Functional Safety in industry applications

Yunxi Zhang 张云禧

TÜV Rheinland Greater China

+86 10 65666660-149

Yunxi.zhang@tuv.com

www.tuvasi.com

TÜVRheinland®
Precisely Right.

Topics under discussion

1 History in Functional Safety

2 Terms of Functional Safety

3 Systematic Faults according to IEC 61508-2

4 Random Faults according to IEC 61508-2

History in Functional Safety

Functional Safety

and

TÜV Rheinland

in

the past 40 years

Use of electronic circuits in safety related application

Safety Consideration - Functional Safety

Beginning in the 1970‘s TÜV Rheinland carried out type approval of safety related electronic circuits, mainly fail-safe technology

Low complex components, hard wired technology
Measures e.g.:

Failure Mode and Effect Analysis (FMEA)
Failure rate (λ), MTBF calculation

TÜV Handbook “Microcomputer in Safety Technique”

Research project computer safety

Results published as book 1984

- Definition of safety classes (5)
- Fault models of integrated circuits
- Structures, redundancy, diversity
- Diagnostic measures for:
  - CPU, RAM, ROM
  - Communication, I/O ….

- *Internal discussion of:*
  - *Failure rates*
  - *Failure rate targets related to safety classes*
  - *Diagnostic coverage*

not accepted in industrial standards at that time

Certification of Programmable Electronic Systems

Early 1980‘s	Microprocessor based Transmitter
1986	First Safety related Programmable Logic Controller (PLC) 1oo2 Architecture
1991	Programmable Logic Controller (PLC) TMR system 2oo3
1992	Programmable Logic Controller (PLC) TMR system 2oo3, hot stand by

Development of safety related standards

Security .....

TÜV handbook

DIN 19250
VDE 0801
VDE 0116

EN 1050
EN 954
VDE 0801 A.1

IEC 61508

IEC 61511
EN 50156

EN ISO 13849
IEC 62061

IEC 61508 Ed. 2

ISO 26262

IEC xxxx

and many other product or application standards

Safety classes

Requirement classes / Safety Category

Safety Integrity Level / Performance Level

Functional Safety Standards used for Certification

Security .....

Application related Standards and TÜV handbook

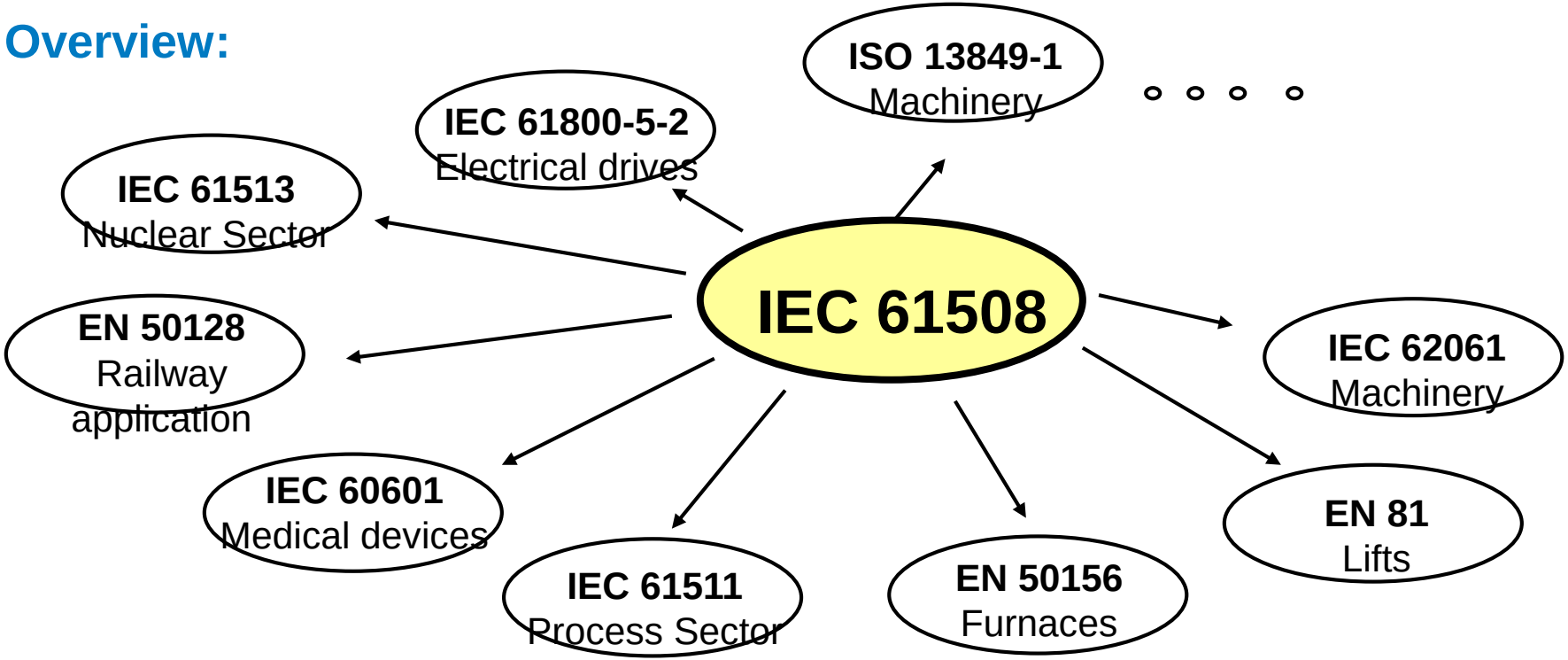
DIN 19250, VDE 0801 VDE 0116 and other Application related Standards

IEC 61508, EN ISO 13849, EN 50156, IEC 61511 and other Application Standards

IEC 61508, ISO 26262 and other product or Application standards

Relation of IEC 61508 / Sector, Application Standards

Overview:



Terms of Functional Safety

„Functional Safety“

A safety system is functionally safe if

- ***Random***,
- ***systematic*** and
- ***common cause***

failures do **not** lead to malfunctioning of the safety system and do not result in

- injury or death of humans
- pollution of the environment

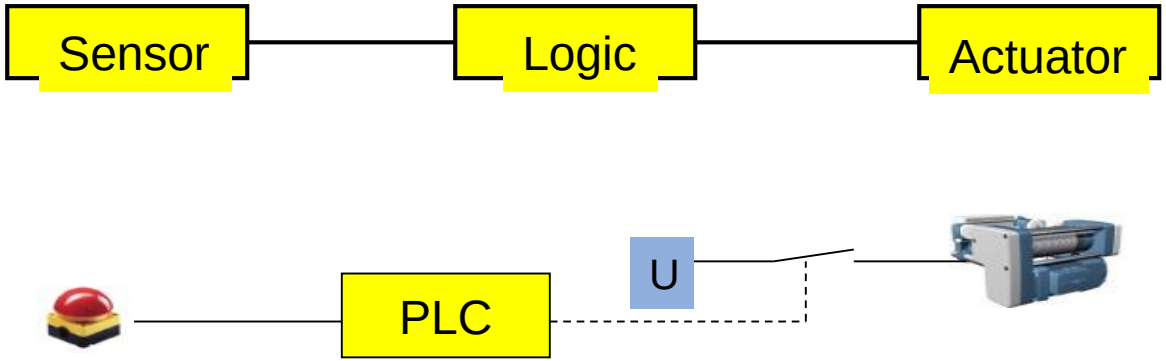
The safety function of a device / control system has to be guaranteed both under normal conditions and in the existence of faults.

„Safety Function“

IEC 61508-4, 3.5.1

A function of a safety related system to reduce the risk in an application with the objective to achieve or keep a safe state.

The safety function is always related to a safety loop, not to a component or device.

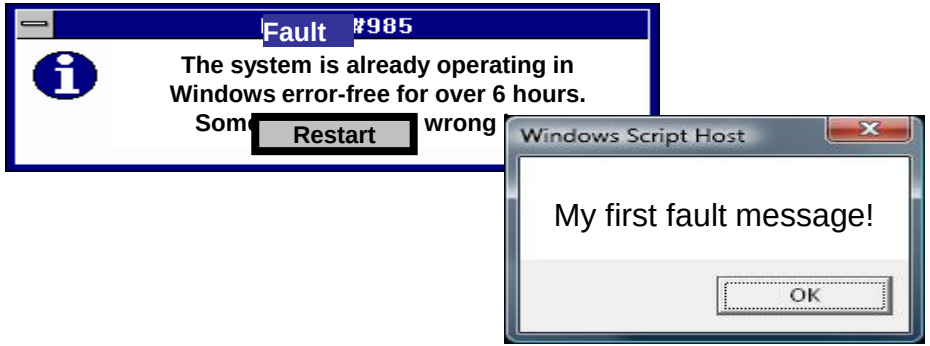


„Systematic and random faults“

IEC 61508-4 3.6.5-6

Systematic faults

- Software Bugs
- Pentium FDIV-Bug
- …



Random faults

- Ageing or worsening of components
- Soft Errors
- …

Target failure measures

IEC 61508-1 , Table 2 / Table 3

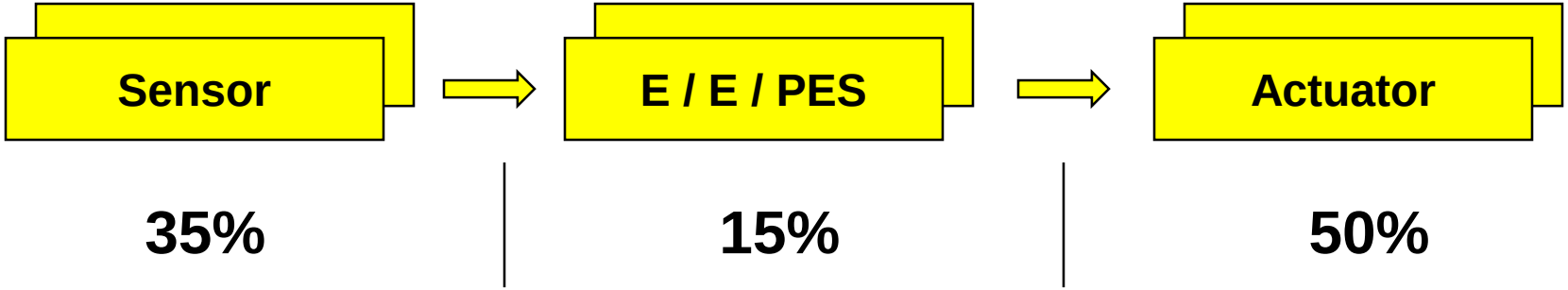
1. target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Low demand mode of operation (Average probability of failure to perform its design function on demand (PFD_{AV})
4	$\geq 10^{-5}$ to $< 10^{-4}$
3	$\geq 10^{-4}$ to $< 10^{-3}$
2	$\geq 10^{-3}$ to $< 10^{-2}$
1	$\geq 10^{-2}$ to $< 10^{-1}$

2. target failure measures for a safety function operating in high demand or continuous mode of operation

Safety integrity level (SIL)	High demand or continuous mode of operation (Probability of a dangerous failure per hour (PFH))
4	$\geq 10^{-9}$ to $< 10^{-8}$
3	$\geq 10^{-8}$ to $< 10^{-7}$
2	$\geq 10^{-7}$ to $< 10^{-6}$
1	$\geq 10^{-6}$ to $< 10^{-5}$

Safety Function, Safety Loop

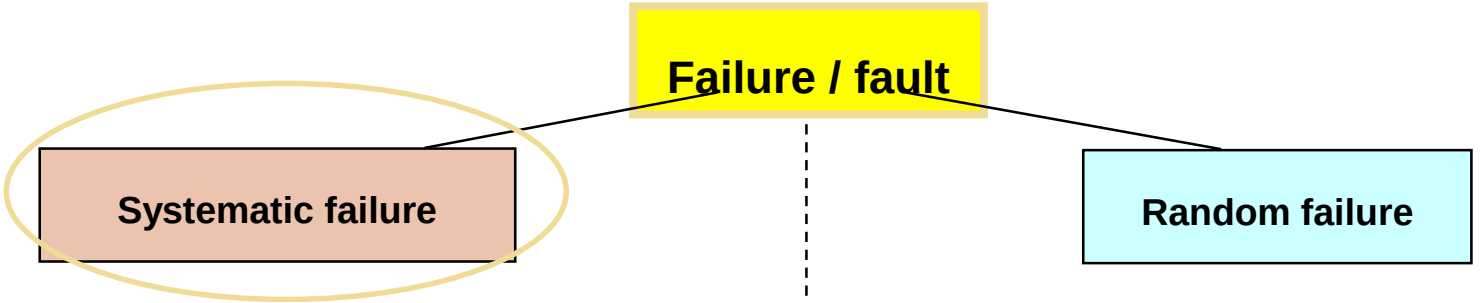


Typical share of failure rates experienced by industrial plants

Systematic Faults according to IEC 61508-2

Type of Faults

Fault: abnormal condition, that may cause loss resp. at least a reduction of a functional unit (system or sub-system) to perform a required function



Failure with definite cause, can only be eliminated by alteration of design, production process, operating mode, operation instructions or other influencing factors

↓

Fault avoidance/ Fault control

Failure, occurring at a random time and whose cause can not be defined distinctively

↓

Fault control

Measures to avoid systematic faults (QM)

Annex B of IEC 61508-2:

Recommendation of measures and methods to avoid systematic faults in hardware during the different life cycle phases

Annex B and C of IEC 61508-7:

Description of measures and methods with further references

Measures to control systematic failures

IEC 61508-2 , Annex A.3

- The standard requires the application of QM measures to avoid failures in the different phases during the life cycle of a product.
  The requirement to apply these measures is dependent on the SIL.

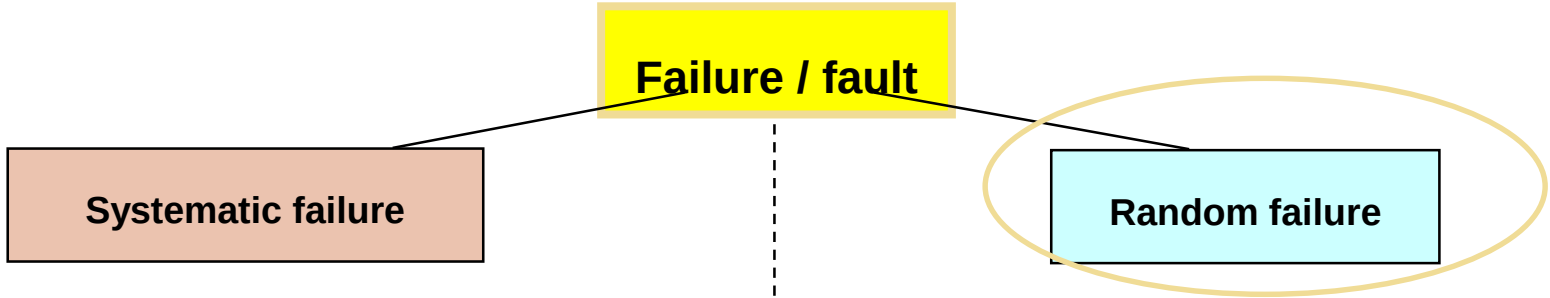
  No matter how well these measures are applied, there is a residual probability of systematic failures occurring.

- That's why the standard requires the implementation of measures and techniques to control systematic failures
  - caused by HW and SW design (see **IEC 61508-2, Table A.15**)
  - due to environmental stress or external influences (incl. EMC) (see **IEC 61508-2, Table A.16**)
  - during operation, (operator mistakes) (see **IEC 61508-2, Table A.17**)

Random Faults according to IEC 61508-2

Type of Faults

Fault: abnormal condition, that may cause loss; at least a reduction of a functional unit (system or sub-system) to perform a required function



Failure with definite cause, can only be eliminated by alteration of design, production process, operating mode, operation instructions or other influencing factors

Fault avoidance/
Fault control

Failure, occurring at a random time and whose cause can not be defined distinctively

Fault control

Measures to control random faults (on-line diagnostic)

Annex A Table A.2 ….. Table A.14 of IEC 61508-2:

Techniques/measures to control random faults of different component

Annex B and C of IEC 61508-7:

Description of measures and methods with further references

Thank you !

Any question please feel free to contact:

肖潇然

jane.xiao@tuv.com

+86 10 6566 6660-174

13811276916