ORGANISATORISCHE BEHEERSMAATREGELEN VOOR HET MANAGEMENT VAN FUNCTIONELE VEILIGHEID

Functionele Veiligheid is van toepassing op de gehele levenscyclus van apparatuur, systemen en installaties – van ontwerp tot ontmanteling – en moet in de hele OEM-organisatie geborgd zijn. Bij veel fabrikanten beperkt Functionele Veiligheid zich echter alleen tot het bepalen van een veiligheidsniveau en het uitrekenen van een SIL of Performance level. In dit artikel gaan we dieper in op de organisatorische beheersmaatregelen die een organisatie moet treffen in het kader van Management Functionele Veiligheid.

>> Volgens IEC 61508 is Functionele Veiligheid: het voorkomen van onacceptabele risico's, het voorkomen van fysiek letsel en het voorkomen van gezondheidsschade bij mensen, direct of indirect, door schade aan omgeving of milieu. Functionele Veiligheid zorgt voor een veilige werking van apparatuur, installaties of systemen, doordat de veiligheidsfuncties correct werken ondanks te voorzien misbruik, omgevingsveranderingen en/of hardwarefalen.

WILLEKEURIG/SYSTEMATISCH FALEN

Functionele Veiligheid beschrijft dus de afwezigheid van een onacceptabel risico door gevaren (mogelijk een bron van letsel of schade) veroorzaakt door het slecht functioneren van het veiligheidssysteem. Het falen van het veiligheidssysteem resulteert in een onmiddellijke verhoging van het risico. Falen kan willekeurig optreden, bijvoorbeeld door veroudering of slijtage, maar ook systematisch.

We spreken van systematisch falen als de aanleiding van het falen ontstaat door een bepaalde oorzaak die alleen kan worden geëlimineerd door een wijziging van het ontwerp, van het proces van de fabrikant, van operationele procedures, van documentatie of van andere relevante factoren.

MACHINEBOUWER VERANTWOORDELIJK

Onder Management Functionele Veiligheid verstaan we de technische en organisatorische maatregelen die een machinebouwer moet implementeren om een systematisch falen van veiligheidssystemen voor of tijdens de systeeminstallatie te voorkomen en om een willekeurig hardwarefalen van veiligheidssystemen te beheersen na de installatie van het systeem.

Functionele Veiligheid zorgt ervoor dat het risico wordt teruggebracht tot een acceptabel niveau. Het risico wordt gemeten aan de hand van de waarschijnlijkheid waarin bepaalde gebeurtenissen zich voordoen, en hoe ernstig de gevolgen hiervan zijn. Functionele Veiligheid wordt bereikt door veiligheidssystemen te gebruiken. Deze systemen zijn bedoeld om fysiek letsel en gezondheidsschade bij mensen, direct of indirect, door schade aan omgeving of milieu te voorkomen. Het management van een bedrijf is altijd eindverantwoordelijk voor de Functionele Veiligheid bij de machines die worden geproduceerd.

BEHEERSING VAN SYSTEEMFALEN

Vanuit de IEC 61508 zijn organisatorische beheersmaatregelen vastgelegd. Functionele Veiligheid is immers niet alleen van toepassing op de gehele levenscyclus van de systemen, maar ook op de gehele organisatie. Vanuit dit Management Functionele Veiligheid zijn het specificeren van het beleid en de strategie voor het bereiken van Functionele Veiligheid van levensbelang.

Bij de start van een project moet een 'veiligheidseisenspecificatie' worden gemaakt. Op deze eisen worden namelijk alle volgende activiteiten in het ontwerp- en realisatieproces gebaseerd. Tijdens het ontwerpproces moet elke stap worden geverifieerd aan de hand van deze 'veiligheidseisenspecificatie'. Bij de realisatiefase moet door validatie gekeken worden of de applicatie doet wat beoogd is. Het resultaat van de verificatie en validatie wordt vervolgens gebruikt om aan te tonen dat de beoogde risicoreductie wordt bereikt met de gekozen veiligheidssystemen. In het beleid en de strategie voor het bereiken van Functionele Veiligheid moeten verificatie en validatie dus een prominente plaats innemen.

VOORAF TE REGELEN

Verificatie- en validatieschema's, beoordelingscriteria, inspectie- en testmethodes, meetnauwkeurigheid, hoe om te gaan met wijzigingen/aanpassingen... al deze onderdelen moeten vooraf zijn vastgelegd. Daarnaast wordt verwacht dat alle personen met verantwoordelijkheden de passende competentie hebben. Hun competentie moet binnen de organisatie zijn gedocumenteerd en regelmatig up-to-date worden gehouden.

Tijdens de bouw van een machine of systeem, maar vooral in de ontwerpfase verlangt Management Functionele Veiligheid minimaal een aantal specifieke maatregelen ter voorkoming van systematisch falen van veiligheidssystemen. Naast inachtneming van de richtlijnen en normen, en een gedegen projectmanagement zijn dat volgens IEC61508:

- **Documentatie**
  De operationele capaciteit en veiligheid, en de zorg tijdens de ontwikkeling door alle betrokken partijen, moet worden aangetoond tijdens de beoordeling. Om de zorg tijdens de ontwikkeling aan te tonen en op ieder moment het bewijs van veiligheid te kunnen garanderen en verifiëren, wordt er veel waarde gehecht aan deze documentatie.

- **Gestructureerd ontwerpen**
  Gestructureerd ontwerpen draagt bij aan een lagere complexiteit. Door het creëren van een hiërarchische structuur van deelvereisten worden verbindingsfouten tussen de vereisten vermeden en wordt de verificatie vereenvoudigd. Bij het ontwerpen van de hardware moet gestructureerd worden ontworpen met gebruik van specifieke criteria of methodes. Zo kan bijvoorbeeld het volgende vereist zijn:
  - een hiërarchisch gestructureerd circuitontwerp;
  - het gebruik van geproduceerde en geteste circuitcomponenten.

  Op eenzelfde wijze kunnen – bij het ontwerp van software – structuurschema's zorgen voor een eenduidige structuur van de softwaremodules die moeten worden gemaakt. De structuur laat zien hoe de modules met elkaar verband houden, welke precieze gegevens tussen de modules moet worden uitgewisseld, en welke precieze controle-elementen tussen de modules bestaan.

- **Modularisatie**
  Om de complexiteit en het voorkomen van falen voortkomend uit de verbinding tussen subsystemen te verminderen, is het gebruik van modularisatie aan te raden. Alle subsystemen, op alle niveaus van het ontwerp, zijn duidelijk gedefinieerd en beperkt in grootte. De verbindingen tussen subsystemen moeten zo simpel mogelijk en de dwarsdoorsnede (lees: de gedeelde gegevensuitwisseling van informatie) moet zo klein mogelijk worden gehouden. De complexiteit van individuele subsystemen moet beperkt blijven.

Ook het gebruik van beproefde componenten – *well tried components* volgens bijvoorbeeld EN 13849-2 – checklists, CAD-tools, simulatie en peer-reviews worden afhankelijk van het veiligheidsniveau in meer of mindere mate aangeraden tijdens de ontwerpfase.

'MOEDERNORM' VOOR ALLE INDUSTRIEËN

De IEC 61508 wordt beschouwd als de 'moedernorm' voor Functionele Veiligheid. Deze norm beschrijft de algehele veiligheid van apparatuur, machines of installaties en hun besturingssystemen, waarbij deze veiligheid afhangt van een correcte werking van elektrische, elektronische, programmeerbare elektronische (E / E / PE) veiligheidssystemen en andere maatregelen voor risicovermindering.

De norm behandelt onder andere functionaliteit, structuur, willekeurig hardwarefalen, diagnose, foutbeheersing en procedures tegen systematisch falen gedurende de gehele veiligheidslevenscyclus. Daaronder het verifiëren en valideren alsmede het uitvoerig documenteren van alle stappen.

Van deze 'moedernorm' is een aantal branchespecifieke normen afgeleid die de industrie een gestructureerde manier van werken bieden. Automotive ISO 26262, Agriculture ISO25119-x, Procesindustrie IEC 61511-x en Machinebouw IEC 62061 of ISO 13849-x zijn bekende voorbeelden.

Deze afgeleide normen, bijvoorbeeld Performance level (ISO 13849-1) en/of SIL (IEC 62061) in de machinebouw, zijn eigenlijk een soort uittreksels van de IEC 61508. Hierdoor zijn ze erg goed werkbaar. Wel worden veel zaken summier aangegeven met daarbij de vermelding dat in de IEC 61508 meer informatie over dit onderwerp te vinden is.

SICK
Sensor Intelligence.

DE PIJLERS VAN MANAGEMENT FUNCTIONELE VEILIGHEID

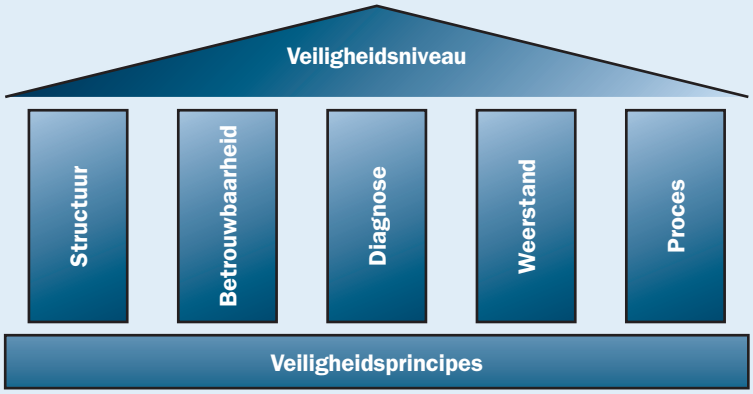
STRUCTUUR
Afhankelijk van het veiligheidsniveau kan voor een bepaalde structuur worden gekozen, waarbij eventueel spontane fouten van hardwarecomponenten op een willekeurig tijdstip worden gedetecteerd. Het toepassen van de basisveiligheidsprincipes (EN 13849-2) – zoals het voorkomen van onverwachts opstarten, spanningsloos schakelen en/of overspanningsbeveiliging – maar ook eventueel beproefde veiligheidsprincipes (well tried safety principles, EN 13849-2) en/of beproefde componenten (well tried components, EN13849-2) zijn daarbij onontbeerlijk.

BETROUWBAARHEID
De betrouwbaarheid van de verschillende onderdelen wordt uitgedrukt in een gemiddelde kans op een gevaarlijke fout. Deze betrouwbaarheid kan worden berekend of gespecificeerd door een componentenleverancier. Mean time to dangerous failure (MTTFd) en Probability of dangerous failure per hour (PFHd) zijn de hiervoor gehanteerde waarden.

DIAGNOSE
Er zijn verschillende maatregelen om een spontane fout van een hardwarecomponent op een willekeurig tijdstip te ontdekken. Relaisterugkoppeling (EDM), gelijktijdigheidsbewaking, ‘gedwongen’ contacten en/of tijdsbewaking in het proces zijn enkele maatregelen die vaak worden toegepast. Ook combinaties zijn mogelijk.

WEERSTAND
Maatregelen ter voorkoming van falen door een of meerdere gebeurtenissen die samenvallende fouten veroorzaken in een redundant systeem, hebben vaak te maken met EMC of omgevingsomstandigheden. Diversiteit, goede ‘beproefde’ componenten en veiligheidsprincipes, alsook ook opleiding en training van de ontwerper en het in acht nemen van een handleiding en de daarin vermelde omgevingsparameters zorgen voor veiligere systemen.

PROCES
Systematisch falen van systemen kan worden voorkomen door een goede specificatie van de verschillende (veiligheids)eisen, door een optimale organisatie met de juiste competentie, door heldere regels rond het ontwerp (bijv. richtlijnen voor codering, modularisatie), door een verificatie- en validatieplan inclusief testcriteria en natuurlijk door een duidelijk documentatie- en configuratiemanagement.



Het veiligheidsniveau van een systeem is afhankelijk van iedere veiligheidsgerelateerde parameter

BEHEERSING VAN WILLEKEURIG FALEN
Management Functionele Veiligheid betreft echter niet alleen de technische en organisatorische maatregelen die een machinebouwer moet implementeren om systematisch falen van veiligheidssystemen voor of tijdens de systeeminstallatie te voorkomen. Het omvat ook het beheersen van willekeurig hardwarefalen van veiligheidssystemen ná de installatie van het systeem.

Het beheersen van willekeurig hardwarefalen van veiligheidssystemen na de installatie van het systeem heeft alles te maken met de structuur, waarmee het systeem is opgebouwd en de daarbij behorende detectiemogelijkheid (diagnose) van fouten en/of falen. Natuurlijk speelt ook de betrouwbaarheid van de componenten zelf een rol en de zogenoemde *common cause*-faalbeheersing (falen door een of meerdere gebeurtenissen die samenvallende fouten veroorzaken in een redundant systeem wat verlies van de veiligheidsfunctie tot gevolg heeft).

DISCUSSIES VOORKOMEN
Voor het bepalen van een veiligheidsniveau van een systeem, zoals SIL (IEC 61508), SILcl IEC 62061 en/of PL ISO 13849-1, zijn alle parameters even belangrijk. Het berekenen van alleen een PFHd-waarde is zeker niet voldoende. Goede kennis en implementatie van Management Functionele Veiligheid binnen het bedrijf draagt zeker bij aan veiligere machines en voorkomt oneindige discussies met de klant over het al dan niet veilig zijn van de machine.

SICK
Sensor Intelligence.

SICK B.V. · Leijenseweg 111 · Postbus 186 · 3720 AD Bilthoven · Tel. 030 - 204 40 00 · Fax 030 - 229 39 94 · E-mail info@sick.nl · www.sick.nl