

Automotive SPICE and Functional Safety



Dr Christian Kreiner

ckreiner@iscn.com

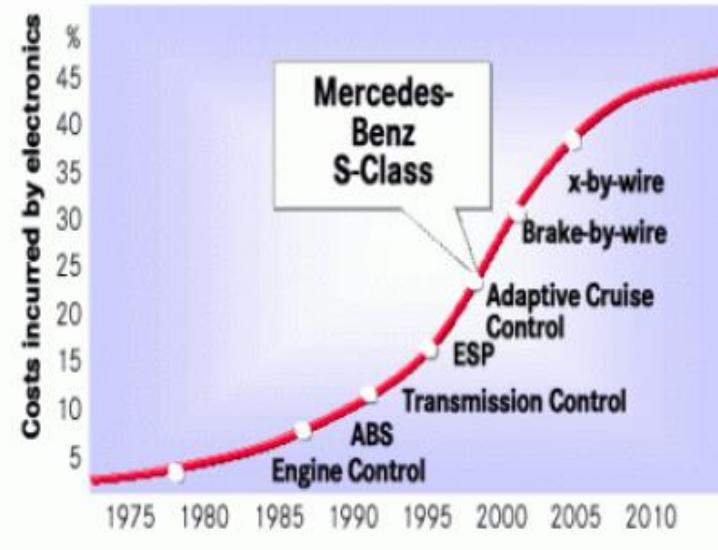
ISCN

a VDA Certified Automotive SPICE Training Partner



The Goal of SPICE: Managing Complexity

- Professional management of increasing complexity caused by the dependence of electronics, and software in the car.



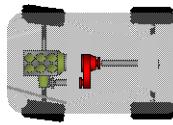
Reference:
Daimler Chrysler AG,
EuroSPI 2001 Conference,
Limerick, Ireland

2001 is the founding year of
HIS pushing ASPICE in Germany

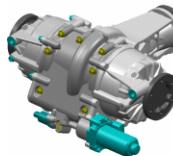
The Goal of SPICE

Understanding the Functional Flows

- Professional Traceability of requirements related with mechanics, electronics, and software in the car.



Requirement Requests (Customer)



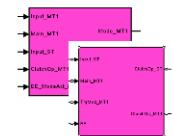
System Requirements

Requirements referring to more than one Sub-System



Sub-System Requirements

- Different components
- No common requirements
- Different responsibilities

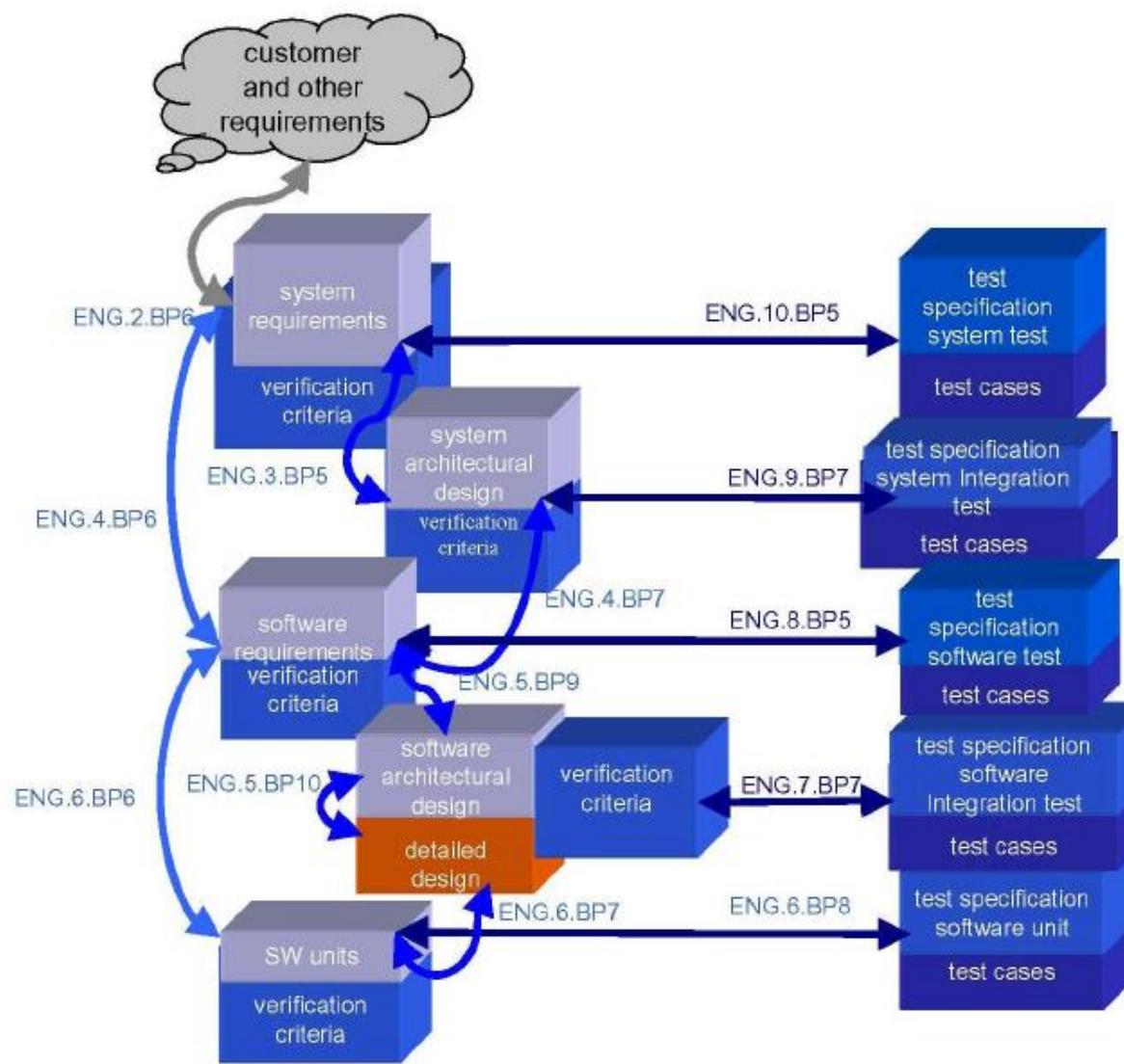


Detailed Requirements



Reference:
Magna Powertrain AG,
Key Note,
EuroSPI 2008 Conference,
Dublin, Irland

Bilateral Traceability



SPICE Assessment

Model German Automotive Scope

HIS Scope: www.his-automotive.de



Engineering Process Group		Support Process Group	
ENG.2	System requirements analysis	SUP.1	Quality assurance
ENG.3	System architectural design	SUP.8	Configuration Management
ENG.4	Software requirements analysis	SUP.9	Problem resolution management
ENG.5	Software design	SUP.10	Change request management
ENG.6	Software construction	Management Process Group	
ENG.7	Software integration	MAN.3	Project management
ENG.8	Software testing	Acquisition Process Group	
ENG.9	System integration	(optional)	
ENG.10	System testing	ACQ.4	Supplier Monitoring

ASPICE Reference Model

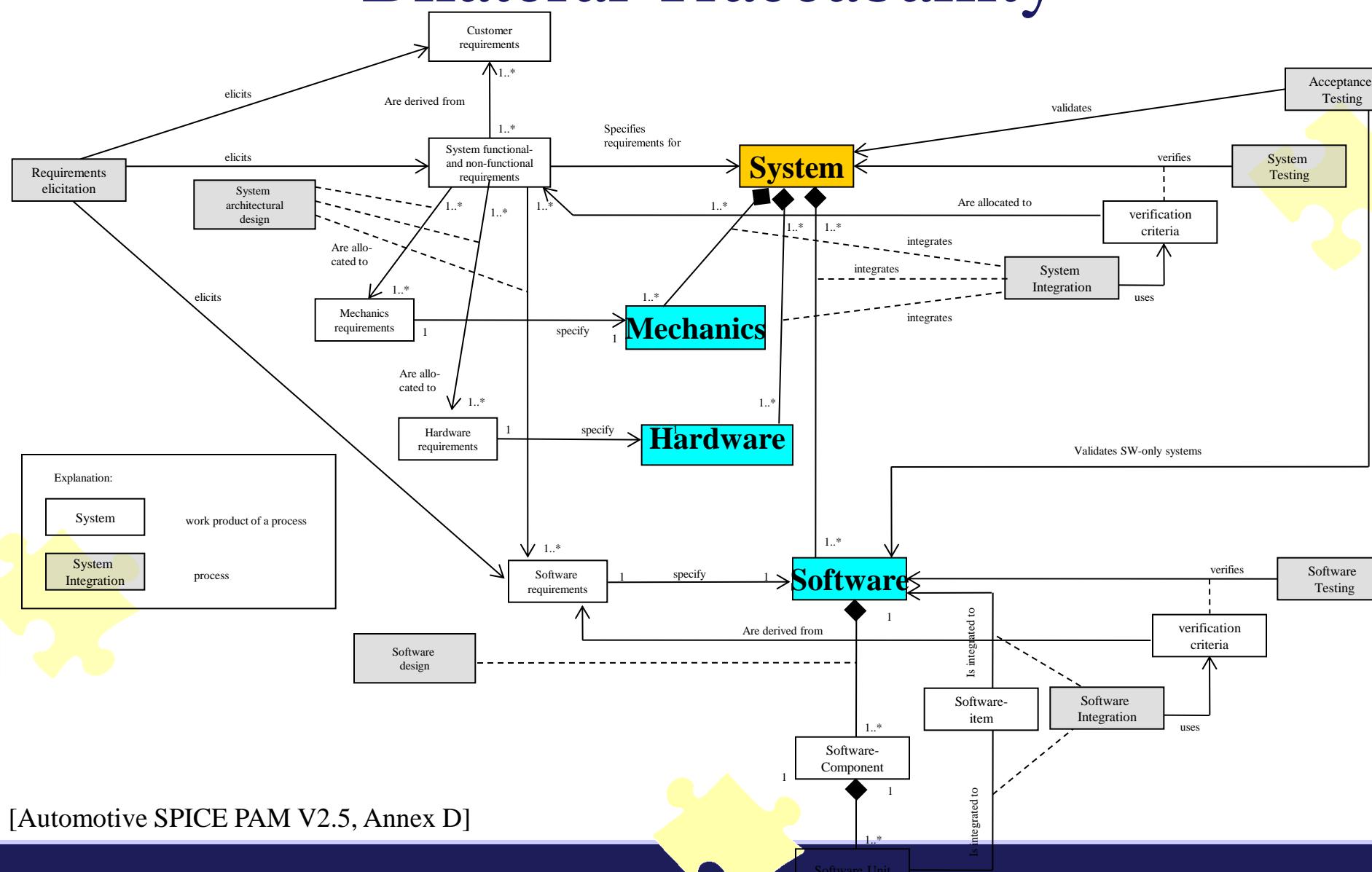
Acquisition Process Group		
ACQ .3	Contract Agreement	
ACQ .4	Supplier Monitoring	H, Fo
ACQ .11	Technical Requirements	
ACQ .12	Legal and Administrative Requirements	
ACQ .13	Project Requirements	
ACQ .14	Requests for Proposals	
ACQ .15	Supplier Qualification	

Support Process Group		
SUP .1	Quality Assurance	H, Fi, Fo
SUP .2	Verification	Fo
SUP .4	Joint Review	Fo
SUP .7	Documentation	
SUP .8	Configuration Management	H, Fi, Fo
SUP .9	Problem Resolution Management	H, Fi, Fo
SUP .10	Change Request Management	H, Fi, Fo

Engineering Process Group		
ENG.1	Requirements Elicitation	Fi
ENG.2	System Requirements Analysis	H, Fi, Fo
ENG.3	System Architectural Design	H, Fi, Fo
ENG.4	Software Requirements Analysis	H, Fi, Fo
ENG.5	Software Design	H, Fi, Fo
ENG.6	Software Construction	H, Fi, Fo
ENG.7	Software Integration	H, Fi, Fo
ENG.8	Software Testing	H, Fi, Fo
ENG.9	System Integration	H, Fi, Fo
ENG.10	System Testing	H, Fi, Fo

Management Process Group		
MAN.3	Project Management	H, Fi, Fo
MAN.5	Risk Management	Fi, Fo
MAN.6	Measurement	
Process Improvement Process Group		
PIM .3	Process Improvement	
Reuse Process Group		
REU.2	Reuse-Program-Management	
Supply Process Group		
SPL.1	Supplier Tendering	
SPL.2	Product Release	Fi

Bilateral Traceability



[Automotive SPICE PAM V2.5, Annex D]

Capability Levels

Optimising

Quantitative measures are implemented to continuously improve the process

Level 5 Optimising

- PA.5.1 Process innovation
- PA.5.2 Continuous optimization

Predictable

Metrics for the measurement and control of process performance and outcomes are applied

Level 4 Predictable

- PA.4.1 Process measurement
- PA.4.2 Process control

Established

Defined processes are tailored to specific projects, resources are managed

Level 3 Established

- PA.3.1 Process definition
- PA.3.2 Process deployment

Managed

Processes and work products are managed, responsibilities are identified

Level 2 Managed

- PA.2.1 Performance management
- PA.2.2 Work product management

Level 1 Performed

- PA.1.1 Process performance

Performed

Processes are intuitively performed, incoming and outgoing work products exist.

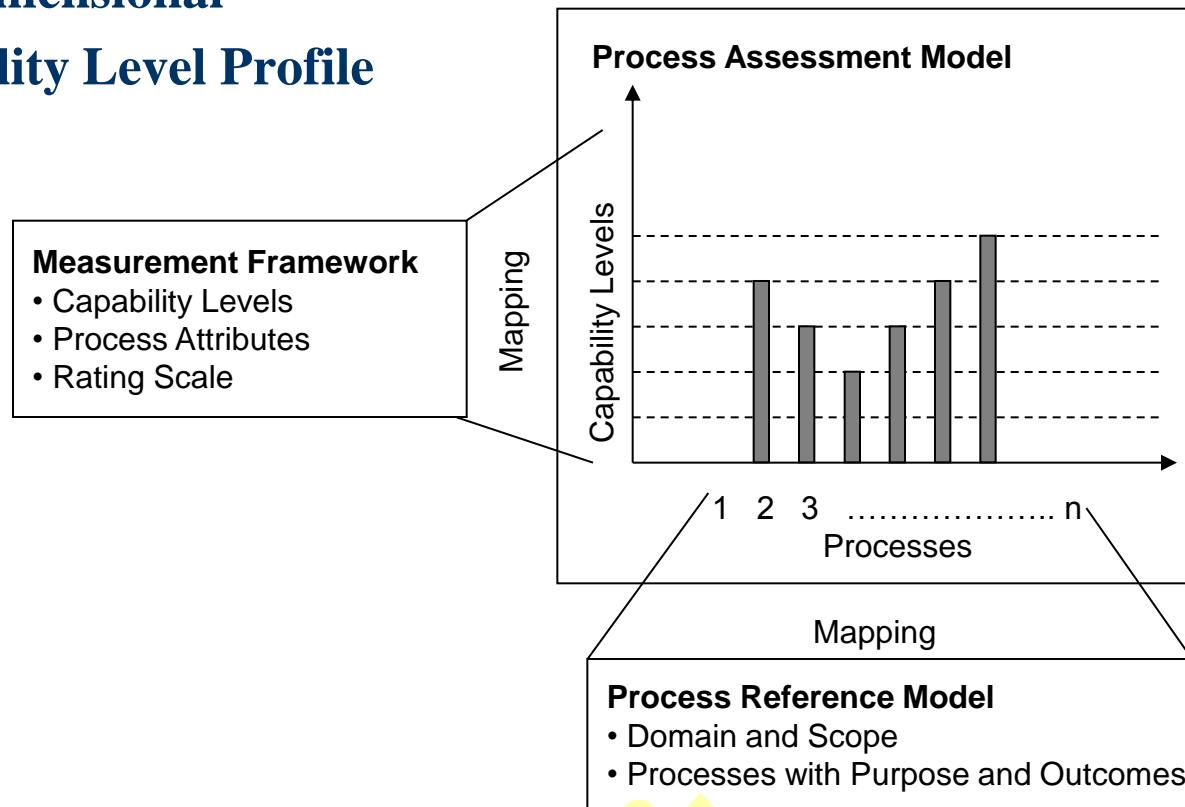
Level 0 Incomplete

Incomplete

Chaotic processes

SPICE Assessment Model

- Two-dimensional
- Capability Level Profile



Rating Scale

N

Not achieved

Outcome/achievement not existent, or not really, implemented

0% to 15 %

P

Partially achieved

Some outcomes/achievements implemented, but projects/OUs still incapable of reaching quality, time, or budget goals & targets

> 15 % to 50 %

L

Largely achieved

Outcome/achievement imply a certain likelihood, however no certainty, of reaching quality, time, and budget goals & targets

> 50 % to 85 %

F

Fully achieved

No process risk with respect to quality, time, budget goals & targets identified, even in presence of imperfections

> 85 % to 100 %

Example Rating

ACQ.4 Supplier Monitoring

Indicator		Rating
BP 1	Establish and maintain communications	L
BP 2	Exchange information on technical progress	F
BP 3	Review supplier performance	F
BP 4	Monitor the acquisition	F
GP 2.1.1	Identify objectives	L
GP 2.1.2	Plan and monitor process	L
GP 2.1.3	Control performance	P
GP 2.1.4	Define responsibilities	P
GP 2.1.5	Identify resources	L
GP 2.1.6	Manage interfaces	F
GP 2.2.1	Define requirements for WP	L
GP 2.2.2	Define req. for doc/control	F
GP 2.2.3	Identify/document/control WP	F
GP 2.2.4	Review/adjust WP	F

Level 1
Process Attribute

Level 2
Process Attributes

Example Rating

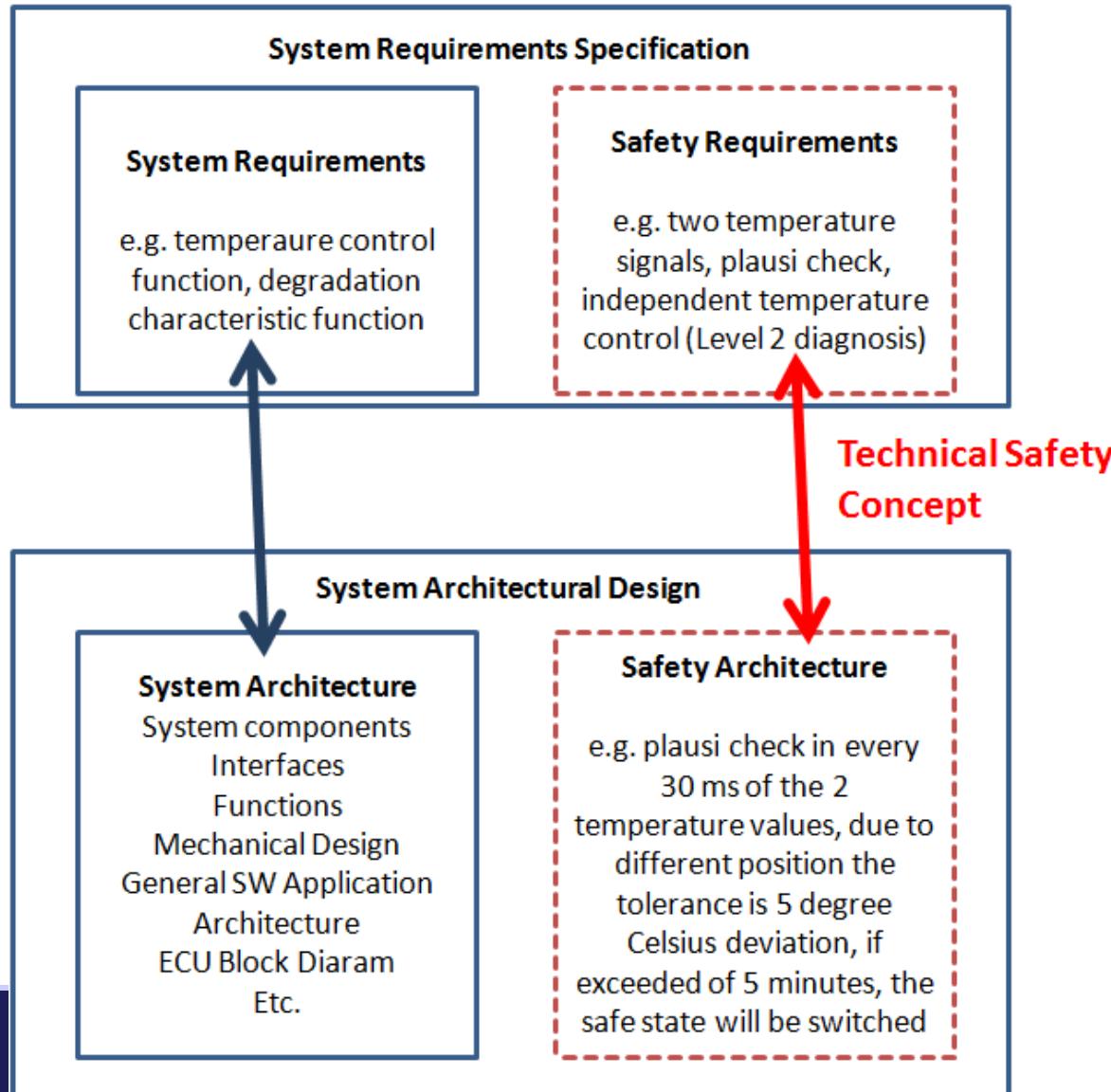
Capability Level Profile across Processes

		Capability Level	1	2	3		4		5	
Process	Process Attribute	PA	PA	PA	PA	PA	PA	PA	PA	PA
		1.1	2.1	2.2	3.1	3.2	4.1	4.2	5.1	5.2
ENG.1	Requirements elicitation	F	L	L	L	P				
ENG.2	System requirements analysis	F	F	L	F	L				
ENG.3	System architectural design	F	F	F	L	L				
ENG.4	Software requirements analysis	P	N	L	P	P				
ENG.5	Software design	L	L	F	P	N				
ENG.6	Software construction	F	F	L	L	P				
ENG.7	Software integration	N	P	P	L	P				
MAN.3	Project management	F	N	P	L	L				
SUP.8	Configuration management	P	N	L	F	P				
SUP.1	Quality assurance	P	F	L	F	L				
ACQ.4	Supplier monitoring	F	L	F	F	P				

← CL 2
 ← CL 2
 ← CL 3
 ← CL 0
 ← CL 1
 ← CL 2
 ← CL 0
 ← CL 1
 ← CL 0
 ← CL 0
 ← CL 2

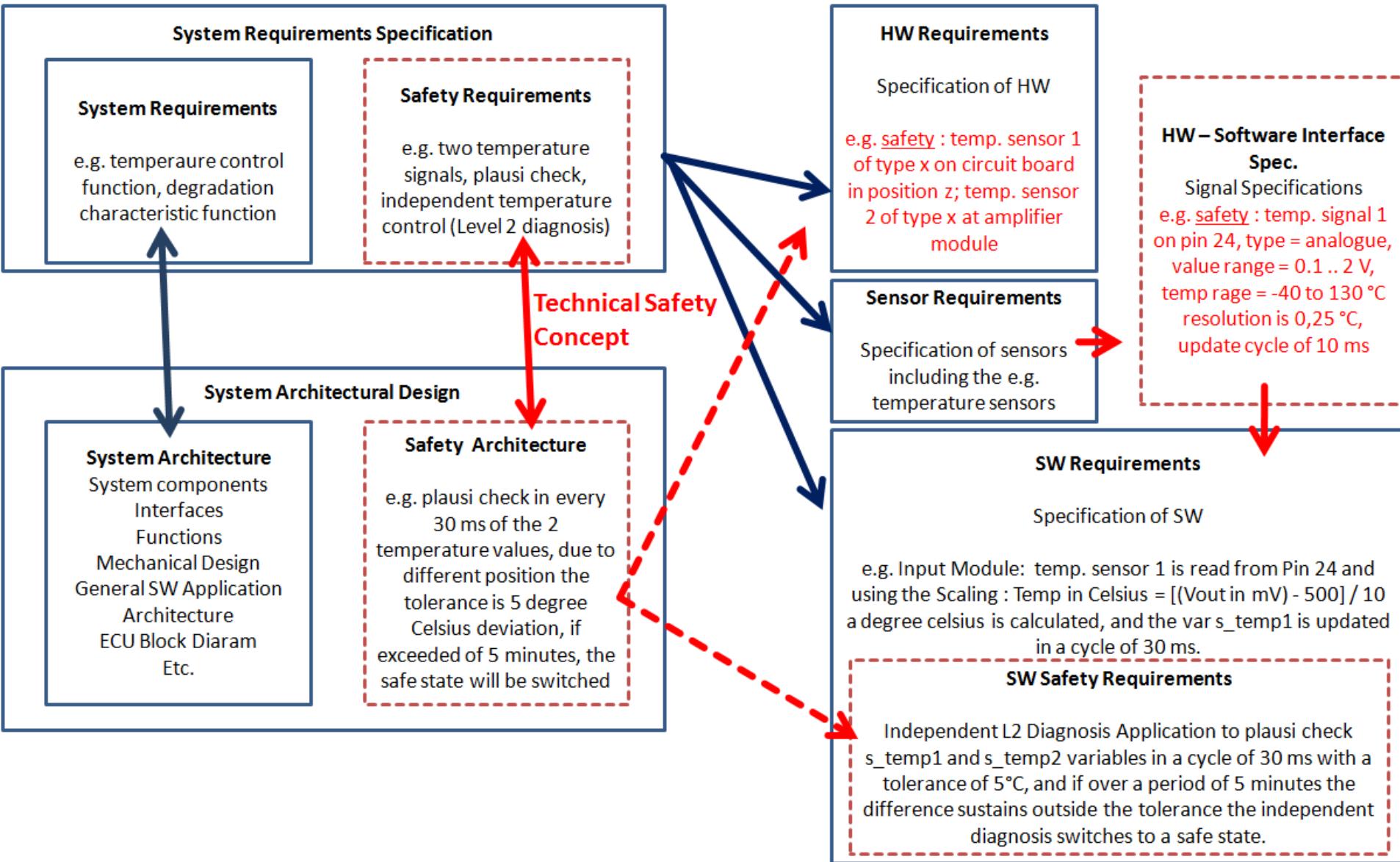
ISO 26262 Integration

Red = Additional Safety Relevant Content



ISO 26262 Integration

Red = Additional Safety Relevant Content



Integrated Assessment 1/2

http://localhost/capadv7/capadv/FAbrowser.php?&tar=prj&dom=246227&A_id=230974

localhost

Datei Bearbeiten Ansicht Favoriten Extras ?
Seite Sicherheit Extras

ACQ.4 Supplier Monitoring
ENG.2 System Requirements Analysis
ENG.3 System Architectural Design
ENG.3.1
ENG.3.2
ENG.3.3
ENG.3.4
ENG.3.5
ENG.4 Software Requirements Analysis
ENG.5 Software Design
ENG.6 Software Construction
ENG.7 Software Integration Test
ENG.8 Software Testing
ENG.9 System Integration Test
ENG.10 System Testing
MAN.3 Project Management
SUP.1 Quality Assurance
SUP.8 Configuration Management
SUP.9 Problem Resolution Management
SUP.10 Change Request Management

Assessments Evidences Export Calculate Learning Settings Help Logout

ENG.3.BP2

Allocate System Requirements.
Allocate all system requirements to the elements of the system architectural design. [Outcome 2]

This includes the allocation of a SIL level to the system requirements and system elements in case that the system requirement / element is part of the required safety functions.

ISO 26262 Part: Part-6, 6.6.4
Chapter: 6.6.4.2

- Measure and demonstrate the coverage of safety requirements (functional and non-functional, and technical)
- Show that safety requirements have an ASIL attribute (see also ENG.2)
- Highlight elements and safety functions which have an impact on the safety of the system, and provide a filter to group the requirements to those elements and functions.
- Demonstrate the linking strategy. E.g. technical safety requirements in the architecture are linked to subsystems (e.g. software, hardware, sensor safety requirement) and the highest ASIL level is inherited.
Remark: Not all children have the same ASIL level inherited, this depends on the decomposition strategy.

NA: PA: LA: FA: Not App.: Safety Note

ENG.3.BP3

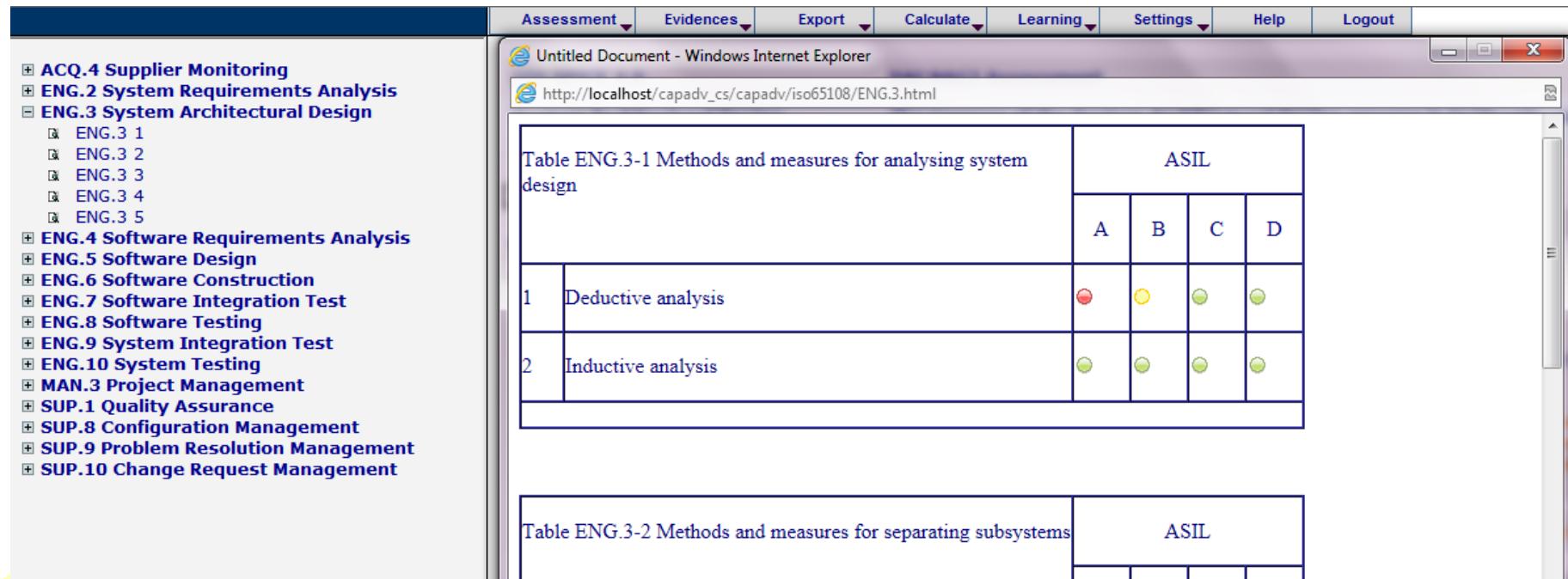
Define interfaces.
Identify, develop and document the internal and external interfaces of each system element. [Outcome 3]

ISO 26262 Part: Part-4, 7.4.6 Hardware-software interface specification (HSI)
Chapter: 7.4.6.4

- Show a signal table which describes it with attributes relating to sensor hw base software raw signal, scaling, functional software / calculated value, refresh rates, latency time, default value, etc.
- Safety relevant features (protection measures) per ASIL-classified signal should be defined (only system level detail to be considered, will be further refined in the software).

Windows Taskbar icons: File Explorer, Internet Explorer, Control Panel, Printers, File Manager, Search, Task View, Start, Taskbar settings, Volume, Battery, Signal strength, Volume, Date/Time: 18:29, 06.03.2015

Integrated Assessment 2/2



The screenshot shows a software application window titled "Untitled Document - Windows Internet Explorer" with the URL "http://localhost/capadv_cs/capadv/iso65108/ENG.3.html". The window contains two tables under the heading "Table ENG.3-1 Methods and measures for analysing system design".

		ASIL			
		A	B	C	D
1	Deductive analysis	●	○	●	●
2	Inductive analysis	●	●	●	●

Below this is another table titled "Table ENG.3-2 Methods and measures for separating subsystems".

		ASIL			
1	Separation by function	●	●	●	●
2	Separation by time	●	●	●	●

Automotive SPICE Assessment Model

- German manufacturers require a level 3 in all HIS processes
 - In VW the capability levels are used to determine the A-,B-,C-supplier rating.
- Fiat (+Chrysler) published a Fiat/Chrysler Scope in 2012.
- Nissan uses a checklist which is 90% similar to Automotive SPICE.
- Ford uses a HIS Scope plus 3 more processes.

Links

Email: ckreiner@iscn.com

Links:

- <http://2015.eurospi.net>
- <http://soocrates.eurospi.net>
- <http://www.intacs.info>
- <http://www.automotivespice.com>
- <http://www.vda-qmc.de>
- <http://www.his-automotive.de>

Courses

- ECQA: <http://ECQA.org>
- ECQA certified Safety Manager/Engineer <http://safeur.eu>
- AQUA <http://www.automotive-knowledge-alliance.eu>