



SIL en PL in de machinebouw

Een geactualiseerde kijk op functionele veiligheid

Gerald van Engeland

EN-IEC 62061
EN-ISO 13849-1

 **kader**
framework for positive change

SIL EN PL IN DE MACHINEBOUW

Een geactualiseerde kijk op functionele veiligheid

Gerald van Engeland

VOORWOORD

Vijf jaar na mijn eerste boek over functionele veiligheid is de tijd rijp voor een nieuw boek. Natuurlijk is er genoeg te melden, want er zijn vernieuwde normen en de machineverordening neemt de plaats van de machinerichtlijn in. D&F consulting is opgenomen in de Kader-groep en we zijn als technisch consultants nu het team Kader Technical Safety. Het werk wat we doen is niet veranderd. SIL en PL blijft een uitdaging voor machinebouwers en machinegebruikers.

De risicobeoordeling verdient aandacht

Iedereen weet wel dat een risicobeoordeling verplicht en belangrijk is. Machinebouwers blijven hier echter structureel te weinig aandacht aan geven. Vaak bouwen ze jarenlang soortgelijke machines en borduren voort op iets dat in het verleden is opgesteld. Innovaties worden uiteraard wel steeds toegevoegd. Men vergeet, dat je een risicobeoordeling niet doet omdat het verplicht is, maar ook omdat je er een betere (veiligere) machine mee bouwt. Met name als je aandacht besteedt aan de taken die bij of aan de machine moeten worden uitgevoerd. Als de machine ‘als een zonnetje’ productie draait, gebeuren er meestal geen ongelukken. Denk dus ook (of vooral) aan onderhoud, afstellen, storing zoeken en schoonmaken.

Iedereen is verantwoordelijk

Bij veel machinebouwers ligt ‘het stukje machineveiligheid’ bij één of enkele personen. Vaak is dat de elektro hardware engineer, want die weet al hoe de noodstopknop moet worden aangesloten. Machineveiligheid is echter ook onderdeel van bijvoorbeeld het vak van de mechanisch ontwerper. Je kan niet zomaar een of andere bottenbreker ontwerpen en dan maar aannemen dat iemand van besturing er wel een lichtschermbewaking voor zet. En als een gevaarlijke bewerking sowieso achter een lichtschermbewaking moet de ontwerper er nog steeds voor zorgen dat de beweging snel kan stoppen en dat er voorzieningen zijn om veilig af te kunnen stellen en te reinigen. Machineveiligheid kun je dus niet zien als een losse expertise. Het maakt deel uit van de kennis van iedereen die betrokken is bij de ontwikkeling van een machine, van salesmedewerker tot inbedrijfsteller.

Formele werkwijze. Wat moet ik maken?

In het verlengde van het vakmanschap hoort ook een goede werkwijze. Vaak wordt tegen de software-engineer gezegd: ‘doe maar een programmaatje’. Volg je de normen van functionele veiligheid, dan moet er eerst een specificatie worden uitgewerkt waarin staat wat de veiligheidsfuncties zijn en met welke hardware deze gerealiseerd worden. Op basis daarvan wordt het software ontwerp gemaakt. Na een review van dat ontwerp kan

Colofon:

Auteur

Gerald van Engeland

Uitgever

Kader Consultancy & Interim B.V.

Eindredactie

Martje van der Heijden, Woord en Beeld

Ontwerp en vormgeving

Wendy Bour, Ipskamp Printing
Marijke Horstink, Kader Group B.V.

Drukwerk

Ipskamp Printing Enschede

ISBN/EAN

978-94-6473-572-7

een goede programmeur dan een leesbaar begrijpelijk en toetsbaar programma maken. Na code review van dat programma kun je je hand in het vuur steken voor de correcte werking. Natuurlijk gaan we ook testen, maar dat is aanvullend. Iedereen die complexe machines automatiseert snapt dit meteen, maar in het 'PLC-wereldje' heerst nog het idee dat we eerst pizza bestellen en dan vanavond dat programma wel even werkend maken.

Controle vraag 1: Vind je het normaal dat er bij het testen van veiligheidsgerelateerde software nog fouten gevonden worden?

Controle vraag 2: Vind je het normaal dat iemand een e-mail stuurt naar een programmeur met een verzoek om de werking van het lichtscherm aan te passen?

Kun je een van deze vragen met 'ja' beantwoorden, dan is er nog werk aan de winkel! Lees vooral verder....

Interpretatie en inspiratie

In dit boek probeer ik diverse normen op een praktische en leesbare manier uit te leggen. Hier en daar zal ongetwijfeld mijn eigen interpretatie te herkennen zijn. Het is altijd raadzaam om de desbetreffende norm erbij te pakken, zeker als de grenzen worden opgezocht. De tabellen in dit boek zijn sowieso slechts een deel van de tabellen in de norm. De voorbeelden in dit boek zijn niet bedoeld als 'als-we-dit-invullen-is-het-klaar'-checklist, maar meer als inspiratie voor het opzetten van een eigen werkwijze met een bij het project passende complexiteit of eenvoud.

Met dank aan

Natuurlijk had ik dit boek niet kunnen schrijven zonder de hulp van mijn collega's. Joris, Dennis, Jorn, Sander, Jaap, Marijke, Jean-Jacques: dank voor het controleren, aanmoedigen, sparren, regelen, checken, terugfluiten, opmaken en narekenen!

Gerald van Engeland.

SECTIES

Het boek is in vijf secties opgedeeld zodat losse onderwerpen ook goed vindbaar zijn. Het is zeker mogelijk om een sectie over te slaan.

A	Introductie vanuit de Machinerichtlijn, Machineverordening en normen.
B	De SIL- en PL-faalkansberekeningen stap voor stap uitgelegd.
C	Het belang van kwaliteit en vakmanschap.
D	Een projectaanpak die kan leiden tot foutloze en juiste veiligheidsfuncties.
E	Belangrijke aspecten, van noodstop en reset tot overbrugging en lichtschermen.

INHOUDSOPGAVE

SECTIE A Introductie vanuit de Machinerichtlijn, Machineverordening en normen

1 INLEIDING VANUIT WET- EN REGELGEVING	17
1.1 Machines moeten veilig zijn	17
1.2 Machinerichtlijn en Machineverordening	18
1.3 Essentiële veiligheids- en gezondheidseisen	19
1.4 Normen	20
1.5 Essentiële eisen aan het besturingssysteem	22
1.6 SIL en PL	23
1.7 CE-markering	23
2 RISICOBEOORDELING	27
2.1 Grenzen van de machine vastleggen	28
2.2 Identificatie van gevaren	29
2.3 Inschatten van risico's	32
2.4 Reduceren van risico's	35
2.5 In de praktijk	37
2.6 Functionele veiligheid	39
3 SIL EN PL	41
3.1 Integriteit of performance van veiligheidsfuncties	41
3.2 Benodigd PL-level	41
3.3 Benodigd SIL-level	45

SECTIE B De SIL- en PL-faalkansberekeningen stap voor stap uitgelegd

4 DE THEORIE ACHTER FAALKANSEN	51
4.1 Toevallig of systematisch?	51
4.2 Lage faalkansen (PFH of PFH_D)	51
4.3 Veilig of gevaarlijk? (RDF)	53
4.4 Failure rate (λ , FIT)	54
4.5 Mean time to Failure (MTTF)	55
4.6 Slijtagegevoelige componenten (B_{10} , n_{op} en C)	56
4.7 De gevaarlijke fractie (D)	57
4.8 Constante faalkansen en levensduur	59

5 DE THEORIE ACHTER ARCHITECTUUR EN DIAGNOSE	63
5.1 Enkelvoudig of redundant	63
5.2 Diagnose	65
5.3 SFF	67
6 VEILIGHEIDSFUNCTIES OPSTELLEN EN ONTWERPEN	71
6.2 Kanalen en blokken/elementen	71
7 DEVICE TYPES	73
8 PL BEREKENINGEN	81
8.1 Architectuur, categorie	81
8.2 Het bepalen van PFH	85
8.3 Rekenvoorbeelden	87
9 SIL-BEREKENINGEN	97
9.1 Architectuur en max SIL	97
9.2 Berekenen van de PFH	98
10 SIL- EN PL-VOORBEELD	109
11 REKENEN MET TOOLS	117
SECTIE C Het belang van kwaliteit en vakmanschap	
12 KWALITATIEVE ASPECTEN	123
12.1 Voorkomen van systematische fouten	123
12.2 Beheersen van systematische fouten	124
12.3 Lees de gebruiksaanwijzing!	124
12.4 Veiligheidsprincipes	126
12.5 Well-tried components	130
13 FOUTUITSLUITING	135
14 TESTPULSEN	137
SECTIE D Een projectaanpak die kan leiden tot foutloze en juiste veiligheidsfuncties	
15 SYSTEMATISCHE WERKWIJZE	143
15.1 Iedereen mag fouten maken	143
15.2 V-model voor functionele veiligheid	145
15.3 Software V-model	151
15.4 Onafhankelijkheid	157

15.5 SRS	158
15.6 HDS	159
15.7 SDS	162
16 GECOMBINEERDE WORKFLOW	167
16.1 Eisen	171
16.2 Ontwerp	175
16.3 Realisatie	193
16.4 Testen	207
16.5 Validatie	209
16.6 En nu jullie!	211
17 LEG HET VAST	213
17.1 V-model en traceerbaarheid	213
17.2 Configuratie management	215
17.3 Wijzigingsprotocol	215
17.4 Functional Safety Plan	216
18 DE GEBRUIKSAANWIJZING	219
SECTIE E Belangrijke aspecten, van noodstop en reset tot overbrugging en lichtschermen	
19 FUNCTIEBLOKKERENDE AFSCHERMINGEN	225
19.1 Definities	225
19.2 Vier typen functieblokkerende afschermingen	228
19.3 Vergrendeling	232
20 SERIESCHAKELING EN MASKEREN VAN FOUTEN	235
21 LICHTSCHERMEN EN VEILIGHEIDSAFSTANDEN	239
21.1 Definities	240
21.2 Berekenen van de veiligheidsafstand	241
21.3 Veiligheidsafstand voor andere componenten	246
22 HET GEBRUIK VAN COMPONENTEN SPECIFIEK VOOR DE PROCESINDUSTRIE	247
22.1 Conclusie	251
23 STARTEN EN STOPPEN VAN MACHINES	253
23.1 Starten	253
23.2 Stoppen	253
23.3 Noodstop	254
23.4 Veiligheidsfuncties in drives	258

24 WERKEN AAN UITGESCHAKELDE MACHINES	261
25 RESET EN OPERATOR LOCK OUT	263
25.1 De resetfunctie als veiligheidsfunctie	264
25.2 Operator Lock-out	266
26 MANIPULATIE	269
27 OVERBRUGGEN VAN VEILIGHEIDSVORZIENINGEN	273
28 VEILIGHEIDSFUNCTIES IN BESTAANDE MACHINES	275
28.1 Richtlijn Arbeidsmiddelen	275
29 INDEX	279

SIL en PL in de machinebouw

Een geactualiseerde kijk op functionele veiligheid

Vijf jaar na mijn eerste boek is het tijd voor een geactualiseerde kijk op functionele veiligheid. De normen zijn vernieuwd en we bereiden ons voor op de overgang van de huidige Machinerichtlijn naar de Machineverordening. Voldoende tijd nemen voor het ontwerptraject van een machine is van groot belang, maar in de praktijk ontbreekt het daar vaak aan. Veel bedrijven worstelen met verificatie en validatie van het besturingssysteem, wat zonder gedegen kennis van SIL of PL nog steeds niet mogelijk is.

In dit boek vind je een praktische benadering van functionele veiligheid.. Door de duidelijke verdeling in vijf secties is dit boek gemakkelijk leesbaar; niet alleen voor hardware engineers, mechanisch ontwerpers, software engineers en inbedrijfstellers maar ook voor managers en de sales afdeling. Veiligheid is namelijk een belangrijk onderdeel van het vakmanschap van iedereen in de keten.

A	Introductie vanuit de Machinerichtlijn, Machineverordening en normen.
B	De SIL- en PL-faalkansberekeningen stap voor stap uitgelegd.
C	Het belang van kwaliteit en vakmanschap.
D	Een projectaanpak die kan leiden tot foutloze en juiste veiligheidsfuncties.
E	Belangrijke aspecten, van noodstop en reset tot overbrugging en lichtschermen.



De auteur:

Gerald van Engeland is sinds 2010 senior consultant en trainer bij Kader Technical Safety (voorheen D&F consulting). Met 35 jaar ervaring in de machinebouw, waarvan 20 jaar machineveiligheid, en het geven van vele uren training heeft hij de kennis en ervaring opgebouwd die nodig is om lastige onderwerpen op een gemakkelijke en praktische manier uit te leggen.

