KUGLER MAAG CIE

How CMMI® supports efficient Implementation of Functional Safety

Bonifaz Maag, CEO
KUGLER MAAG CIE GmbH
Leibnizstrasse 11, 70806 Kornwestheim / Stuttgart
Germany
http://www.kuglermaagusa.com

Throughout this presentation CMMI is used as abbreviation of CMMI-DEV V1.2

Agenda

- Introduction
- Functional Safety – The Standards
- Comparison with CMMI – Overlaps and Differences
- How Functional Safety impacts Engineering Processes and the Organization – Examples
- Efficient Implementation of Functional Safety with CMMI – Examples
- Limitations – Where does Safety go beyond CMMI?

Objective of this Presentation

- To become more familiar with
  - the standards and concepts of functional safety
  - how these standards and concepts map onto CMMI
  - how CMMI facilitates the implementation of functional safety
- This presentation
  - does not provide a detailed nor a complete mapping between functional safety and practices of CMMI
  - it focuses on organizational aspects and some basic concepts

KUGLER MAAG CIE - Facts

Facts

- Founded in 2004, today an high performing team with many years experience in industry and academia, unique skills, acknowledged experts

Partners

- In industry and academia, Japan and US, Member of Lero/Ireland, Partner of ibi, Partner of SEI/US, Sponsor of SEI Europe, Co-founder of iNTACS™

MASTER SYSTEMS® iNTACS™ ibi SEIPartner

MBtech Biz³ NTC

Customers

- Global players, culturally diverse, operating in Europe, North America, and Japan

KUGLER MAAG CIE Service Areas

- **Knowledge Services**
  - Training and Qualification of Practitioners, EPG, Quality Group, Assessors, Management, and Executive Management
  - Qualifying for Customers' or 3rd party Assessments
- **Improvement Services**
  - Managing Change for the Purpose of lasting Quality and Productivity Improvement
  - Evaluating Performance Improvement Potential
- **Change Engine Services**
  - organizational Change Control
  - agile Process Management
  - Strategy implementation
- **Appraisal Services**
  - Improvement "Readiness Check"
  - Improvement "Health Check"
  - CMMI® Appraisals
  - ISO/IEC 15504 SPICE Assessments
  - Tailored Supplier Evaluations
- **Process Application**
  - "Off-the-shelf" processes tailored for an accelerated and sustained Process Performance Improvement
  - "Project Rescue" Services
  - Operative Process Execution

KUGLER MAAG CIE

Safety
deals with the protection against hazards and risks that originate from the operation of a device / system

Security
deals with the protection of persons or systems against external hazards

Functional Safety
focuses on risks emerging from the functions of a device / system. It does not focus on risks like fire or environmental pollution

KUGLER MAAG CIE

Standards on Functional Safety for (Embedded) Electronic Systems are necessary because

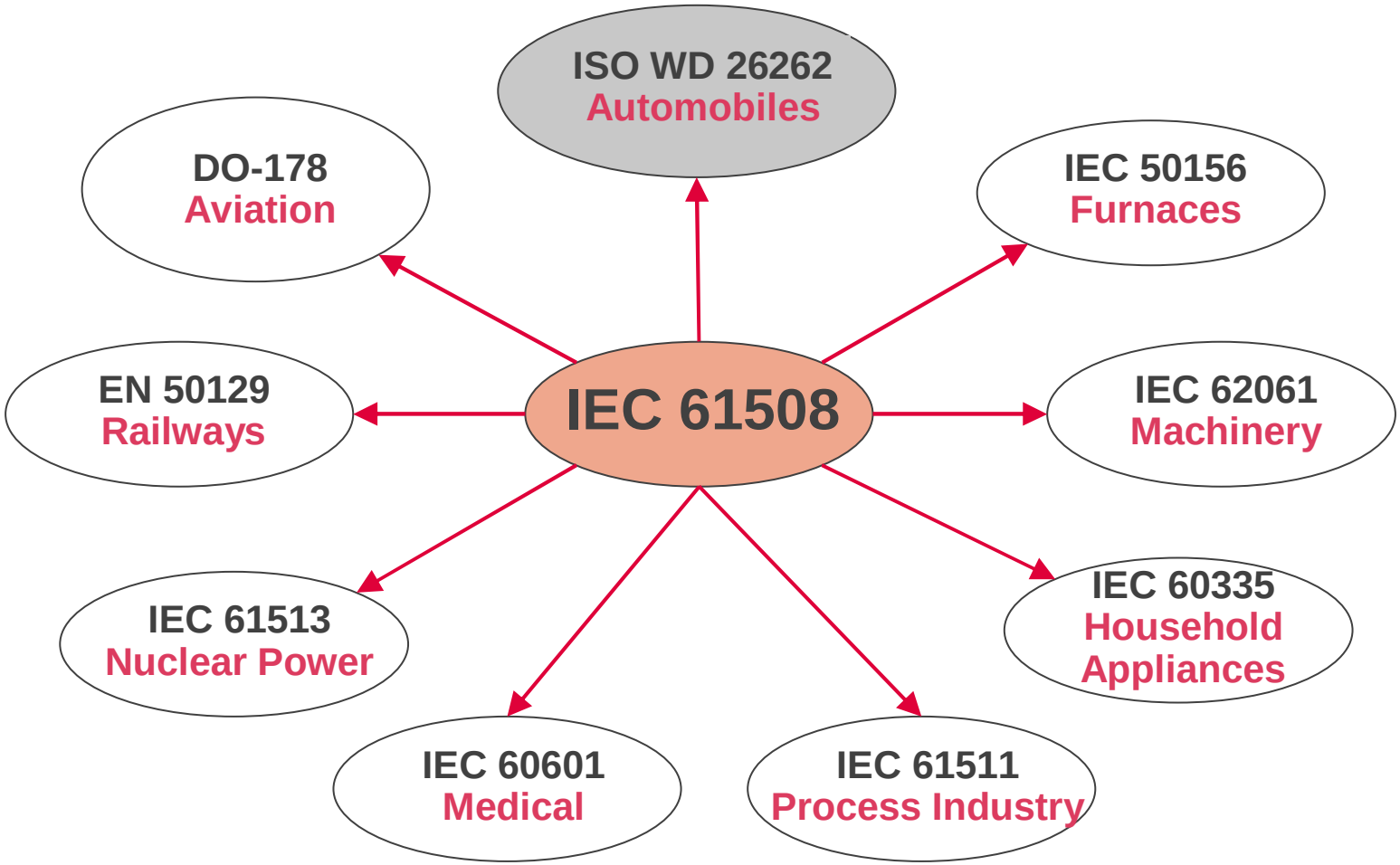
- the complexity of systems is increasing
- the work split in the industry is changing
- engineering deadlines and budgets are continuously under pressure
- software drives functionality more and more
- the perception of “tolerable risk” in society itself is changing
- …

The answer to the question “Is a system safe?” is not always obvious and not necessarily easy to answer

Definitions

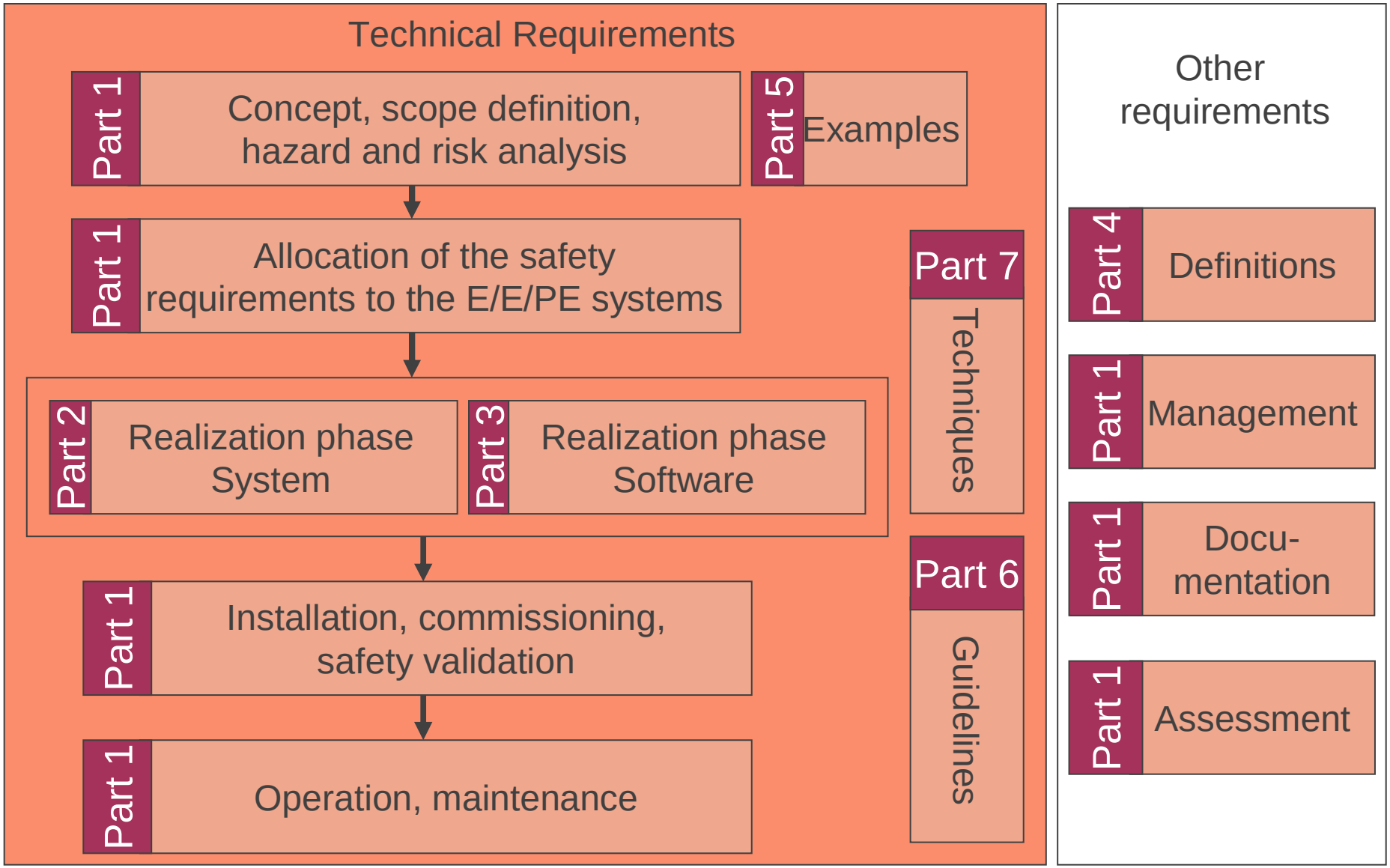
harm	physical injury or damage to the health of people either directly or indirectly as a result of damage to property or to the environment
hazard	potential source of harm
hazardous event	hazardous situation which results in harm
risk	combination of the probability of occurrence of harm and the severity of that harm
tolerable risk	risk which is accepted in a given context based on the current values of society
safety	freedom from unacceptable risk

Standards related to Functional Safety



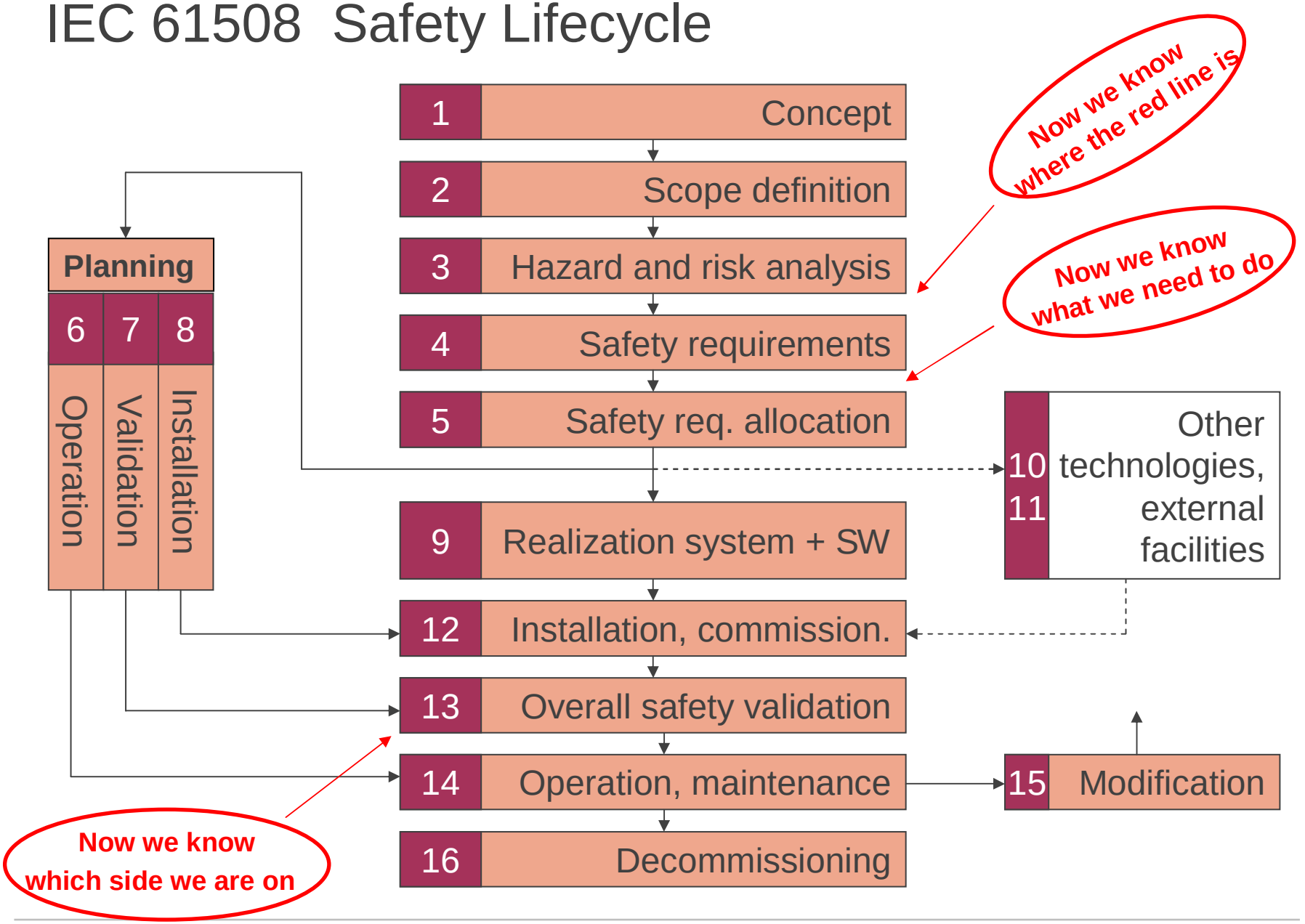
KUGLER MAAG CIE

Overall Framework of IEC 61508



KUGLER MAAG CIE

IEC 61508 Safety Lifecycle



KUGLER MAAG CIE

Functional Safety - Safety Integrity Level (SIL)

Probability of failure (with regards to the safety function)

(cf. IEC 61508-1 tables 2&3)

- determined by the required Safety Integrity Level (SIL) and the mode of operation
- Covers Hardware failures only

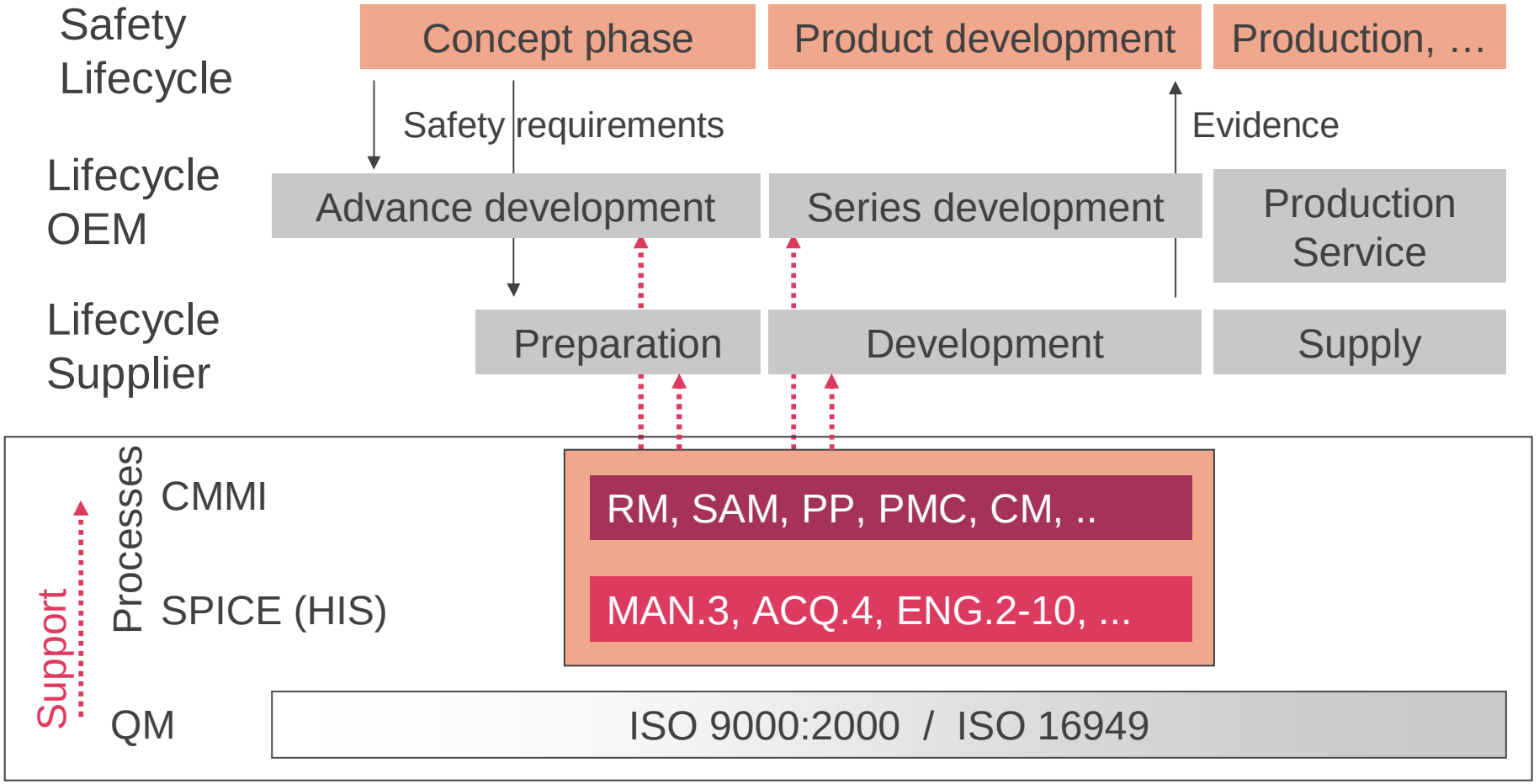
SIL	"low demand": Probability of failure on demand **PFD**	"high demand": Probability of failure per hour **PFH**
1	$< 10^{-1}$	$< 10^{-5}$ /h = 10.000 Fit
2	$< 10^{-2}$	$< 10^{-6}$ /h = 1000 Fit
3	$< 10^{-3}$	$< 10^{-7}$ /h = 100 Fit
4	$< 10^{-4}$	$< 10^{-8}$ /h = 10 Fit

Focus of Process Maturity Models

They

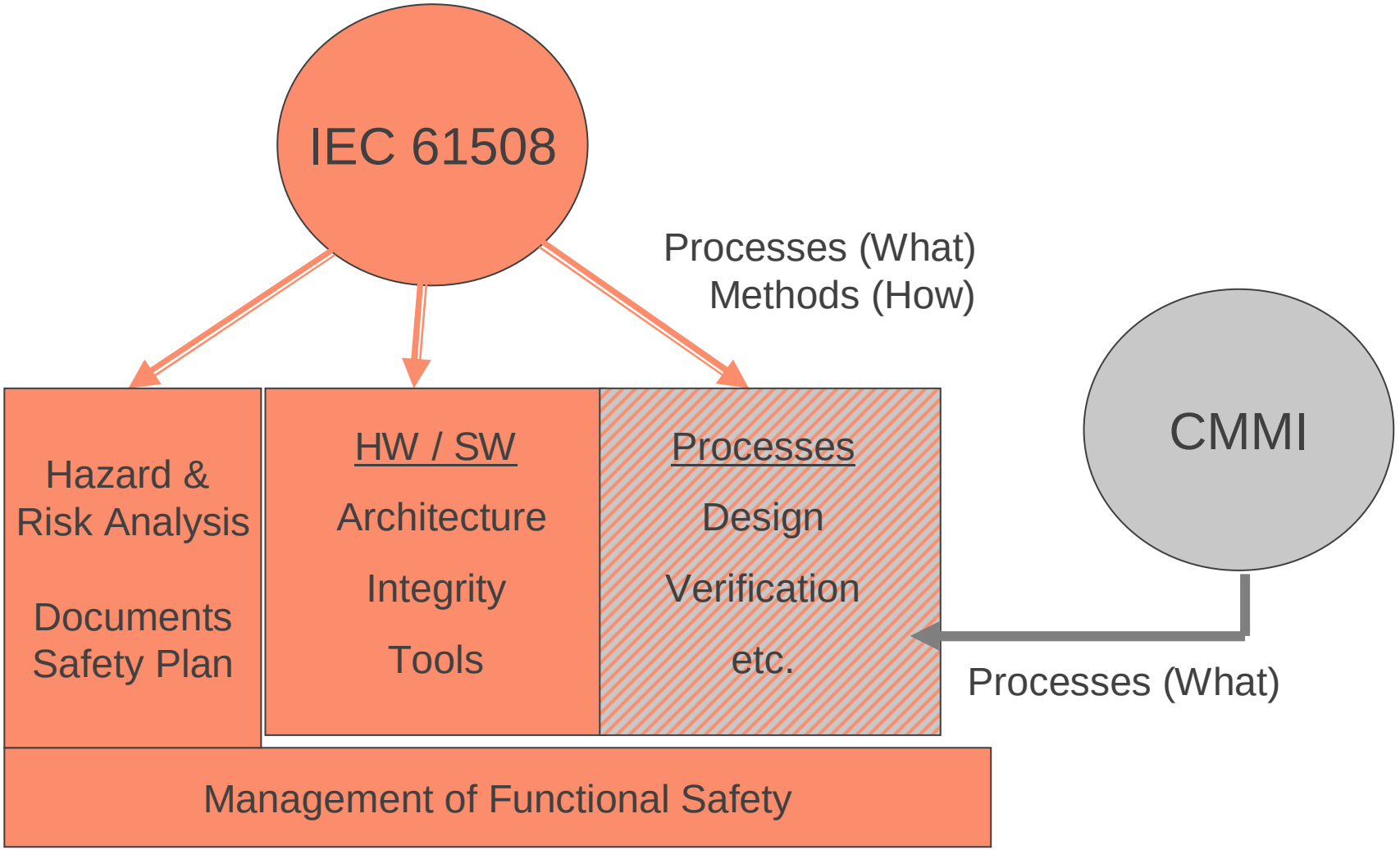
- describe best practices of organizations
- support assessments for determining strengths and weaknesses of processes in an organization or project
- support process improvements by implementing best practices step by step
- Process models define requirements with regard to the activities of the respective processes

The Standards on Functional Safety support the whole Product Lifecycle – Example: The Automotive Industry



KUGLER MAAG CIE

Standards on Functional Safety define Processes, Methods, Architectural Constraints, and Organizational Aspects



KUGLER MAAG CIE

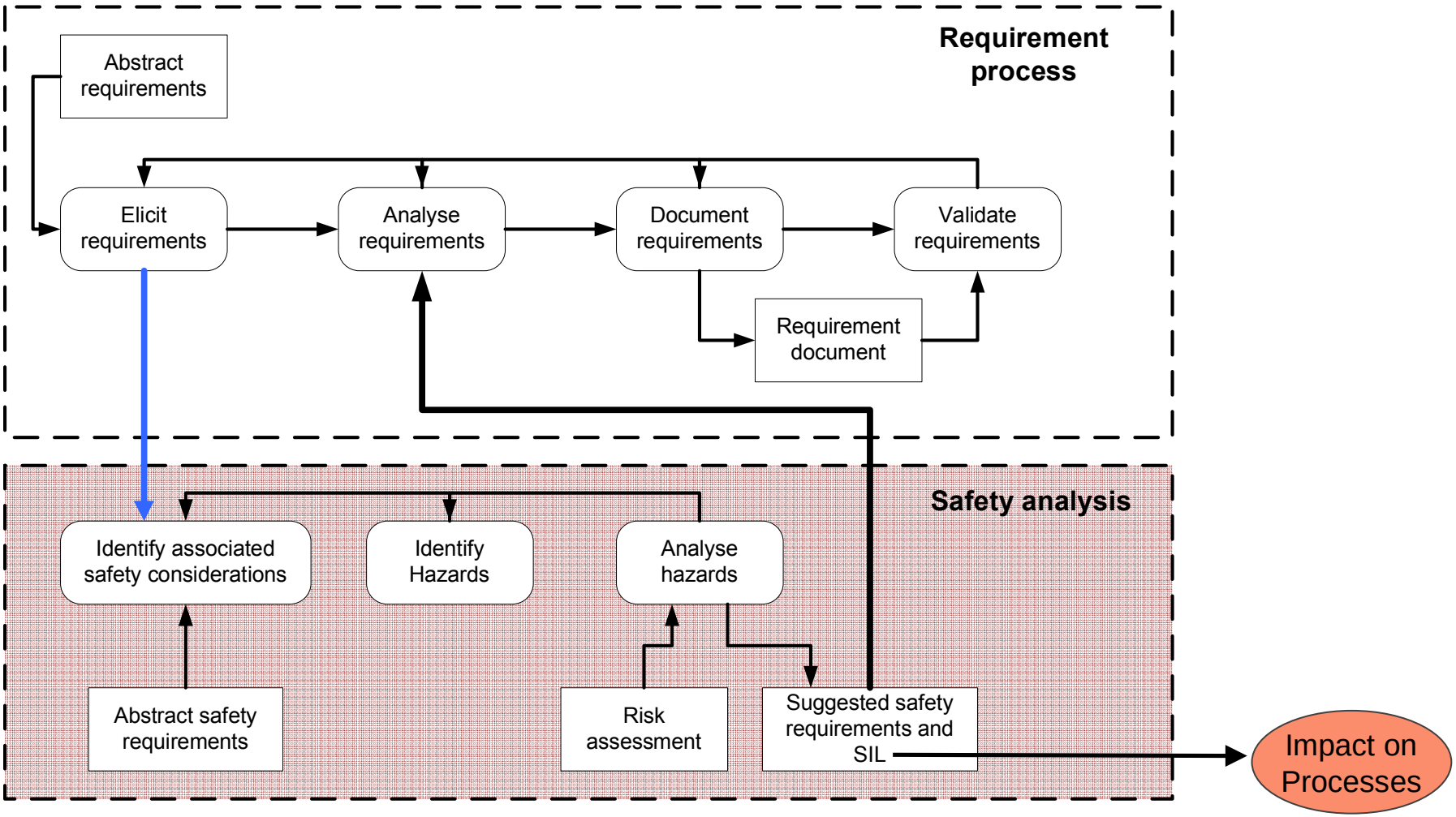
Functional Safety compared to CMMI - Overview

Impact on	Functional Safety	CMMI
Processes	All processes directly and indirectly supporting the development and operation of a device or system including methods to be applied	Main focus is on engineering and management processes
Product Lifecycle	Whole product lifecycle from the first idea until decommissioning	Mainly the engineering phase of the product lifecycle
Product	Mainly architecture (SW, HW)	Not addressed by CMMI
Organization	All organizational units and organizations involved in product development and operation	Main focus is on the engineering organizational unit

Functional Safety impacts Processes and the Organization – Examples

- The Hazard and Risk Analysis impacts architecture and processes
- Decision tables put constraints on the technical solution and the implementation
- Organizational requirements need to be met

The Safety Analysis (Hazard and Risk Analysis) impacts Architecture and Processes



KUGLER MAAG CIE

Decision Tables put Constraints on the Technical Solution and the Implementation

i.e.

Technique/Measure	SIL1	SIL2	SIL3	SIL4
1 Fault detection and diagnosis	---	R	HR	HR
2 Error detecting and correcting codes	R	R	R	HR
3a Failure assertion programming	R	R	R	HR
3b Safety bag techniques	---	R	R	R
3c Diverse programming	R	R	R	HR
3d Recovery block	R	R	R	R
3e Backward recovery	R	R	R	R
3f Forward recovery	R	R	R	R
3g Re-try fault recovery mechanisms	R	R	R	HR
3h Memorising executed cases	---	R	R	HR
4 Graceful degradation	R	R	HR	HR
5 Artificial intelligence - fault correction	---	NR	NR	NR
6 Dynamic reconfiguration	---	NR	NR	NR
7 Defensive programming	---	R	HR	HR

Details to all techniques in part IEC61508 Part 7!

Decision Tables put Constraints on the Technical Solution and the Implementation (cont.)

Design and Coding Standards

Cf. part 3 table B.1 (extract)

Safety Integrity Level

Technique / Measure	SIL1	SIL2	SIL3	SIL4
Limited use of pointers	o	+	++	++
Limited use of interrupts	+	+	++	++
No dynamic variable	o	+	++	++
Online checking of the installation of dynamic variables	o	+	++	++

++ mandatory
+ recommended
o no recommendation
options

KUGLER MAAG CIE

Organizational Requirements need to be met

Part 2-4: Overall project independent safety management

4.4 Requirements

4.4.1 Safety culture

4.4.2 Quality management

4.4.3 Continuous improvement

4.4.4 Training and qualification

4.4.5 Application of the lifecycle

Applies to ASIL A, B, C, D: Following the item definition according to WD 26262-3, clause 4, a decision is then required according to WD 26262-3, clause 5 "Initiation of the safety lifecycle", on which phases of the safety lifecycle shall be carried out.

4.4.6 Allocation of safety responsibility and duties

a. A project leader shall be appointed at the beginning of the project, who is responsible for ensuring functional safety.

b. The project leader should appoint a person to fill in the roll of safety manager responsible for functional safety management tasks.

c. The project manager shall ensure that the safety activities are carried out.

d. Communication and decision-making paths shall be defined for the implementation of planned activities to ensure functional safety and eliminate safety shortcomings.

e. Safety responsibilities shall be allocated such that the qualifications (see Annex A, Table A.1) and competencies (see Annex A, Table A.2) of the persons and organisations responsible for the tasks are sufficient and this shall be documented as described in 4.4.4

Source: ISO TC22 SC3 WG16 Functional Safety, Convenor Ch. Jung, Introduction in ISO WD 26262, 6.12.2006, Page 21ff, (EUROFORM-Seminar April 2007)

CMMI supports the Implementation of Functional Safety

- Organization Process Definition supports the management of processes supporting different SILs
  - OPD – SP 1.2 “Establish and maintain descriptions of the lifecycle models approved for use in the organization”
  - OPD – SP 1.3 “Establish and maintain tailoring criteria and guidelines for the organization’s set of standard processes”
- Maintaining the Safety Case
  - The safety case is the set of information / documents that contains sufficient information to provide evidence that all safety requirements are satisfied
  - GP 2.6 “Place designated work products under appropriate levels of control” clearly supports the management of the safety case
  - Obviously the process area “Configuration Management”

CMMI supports the Implementation of Functional Safety (cont.)

- Generic Practices in general strongly facilitate the implementation of functional safety - especially regarding organizational aspects like
  - Safety Culture
  - Quality Management
  - Continuous Improvement
  - Training and Qualification
  - ...

Standards on Functional Safety have a different Focus than Process Models like CMMI

Impact on	Functional Safety	CMMI
Processes	All processes directly and indirectly supporting the development and operation of a device or system including methods to be applied	Main focus is on engineering and management processes
Product Lifecycle	Whole product lifecycle from the first idea until decommissioning	Mainly the engineering phase of the product lifecycle
Product	Mainly architecture (SW, HW)	Not addressed by CMMI
Organization	All organizational units and organizations involved in product development and operation	Main focus is on the engineering organizational unit

Summary

- Standards on functional safety become more and more important in industries (embedded software)
- Established and active CMMI Level 3 environments facilitate an efficient implementation of standards on functional safety
- Functional safety addresses more than engineering. However, an active and alive CMMI culture strongly facilitates implementation of such standards even outside engineering

Any Questions?

Thank you

If you want to contact us

in USA

Mike Staszel
456 Berkley Street
48124 Dearborn, MI
USA
mike.staszel@kuglermaag.com

in Germany

Bonifaz Maag
Leibnizstrasse 11
70806 Kornwestheim
Germany
bonifaz.maag@kuglermaag.com