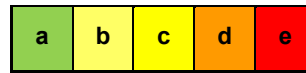




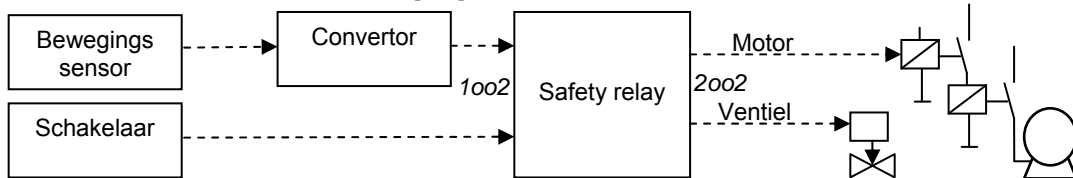
## Overzicht PL verificatie volgens ISO 13849-1

### 1. Neem de risiobeoordeling door.

Weet wat het gevaar, het risico en vereiste  $PL_r$  is



### 2. Maak een blokschema van de beveiliging.



Toon alle relevante onderdelen.

### 3. Bepaal of de beveiliging functioneel juist is (dus de gevaarlijke situatie voorkomt).

- De beveiliging is snel genoeg.
- De sensoren nemen de potentieel gevaarlijke situatie/handeling waar.
- De juiste actuators worden aangestuurd.
- De beveiliging is voldoende 'hufferproof' (niet overbrugbaar).

### 4. Bepaal $MTTF_d$ (Mean Time To dangerous Failure) van ieder component.

$MTTF_d \geq 3$ jaar	Low
$MTTF_d \geq 10$ jaar	Medium
$MTTF_d \geq 30$ jaar	High

Soms is een  $B_{10D}$  waarde opgegeven (aantal schakelingen waarbij 10% gevaarlijk faalt). Deze omrekenen naar  $MTTF_d$  met de formule  $MTTF_d = B_{10D} / (0,1 \cdot n_{op})$ .  
 $n_{op} = (\text{operatie-dagen/jaar} \cdot \text{operatie-uren/dag} \cdot 3600) / \text{cyclustijd in seconden}$ .

### 5. Bepaal de DC (Diagnostic Coverage) van ieder component / deelsysteem

$DC < 60\%$	Geen DC
$60\% \leq DC < 90\%$	Low
$90\% \leq DC < 99\%$	Medium
$DC \geq 99\%$	High

$DC = \text{Diagnostic Coverage}$ . Faalfrequentie gevaarlijke fouten  
 $\lambda_D = 1 / (MTTF_d \cdot 24 \cdot 365) h^{-1}$ .  
 $\lambda_{DD}$  is de frequentie van de gedetecteerde gevaarlijke fouten.  $\lambda_{DD} = DC \cdot \lambda_D$ .  
 $\lambda_{DU}$  is de frequentie van de ongedetecteerde gevaarlijke fouten.  $\lambda_{DU} = (1 - DC) \cdot \lambda_D$   
 Wanneer een gevaarlijke fout is gedetecteerd door diagnostiek, moet er een automatische beveiligingsactie optreden.

### 6. Bepaal de categorie van ieder deelsysteem (SRP/CS – sensor / logic solver / actuators).

**Cat. B** Enkel, geen DC, Low/Med  $MTTF_d$ , basic safety principle (bv. fail safe).

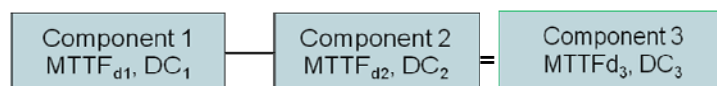
**Cat. 1** Enkel, geen DC, High  $MTTF_d$ , basic safety principle + 'well tried', 'widely used'.

**Cat. 2** Enkel, Low/Med DC, basic safety principle + 'well tried', 'widely used',  
 Testrate van test equipment  $\geq 100x$  Demand rate van Safety Function.

**Cat. 3** Redundant, Low/Med DC, 'well tried', score  $CCF \geq 65$  (zie achterzijde van dit blad).

**Cat. 4** Redundant, High DC, High  $MTTF_d$ , (elk kanaal) 'well tried', score  $CCF \geq 65$  (achterzijde).

Omrekenformules:



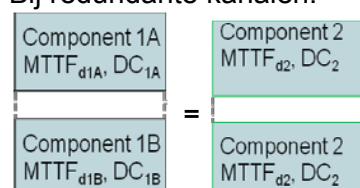
$$\lambda_{du3} = \lambda_{du1} + \lambda_{du2}$$

Als we uitgaan van:  $\lambda_{d3} = \lambda_{d1} + \lambda_{d2}$

Ofwel:  $1/MTTF_{d3} = 1/MTTF_{d1} + 1/MTTF_{d2}$

Dan is:  $DC_3 = (DC_1 \cdot \lambda_{d1} + DC_2 \cdot \lambda_{d2}) / \lambda_{d3}$

Bij redundante kanalen:



$$MTTF_{d2} = \left\{ \frac{2/3 \cdot MTTF_{d1A} + MTTF_{d1B} - \frac{MTTF_{d1A} \cdot MTTF_{d1B}}{MTTF_{d1A} + MTTF_{d1B}}}{1} \right\}$$

Kies voor  $DC_2$  de laagste  $DC_{1A}$  of  $DC_{1B}$ . Optie:  $DC_2$  berekenen.



No.	Cat. 3 en Cat. 4: Bepaal of de CCF (Common Cause Failure) score $\geq 65$ is.	Score max
1	Separation/ Segregation Physical separation between signal paths: separation in wiring/piping, sufficient clearances and creep age distances on printed-circuit boards.	15
2	Diversity Different technologies/design or physical principles are used, for example: first channel programmable electronic and second channel hardwired, kind of initiation, pressure and temperature, Measuring of distance and pressure, digital and analog. Components of different manufactures.	20
3.1	Design/application/experience Protection against overvoltage, overpressure, overcurrent,	15
3.2	Design/application/experience Components used are well-tried.	5
4	Assessment/analysis Are the results of a failure mode and effect analysis taken into account to avoid common-cause-failures in design?	5
5	Competence/training Have designers/ maintainers been trained to understand the causes and consequences of common cause failures?	5
6.1	Environmental Prevention of contamination and electromagnetic compatibility (EMC) against CCF in accordance with appropriate standards. Fluidic systems: filtration of the pressure medium, prevention of dirt intake, drainage of compressed air, e.g. in compliance with the component manufacturers' requirements concerning purity of the pressure medium. Electric systems: Has the system been checked for electromagnetic immunity, e.g. as specified in relevant standards against CCF? For combined fluidic and electric systems, both aspects should be considered.	25
6.2	Environmental Other influences Have the requirements for immunity to all relevant environmental influences such as, temperature, shock, vibration, humidity (e.g. as specified in relevant standards) been considered?	10
<b>Totale score</b>		<b>100</b>

**7. Bepaal de PL van ieder deelsysteem (SRP/CS- sensor, logic solver, actuators).**

	Cat.B	Cat. 1	Cat. 2	Cat. 2	Cat. 3	Cat. 3	Cat.4
$DC_{avg}$	-	-	low	med	low	med	high
$MTTF_d=Low$	a	-	a	b	b	c	-
$MTTF_d=Med$	b	-	b	c	c	d	-
$MTTF_d=High$	-	c	c	d	d	d	e

**8. Bepaal de PL van de beveiliging (Safety Function) en controleer dat deze  $\geq PL_r$  is.**  
Bepaal de laagst voorkomende PL van een SRP/CS en hoeveel SRP/CS deze PL hebben.

$PL_{low}$	$N_{low}$	$PL_{SF}$
a	$>3$	-
	$\leq 3$	a
b	$>2$	a
	$\leq 2$	b
c	$>2$	b
	$\leq 2$	c
d	$>3$	c
	$\leq 3$	d
e	$>3$	d
	$\leq 3$	e

**9. Documenteer de relevante informatie**

Bv. ontwerptekeningen, specificaties, logics, testmethodiek.

**10. Verificaties en (uiteindelijk) validatie**

Verificaties: Is de applicatie software juist? Is het ontwerp gecontroleerd? PL verificatie.

Validatie: Testen van het daadwerkelijke functioneren.