PS4.3(new) prEN ISO 13849-1:2003 rev. (EN 954-1rev.)

Design of safety-related parts of control systems (SRP/CS)

Scope and Safety Functions (SF) (1)

From Risk Assessment

ISO 12100 § (EN 292) § ISO 14121 (EN 1050)

Scope:

- Part of Overall Risk Assessment
- Safety-Related Parts of Control Systems
- Regardless of Technology
- Based on Safety Functions

Examples for **safety functions (SF):**

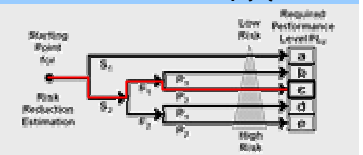
- Stop Function STOP
- Safe Standstill ∞
- Safely Reduced Speed 10
- Safely Reduced Step

SF_1 SF_2 ∞ SF_n

To next step

Required Performance Level PL_r (2)

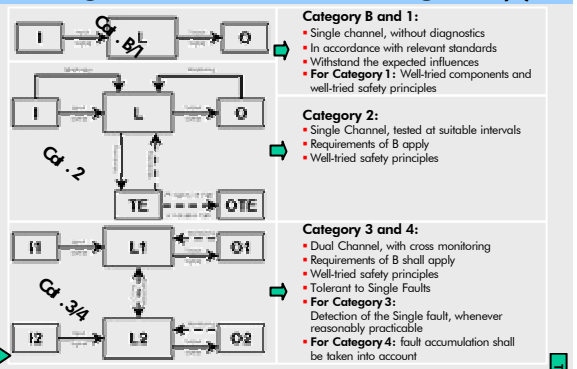
- Estimation of risk reduction for each SF
- Qualitative and empirical method based on experience
- Aid for designer
- Gradation of risk from low (PL_r = a) to high (PL_r = e).



PL_{r1} PL_{r2} ∞ PL_{rn}

To next step

Designated Architectures & Categories (3)



Category B and 1:
- Single channel, without diagnostics
- In accordance with relevant standards
- Withstand the expected influences
- **For Category 1:** Well-tried components and well-tried safety principles

Category 2:
- Single Channel, tested at suitable intervals
- Requirements of B apply
- Well-tried safety principles

Category 3 and 4:
- Dual Channel, with cross monitoring
- Requirements of B shall apply
- Well-tried safety principles
- Tolerant to Single Faults
- **For Category 3:** Detection of the Single fault, whenever reasonably practicable
- **For Category 4:** fault accumulation shall be taken into account

Used designated architectures (Categories)

To next step

Verification and Validation (9)

To Risk Assessment

ISO 12100 § (EN 292) § ISO 14121 (EN 1050)

All SF considered? → no → Next SF, Box (2)

ok

Check prEN ISO 13849-2 → not ok → Redesign, Box (3)

yes

PL ≥ PL_r? → no → Redesign, Box (3)

To next step

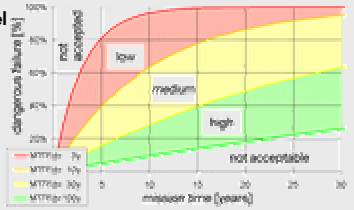
total PL

Without and With SRP/CS

Reliability of Components Used: ($MTTF_d$) (4)

Mean Time to Dangerous Failure of a Single Channel ($MTTF_d$):

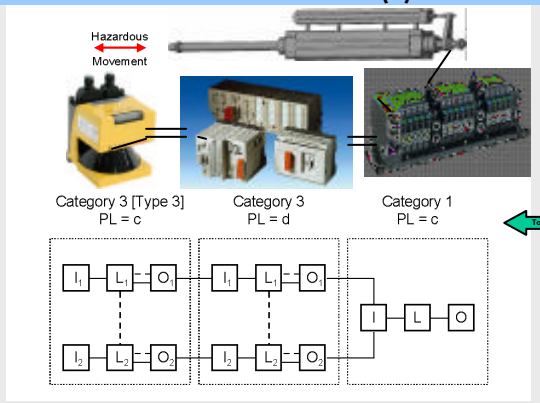
- Refers to a single channel
- Component values from data-bases or manufacturers
- Worst-case-values listed in the standard
- Parts-Count-Method for each channel
- Symmetrization for multiple channels



$MTTF_d$

To next step

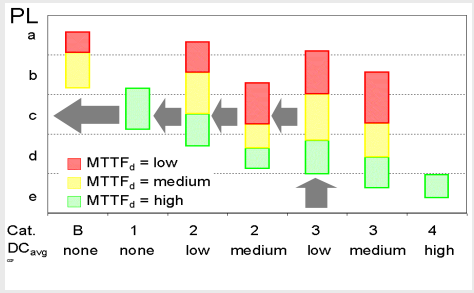
Combination of SRP/CS (8)



PL_1 PL_2 ∞ PL_n

To next step

Estimation of achieved Performance level PL (7)



Category

$MTTF_d$

DC_{avg}

To next step

Fault detection (Diagnostics) (5)

Diagnostic Coverage (DC):

- Typical measures listed in the standard
- Estimates for achievable DC-values
- Divided into three ranges
- Average DC (DC_{avg}) calculated by formula, taking $MTTF_d$- and DC-values of all parts into account

DC	Range
None	< 60%
Low	60% to < 90%
Medium	90% to < 99%
High	>99%

DC_{avg}

To next step

Common Cause Failure (CCF) (6)

Scoring Process for different measures against CCF:

For category 2, 3 and 4 at least 65 of 100 points are necessary.

BIA
Berufsgenossenschaftliches Institut für Arbeitsschutz

Fachausschuss Druck und Papierverarbeitung

Dr. M. Schaefer, M. Hauke, BIA
K. Becker, FA DP
Contact:
Michael.Hauke@hvbg.de
kdbecker@bgdp.de