Safety Related Control Systems & Functional Safety

Amber Gray, FS Tech (TÜV Rheinland, #324/ 15, Machinery)

1

Safety-related parts of controls systems (SRP/CS)

The part of the control system of a machine that prevents a hazardous condition from occurring.

Safety Function

A function of a machine that reduces the risk presented by the machine to an acceptable level determined by the risk assessment.

2

Functional Safety

Safety Function

- If each safety function is executed according to the risk determined by the risk assessment, the machinery can be considered safe and functional safety is achieved.

Safety Integrity

- Safety integrity is the probability that safety related system will satisfactorily perform the required safety function under all stated conditions within a stated period of time when required to do so.

3

Basic Elements of a Safety Function

- Triggering Event
- Safety-related reaction
- Dangerous part of the machine

4

Safety Function Example

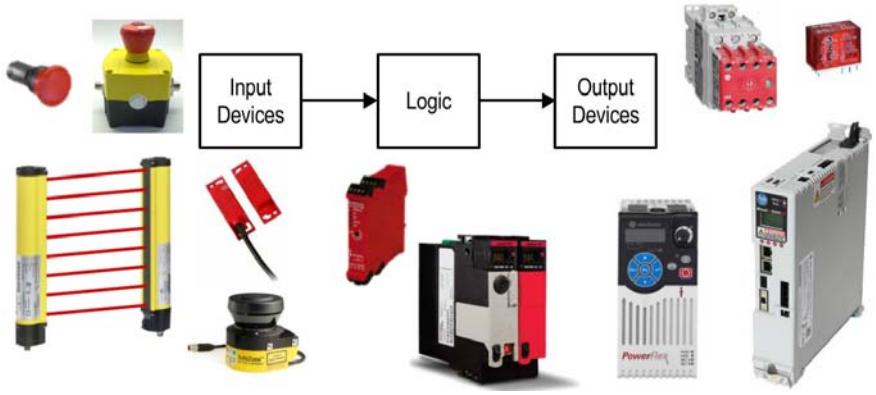
Requirements:

- The rotor cannot start until the guard is closed
- Opening the guard will cause the rotor to stop
- Closing the guard does not restart the machine
- The circuit that issues the stop command is required to meet the requirements of PLe/ Cat 4

5

Safety Function

The safety function is executed by all components which are involved in the safety function:



6

Control System Functional Safety Standards

- ISO 13849-1: Safety of machinery - Safety-related parts of control systems - Part 1: General principles for design
- IEC 62061: Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems
- IEC 61508: Functional safety of electrical/electronic/programmable electronic safety-related systems
- IEC 61511: Functional safety - Safety instrumented systems for the process industry sector

7

ISO 13849 and IEC 62061

Performance Level (PL) or Safety Integrity Level (SIL)

What's the difference?

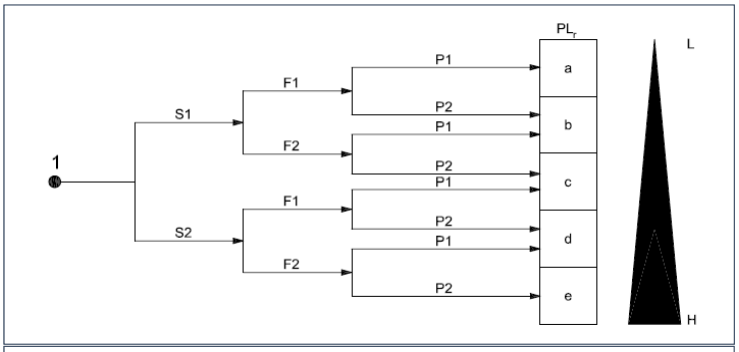
8

Performance Level (PL)
ISO 13849

- Architecture of the system (Category)
- Reliability Data, Mean Time To Dangerous Failure (MTTFd)
- Protection against Common Cause Failure (CCF)
- Protection against systematic faults
- Environmental conditions
- Where relevant, specific requirements for software

9

ISO 13849 Risk Graph



Key

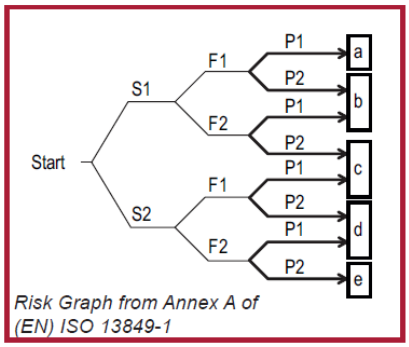
1 starting point for evaluation of safety function's contribution to risk reduction
L low contribution to risk reduction
H high contribution to risk reduction
PL_r required performance level

Risk parameters:

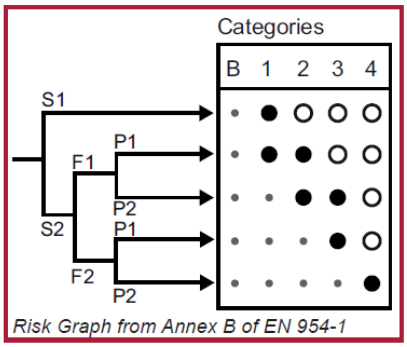
S severity of injury
S1 slight (normally reversible injury)
S2 serious (normally irreversible injury or death)
F frequency and/or exposure to hazard
F1 seldom-to-less-often and/or exposure time is short
F2 frequent-to-continuous and/or exposure time is long
P possibility of avoiding hazard or limiting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

10

Performance Level (PL) & Categories (Cat)



Risk Graph from Annex A of (EN) ISO 13849-1



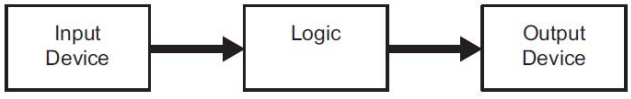
Risk Graph from Annex B of EN 954-1

11

Designated Architecture Categories

Category B

- Basic safety principles
- Fault tolerance of zero



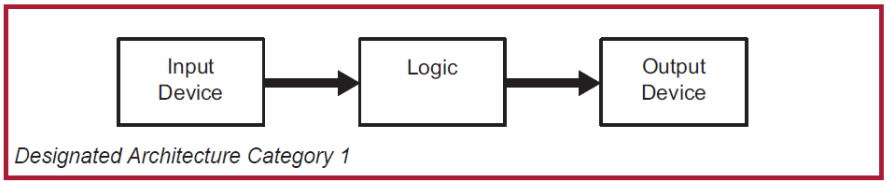
Designated Architecture Category B

12

Designated Architecture Categories

Category 1

- Basic safety principles
- Well tried safety components and principles
- Fault tolerance of zero – but the probability of occurrence is lower than for Category B

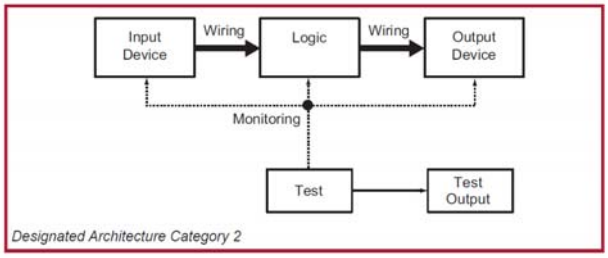


13

Designated Architecture Categories

Category 2

- Basic safety principles
- Well tried safety components and principles
- Diagnostic monitoring via a functional test of the system or subsystem
- Fault tolerance of zero, the loss of the safety function is detected

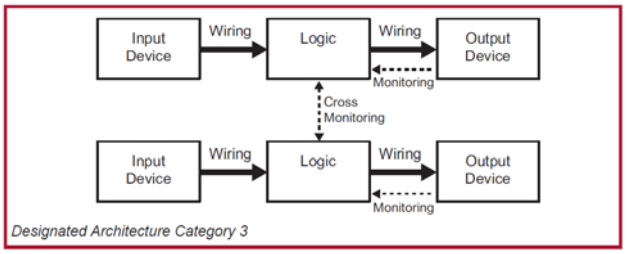


14

Designated Architecture Categories

Category 3

- Basic safety principles, Well tried safety components and principles
- Diagnostic Coverage at least 60%
- Fault tolerance of one, the single fault is detected
- Some but not all faults are detected
- Accumulation of undetected faults can lead to the loss of the safety function



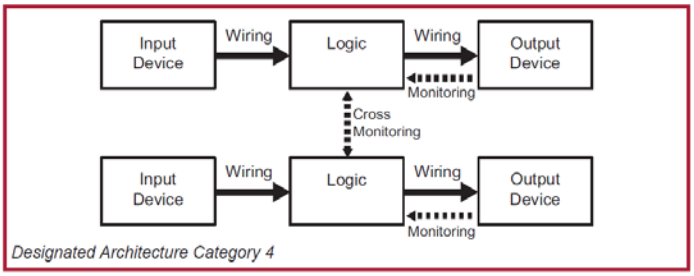
Designated Architecture Category 3

15

Designated Architecture Categories

Category 4

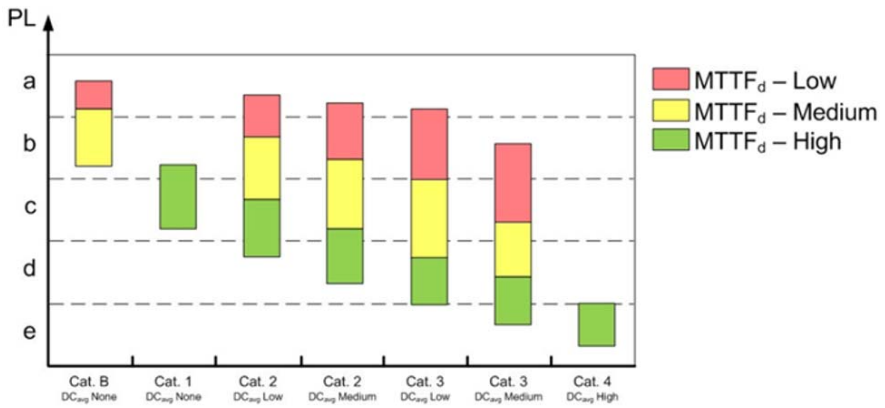
- Basic safety principles
- Well tried safety components and principles
- Diagnostic Coverage at least 99%
- All single dangerous faults and dangerous combinations of faults must be detected



Designated Architecture Category 4

16

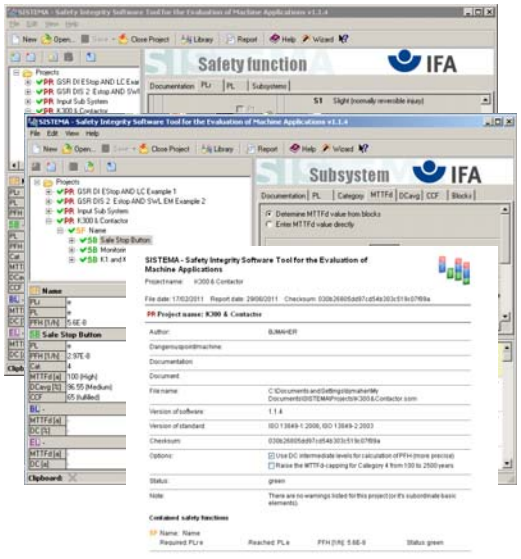
Graphical Determination of PL



17

SISTEMA

- Safety Integrity Software Tool for the Evaluation of Machine Applications
- Developed by the Institute for Occupational Safety and Health of the German Social Accident Insurance (IFA)
- Automates calculation of the attained Performance Level from the safety-related parts of a machine's control system to ISO 13849



18

Safety Integrity Level (SIL)
IEC 62061

Element for SIL Consideration	Symbol
Probability of Dangerous Failure per Hour	PFH_D
Hardware Fault Tolerance	HFT
Safe Failure Fraction	SFF
Proof Test Interval	T_1
Diagnostic Test Interval	T_2
Susceptibility to Common Cause Failures	β
Diagnostic Coverage	DC

19

PL / PFHd / SIL

PL (Performance Level)	PFH_D (Probability of dangerous failure per hour)	SIL (Safety Integrity Level)
a	$\geq 10^{-5}$ to $<10^{-4}$	None
b	$\geq 3 \times 10^{-6}$ to $<10^{-5}$	1
c	$\geq 10^{-6}$ to $<3 \times 10^{-6}$	1
d	$\geq 10^{-7}$ to $<10^{-6}$	2
e	$\geq 10^{-8}$ to $<10^{-7}$	3

20

Questions?

21