Functional Safety in the Entertainment Industry: The new standard EN 17206

08 October 2019

Add value.
Inspire trust.

Our Experts

Udo Gruner
Safety Expert for Entertainment Technology, Lifts and Cranes at TÜV SÜD

Background:
- Over 30 years of experience in testing Lift and Cranes
- 10 years ago, he specialized in entertainment industry installations focusing on the application of control systems
- Member of the German delegation in CEN TC 433 Working Group 1 “Entertainment Technology - Machinery for Stages and other Production Areas - Safety requirements and inspections.”

Matthias Ramold
Technical Certifier and Manager Safety Components at TÜV SÜD

Background:
- Experienced assessor, project manager and technical certifier for testing and certification of electrical / electronic components and systems used for functional safety applications in various industries
- Working with TÜV SÜD since over 13 years and managed various international projects as safety expert
- Trainer for functional safety and its industry-specific standards

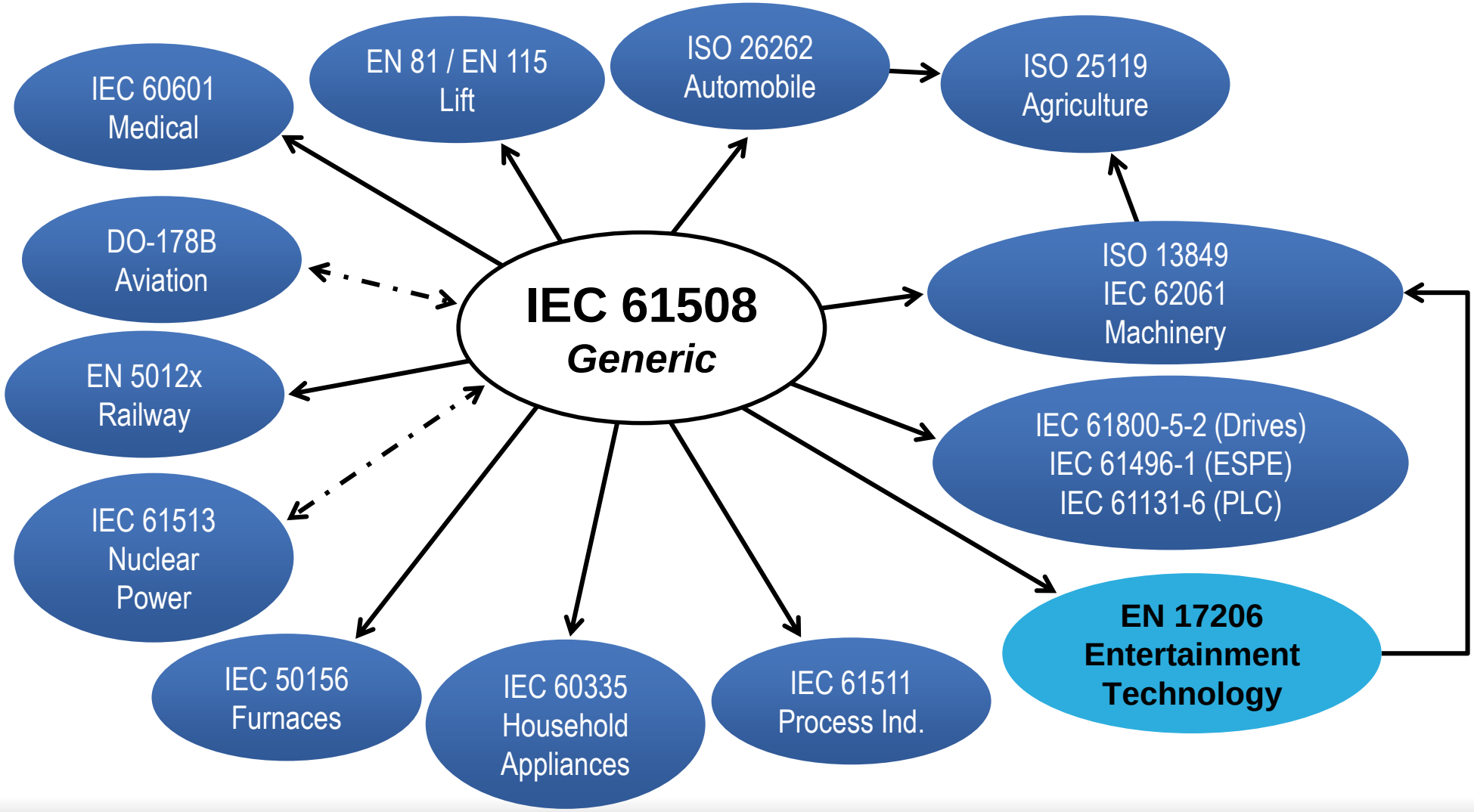
Agenda

1. Introduction: New standard EN 17206
2. Typical Safety Functions
3. Risk Analysis Approach
4. Functional Safety Basics
5. Certification: V-Model
6. Q&A

Example: Stage accident – Pink concert

Link to Video: https://www.youtube.com/watch?v=82Ht4YaeDMo

Links between Functional Safety Standards



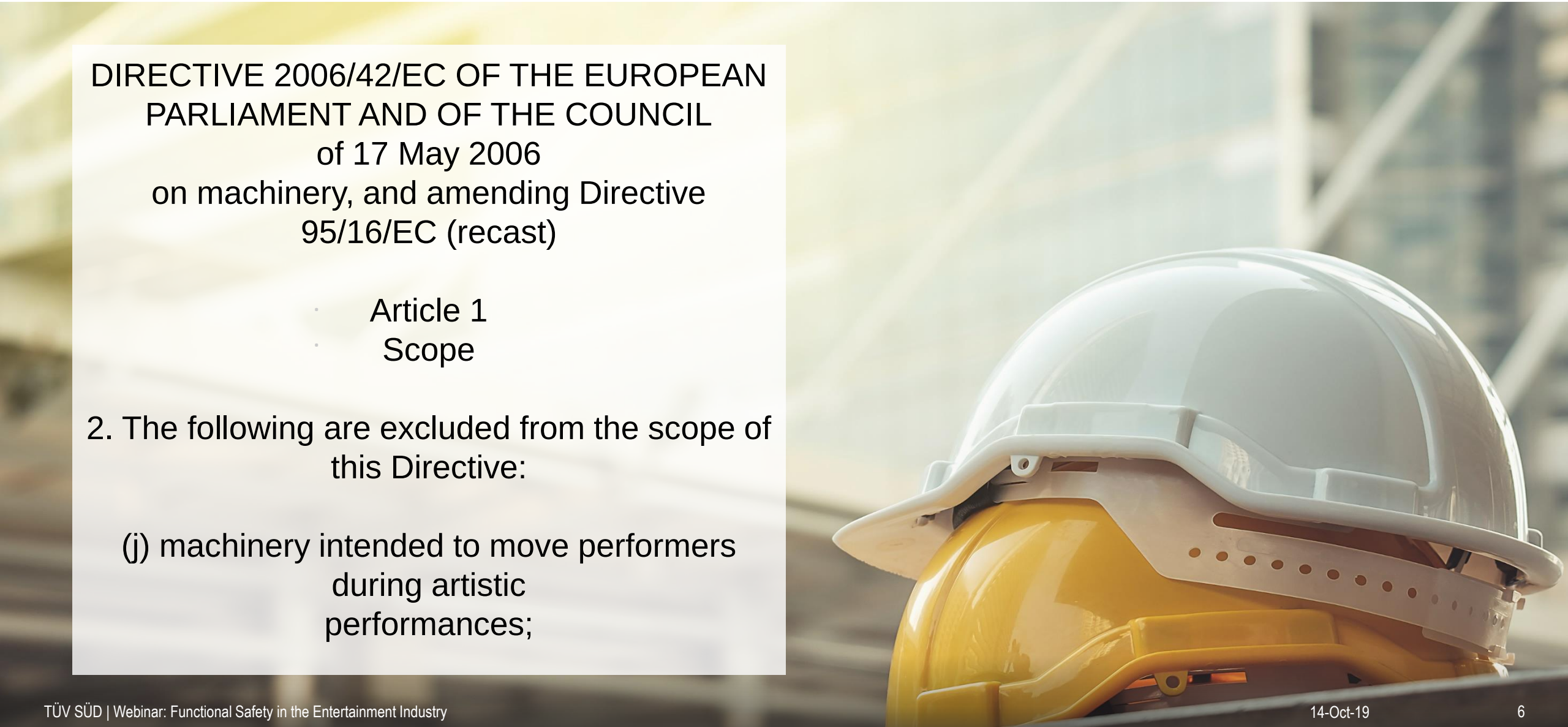
Functional Safety in the Entertainment Industry

DIRECTIVE 2006/42/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 17 May 2006
on machinery, and amending Directive 95/16/EC (recast)

- Article 1
- Scope

2. The following are excluded from the scope of this Directive:

(j) machinery intended to move performers during artistic performances;



Functional Safety in the Entertainment Industry

DGUV Vorschrift 17/18
Unfallverhütungsvorschrift
Veranstaltungs- und
Produktionsstätten für
szenische Darstellung
vom 1. April 1998

New Standard: EN 17206

EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

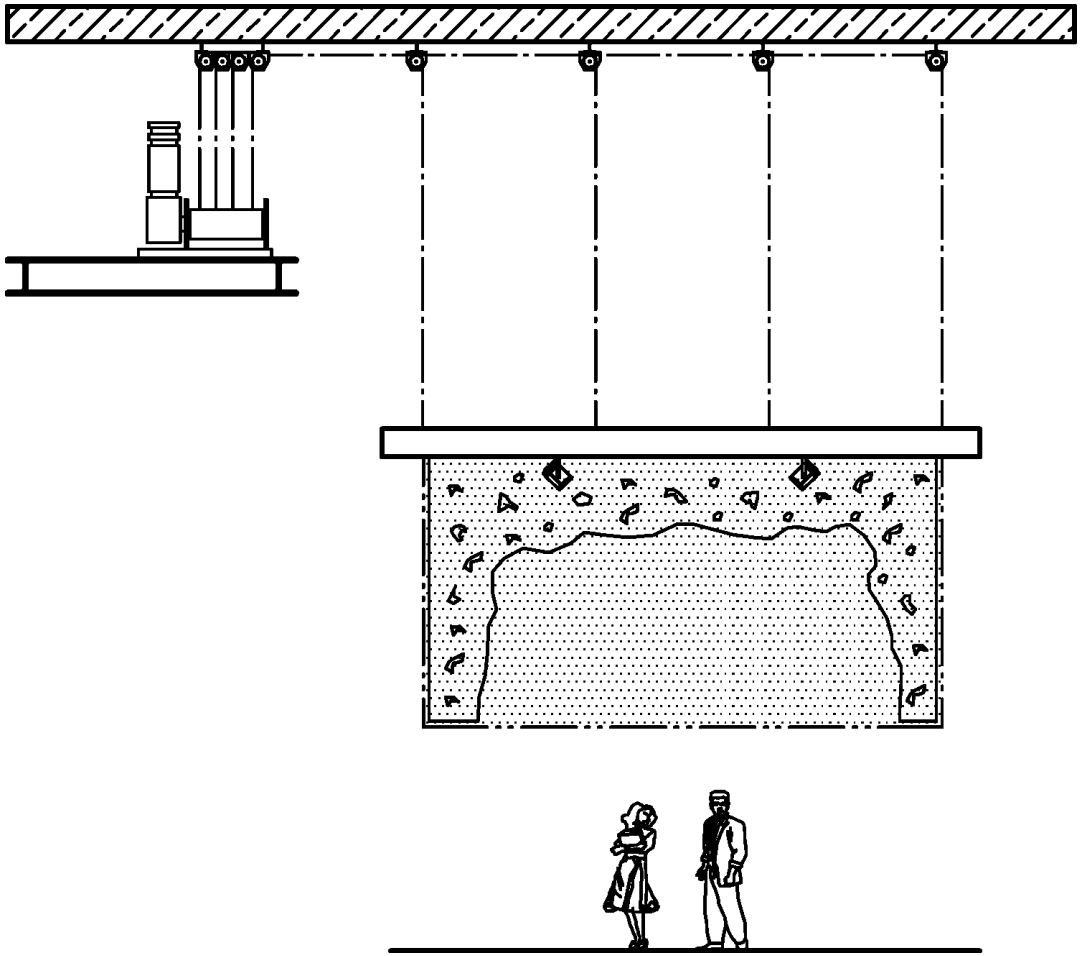
DRAFT prEN 17206

Entertainment Technology - Lifting and Load-bearing Equipment for Stages and other Production Areas within the Entertainment Industry - Specifications for general requirements (excluding aluminum and steel trusses and towers)

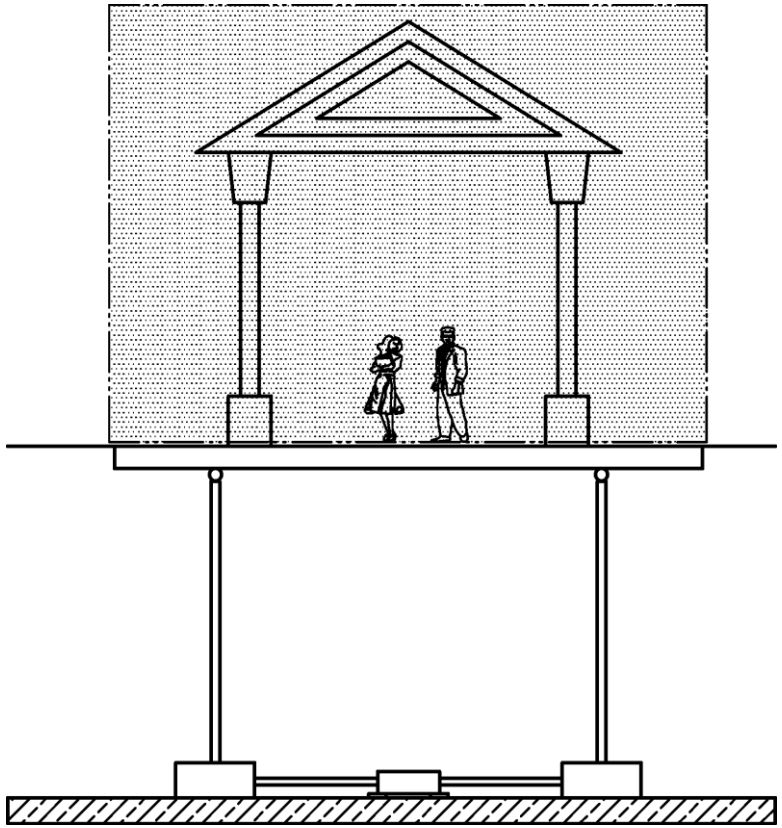
Agenda

1. Introduction: New standard EN 17206
2. Typical Safety Functions
3. Risk Analysis Approach
4. Functional Safety Basics
5. Certification: V-Model
6. Q&A

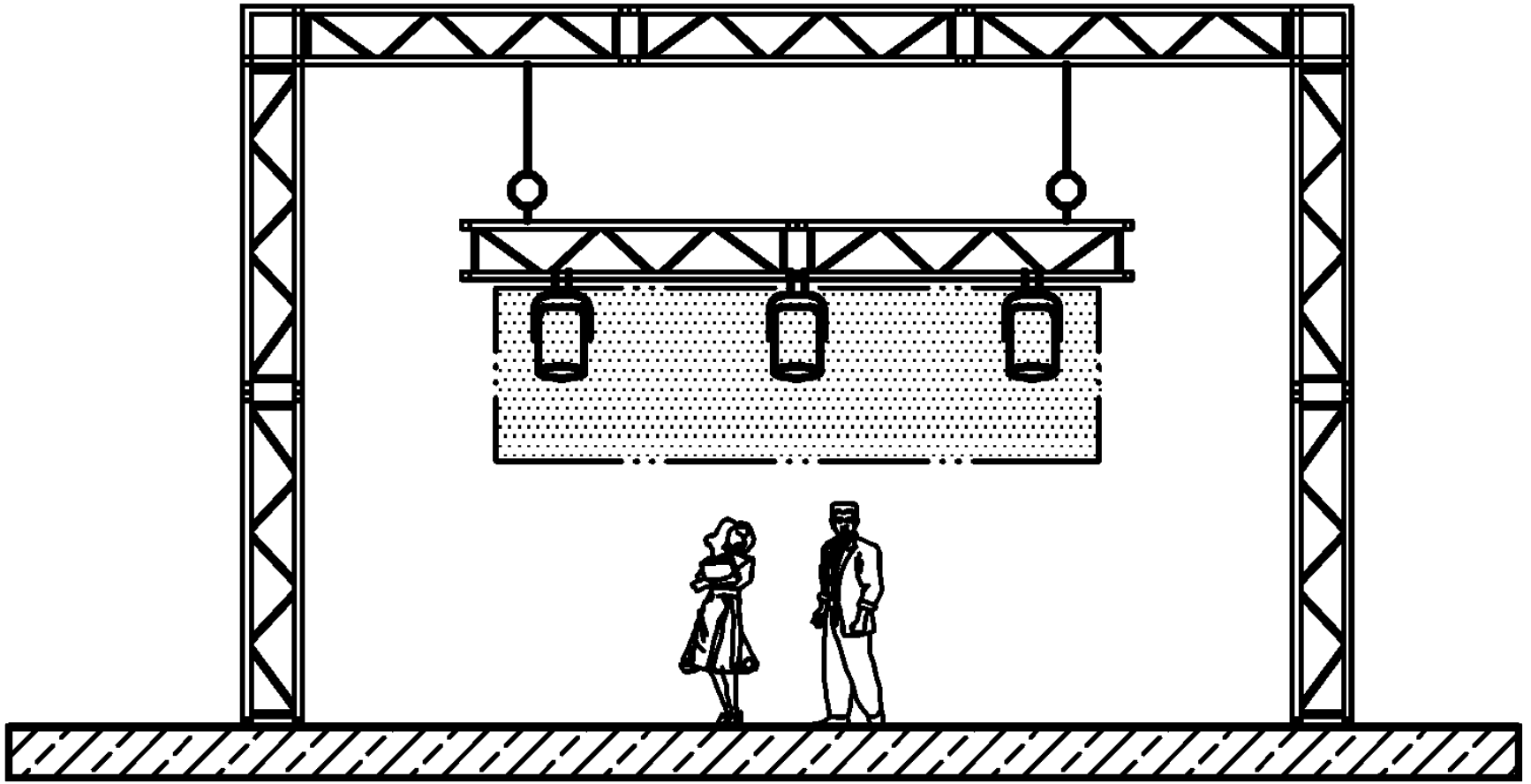
Safety Functions: Upper machinery



Safety Functions: Lower machinery



Safety Functions: Rock´n roll



Safety Functions: EN 17206

UC1 No-one in hazard zone during motion, SD Load, Speed < 0.2m/s,

UC6 Moving person(s) suspended, multiple axis,

Safety Functions: EN 17206

Upper machinery recommended safety functions and measures (prEN 17206)						
Safety Function	**UC1**	**UC2**	**UC3**	**UC4**	**UC5**	**UC6**
Emergency Stop – category 0 or 1	HR	HR	HR (Cat 1)	HR (Cat 1)	HR (Cat 1)	HR (Cat 1)
Stop on “Deadman” Release – category 0, 1 or 2	HR	HR	HR	HR	HR	HR
Protection against position deviation			HR	HR	HR	HR

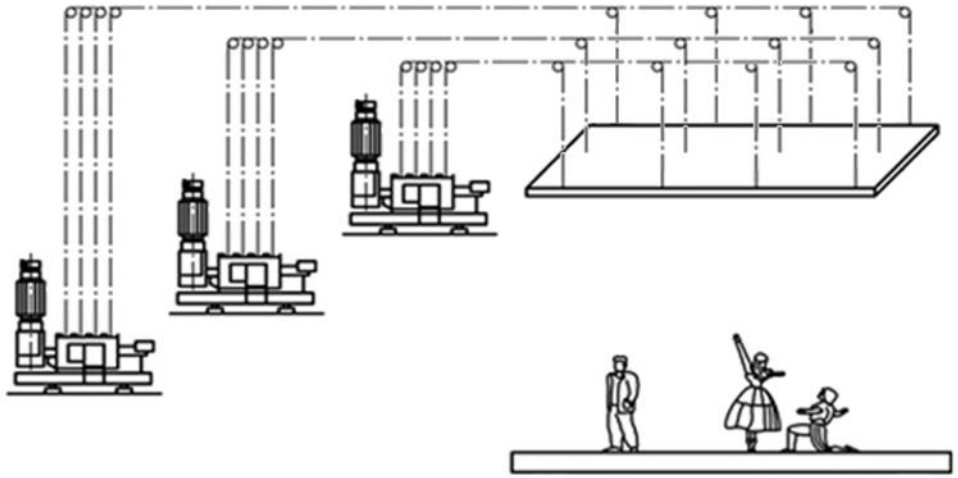
Example from the entertainment industry

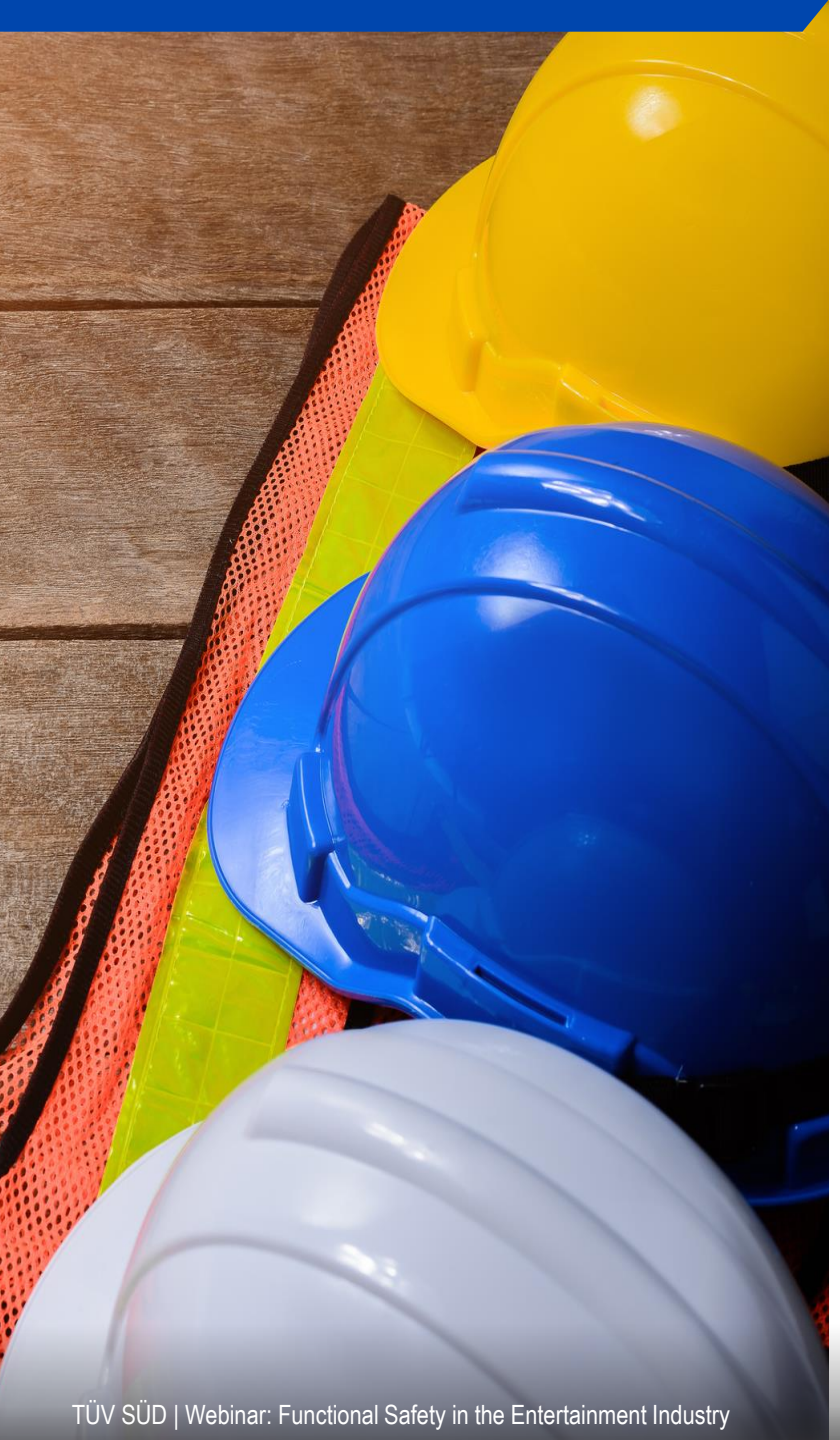
Risk assessment

During a lifting operation is a failure in one of the hoists. The operator might have limited visibility. The control system shall stop motion of any machine in the group once the synchronisation tolerances are exceeded.

Requirement

Protection against loss of group synchronisation safety function would prevent this event from happening.





Example from the entertainment industry: Safety functions

- Protection against speed deviation
- Protection against over-speed
- Protection against overload
- Protection against underload / slack situation
- Protection against unplanned load change
- Protection against loss of group synchronisation
- Limitation of Travel
- Protection against improper winding
- Protection against crushing / shearing
- Automatic protection against brake failure
- Protection against power source failures
- Protection against collisions with other machines

Agenda

1. Introduction: New standard EN 17206
2. Typical Safety Functions
3. Risk Analysis Approach
4. Functional Safety Basics
5. Certification: V-Model
6. Q&A

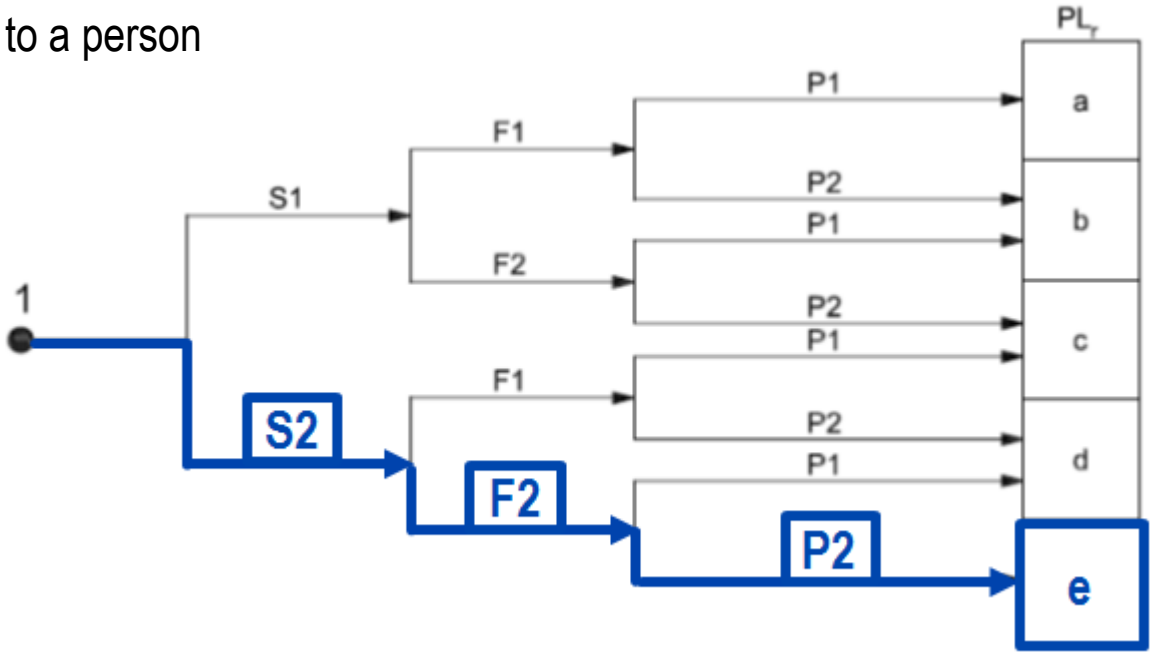
Risk Graph

Severity (S)
This unwanted occurrence would take place above the stage surface, and in the event of failure, serious injuries to one or more persons, or even death to a person could be expected.

Frequency and/or exposure to hazard (F)
On the stage, people are often in the danger zone.

Possibility of avoiding hazard or limiting harm (P)
This hazard can only be avoided when the operator reacts (e.g. operator initiates an emergency stop), although the period during which this is possible is indefinable.

Risk parameter selections lead to a
- required Performance Level (PL) of e according to EN ISO 13849-1 or
- required Safety Integrity Level (SIL) of 3 according to EN 62061



lead to **PL e** or **SIL 3**

Agenda

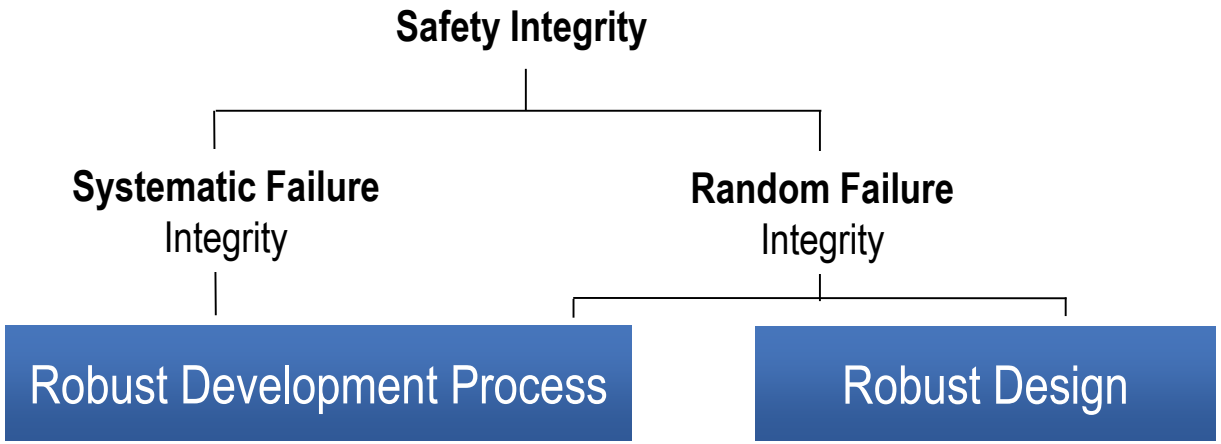
1. Introduction: New standard EN 17206
2. Typical Safety Functions
3. Risk Analysis Approach
4. Functional Safety Basics
5. Certification: V-Model
6. Q&A

Safety Integrity

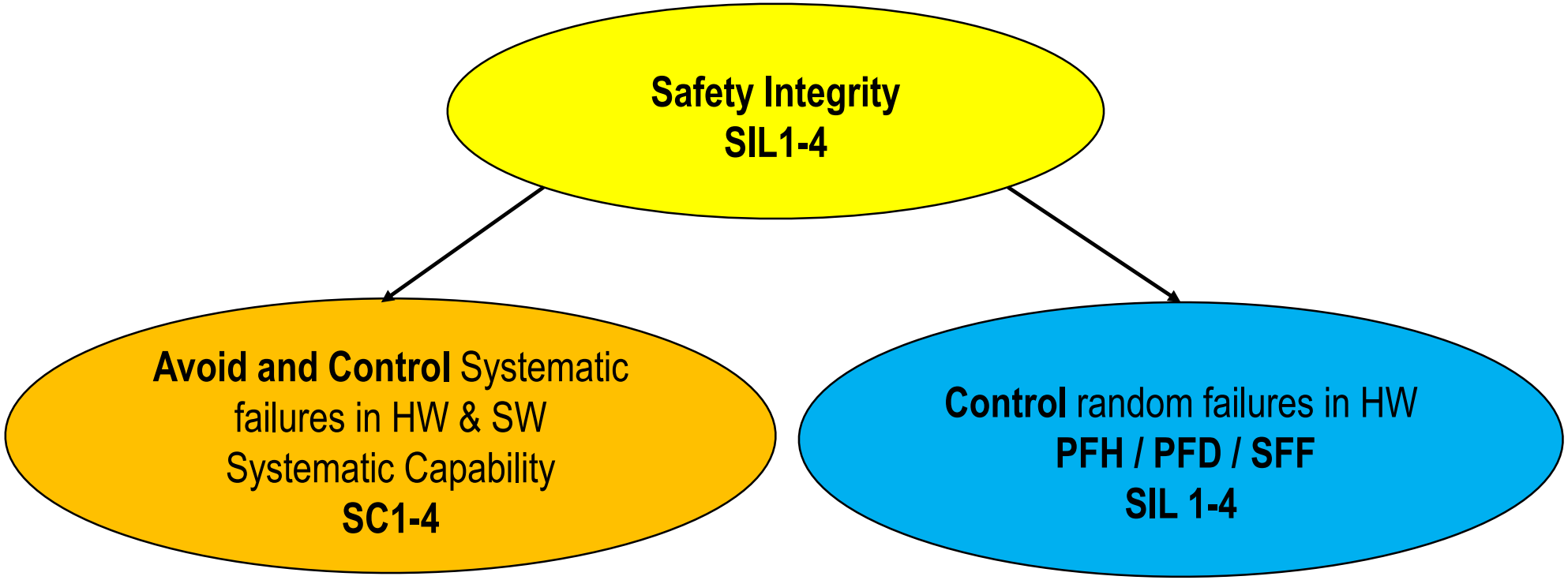
EN 17206:2018 - For functional safety related topics the standards EN 61508, EN 62061 or EN ISO 13849-1 have to be used…

A system meets its Performance Level or Safety Integrity Target when it …

- is sufficiently free from systematic failures in hard and software,
- meets all safety requirements in the event of random hardware failures,
- has a specified reaction on random faults and
- executes safety function under specified environmental conditions, e.g.
  - EMC
  - Temperature, Humidity
  - Vibration, Shock
  - Chemical influences
  - Water, Dust
  - Operation



Safety Integrity



Systematic Failure - Programming error

Mariner 1: 22th of July 1962, Cape Canaveral/Florida

- Intended to fly to Venus
- Not controllable due to software malfunction
- Deviation of the planned flight path
- Self-destructing 290 seconds after launch

REASON

DO 5 K = 1.3	⇔	**DO 5 K = 1,3**
…		…
5 CONTINUE		**5 CONTINUE**
(non-declared variable)		(loop)

Point instead of comma in Fortran Code

Source: Wikipedia

Functional Safety Management

High contribution to the overall risk of a safety-critical system rests upon systematic failures, which are not identified, not thoroughly analysed and measures not sufficiently evaluated

QM

(e.g. ISO 9001)

General

requirements

FSM (IEC 61508)

Quality management Processes

General requirements (Organisational Level)

e.g. leadership, continual improvement, factual approach to decision making, etc.

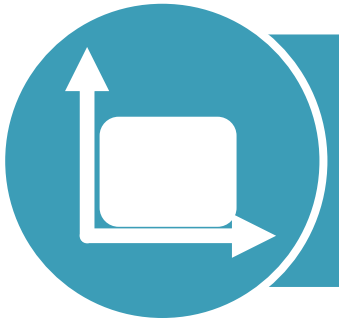
General requirements (Department Level)

e.g. personnel training, internal audits, document management, maintenance, corrective actions, etc.

Specific Safety Assurance Requirements (Project Level)

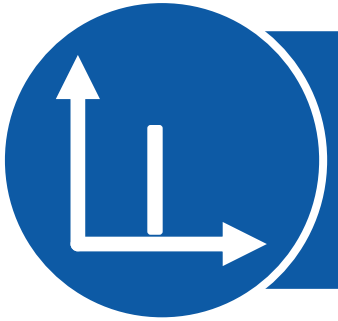
Defined in a Safety Plan incl. hazard and safety analysis, risk control, V&V, test strategy, etc.

Random Faults



Permanent hardware faults

Intermittent hardware faults



Transient hardware faults

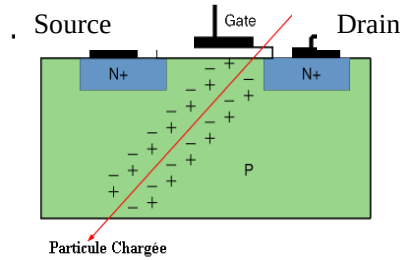
Transient Hardware Faults

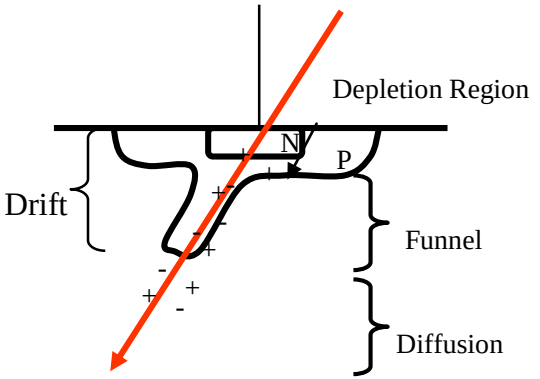
Transient Hardware Faults

- Mainly caused by energetic particles colliding with sensitive regions of a semiconductor leading to logic errors by changing stored information in e.g. SRAM, DRAM, microprocessors, and FPGA
- Major concern due to decreasing manufacturing size of semiconductors and resulting reduction in critical charge of logic circuits

Soft Error

- Storage element (memory cell, latch, or register) state change
- No permanent hardware damage





Example

- Single Event Upsets (SEU) induced by the strike of a single energetic particle in a semiconductor

Effect

- A single strike can leave an ionized track with free electrons and holes
- Near a p-n junction electron hole pairs may not recombine back to a normal state
- Electrons\holes can be attracted to a higher\lower voltage causing the change of state of a storage element

Probability of failure – PFD, PFH

Safety integrity levels – target failure measures for a safety function operating in low demand mode of operation

Safety integrity level (SIL)	Average probability of a dangerous failure on demand of the safety function (PFD_{avg})
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 $< 10^{-1}$

Safety integrity levels – target failure measures for a safety function operating in high demand mode of operation or continuous mode of operation

Safety integrity level (SIL)	Average frequency of a dangerous failure of the safety function [h^{-1}] (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 $< 10^{-5}$

Safe Failure Fraction (SFF) and DC

Safe **F**ailure **F**raction =

the relation of safe resp. detected failures to all failures

safe failures $\sum \lambda_S$ + dangerous detected failures $\sum \lambda_{DD}$ + dangerous undetected failures $\sum \lambda_{DU}$

complete safe failure rate

complete failure rate

$$SFF = \frac{\sum \lambda_S + \sum \lambda_{DD}}{\sum \lambda_S + \sum \lambda_{DD} + \sum \lambda_{DU}}$$

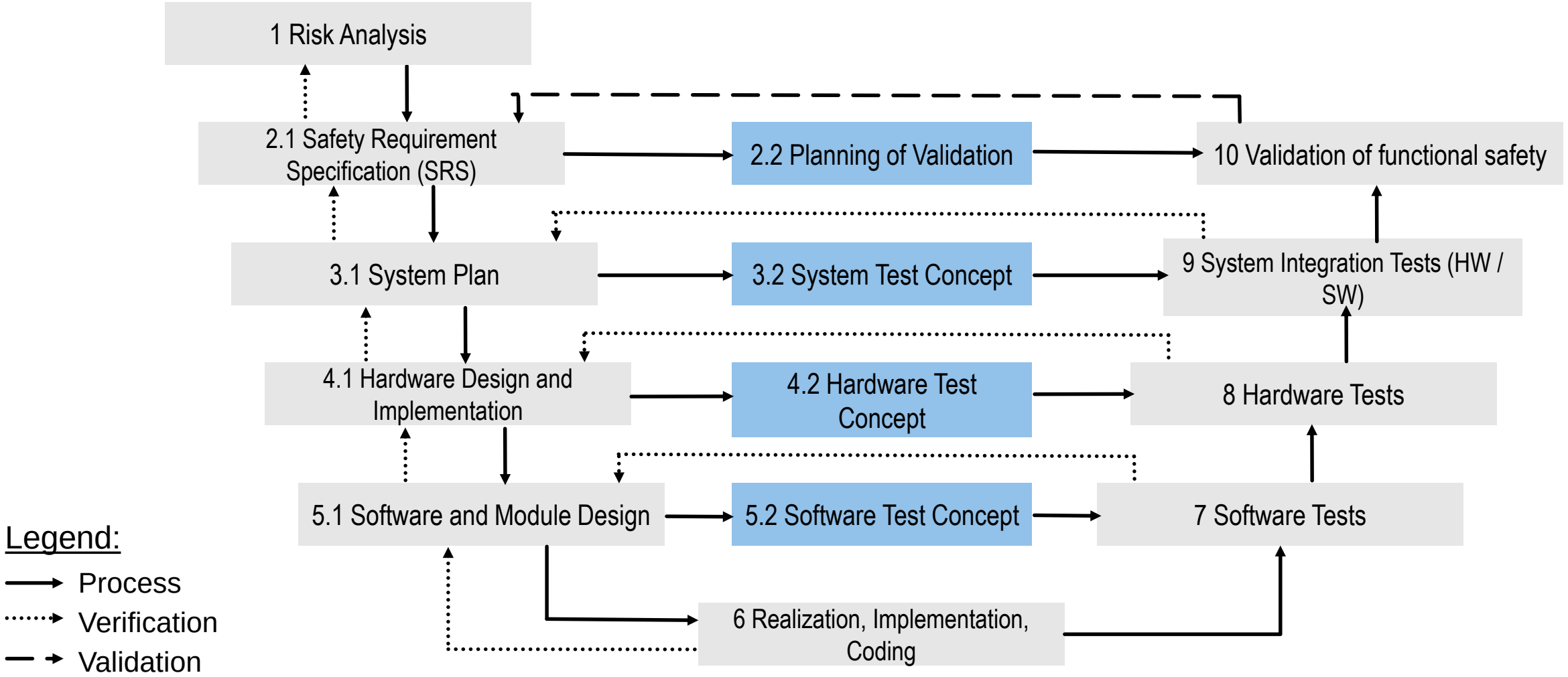
Diagnostic **C**overage

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}}$$

Agenda

1. Introduction: New standard EN 17206
2. Typical Safety Functions
3. Risk Analysis Approach
4. Functional Safety Basics
5. Certification: V-Model
6. Q&A

Certification: V-Model



Certification: Necessary documentation from the manufacturer (1/2)

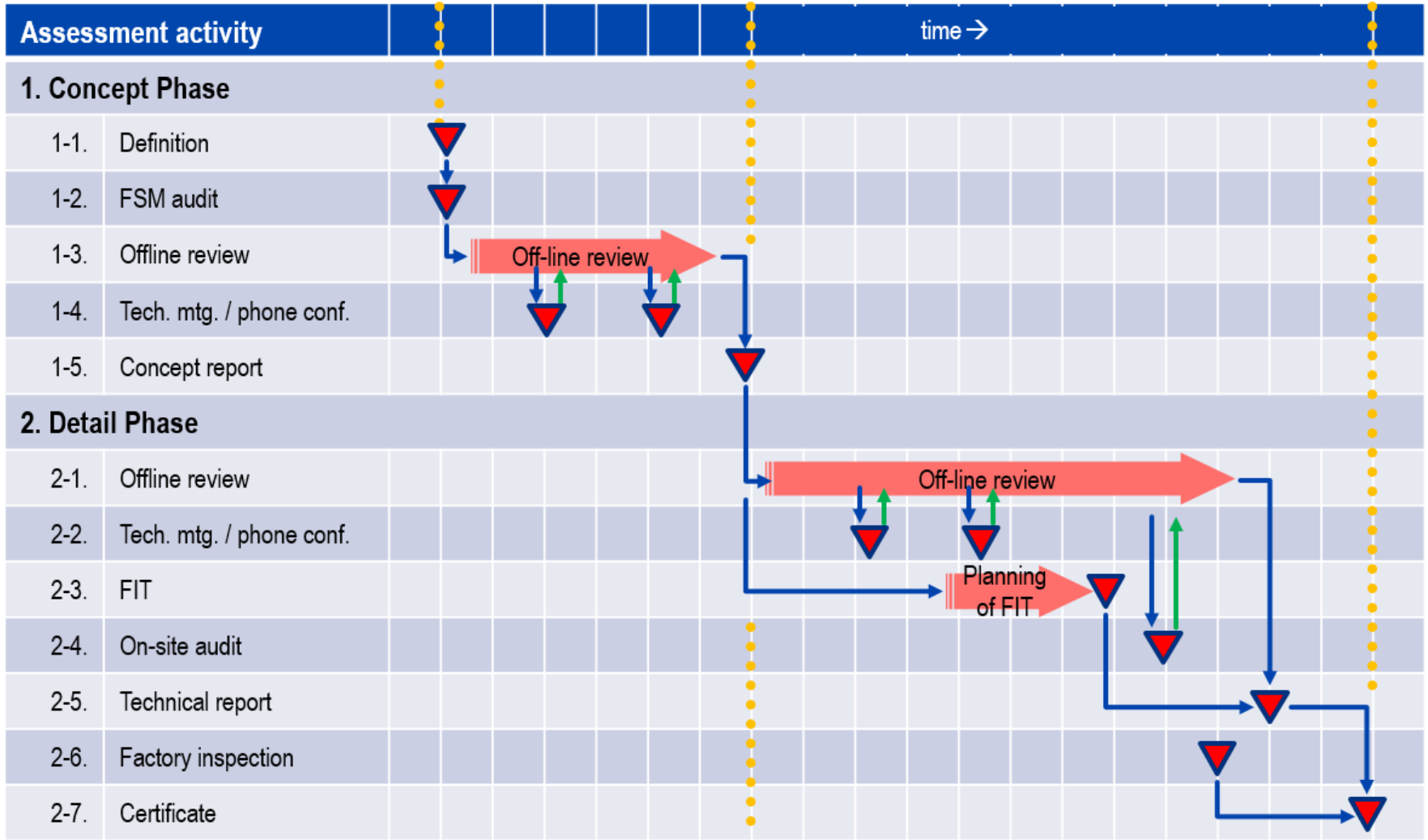
Phase	Document
2.1 Safety requirement specification	▪ SRS
2.2 Planning of validation	▪ Validation plan, safety plan
3.1 System plan	▪ System-Specification and system architecture (hard- and software)
	▪ System-FMEA and block diagrams
3.2 System test concept	▪ System test plan
4.1 Hardware design and implementation	▪ Hardware description and schematics, part lists, layouts and information on the components and materials used
	▪ Component FMEA (FMEDA)
	▪ MTTFd/DC/CC calculation according to ISO 13849-1
	▪ SFF/PFH/PFD calculation according to IEC 61508-2
4.2 Hardware test concept	▪ Hardware test plan

Certification: Necessary documentation from the manufacturer (2/2)

Phase	Document
5.1 Software design	▪ Software architecture and design specification (structured or semi-formal) (according to IEC 61508-3)
	▪ Documentation of the software tool qualification
	▪ Coding standards
	▪ Software criticality analyse
5.2 Software test concept	▪ Software test plan
6 Realization: implementation / coding	▪ graphical explanation, source code
7 Software test: verification of all SW requirements	▪ Documentation of test results

Assessment approach of functional safety products

- Functional Safety Certification of products is a **development accompanying** task
- Duration (0,5 – 4 years) and timing heavily depends on each specific project



Certificate

- Independent third party assessment
- No evaluation by the end user necessary
- Conformity to the relevant standards, i.e. proof that development and planning have been performed according to the state of the art
- Supervision of the production
- Comparability between products

- Describes the product
- States the achieved Safety Integrity Level / Performance Level
- States specified environmental conditions

ZERTIFIKAT ◆ CERTIFICATE ◆ СЕРТИФИКАТ ◆ CERTIFICADO ◆ CERTIFICAT

CERTIFICATE

No. Z10 12 01 5356

Holder of Certificate

Factory(ies): 53567, 73847

Certification Mark:

Product: Safety Related Programmable Electronic System

Model(s): SIPLUS extreme S7 Distributed Safety

Parameters:

Logic solver: 1oo1D with coded processing and comparison by safety-related output modules

Fieldbus: 1oo1 PROFIsafe

I/O modules: 1oo2D with normally energized outputs

The report below and the user documentation in the currently valid revision are mandatory part of this certificate. The product complies with the following listed safety requirements only if the specifications documented in the currently valid revision of this report are met.

Tested according to:

IEC 61508-1:1998; up to SIL 3
IEC 61508-2:2000; up to SIL 3
IEC 61508-3:1998; up to SIL 3
ISO 13849-1:2008; up to PL e, Cat. 4
IEC 61511:2003
IEC 62061:2005
IEC 60721-3-3:1994; Classes 3B2, 3C4, 3S4
DIN EN 50155:2008; Cat. 1 Cl. A, B

The product was tested on a voluntary basis and complies with the essential requirements. The certification mark shown above can be affixed on the product. It is not permitted to alter the certification mark in any way. In addition the certification holder must not transfer the certificate to third parties. See also notes overleaf.

Test report no.: SF84100C

Date, 2012-02-01 (Peter Weiss)

Page 1 of 1

472180

TÜV SÜD Product Service GmbH · Zertifizierstelle · Ridlerstraße 65 · 80339 München · Germany

TÜV SÜD issued

574,000(*)

CERTIFICATES

*As of 2017-12-31 ^Based on clients' locations (Figures have been rounded off.)

Agenda

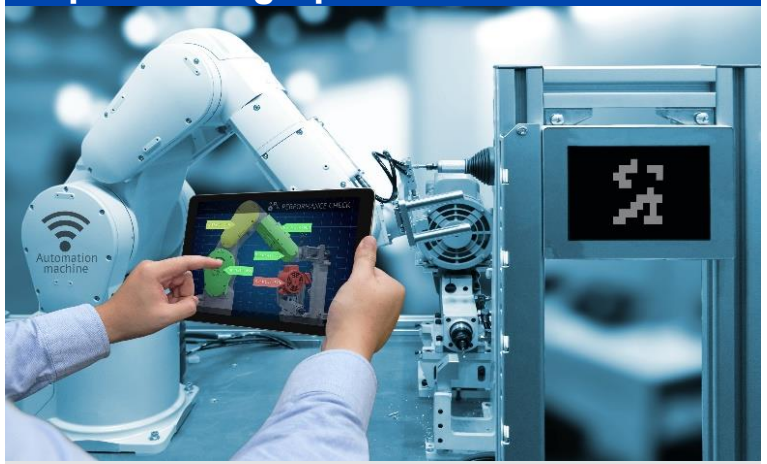
1. Introduction: New standard EN 17206
2. Typical Safety Functions
3. Risk Analysis Approach
4. Functional Safety Basics
5. Certification: V-Model
6. Q&A

Stay up-to-date!

Register for our industry E-ssentials

- Register here

Download our Functional Safety White Paper & Infographic



- Read more about "Functional safety for a digital world - Smart solutions from chip design to whole system design"
- Download our infographic Functional Safety in a nutshell

Watch our On-Demand webinars about Functional Safety

- Webinar: Safety-related Motor Drives and 2nd Edition of IEC 61800-5-2
- Webinar: Finding the right software tools for functional safety projects
- Webinar: Top Misunderstandings about Functional Safety

Thank you very much for your attention!

Add value.
Inspire trust.

Contact us:

www.tuvsud.com
functional-safety@tuvsud.com

Follow us on social media:

@tuvsud
linkedin.com/company/tuvsud
@tuvsud
xing.com/companies/tuvsud
youtube.com/tuvsud