

Lean Standard Development Processes – How to Do Without Extra Safety Plans, Confirmation Reviews, and Safety Audits

Pierre Metz, Brose Fahrzeugteile GmbH &
Co. KG, Bamberg

**Int. IQPC ISO 26262 Conference,
March, 2017, Frankfurt**

A 3D graphic of a light blue rectangular block with a dark blue top edge. On the front face of the block, the word "brose" is written in a large, bold, red, sans-serif font. Below it, the phrase "Technik für Automobile" is written in a smaller, red, sans-serif font, angled slightly upwards to the right.

brose
Technik für Automobile

Product range

Mechatronic Systems and Drives for Automobiles



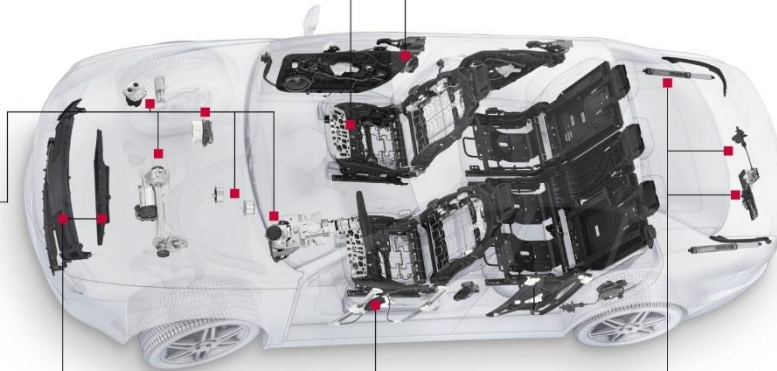
Structures and components for vehicle seats



Systems and components for vehicle doors



Electric motors and drives



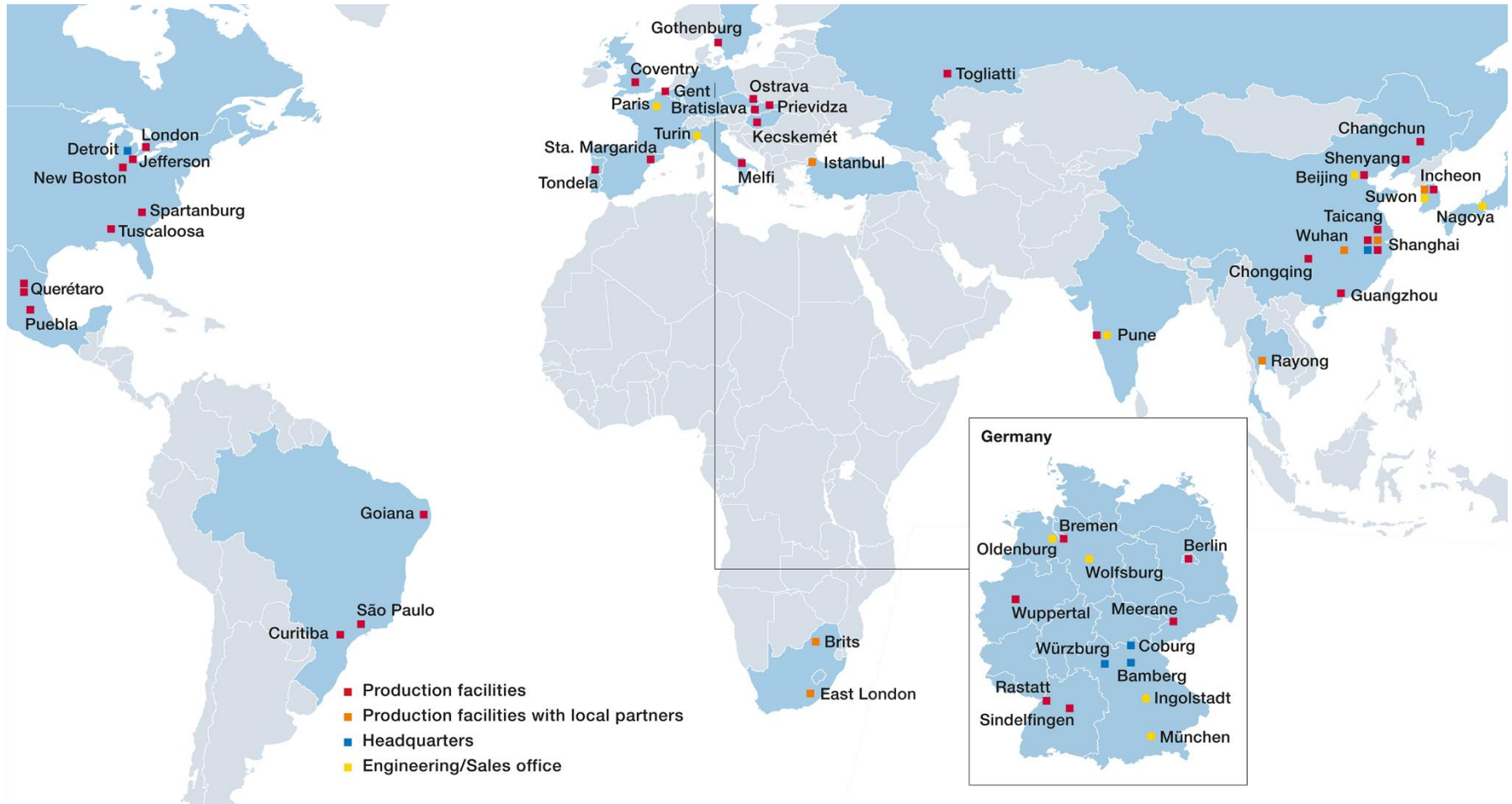
Motor cooling systems



Liftgates and closure systems

Global presence

60 locations, 23 countries, 5 continents, almost 25,000 employees



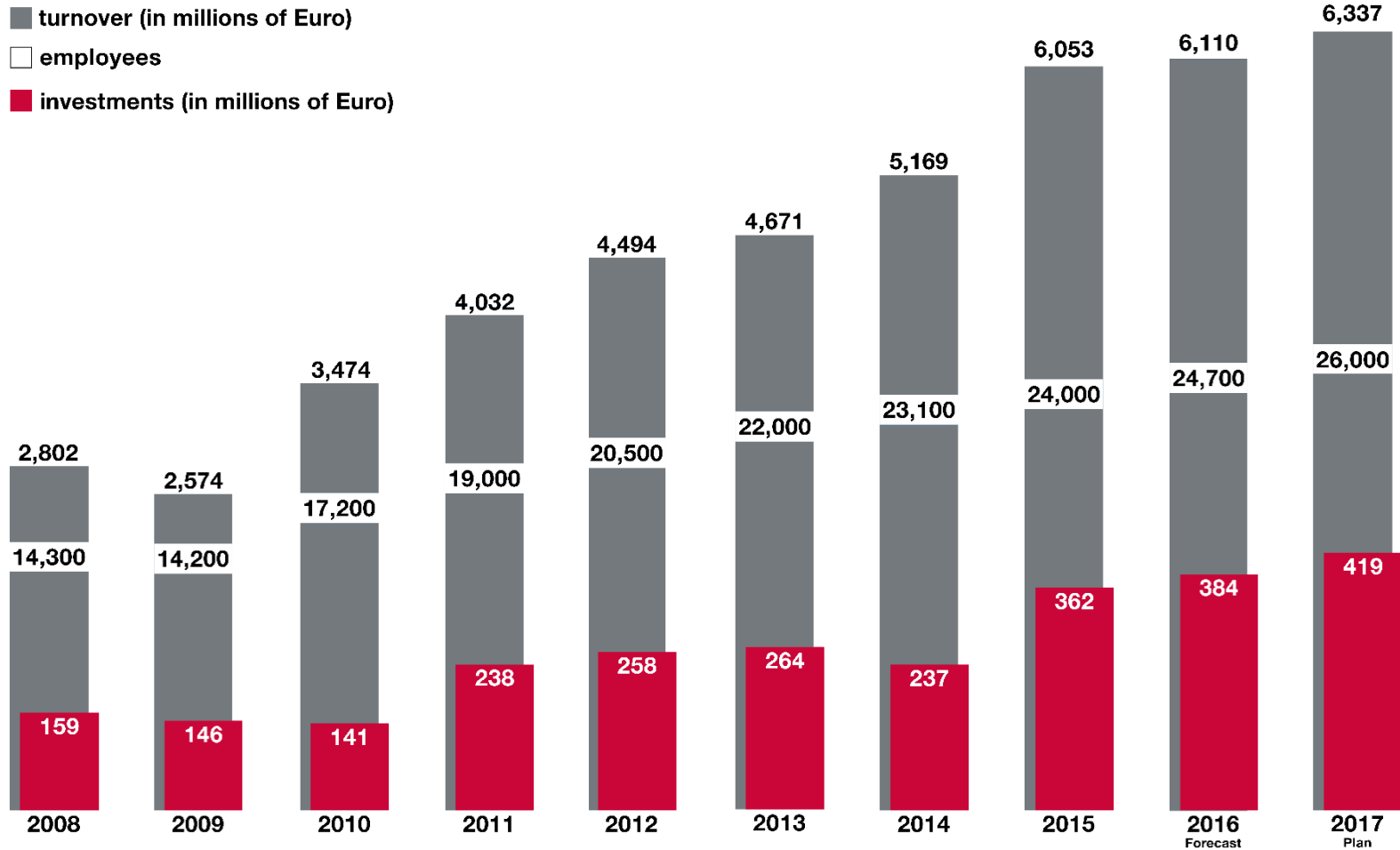
Customers worldwide

 AECAS AUTOMOTIVE EQUIPMENT	 北汽集团 BAIC Group	 FOTON	 BMW	 MINI	 ROLLS ROYCE	 Bei Ben Trucks	 BRILLIANCE			
 CHERY	DAIMLER		 Mercedes-Benz	 AMG	 smart	 Dongfeng	 FAW			
 FCA FIAT CHRYSLER AUTOMOBILES	 FIAT	 CHRYSLER	 DODGE	 FERRARI	 FIAT	 IVECO	 Jeep	 LANCIA	 MASERATI	 RAM
 Ford	 LINCOLN		 GM	 Cadillac	 CHEVROLET	 DAEWOO	 GMC	 GMC	 GMC	 VAUXHALL
 GAZ	 GREAT WALL	 VOLVO	 Great Wall	 MAZDA	 McLaren	 HONDA	 HYUNDAI	 KIA MOTORS		
 MITSUBISHI MOTORS	 Lotus	 LOTUS	 RENAULT	 DACIA	 DATSUN	 Renault Samsung Motors	 NISSAN	 INFINITI		
 SAIC	 ROEWE 荣威	 MG	 CITROËN	 PEUGEOT	 NEW	 SUBARU				
 SUZUKI	 TATA	 JAGUAR	 LAND- ROVER	 TOYOTA	 DAIHATSU	 LEXUS				
 Volkswagen	 AUDI	 BENTLEY	 BUGATTI	 LAMBORGHINI	 MAN	 Volkswagen	 PORSCHE	 SEAT	 SCANIA	 ŠKODA

Business development

Continuous self-financed growth



1. Recollection and Critique – Safety Plan

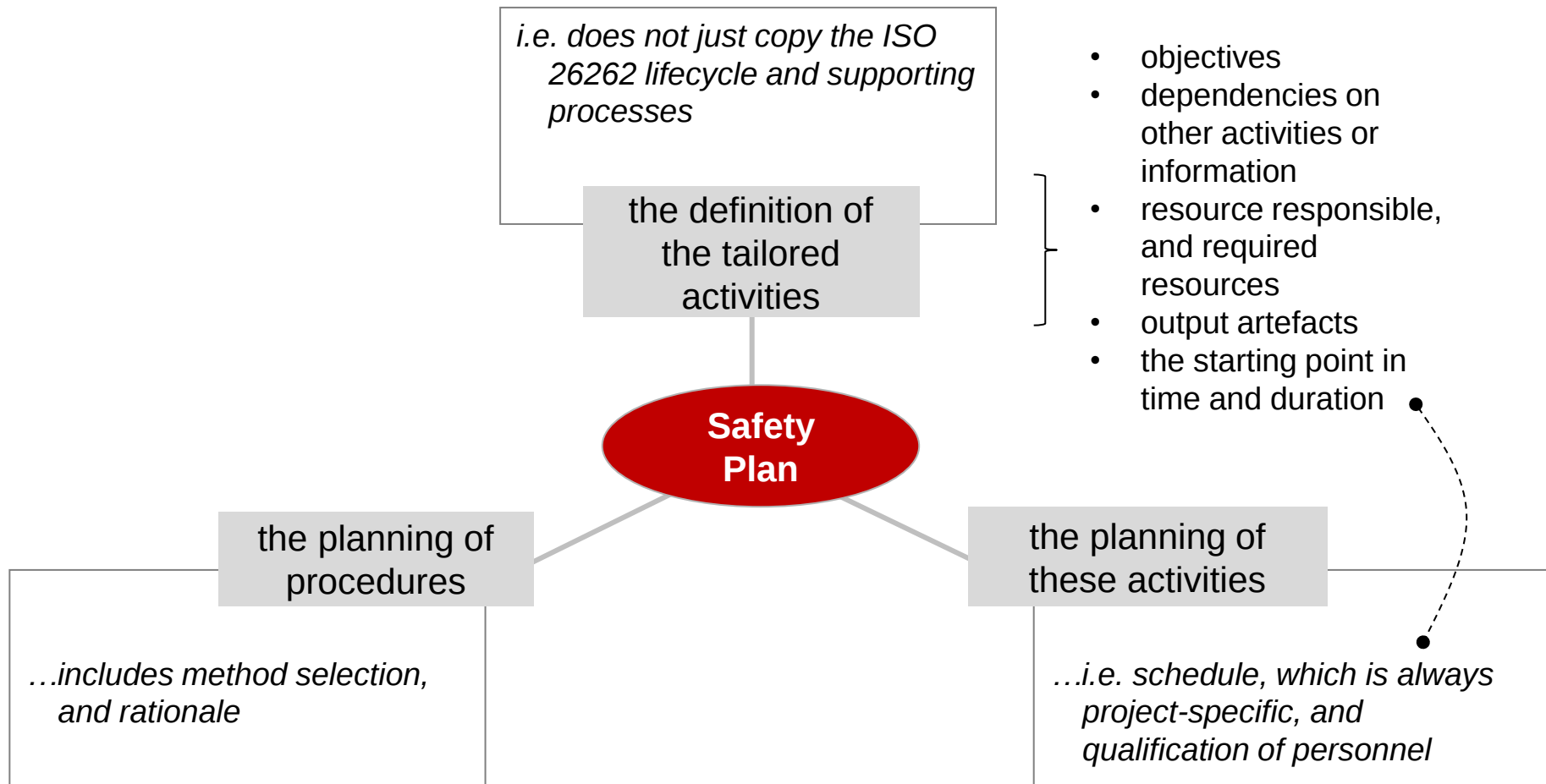
2. Standard processes – Implicit Safety Plans

3. Recollection and Critique – Confirmation Reviews

4. Standard processes – Implicit Confirmation Reviews

5. Connection to Safety Audits

Recollection – a Safety Plan contains all safety-related instructions



Critical observations – safety plan

- In practice, many safety assessors require extra project-specific safety plan documents, even though ISO 26262 clearly states:
 - “The *organization* shall ... execute ... *organization-specific rules and processes* to comply with the requirements of ISO 26262.
- NOTE* Such ... can include ... a *generic safety plan and process description*“
(ISO 26262-2, clause 5.4.2.2)
- Possible reasons for such an assessor’s opinion:
 - Work Product sections in ISO 26262 sound like that a first-class artefact needed for them
 - the above note is easily overlooked
 - some assessors probably do not have a standard process background
 - ISO 26262 does not have a sufficient view on the domains of “organizational standard processes” and “process change management”

(for experts: ISO 26262 primarily describes an Automotive SPICE® level 1 and 2 perspective, but „flattened out“)

Content

1. Recollection and Critique – Safety Plan

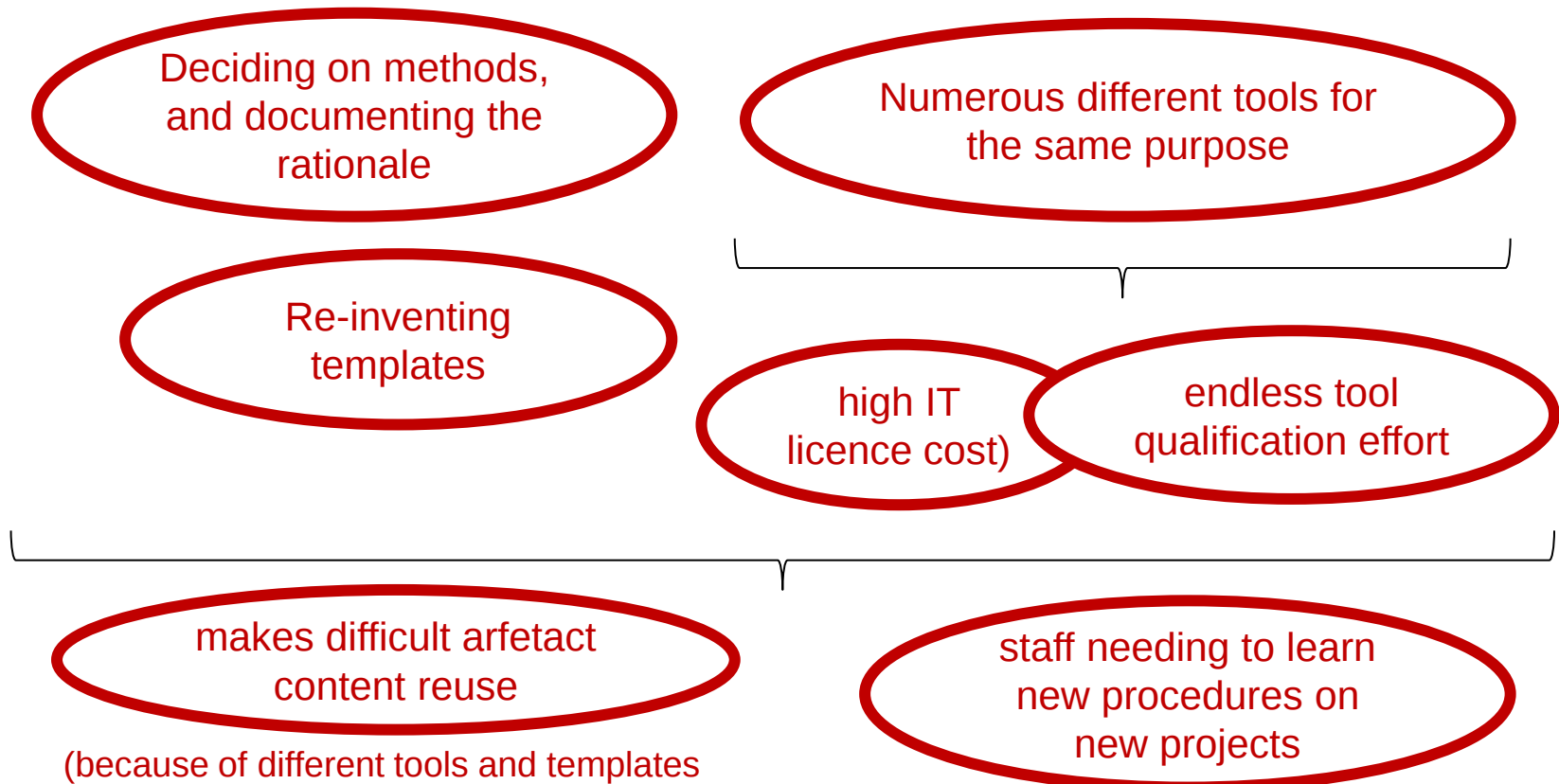
2. Standard processes – Implicit Safety Plans

3. Recollection and Critique – Confirmation Reviews

4. Standard processes – Implicit Confirmation Reviews

5. Connection to Safety Audits

Repeated effort when you do not have standard processes



Is it a solution to copy everything from project to project?

No because...

...some projects still might do things differently

...a project might take over from a poor source

... people tend to neglect analyzing if the artefacts really fit to the new project

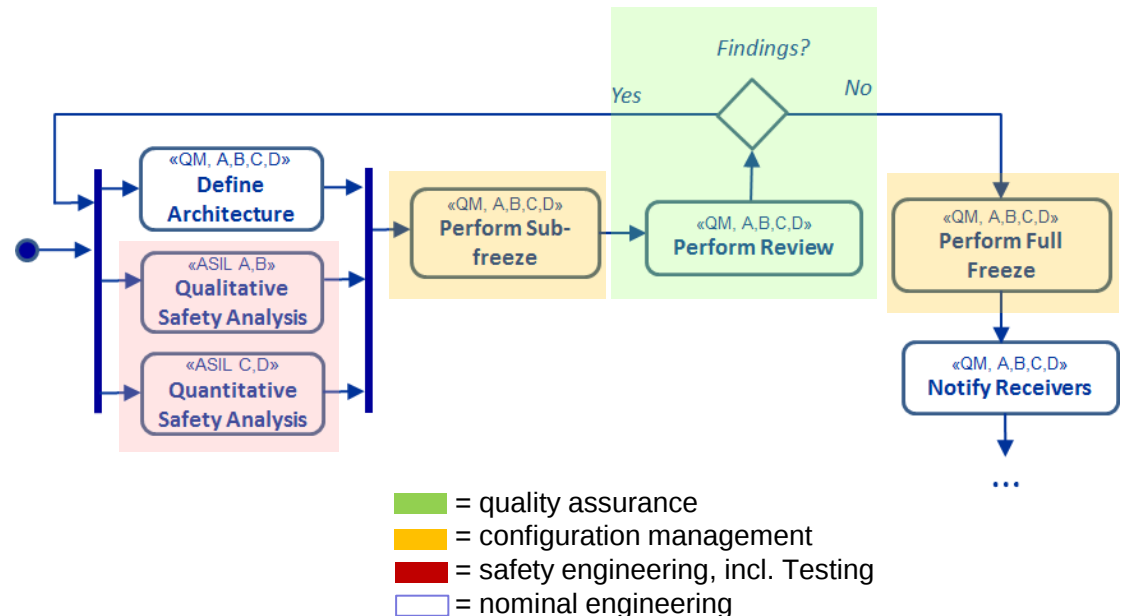
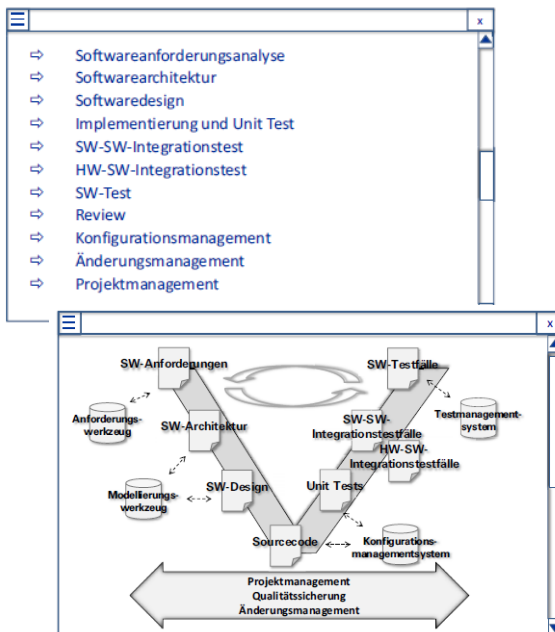
...there is no institutionalized improvement feedback loop

**Good practices not exploited,
mistakes still repeated**

Expectation #1 – a standard process shall offer logical workflows of interwoven topics

Disadvantageous approaches:

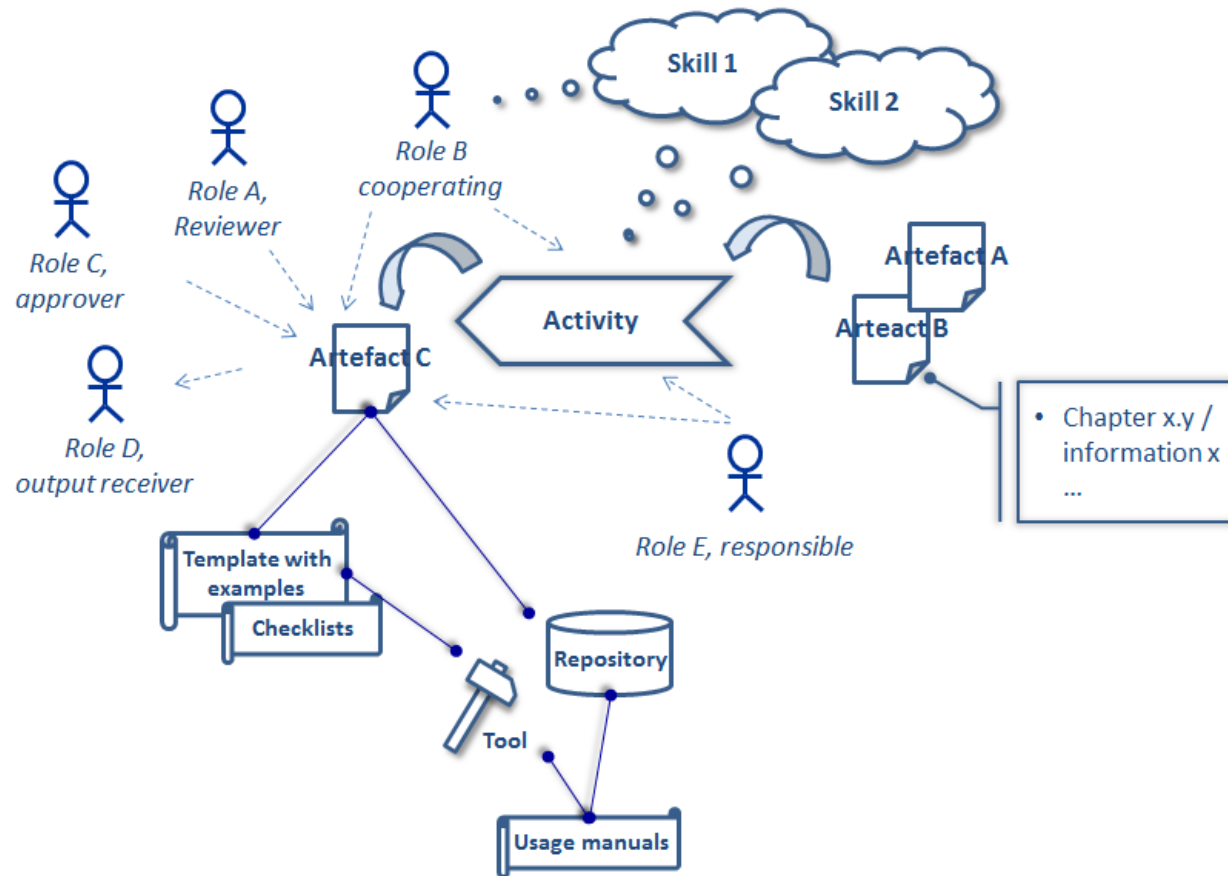
Desirable approach:



Source

P.Metz, "Automotive SPICE® Capability Level 2 and 3 in der Praxis", dpunkt Verlag, 2017

Expectation #2 – Besides activities, what must a standard process further contain?

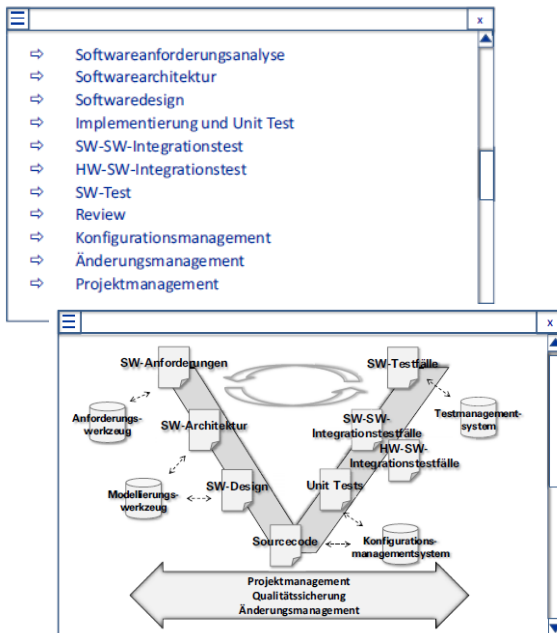


Source

P.Metz, "Automotive SPICE® Capability Level 2 and 3 in der Praxis", dpunkt Verlag, 2017

Expectation #3 – How many standard processes?

Disadvantageous approaches –
“one-size-fits-all”



Instead –
we need standard processes for the typical types of developments:

1. New development
2. Carry-over
3. New product line
4. Application of a product line
5. Change Request

These

- are “reading entry points”
- may considered “predefined standard tailorings”

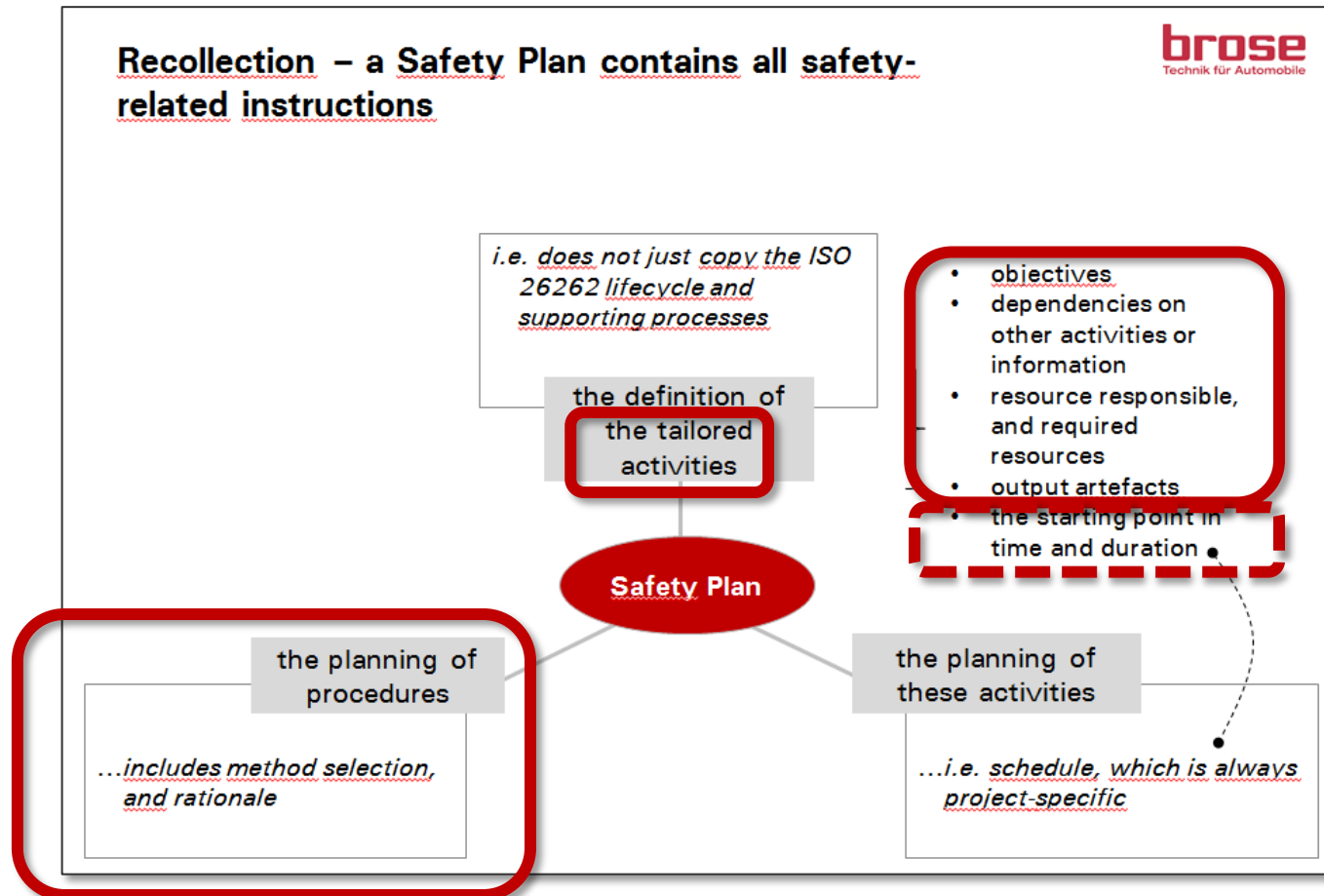
Source

P.Metz, “Automotive SPICE® Capability Level 2 and 3 in der Praxis”, dpunkt Verlag, 2017

Tailoring of standard processes

- **Standard processes are abstractions from concrete projects – otherwise they would not be widely applicable**
- **Therefore:**
 - standards are tailored to a concrete project context...based on arguments!
 - which means: adding, redefining, or removing something.
- **Such tailorings are to be done by both**
 - quality assurance representatives
 - the project members

Conclusion: most of the safety plan is inherent in an instantiation of a standard process tailoring



Content

1. **Recollection and Critique – Safety Plan**
2. **Standard processes – Implicit Safety Plans**
3. **Recollection and Critique – Confirmation Reviews**
4. **Standard processes – Implicit Confirmation Reviews**
5. **Connection to Safety Audits**

- **ISO 26262:2011 says Confirmation Reviews...**

- *are about ISO 26262 compliance of ... work products to the ... requirements of ISO 26262 with respect to **formality***

(combination of ISO 26262-2, clause 6.2 and Table 2)

- *...include the checking of correctness with respect to **formality, contents, adequacy and completeness** regarding the requirements of ISO 26262*

(ISO 26262-2, 6.4.7.1, Note 2)

- **NOTE: the only distinction criterion is “formality against ISO 26262” as *content* and *completeness* is a matter of verification reviews and safety assessments ¹**

1) P.Metz, A.Schnellbach “Critical View on, and Revision of, the Confirmation Measures in ISO 26262:2011”, 6th IQPC International Conference “Applying ISO 26262”, March, 21st – 23rd March, Berlin, Germany

Content

1. Recollection and Critique – Safety Plan
2. Standard processes – Implicit Safety Plans
3. Recollection and Critique – Confirmation Reviews
4. Standard processes – Implicit Confirmation Reviews
5. Connection to Safety Audits

Putting it all together...

- **What we have seen so far:**

- standard process instantiation (as expected above) will implicitly contain the safety plan (except schedules)
- confirmation reviews address *structural* ISO 26262 compliance



- **Conclusion to draw:**

- confirmation reviews take place at the time the standard process elements are defined (ISO 26262 mapping)
- so for projects they are implicit !



- **Prerequisite, however:**

- we so need an effective standard process adherence monitoring 1

NOTE! Such standard process audits do *not* require external service providers ³

3) P.Grabs, P.Metz "A Critical View on "Independence" in ISO 26262-2", 4th EUROFORUM conference "ISO 26262", Sept 12th–14th, 2012, Leinfelden-Echterdingen, Germany

Content

- 1. Recollection and Critique – Safety Plan**
- 2. Standard processes – Implicit Safety Plans**
- 3. Recollection and Critique – Confirmation Reviews**
- 4. Standard processes – Implicit Confirmation Reviews**
- 5. Connection to Safety Audits**

Mechanisms for process adherence monitoring (combinations meaningful):

- **Internal process audits**
- **Lessons learned workshops**
- **Stage gate reviews / quality gates between development phases**
- **Automated work product monitoring, see below...**

Work Product-Centric Standard Process “Instantiation“

Upload of work products
(WP) and review evidence...

WP lifecycle
states

WP version and
version history...

The screenshot displays the 'PROJECT KIT' web-frontend. At the top, there's a navigation bar with 'Intocenter' and 'Process Workbench'. The main content area shows a 'Hardware Software Interface Description (HWSWIF)' with a 'Review HWSWIF' link. Below this, there's a section for 'Template' (DOORS module reference note), 'Example' (with a '[Change]' link), and 'Checklist' (Checklist (download)). The bottom section is divided into four columns: 'Responsible' (Software Coordinator, Hardware Developer), 'Cooperation' (Software Coordinator, System Engineer, System Architect, Software Developer), 'Release' (PPQA [BROSE > PPQA Portal]), and 'Additional Release Notification' (Configuration Manager, Test Engineer (VI), Function Tester, Software Developer, Software Tester, Test Manager). Each column has a '[Change]' link. A search bar with 'Suchen' is in the top right.

Web-frontend for our
config mgmt
system

Work product
owner...

...and co-workers, or
input providers

Independent approval
(state 'released' *cannot*
be set by WP owner)

Automated stakeholder
notification of any state
change

Further mechanisms for process adherence monitoring – automated work product monitoring

Project XXX		System	HW	SW	SW	SW
		< sample 1 >	< sample 2 >	< sample 1 >	< sample 2 >	< sample 3 >
Start		< date >	< date >	< date >	< date >	< date >
End		< date >	< date >	< date >	< date >	< date >
1. Project Management						
Project Plan						
Project Schedule						
2. System						
2.1 System Requirement Analysis						
System Requirements Specification (SRS)						
Hazard & Risk Analysis Revision						
2.2 System Design						
Mechatronic System Requirements Specification (SRS)						
System FMEA						
3. Hardware						
Schematic						
Fault Trees						
FMEDA						
Worst case Analysis						
Layout						
Hardware Software Interface (HWSWIF)						
4. Software						
Software Design Description (SWDD)						
MISRA Compliance / Deviation Report						
Source Code Baseline						
4. Integration Testing						
4.1 HW-SW						
HW SW Test Description (HWSWIF TD)						
HW SW Interface Test Report (HWSWIF TR)						
4.2 SW-SW						
SW SW Test Description (SW TD)						
SW SW Test Report (SW TR)						
2.4 System Test						
SRS Test Description (SRS TD)						
SRS Test Report (SRS TR)						
Product Release V0,1,2						
SRS TD (EMC)						
SRS TR (EMC)						
SRS TD (Environmental Compatibility)						
SRS TR (Environmental Compatibility)						
Safety Case						

Exploited for

- progress tracking at project level
- reporting to higher level mgmt
- process adherence monitoring

In addition to that:

- Semantic rule checks for, and across, work products in the tool chain

Conclusion – extra artefacts for safety plans and confirmation reviews are not necessarily required

- **In a state-of-the-art standard process approach the following is implicit:**
 - safety plan (except schedules)
 - confirmation reviews
- **The confirmation review of the “safety plan“ itself is represented by**
 - standard process compliance checks against ISO 26262
- **Safety audits are represented by**
 - standard process compliance checks against ISO 26262
 - standard process adherence monitoring

**NOTE: this also contributes to
an Automotive SPICE® Level
3 capability ! ⁴⁾**

4) P.Metz, “Automotive SPICE® Capability Level 2 and 3 in der Praxis”, dpunkt Verlag, 2017

Lean Standard Development Processes – How to Do Without Extra Safety Plans, Confirmation Reviews, and Safety Audits

Pierre Metz, Brose Fahrzeugteile GmbH &
Co. KG, Bamberg

**Int. IQPC ISO 26262 Conference,
March, 2017, Frankfurt**

A 3D graphic of a light blue rectangular block with a dark blue top edge. On the front face of the block, the word "brose" is written in a large, bold, red, sans-serif font. Below it, the phrase "Technik für Automobile" is written in a smaller, red, sans-serif font, angled slightly upwards to the right.

brose
Technik für Automobile