

Finding the right software tools for functional safety projects

Development support tools in functional safety projects

16 January 2018



**Choose certainty.
Add value.**



Dr. Thomas Maier

Business Development Manager at TÜV SÜD Rail since July 2016

Background:

- 6 years at UL, principal engineer for functional safety
- 8 years with Danfoss Drives, functional safety in motion control.
- 3 years at LM Ericsson A/S: software processes and tools, CMMi, UML and SDL.
- 3 years at Daimler-Benz: system safety and functional safety of drive-by-wire systems and in avionics.
- 4 years at the Joint Research Centre of the European Commission: system & software safety in fusion technology.
- International standardization (ISO 26262, ISO 13849 & IEC 62061, IEC 61800-5-2, IEC 61508 maintenance, UL 1998).
- Dr.-Ing. from University of Stuttgart



1 Functional Safety: Principles, Concepts, Standards

2 Role of software based development support tools

3 Generalised requirements on tools

4 Details of IEC 61508 – ISO 26262 – ISO 13849

5 Selection of tools – Certified tools

Where safety depends on embedded control functions



INDUSTRIAL AUTOMATION AND MACHINERY



RAILWAY ROLLING STOCK AND SIGNALLING



AUTOMOTIVE



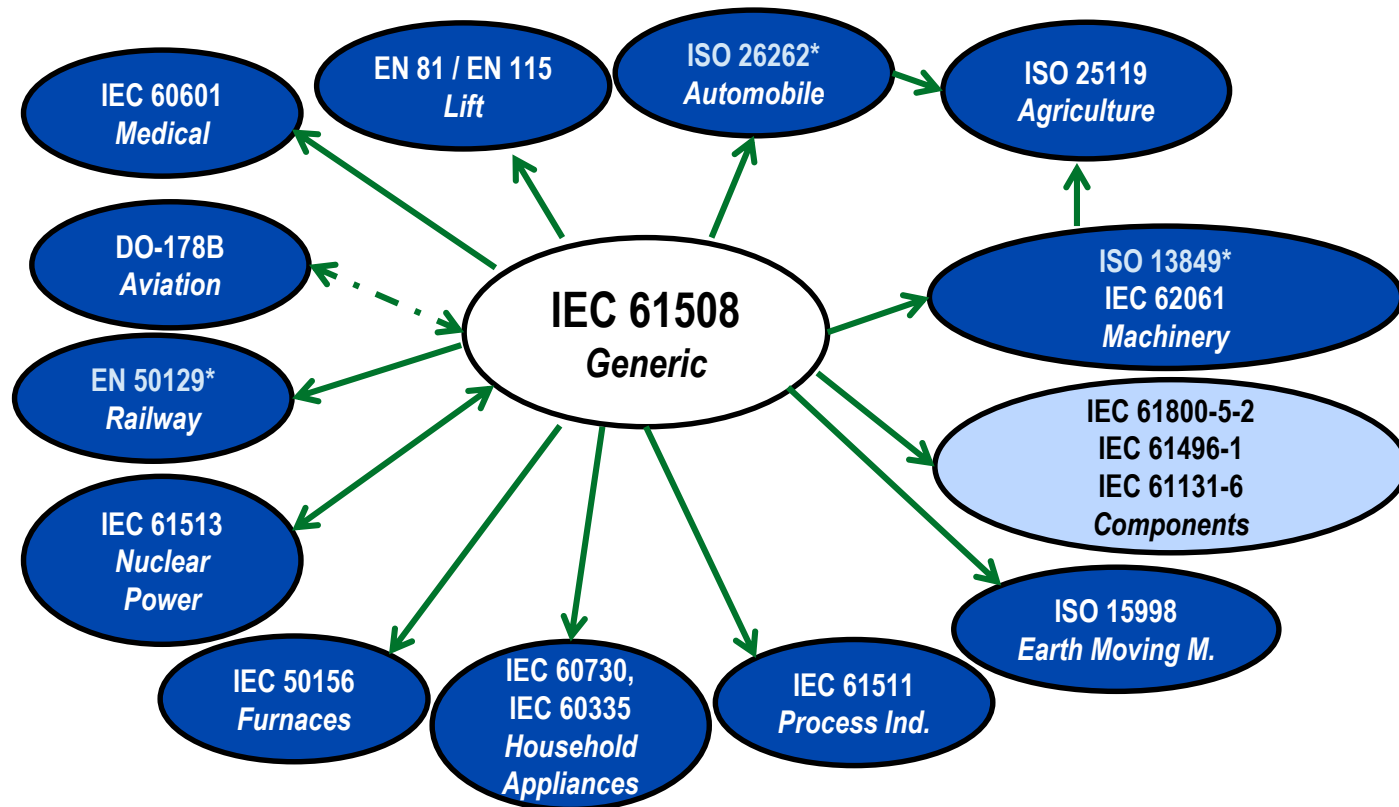
MEDICAL DEVICES



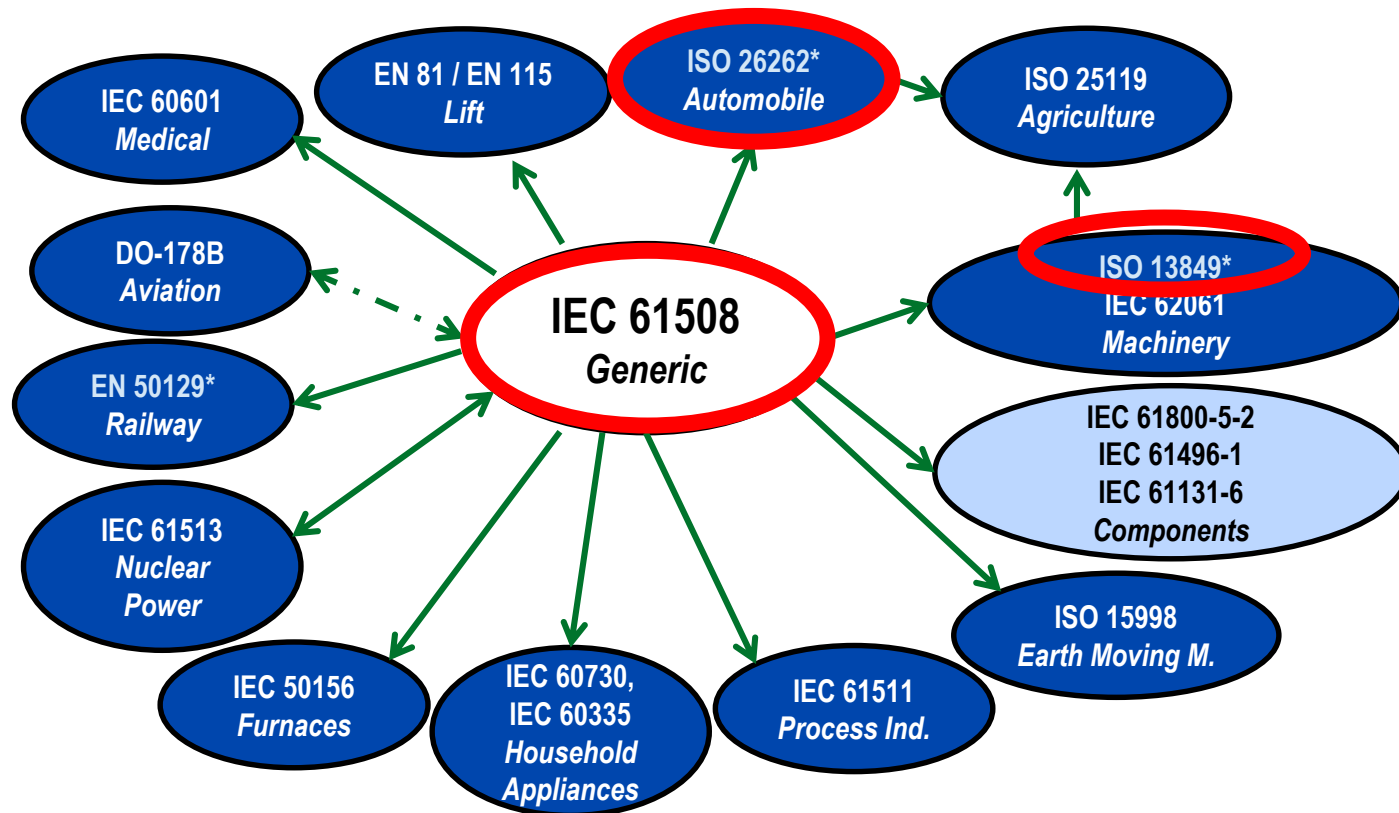
PROCESS INDUSTRY



ALTERNATIVE ENERGY



**Also applicable to generic safety components*



**Also applicable to generic safety components*

Risk-based

- Requires system approach
- Hazard identification and risk assessment

Management of functional safety

- Lifecycle
- Roles and organisation
 - Independence of assessors
- Supplier management

Address hardware random failures

- Architecture and failure control
 - Redundancy and diversity
 - Diagnostics
- Reliability and failure exclusion

Address software-related ("systematic") failures

- Fault avoidance
 - Modular design
 - Processes, methods, tools
 - Quality assurance

Risk-based

- Requires system approach
- Hazard identification and risk assessment

Management of functional safety

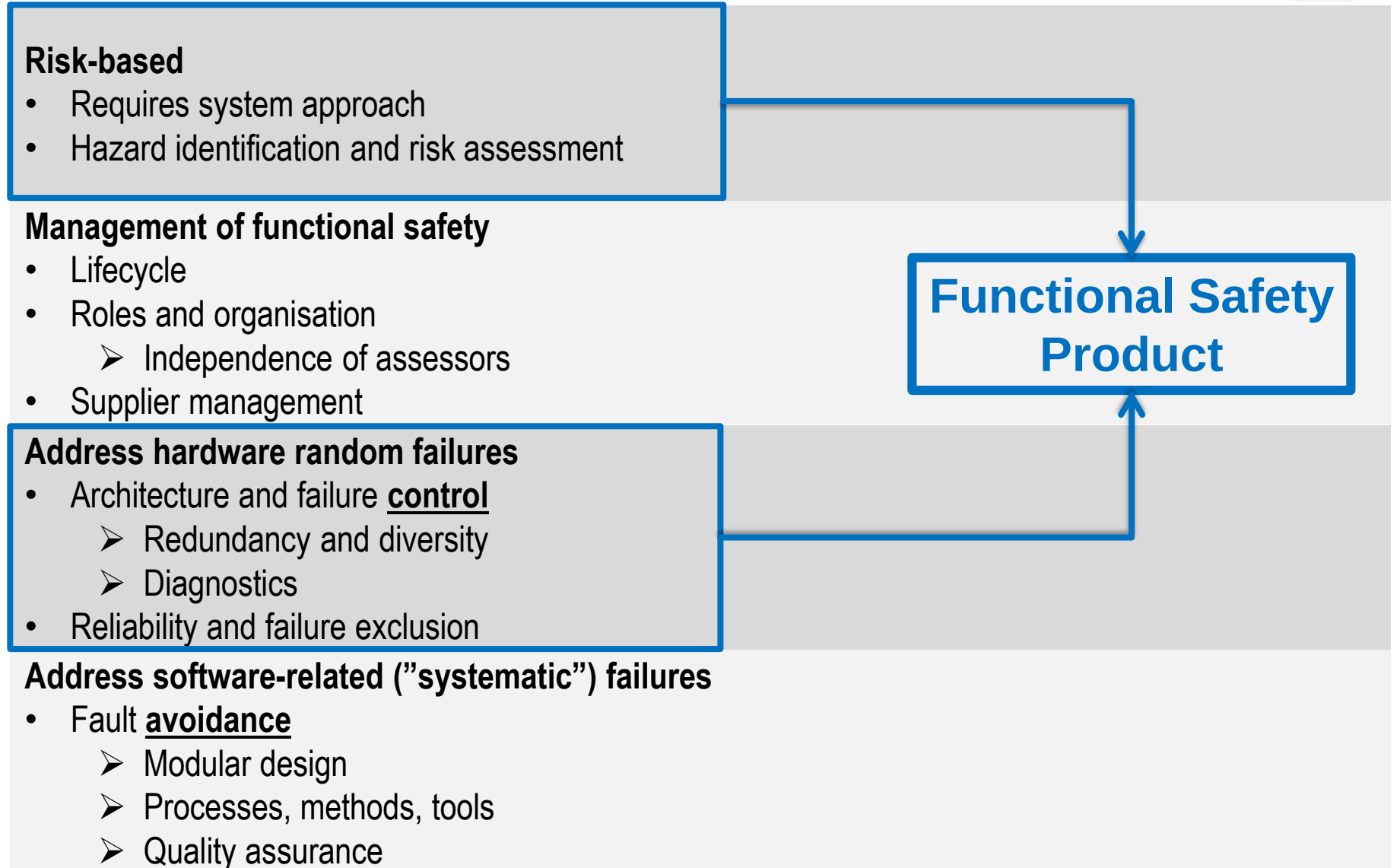
- Lifecycle
- Roles and organisation
 - Independence of assessors
- Supplier management

Address hardware random failures

- Architecture and failure control
 - Redundancy and diversity
 - Diagnostics
- Reliability and failure exclusion

Address software-related ("systematic") failures

- Fault avoidance
 - Modular design
 - Processes, methods, tools
 - Quality assurance



**Functional Safety
Product**

Risk-based

- Requires system approach
- Hazard identification and risk assessment

Management of functional safety

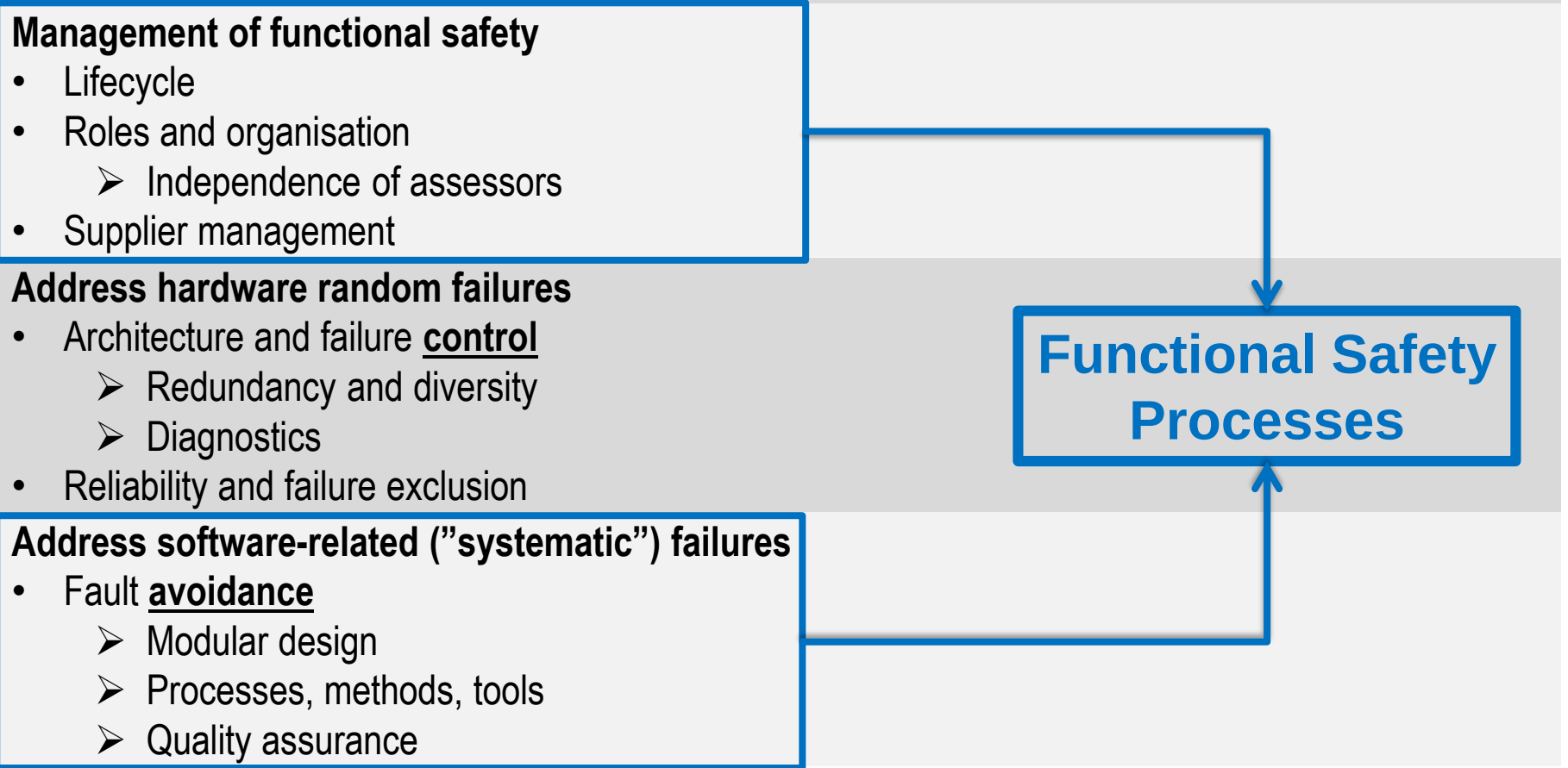
- Lifecycle
- Roles and organisation
 - Independence of assessors
- Supplier management

Address hardware random failures

- Architecture and failure control
 - Redundancy and diversity
 - Diagnostics
- Reliability and failure exclusion

Address software-related ("systematic") failures

- Fault avoidance
 - Modular design
 - Processes, methods, tools
 - Quality assurance



**Functional Safety
Processes**

Risk-based

- Requires system approach
- Hazard identification and risk assessment

Management of functional safety

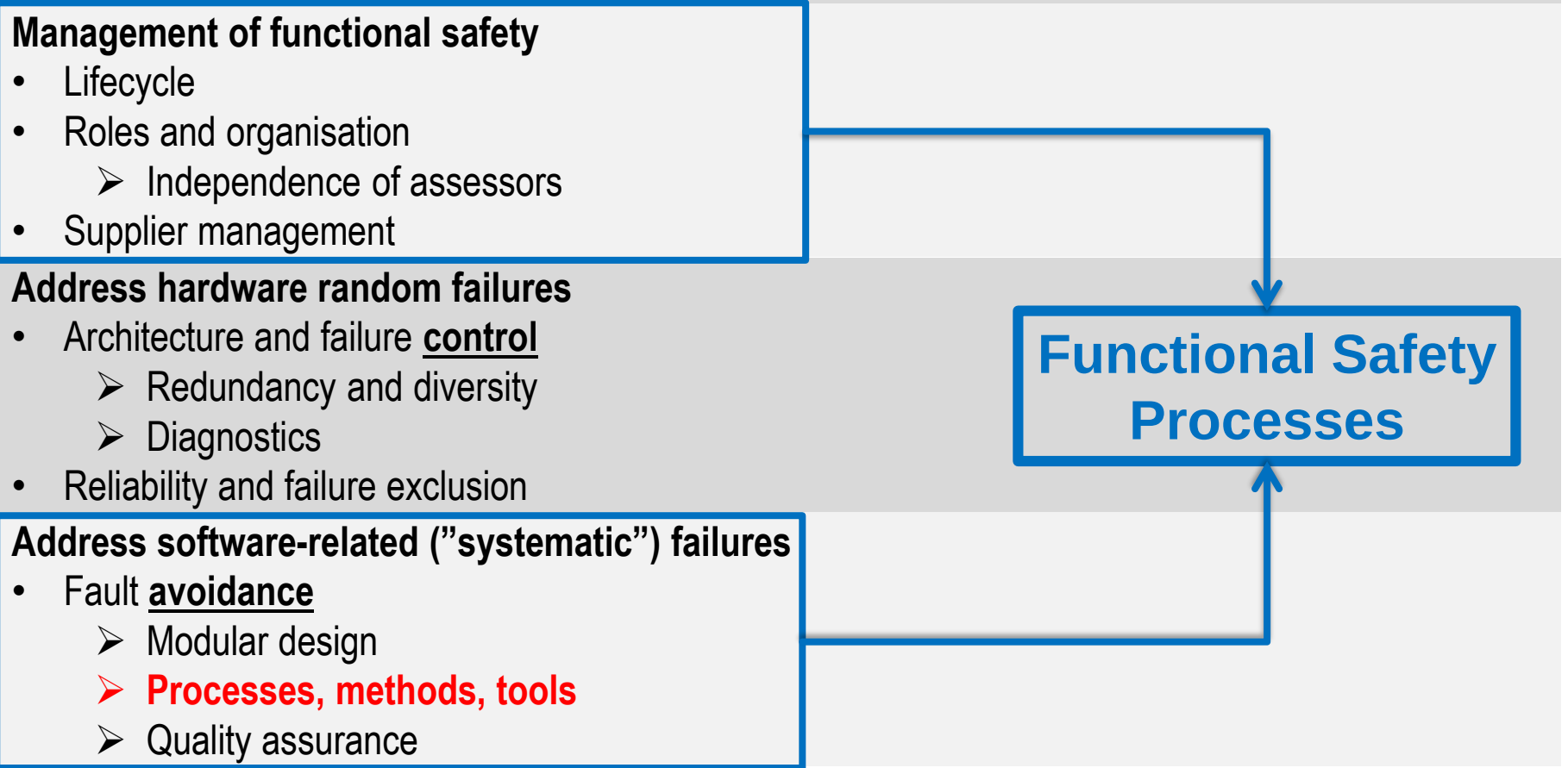
- Lifecycle
- Roles and organisation
 - Independence of assessors
- Supplier management

Address hardware random failures

- Architecture and failure control
 - Redundancy and diversity
 - Diagnostics
- Reliability and failure exclusion

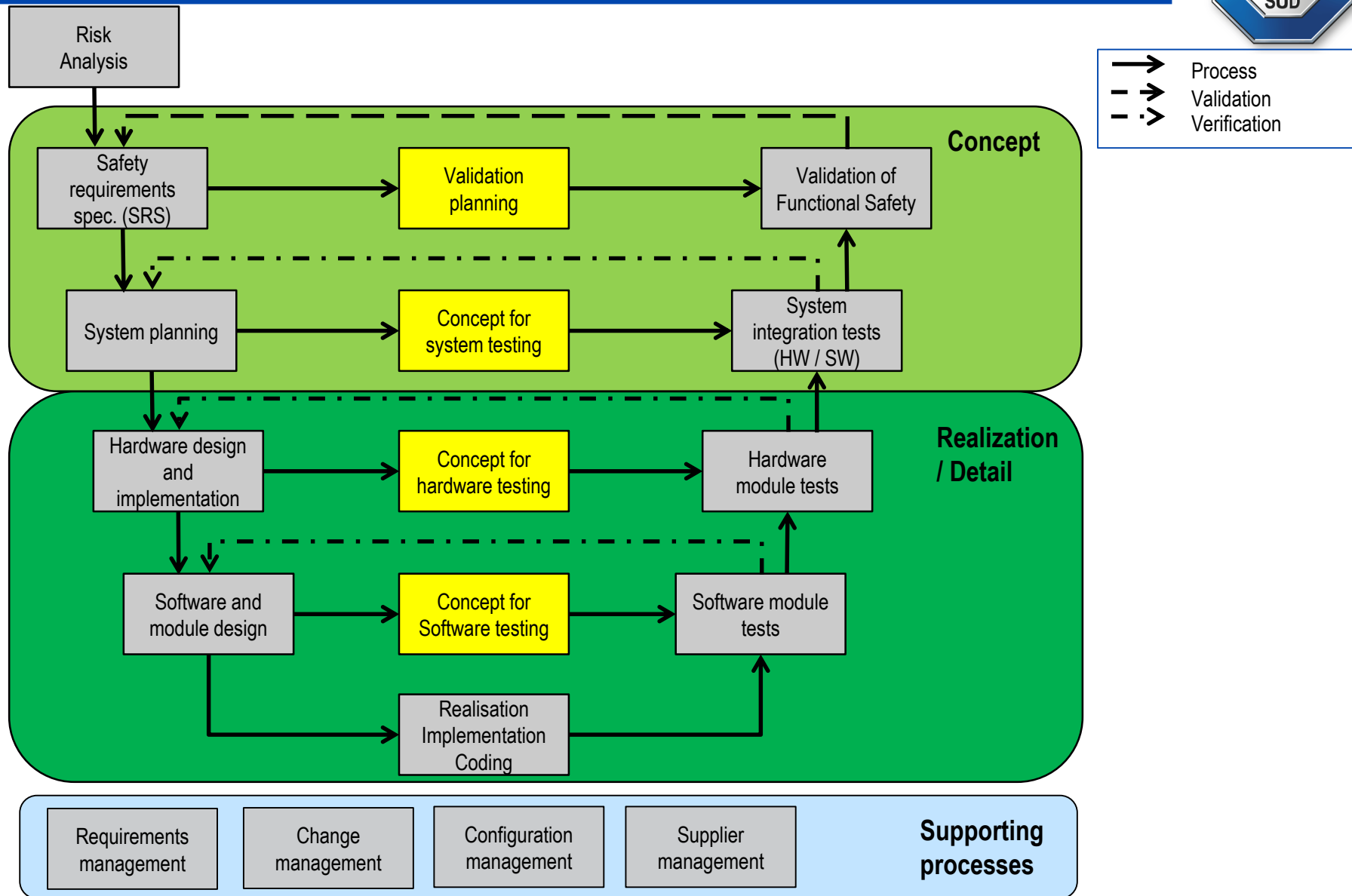
Address software-related ("systematic") failures

- Fault avoidance
 - Modular design
 - **Processes, methods, tools**
 - Quality assurance

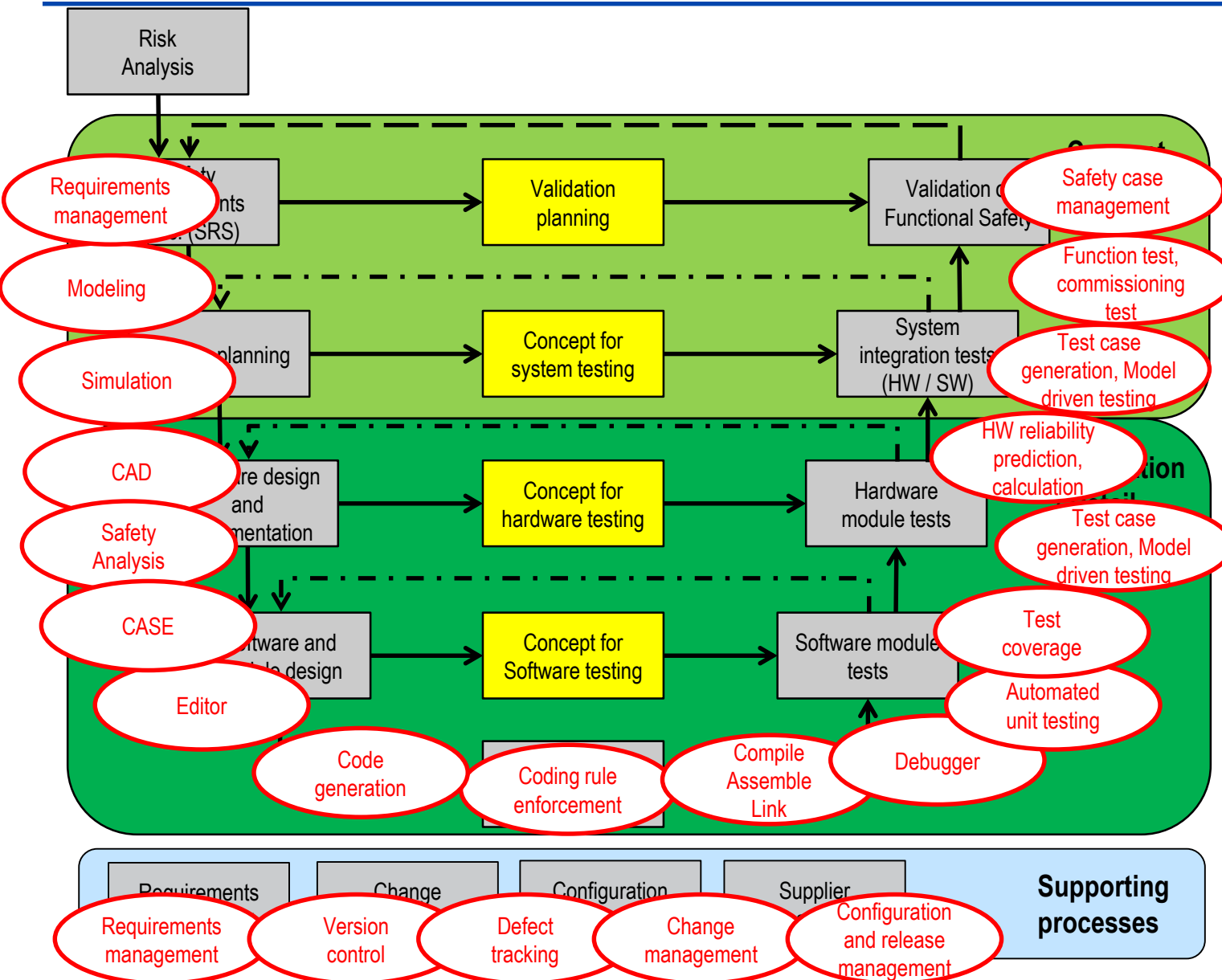


**Functional Safety
Processes**

Safety Development Life Cycle (Condensed and generalised for different standards)



Use of tools



Standards generally recommend tool support to minimize human error.

For higher safety integrity levels, specific tool support is required, e.g. CASE tools in SW Design.

But of course: Tools have failure modes, too!

(Condensed and generalised for different standards)

- All tools (planned to be) used in a functional safety project shall be listed and described (for example in the Safety Plan)
 - In terms of role in development process, use cases, and integration with other tools
 - Also MS Word, Visio, scripts, bridges, Excel applications, ...
- All tools shall be classified in accordance to their criticality for the system to be developed
 - Ideally in a systematic manner, e.g. by HazOp or functional FMEA, identifying
 - Impact of a tool malfunction on product to be developed
 - Likelihood of detection or mitigation of a malfunction before it causes a fault in the final product.
- Tools are qualified in accordance with criticality
- Tools are configuration items, e.g. subject to configuration management

Offline tools, 3 classes (IEC 61508-4, 3.2.11)

- T1** generates no outputs which can directly or indirectly contribute to the executable code
(e.g. text editor, design describing tool, ...)
- T2** errors in the tool can fail to reveal defects but cannot directly create errors in the executable software
(e.g. test generator, test coverage tool, static analysis tool, ...)
- T3** can directly or indirectly contribute to the executable code
(e.g. code generator, optimizing compiler, linker, ...)

T2 and T3

- Specification or product description, clearly defining behavior, use instructions and constraints
- Avoidance, detection, mitigation measures for tools failure mechanisms

T3 in addition

- Evidence that tool conforms to its specification or documentation
 - Validation
 - Chronological records of validation activities
 - Version of tool and product documentation
 - Validation scope, test cases, equipment, results
 - Discrepancies (resulting in additional instructions and constraints)
 - Operational history (similar application, version history should be considered)

Configuration management

- Tool and documentation
- Qualification evidence

- **For Performance Levels c and d:** “use of suitable programming languages and computer-based tools with confidence from use”
 - No further requirements or guidance on what confidence from use means
- **For Performance Level e:** IEC 61508-3 Clause 7 for SIL 3 applies, thus also tool qualification as detailed on previous slides.
- ISO 13849 is primarily an application level standard. It has detailed requirements for parameterization or customization tools in terms of functionality and usage procedure. (see ISO 13849-1, clause 4.6.4 Software-based parameterization)

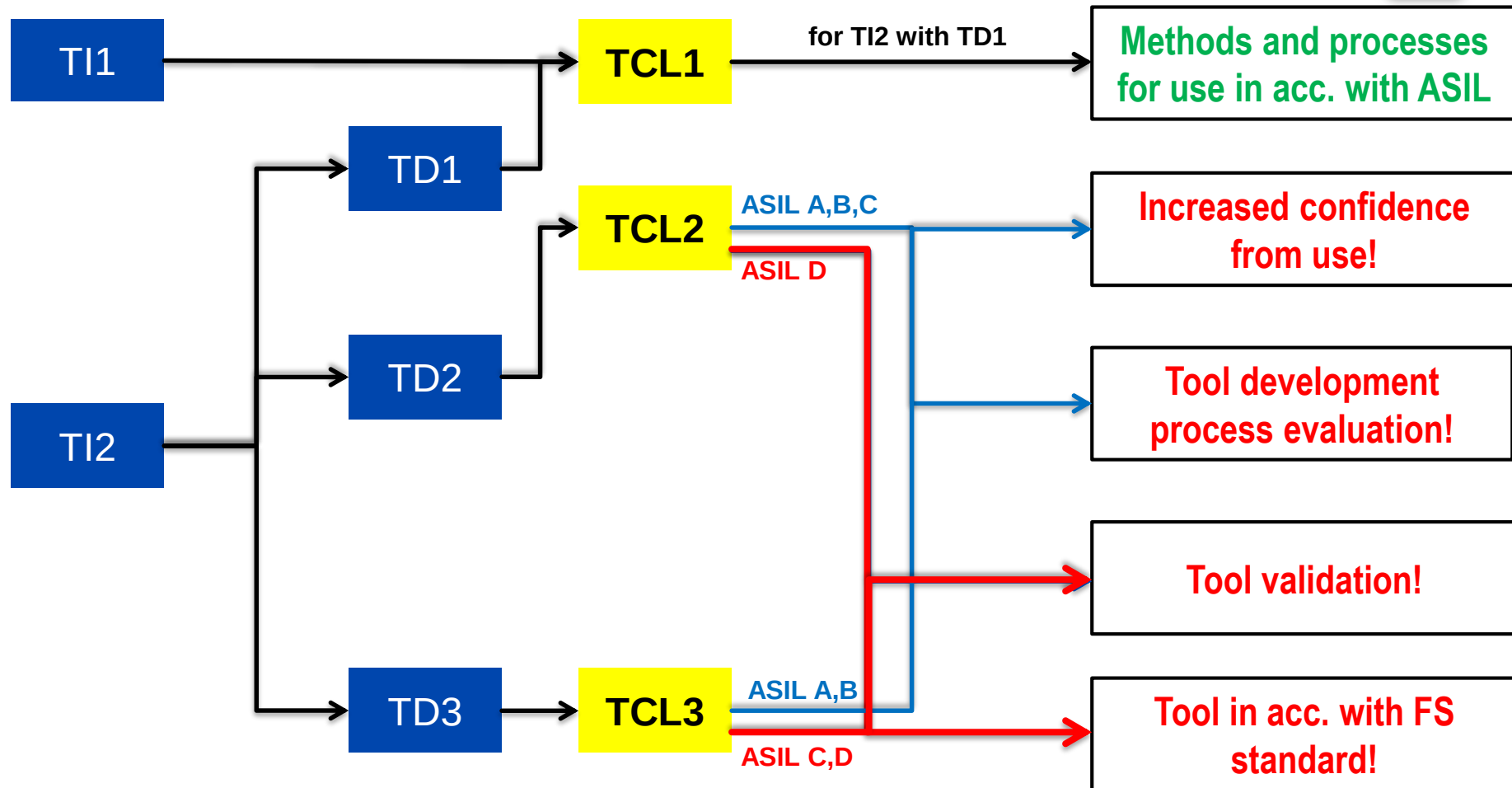
The two aspects **impact** and error **detection**/mitigation are reflected by dedicated parameters:

TI (Tool Impact)

- **TI1:** a failure of this tool has no impact on the safety relevant items (no introduction of failure or failure to detect errors is possible)
- **TI2:** all the other cases

TD (Tool Error Detection)

- **TD1:** high degree of confidence that a failure of tool or related output failure is detected
- **TD2:** medium degree of confidence that a failure of tool or related output failure is detected
- **TD3:** all other cases

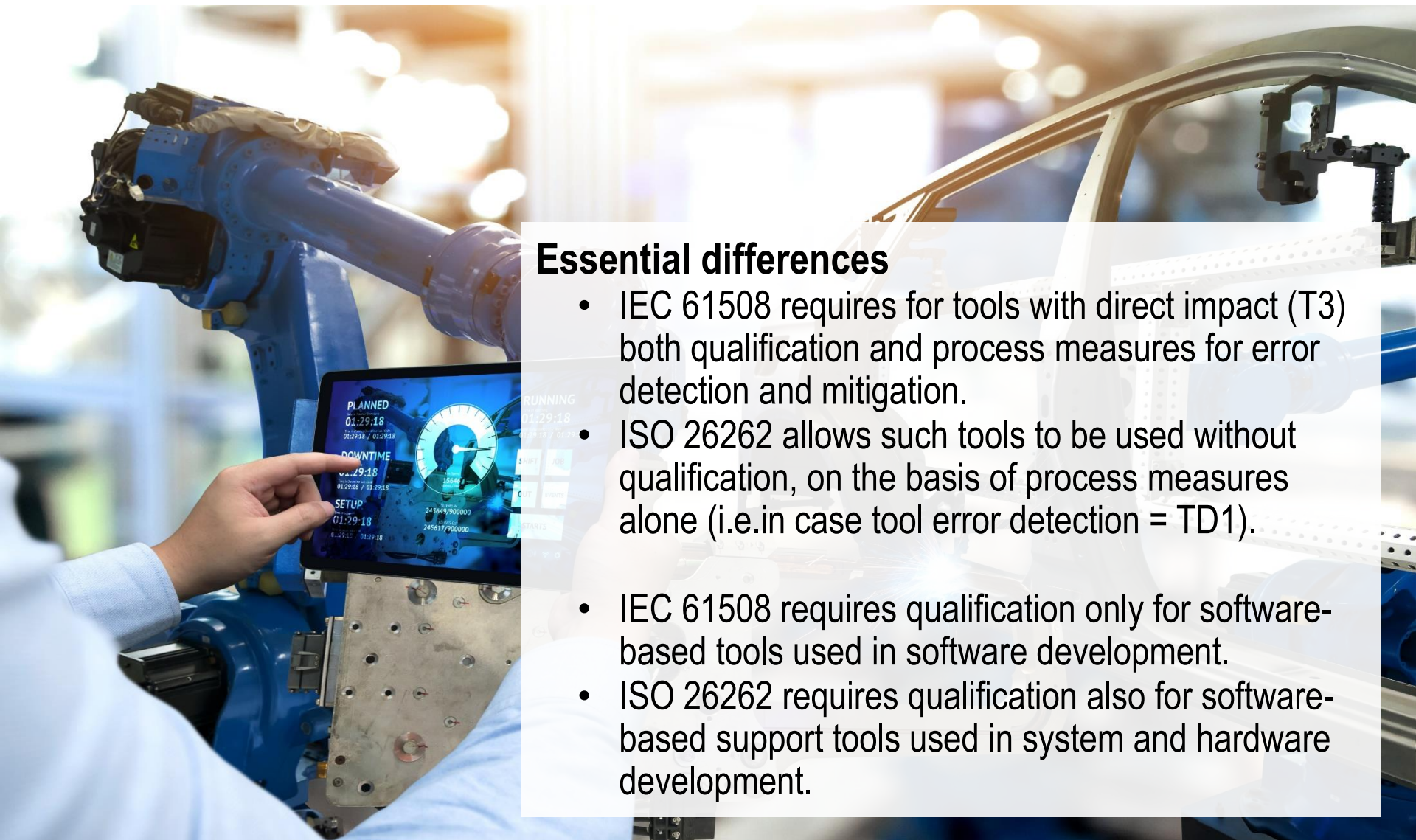


Determine possibility
that an error is
introduced or not
detected by tool

Determine confidence in
measures for prevention
and detection of
malfunctions

Determine
maximally required
ASIL

Qualify SW tool, or
methods & processes
("workflow" for the
SW tool)



Essential differences

- IEC 61508 requires for tools with direct impact (T3) both qualification and process measures for error detection and mitigation.
- ISO 26262 allows such tools to be used without qualification, on the basis of process measures alone (i.e. in case tool error detection = TD1).
- IEC 61508 requires qualification only for software-based tools used in software development.
- ISO 26262 requires qualification also for software-based support tools used in system and hardware development.

- While the standards include generic pre-qualification of tools, there is no requirement to select pre-qualified/certified tools. It is primarily assumed that appropriate qualification of tools is, and can be, done in a project.
- Tool qualification (e.g. validation) can however require significant effort. It may even require cooperation with the tool vendor
- **Why select a certified tool?**
 - Significantly reduced qualification effort
 - Instructions or workflow provided for functional safety compliant implementation and use
 - **But:** No formal definition of certification... What does tool certification mean then?
 - What does TÜV SÜD mean by tool certification?

Functional Safety Mark



TCL1 Certification



Which one is the best for your project?

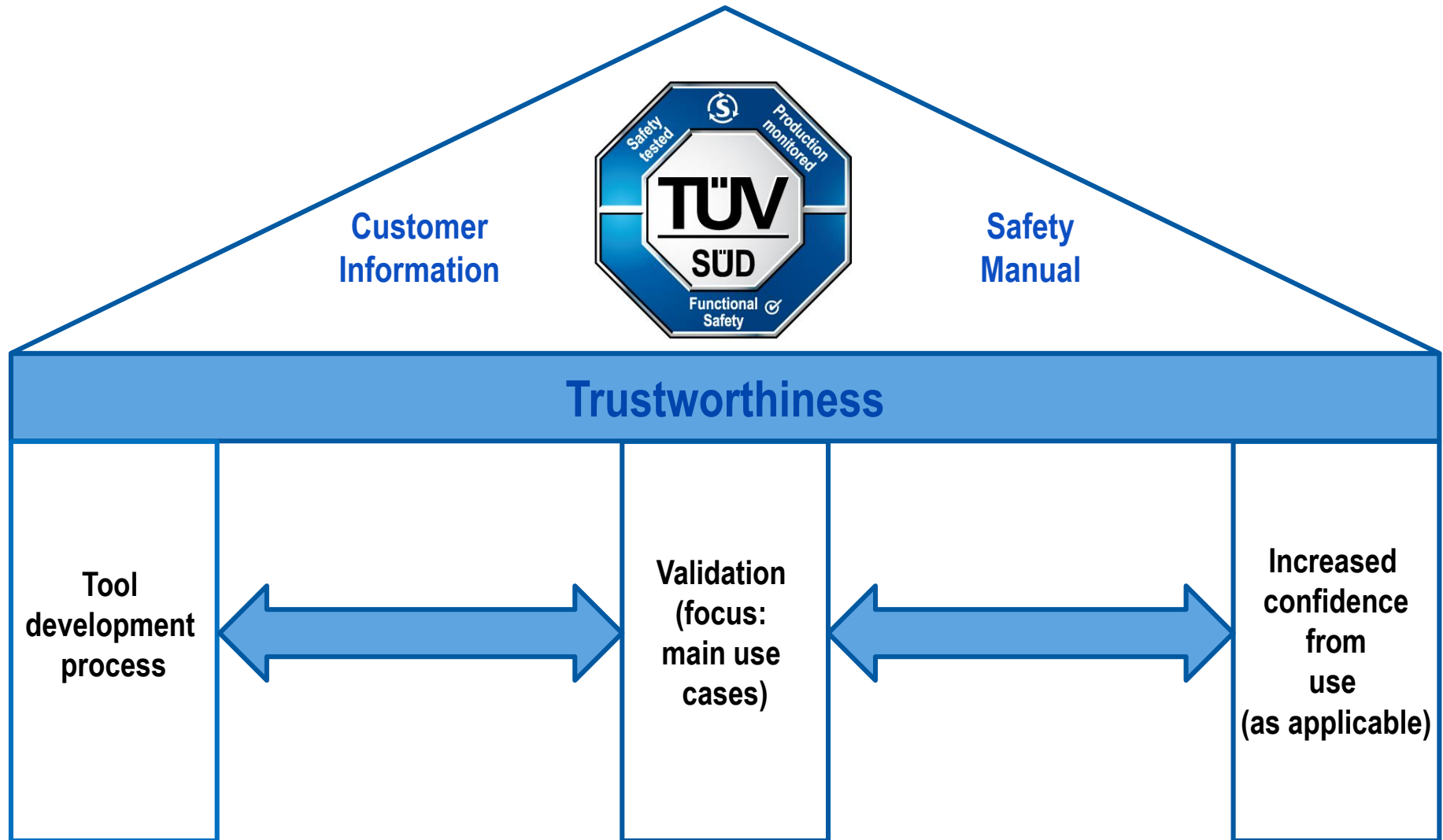
Functional Safety Mark



***Software Tools for Safety
Related Development***

TCL1 Certification





Functional Safety Mark



TCL1 Certification



***Software Tools for Safety
Related Development***



**Customer
Information**



**Safety
Manual**

Trustworthiness

Review of tool safety documentation

(safety analysis of tool impact and tool detection measures)

Functional Safety Mark



TCL1 Certification



- Wide scope (different standards, [A]SIL, Tx, TCLx, ...)
- For tools that may reduce V&V effort in product development
- 3rd party tool qualification

- Applicable for ISO 26262 only
- Tool automates a specific task, but full V&V effort in product development still required

For both options:

3rd party assessed tool documentation (use instructions, workflow descriptions)
facilitates compliance with functional safety management and process requirements



IEC 61508

- 3rd edition IEC 61508: Working groups are still at an early stage. Expectations:
 - Procedure uses two parameters (impact, detection/mitigation)
 - Tool qualification requirements extended to software-based tools in hardware development

ISO 26262

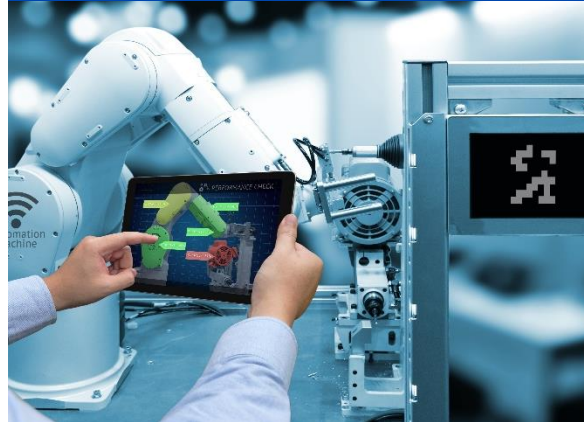
- 2nd edition of ISO 26262 to be published in 2018. No change to the procedure of 1st edition.

Register for our industry E-ssentials



- [Rail](#)
- [Automotive](#)
- [Consumer Products & Retail](#)
- [Healthcare & Medical Devices](#)
- [Chemical, Oil and Gas](#)
- [Power & Energy](#)
- [Real Estate & Infrastructure](#)

Download our Functional Safety White Paper



- Read more about [“Functional safety for a digital world - Smart solutions from chip design to whole system design”](#)

Find out more about our Functional Safety offers



- Learn more about our [Functional Safety services](#)
- Apply for one of our [Functional Safety trainings](#)

Thank you for your participation and attention!

Your questions and comments are welcome:

Dr.-Ing. Thomas Maier
TÜV SÜD America
10040 Mesa Rim Road
San Diego, CA 92121
Phone: +1 858-220-0783
E-mail: tmaier@tuvam.com



**Choose certainty.
Add value.**