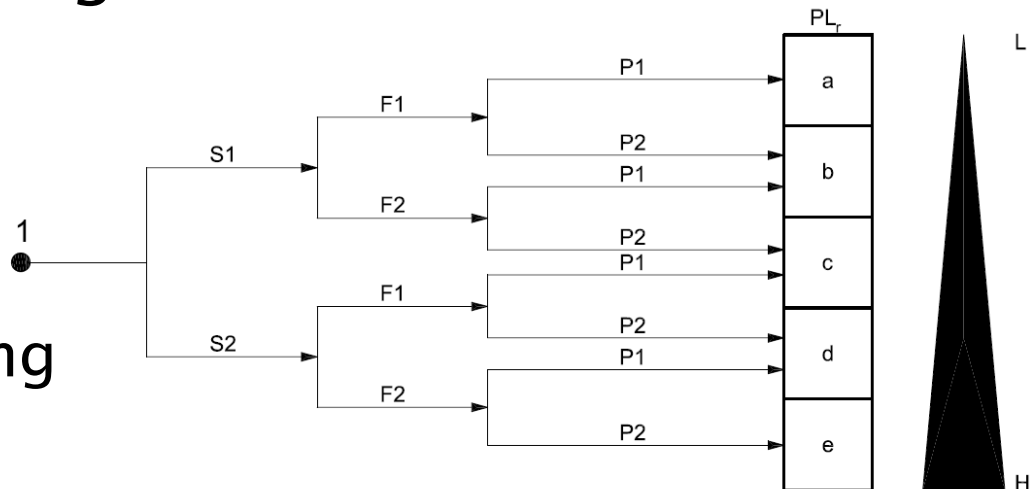


EN13849

1. Risicobeoordeling

- Effect
(severity)
- Blootstelling
(frequentie)
- Gevaarafwending
(avoiding hazard)



2. PL-required

Key

- 1 starting point for evaluation of safety function's contribution to risk reduction
- L low contribution to risk reduction
- H high contribution to risk reduction
- PL_r required performance level

Risk parameters:

- S severity of injury
- S1 slight (normally reversible injury)
- S2 serious (normally irreversible injury or death)
- F frequency and/or exposure to hazard
- F1 seldom-to-less-often and/or exposure time is short
- F2 frequent-to-continuous and/or exposure time is long
- P possibility of avoiding hazard or limiting harm
- P1 possible under specific conditions
- P2 scarcely possible

Figure A.1 — Risk graph for determining required PL_r for safety function

EN13849

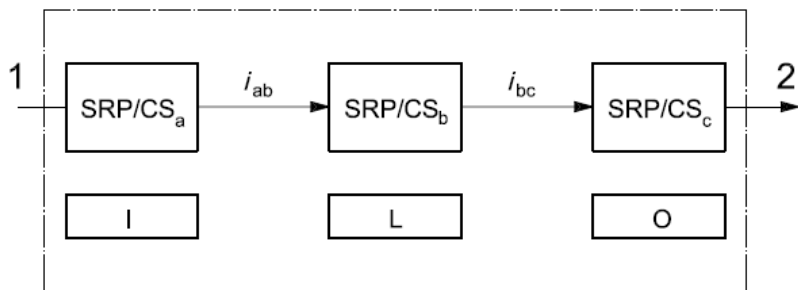
Hoe zeker wilt u ervan zijn dat een bepaalde gevaarlijke fout niet voorkomt?

PL	Average probability of dangerous failure per hour 1/h
a	$\geq 10^{-5}$ to $< 10^{-4}$
b	$\geq 3 \times 10^{-6}$ to $< 10^{-5}$
c	$\geq 10^{-6}$ to $< 3 \times 10^{-6}$
d	$\geq 10^{-7}$ to $< 10^{-6}$
e	$\geq 10^{-8}$ to $< 10^{-7}$

NOTE Besides the average probability of dangerous failure per hour other measures are also necessary to achieve the PL.

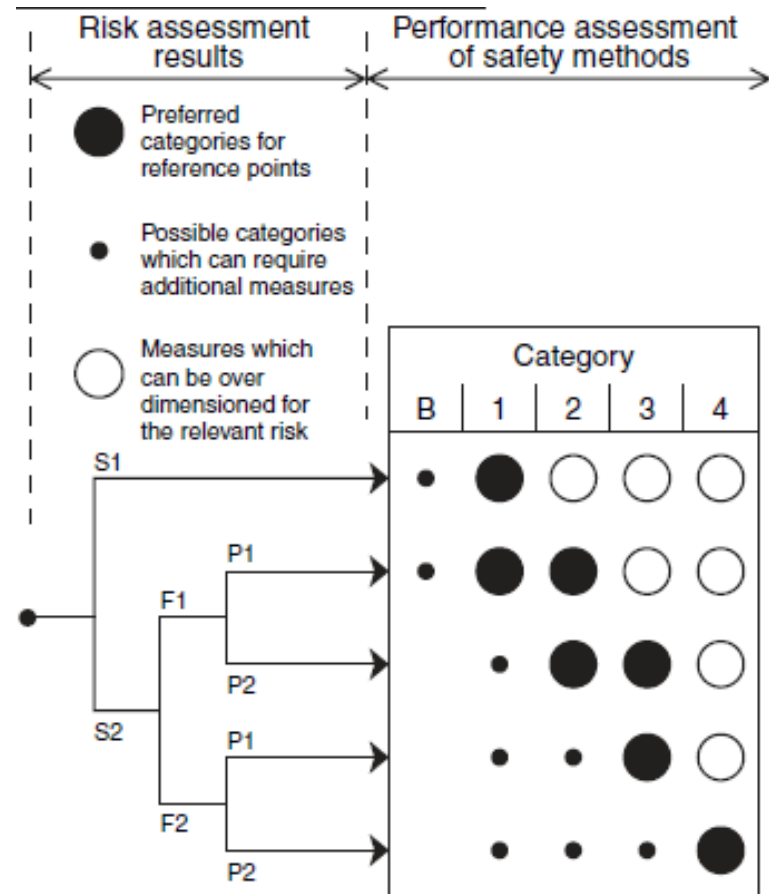
EN13849

Categorie volgens EN954-1:1996



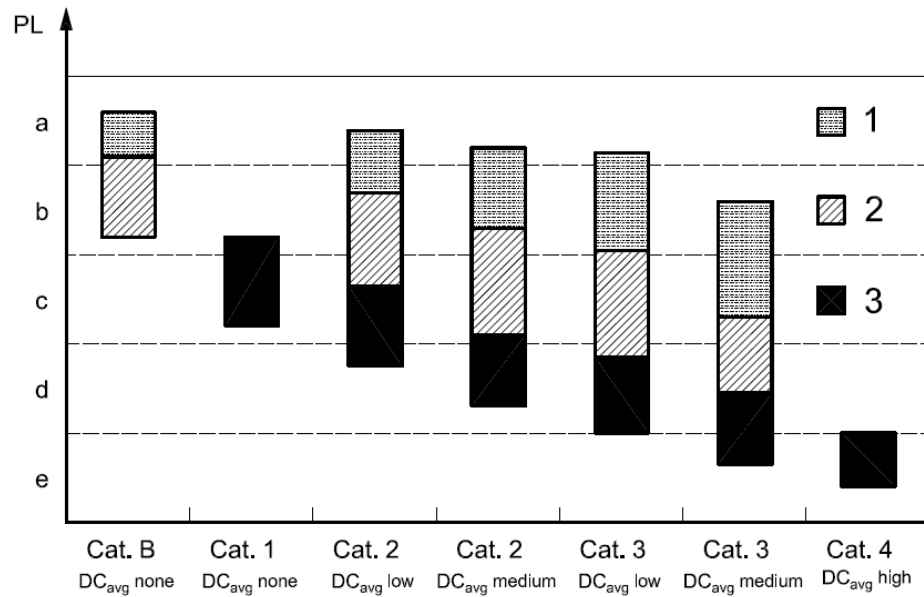
Key

- I input
- L logic
- O output
- 1 initiation event (e.g. manual actuation of a push button, opening of guard, interruption of beam of AOPD)
- 2 machine actuator (e.g. motor brakes)



EN13849

Van Categorie naar PL



Key

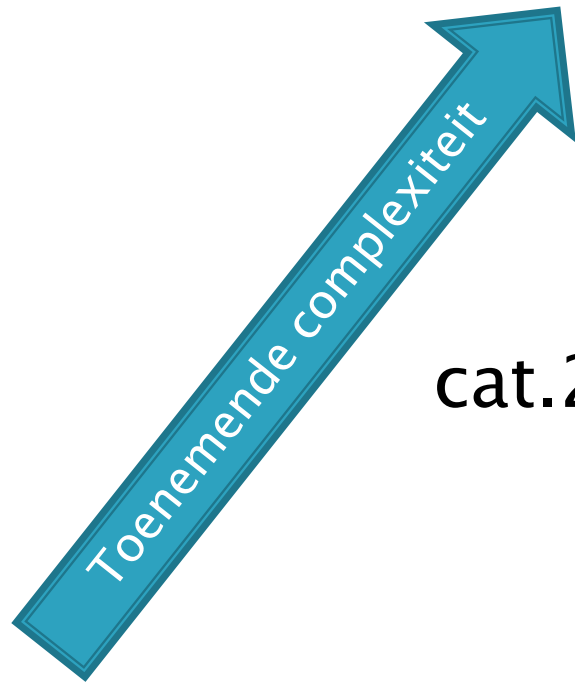
PL performance level

1 MTTF_d of each channel = low

2 MTTF_d of each channel = medium

3 MTTF_d of each channel = high

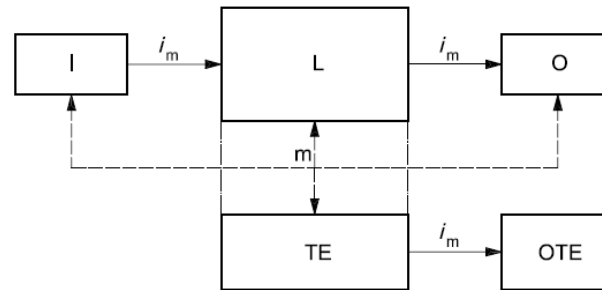
EN13849



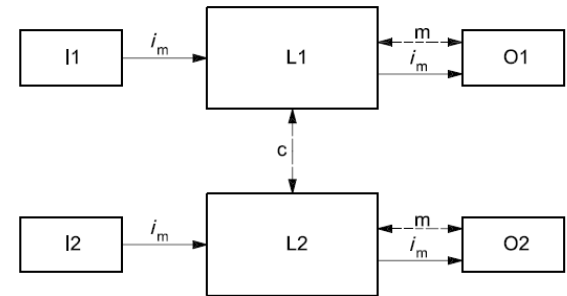
cat.b / cat.1



cat.2



cat.3 / cat.4



EN13849

DC (diagnostic coverage)

- ▶ Hoeveel procent van alle gevaarlijke fouten wordt gedetecteerd?
- ▶ Maat voor de kwaliteit van de terugkoppeling
- ▶ Vanaf category 2 en hoger

DC	
Denotation	Range
None	$DC < 60 \%$
Low	$60 \% \leq DC < 90 \%$
Medium	$90 \% \leq DC < 99 \%$
High	$99 \% \leq DC$

EN13849

CCF (common cause failure)

- ▶ 1 fout die beide kanalen laat falen
- ▶ Vanaf category 2 en hoger
- ▶ Checklist (punten verzamelen)
 1. Scheiding (bedrading, printsporen)
 2. Diversiteit (verschillende principes; bijv. druk en afstand, digitaal en analoog)
 3. Defensief ontwerp; bijv.: beveiligd te hoge stroom, etc.) en well-tried components
 4. De gevolgen van alle faalmodi zijn in het ontwerp meegenomen ter voorkoming fouten in het ontwerp
 5. Ontwerpers getraind om de gevolgen van CCF te overzien?
 6. Omgeving (EMC, temperatuur, schokken, trillingen, luchtvochtigheid).

EN13849

Probability of dangerous failure (PFHd)

- ▶ $PFHd = PFHd_{input} + PFHd_{logic} + PFHd_{output}$;
tools:
 - Sistema (BGUV; PL)
 - Safety Evaluation Tool (SET; Siemens; PL en SIL)
- ▶ Waarde voor PFHd is niet altijd beschikbaar, maar wel te bepalen uit een karakteristieke waarde, zoals:
 - ▶ MTTFd (mean time between dangerous failure – gemiddelde tijd tussen gevaarlijk falen)
 - ▶ B10d (aantal maal aanspreken van een component waarbij 10% van de populatie aan componenten gevaarlijk is gefaald)