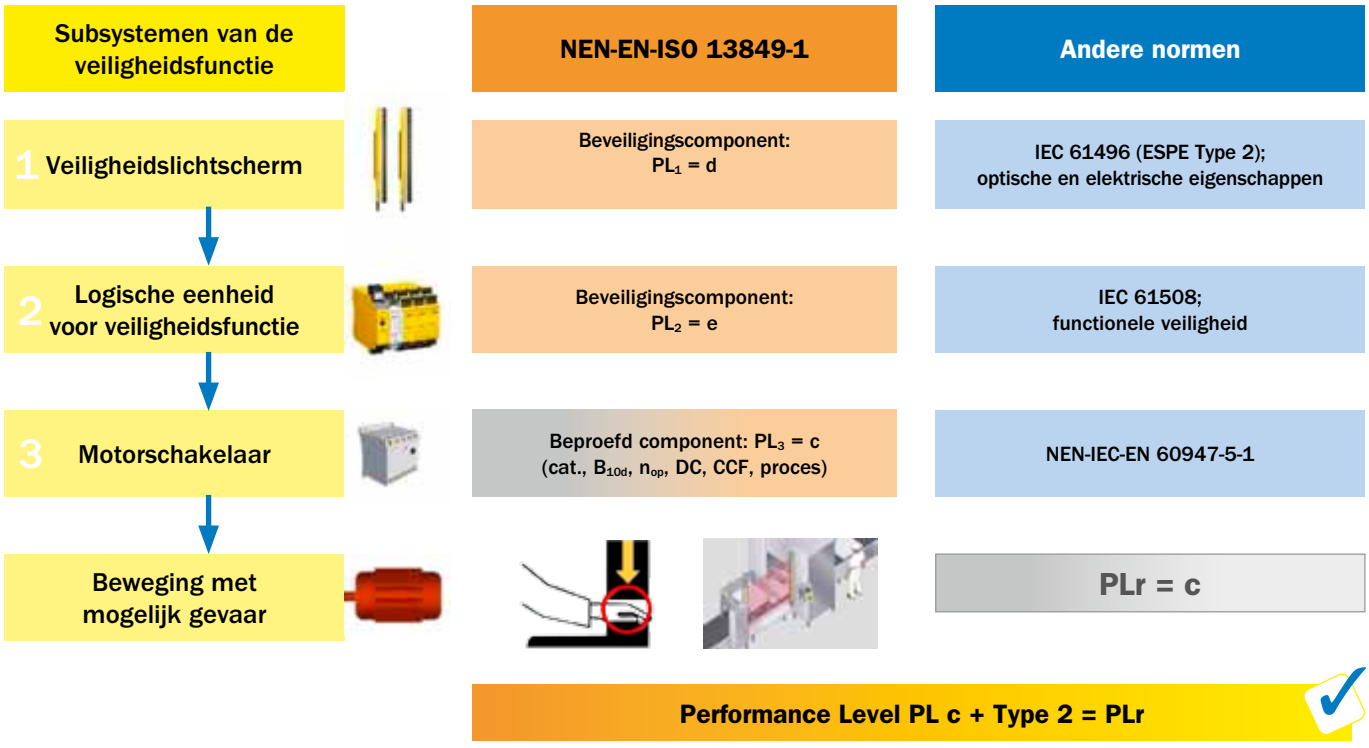


Fig. 12: Veiligheidssysteem met subsystemen voor oplossing 2.1, de beoordeling ervan conform NEN-EN ISO 13849-1 en de relevante productnormen

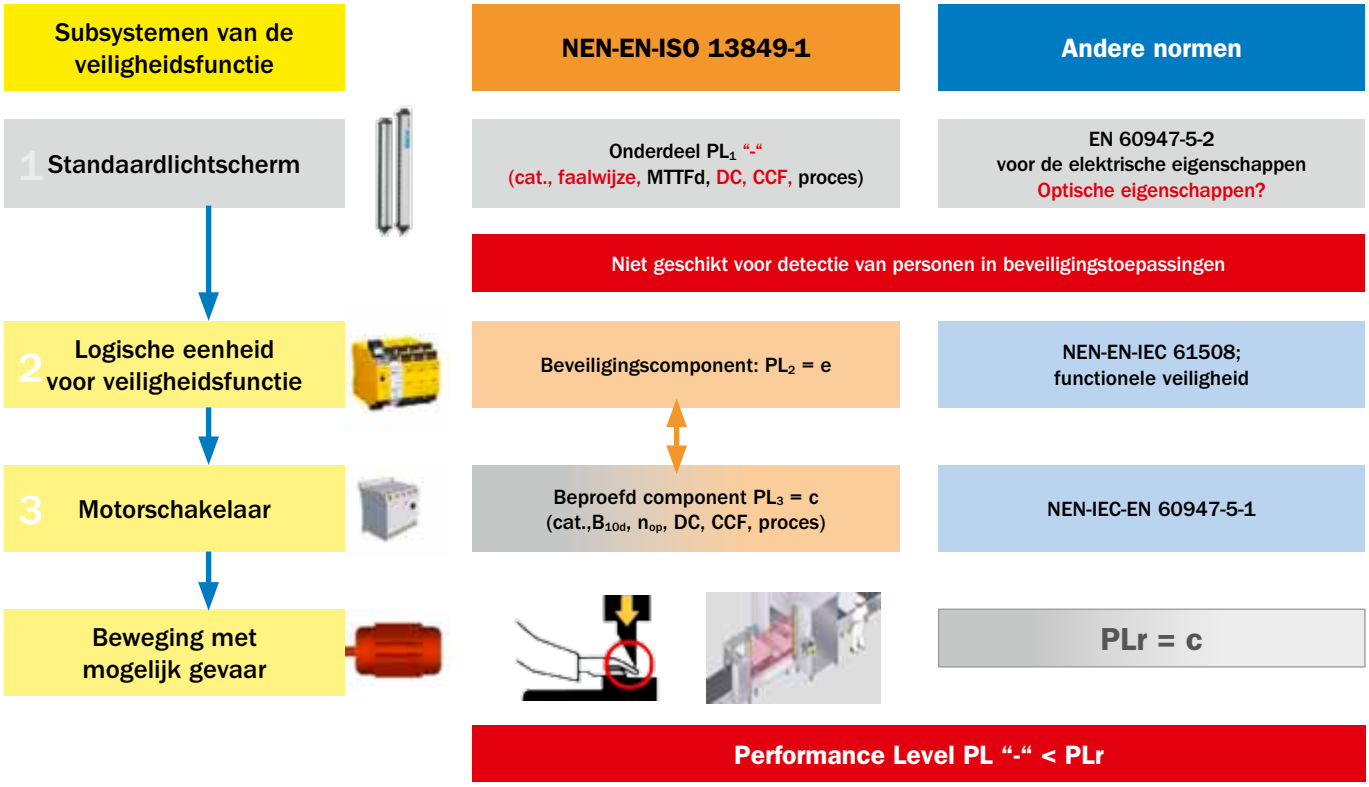
In sommige gevallen voldoen de subsystemen in figuur 12 aan een hogere Performance Level dan noodzakelijk. Een veiligheidslichtscherm van type 2, zoals gedefinieerd door de IEC 61496, wordt gebruikt als de sensor. Voor optische beveiligingsinrichtingen is type 2 het 'optische equivalent' van PL c. De gebruikte onderdelen en de eenkanaals architectuur bij de motorschakelaar voldoen aan categorie 1.

Resultaat: met oplossing 2.1 wordt aan het vereiste veiligheidsniveau (PLr) en de eisen voor de optische eigenschappen voldaan. Daarbij geldt wel als voorwaarde dat de software van de logische eenheid (de programmeerbare veiligheidsbesturing) voldoet aan de eisen van 'logisch programmeren van systemen met een veiligheidsfunctie' volgens NEN-EN ISO 13849-1.

Voor de eenkanaals besturing van de schakelaars zonder terugkoppeling, zoals weergegeven in figuur 12 in het subsysteem 'Motorschakelaar' geldt DC = nul. CCF is niet relevant, omdat het uitgangscircuit een eenkanaals architectuur heeft. De vereiste PLr = c wordt echter bereikt als de schakelaar een beproefd component is met een hoge MTTFd (≥ 30 jaar). De MTTFd-waarde kan worden berekend aan de hand van de B10d-waarde en de schakelfrequentie (zie 'De termen toegelicht').

Oplossing 2.2 – Standaardlichtscherm

>> Er wordt een standaardlichtscherm gebruikt voor de veiligheidsfunctie in plaats van een veiligheidslichtscherm (figuur 13).

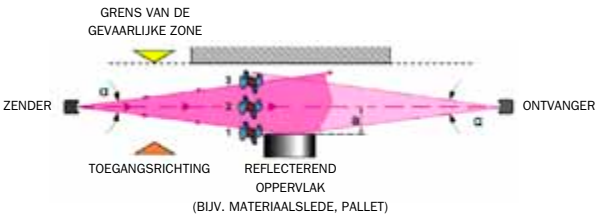
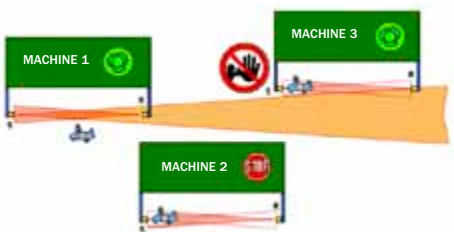


Figuur 13: Subsystemen voor oplossing 2.2, de beoordeling ervan conform NEN-EN ISO 13849-1 en de relevante productnormen

Er is geen productnorm voor de optische eigenschappen van het standaardlichtscherm. De criteria voor de detectie van personen en functionele veiligheid, zoals gedefinieerd in IEC 61496, zijn tijdens de ontwikkeling niet opgevolgd door de fabrikant. De fabrikant kan de faalwijze niet aanduiden bij een interne fout, omdat dit standaardcomponent is uitgerust met complexe elektronische onderdelen (bijvoorbeeld µC, ASIC). Dit betekent dat dit lichtscherm geen beproefd component is volgens de beproefde veiligheidsprincipes die zijn gedefinieerd in NEN-EN ISO 13849-2. De optische eigenschappen van dit standaardlichtscherm voldoen niet aan de eisen van de normen uit de IEC 61496-serie voor opto-elektronische beveiligingsapparatuur, zoals bedoeld voor de bescherming van personen (zie tabel op pagina 11).

Resultaat: het vereiste Performance Level c wordt niet bereikt met oplossing 2.2. Net als bij de standaard inductieve sensor (oplossing 1.2) kan dit resultaat niet worden verbeterd met de toevoeging van een extern testmechanisme.

Enkele eisen voor opto-elektronische beveiligingen die bedoeld zijn voor de detectie van personen

Enkele eisen voor AOPD (actieve opto-elektronische beveiligingsapparatuur) volgens IEC 61496	Achtergrond	Voorbeelden van verlies van detectievermogen voor personen indien de eisen worden genegeerd
Conform de functionele veiligheid (categorie)	Gebruik voor persoonlijke beschermingsfuncties	1. Reflectie 
Resolutietest		
Hogere EMC-eisen	Hogere weerstand tegen veiligheidsgerelateerde fouten en een betere beschikbaarheid van het systeem	
Maximale effectieve openings-hoek van de optische apparatuur: 10° / 5°	Behoud van detectiecapaciteit ingeval van interferentie door reflectie en omgevingslicht	2. Interferentie door omgevingslicht 
Minimale afstand van reflecterende oppervlakken		
Geen storing door meerdere zenders van hetzelfde type binnen één productieomgeving		

Bij ESPE (aanrakingsvrije elektronische beveiligingsinrichtingen) is het altijd uiterst belangrijk om niet alleen rekening te houden met de functionele veiligheidsaspecten, maar ook met de optische eigenschappen die het detectievermogen bepalen.

Samengevat

Wat zijn de voor- en nadelen van het gebruik van standaardsensoren voor veiligheidsfuncties?

>> Het is mogelijk om materiaalkosten te besparen door standaardcomponenten in veiligheidstoepassingen te gebruiken. Gaat het echter om bescherming van personen, dan moet de gebruiker zeer goed op de hoogte zijn van alle toepassingsomstandigheden. Ook moet hij weten welke maatregelen moeten worden genomen en moet hij kennis hebben van veiligheidsmechanismen. Met andere woorden: hij moet weten of een component geschikt is voor gebruik in veiligheidscircuits.

Als er slechts één standaardsensor wordt gebruikt in toepassingen met PL = c of hoger, dan moet de gebruiker zelfs kennis hebben van de interne foutdetectiemechanismen. En dat is meestal niet realistisch ingeval van complexe componenten. Basisregel is dat het niet is toegestaan om standaard optische sensoren te gebruiken voor het detecteren van personen, tenzij u een speciale procedure voor de beoordeling van de conformiteit opvolgt volgens de Machinerichtlijn. Dit geldt voor zowel fabrikanten als gebruikers.

Fabrikanten werken niet volgens de normen die relevant zijn voor veiligheidstoepassingen, wanneer ze standaardonderdelen produceren. Ook hoeven extra veiligheidsparameters (PL, SIL, PFHd, DC...) niet te worden gespecificeerd, zoals wel het geval is voor beveiligingscomponenten. Die moeten namelijk voldoen aan de Machinerichtlijn.

Voordelen van beveiligingscomponenten:

- Beveiligingscomponenten worden door de fabrikant ontwikkeld en geproduceerd volgens de laatste technologische ontwikkelingen en volgens de geldende veiligheidsnormen. Ook wordt rekening gehouden met eventuele factoren in de toepassing die van invloed kunnen zijn op de veiligheid.
- De faalwijze van een veiligheidsonderdeel wordt door de fabrikant gedefinieerd.
- Voor veel soorten veiligheidsonderdelen laat de fabrikant een EG-prototypetest uitvoeren door een erkende instantie (zoals TÜV of IFA).
- De fabrikant besteedt bijzondere aandacht aan de manier waarop de producten in de praktijk presteren.
- De veiligheidsparameters voor het evalueren van de veiligheidscircuits, zoals PL, SIL, PFHd, B_{10d}, en de categorie worden door de fabrikant geleverd.

De conclusie

De voorbeelden illustreren de belangrijkste basisaspecten van het gebruik van standaardsensoren voor veiligheidsfuncties. U ziet dat zelfs met een goede (hoge) MTTFd-waarde slechts aan een klein deel van de vereiste criteria en maatregelen wordt voldaan. Optimalisatie en andere maatregelen voor het gebruik van standaardsensoren, zoals maatregelen die tests ondersteunen, of maatregelen die het gebruik vergemakkelijken door fouten uit te sluiten, zijn mogelijk en worden nu al in praktijk gebracht. Fabrikanten van onderdelen, zoals SICK en bevoegde instanties zoals de Duitse IFA (voorheen BGIA) of TÜV, zijn beschikbaar voor advies en begeleiding.

Machinefabrikanten hebben zeker de mogelijkheid om standaardonderdelen te gebruiken voor veiligheidsfuncties. Het verstrekken van gedocumenteerd bewijs van de geschiktheid van alle onderdelen die worden gebruikt voor veiligheidsfuncties, behoort tot de verplichtingen van de machinefabrikant. Het is duidelijk dat het verstrekken van dit gedocumenteerde bewijs van geschiktheid heel veel moeilijker is bij standaardsensoren.

Meer lezen?

- NEN-EN ISO 13849-1: Veiligheid van machines - Onderdelen van besturingssystemen met een veiligheidsfunctie – Deel 1: Algemene regels voor ontwerp (ISO 13849-1:2006)
- EN ISO 13849-2: Veiligheid van machines - Onderdelen van besturingssystemen met een veiligheidsfunctie – Deel 2: Validatie (ISO 13849-2:2003)
- NEN-EN-IEC 62061:2005 Veiligheid van machines - Functionele veiligheid van elektrische, elektronische en programmeerbare systemen met een veiligheidsfunctie
- NEN-EN-IEC 61496 serie: Machineveiligheid - Aanrakingsvrije elektrische beveiligingsinrichtingen
- Guidelines Safe Machinery, “Six steps to a safe machine” EU versie, deel Nr. 8007988, Noord-Amerikaanse versie, deel Nr. 7028282, te downloaden en te bestellen via www.sick-safetyplus.com

SICK
Sensor Intelligence.

SICK B.V. · Leijenseweg 111 · Postbus 186 · 3720 AD Bilthoven · Tel. 030 - 229 25 44 · Fax 030 - 229 39 94 · E-mail info@sick.nl · www.sick.nl

De termen toegelicht

Voor de veiligheidsfuncties van categorie B en hoger is het naleven van de **basisveiligheidsprincipes** verplicht. Deze principes omvatten algemeen erkende, goede technische praktijken die de componentenfabrikant moet opvolgen, zoals beschreven in productnormen (omgevingsomstandigheden, werkingsprincipes enz.). Tijdens de ontwikkeling en productie worden maatregelen getroffen om systematische fouten te beheersen.

De gebruiker heeft ook bepaalde verplichtingen, zoals het voldoen aan de specificaties en het zorgen voor de juiste bevestiging (zie NEN-EN-ISO 13849-2, paragraaf A.2, B.2, C.2 en D.2). U moet een component zo kiezen dat het correct functioneert onder alle verwachte **toepassingsomstandigheden en omgevingsinvloeden** (bijvoorbeeld temperatuur, vochtigheid, trillingen, elektromagnetische interferentie, optische storing). Of het moet zo geregeld zijn dat de machine in de veilige stand gaat of blijft als het component niet juist functioneert.

Voor categorie 1 en hoger is het naleven van **beproefde veiligheidsprincipes** verplicht. Dit verwijst naar principes die het mogelijk maken om bepaalde fouten uit te sluiten door het gebruik of de configuratie van componenten. Bijvoorbeeld door het gebruik van componenten met een gedefinieerde (bekende) faalwijze of met positief geleide contacten, of door technieken zoals redundantie en diversiteit (NEN-EN-ISO 13849-2, paragraaf A.3 en D.3).

Het gebruik van **beproefde componenten** is een voorwaarde voor categorie 1. Beproefde componenten zijn die componenten die in het verleden op grote schaal met succes zijn gebruikt voor specifieke beveiligingstoepassingen, of die zijn gemaakt en getoetst aan de hand van theorieën die hun geschiktheid en betrouwbaarheid voor beveiligingstoepassingen aantonen. Voorbeelden hiervan zijn opgenomen in de NEN-EN-ISO 13849-2, paragraaf B.4 en D.4. Sommige componenten zijn niet opgenomen in deze definitie, zoals standaard PLC's of standaard foto-elektrische schakelaars.

De **MTTFd-waarde (Mean Time To Dangerous Failure)**
MTTFd (Mean Time To Dangerous Failure) is de verwachte betrouwbaarheid van componenten in relatie tot het optreden van een gevaarlijke fout, uitgedrukt in jaren. Het is een statistische waarde die wordt bepaald door levensduurtests of betrouwbaarheidsvoorspellingen op basis van de faalkans van de gebruikte componenten.

MTTFd heeft niets te maken met 'gegarandeerde levensduur' of 'storingsvrije periode'. Een gevaarlijke fout in een component van het veiligheidsgerelateerde gedeelte van het besturingssysteem kan ertoe leiden dat een veiligheidsfunctie niet naar behoren wordt uitgevoerd. Hierdoor is een potentieel gevaar voor het bedienend personeel niet uitgesloten. In een dergelijk geval is het bijvoorbeeld mogelijk dat de machine niet stopt als de veiligheidsinrichting wordt geopend.

MTTFd is slechts één van de factoren die de kwaliteit van de gebruikte componenten beschrijft. Componenten waarvoor uitsluitend een MTTFd of B10d waarde wordt vermeld en die voldoen aan de basisveiligheidsprincipes, kunnen in subsystemen worden gebruikt (zoals de motorschakelaar in figuur 2). De MTTFd waarde is hoger dan of gelijk aan de MTTF (Mean Time To Failure) en houdt uitsluitend rekening met fouten die zouden leiden tot een gevaarlijke storing. Als de componentenfabrikant alleen de MTTF-waarde noteert, dan moeten gebruikers ofwel zelf bepalen welk deel van de fouten in hun toepassing gevaarlijk zijn, óf ze moeten de fabrikant raadplegen. Het is ook mogelijk om zowel de MTTF-waarde als de MTTFd-waarde toe te passen. In de bijlagen C en D van de NEN-EN-ISO 13849-1 staan andere benaderingen beschreven.

Systematische fouten zijn fouten die kunnen worden teruggevoerd naar fouten die tijdens een specifieke toestand, belasting of invoeromstandigheid zijn ontstaan. Deze fouten zijn het gevolg van vergissingen die zijn gemaakt tijdens de ontwikkeling, de fabricage, de bediening of het onderhoud.

De **B_{10d} waarde** is een statistische waarde voor onderdelen die onderhevig zijn aan slijtage. De waarde geeft het gemiddeld aantal schakelingen aan waarop 10% van de onderdelen het gevaar loopt om gevaarlijk te falen. De overeenkomstige MTTFd-waarde wordt berekend uit de B10d waarde en de schakelcycli van het onderdeel (zie NEN-EN-ISO 13849-1).

NEN-EN-ISO 13849-1 beschrijft de **maatregelen die nodig zijn om fouten met een gemeenschappelijke oorzaak (CCF: common cause failures) aan te pakken**, zoals:

- Fysieke scheiding tussen de signaalpaden
- Diversiteit
- Beveiliging tegen overspanning
- Integratie van de resultaten van een FMEA (faalwijzen- en gevolgenanalyse) in het ontwikkelingsproces
- Beveiliging tegen elektromagnetische interferentie
- Beveiliging tegen alle relevante omgevingsinvloeden

In de norm wordt een puntensysteem gehanteerd om de maatregelen te evalueren.

DC (Diagnostic Coverage) is de capaciteit van het systeem om interne gevaarlijke fouten te detecteren of identificeren. De DC wordt berekend uit de verhouding tussen het aantal gedetecteerde gevaarlijke fouten gedeeld door de som van zowel de niet-gedetecteerde als wel-gedetecteerde gevaarlijke fouten.

PFHd; Probability of a Dangerous Failure per Hour; oftewel faalkans per uur. Wordt in figuur 5 weergegeven ter bepaling van de Performance level. In bijlage K van de NEN-EN-ISO 13849-1 wordt deze grafiek numeriek met behulp van de PFHd weergegeven. Berekeningsprogramma's zoals Systema werken met deze waarden. Deze waarde komt overeen met de PFHd zoals gebruikt in de NEN-EN-62061,