

Experience with the Combined use of ASPICE 3.1 and ISO 26262 assessments

EuroSPI, 7. 9. 2020

Authors: R. Messnarz & D. Ekert, based on

<https://soqrates.eurospi.net>

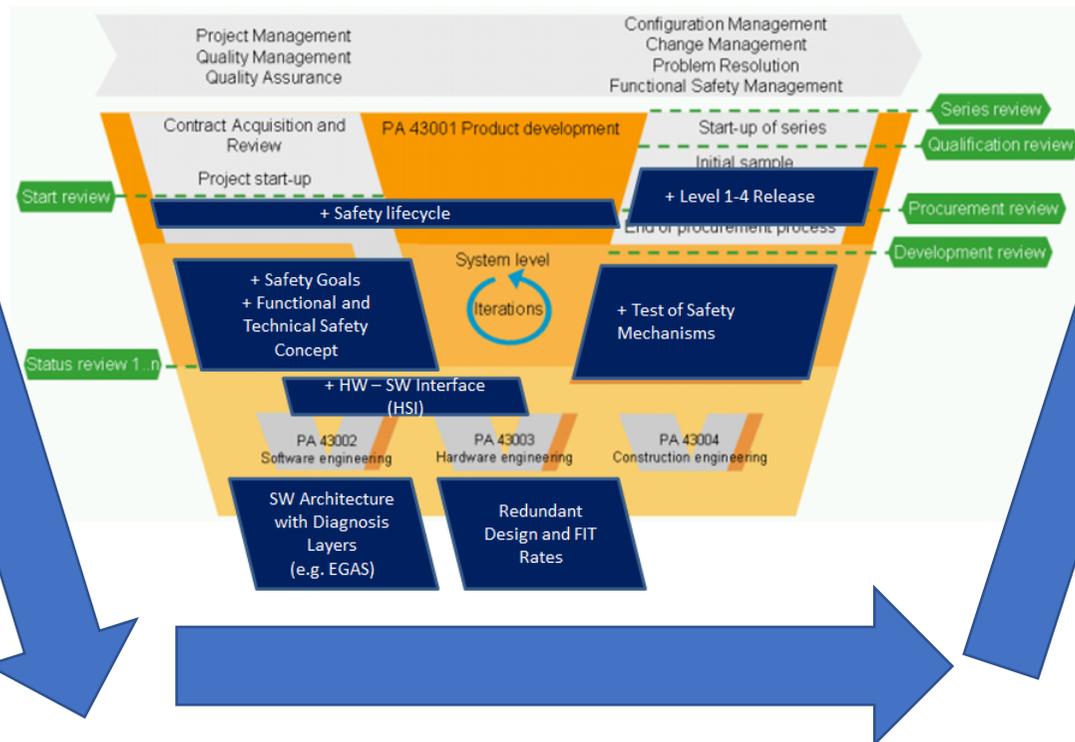
Motivation

- ASPICE 3.1 extension
 - Assignment of ISO 26262 clauses to BPs and GPs
 - Design of so called extended sub-questions per BP/GP
 - Parts 4,5,6,7 of ISO 26262 mapped in detail and integrated to the portal, other parts mapped on a general level
- **One integrated V**



- SOQRATES Baseline Dec 2019

Approach



- ✓ Safety Audit
 - ✓ Check **per process using extension**
 - ✓ Rating BPs/GPs up to L2
 - ✓ Traceability of the safety case
 - ✓ Process rating done based on ASPICE
- ✓ Safety Assessment:
 - ✓ Check **per Safety Goal**
 - ✓ Technical Review along V Model
 - ✓ Traceability of the safety case
 - ✓ Work Products related will be checked

Kreiner C. et al. (2013) **Automotive Knowledge Alliance AQUA – Integrating Automotive SPICE, Six Sigma, and Functional Safety**. In: McCaffery F., O’Connor R.V., Messnarz R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2013. Communications in Computer and Information Science, vol 364. Springer, Berlin, Heidelberg

Safety Audit

- ✓ Safety Audit
 - ✓ Process Related comments
 - ✓ ASPICE Report with levels
 - ✓ Usually level 2 is the target (level 1 gaps are critical)
 - ✓ Deviations written to a ISO 26262 assessment sheet

The screenshot displays the CapAbility Adviser web application. The browser address bar shows a URL starting with 'https://www...'. The application header includes 'All Assessments', 'Evidences', 'Export', 'Rating', 'Settings', and 'Help'. The main content area is titled 'SYS.2.1' and features a 'Safety' tab highlighted with a red circle. Below the tab, the text reads: 'Specify system requirements. Use the stakeholder requirements and changes to the stakeholder requirements to identify the required functions and capabilities of the system. Specify functional and non-functional system requirements in a system requirements specification. [OUTCOME 1, 5, 7]'. A red box highlights the 'ISO 26262 Extended Questions:' section, which lists several safety-related questions. Below this, there are sections for 'Strengths:', 'Weaknesses:', and 'Comments/Suggestions:'. The 'Comments/Suggestions:' section contains the text: 'Evidence: SYRS_ProdName baseline 10.4, System PIC SYRS_1234'. The bottom of the interface shows a Windows taskbar with various application icons and a search bar.

Safety Assessment

- ✓ Safety Assessment
 - ✓ Per Safety Goal Findings per BP/GP
 - ✓ Technical Details checked by **Safety Expert** (more detail than in ASPICE)
 - ✓ Even if the ASPICE is a process checklist we follow the V and open product details
 - ✓ Deviations written to a ISO 26262 assessment sheet

The screenshot shows the CapAbility Adviser web application. The left sidebar lists various units under 'All Units', including ACQ.4, MAN.3, SUP.1, SUP.8, SUP.9, SUP.10, SWE.1, SWE.2, SWE.3, SWE.4, SWE.5, SWE.6, SYS.2, SYS.3, SYS.4, and SYS.5. The main content area is titled 'SYS.2.1' and has tabs for 'Summary', 'Notes', 'Save All', 'Evidences', 'Recommendations', 'Rules', and 'Safety'. The 'Safety' tab is selected and circled in red. Below the tabs, there is a section for 'ISO 26262 Extended Questions' with a list of questions. Below that, there are sections for 'Strengths', 'Weaknesses', and 'Comments/Suggestions', each containing text-based findings related to safety goals and technical requirements.

Approach – 2 reports

- ✓ Process based Audit Report – ASPICE with extension

UNITS	1	2.1
MAN.3 Project Management	L	L
SUP.1 Quality Assurance	F	L
SUP.8 Configuration Management	F	L
SUP.10 Change Request Management	F	L
SWE.1 Software Requirements Analysis	L	L
SWE.2 Software Architectural Design	F	L
SWE.6 Software Qualification Test	F	F

- ✓ ISO 26262 assessment sheet – Using ASPICE extension as an input, apply safety expert know how, add product findings to portal, fill in the ISO 26262 assessment sheet

ID	ISO26262 reference					in scope of assessment	< compang >		Action Plan	
	Part	Clau	Req	Workproduct	Sub-Workproduct		Evidences Referenced from the Organisation	Rating	Improvement Recommendation	
25	3		5,2	Safety goals		Yes		Safety Case V1.9, chapter 4.8: Main FSC requirements related to Safety goals are described, ASIL B rating is highest level (is state of the art for HCM systems).	F	Note: Turning indicators incorrectly on is not covered? This is where the market seems to have ASIL-B?
26	3		5,3	Verification report on H&R and SGs		Yes		This is done by the customer.	-	
27	3	8	5,1	Functional safety concept		Yes		Safety Case V1.9, chapter 4.8: Main FSC requirements related to Safety goals are described, ASIL B rating is highest level (is state of the art for HCM systems).	F	Note: Turning indicators incorrectly on is not covered? This is where the market seems to have ASIL-B?
28	3		5,2	Verification report on functional safety concept		Yes		Informal review of functional safety concept is visible in the change log of the safety case v1.9.	L	A formal review with a person independent from the author and using a checklist is missing.



- ✓ Assessments, consulting and training in the field of System, Services and Software Process Improvement and Innovation



- ✓ Organiser of the EuroSPI (European Software, Sytem and Services Process Improvement and Innovation) conference series since 1994 (www.eurospi.net)



- ✓ Founding member, vice-president and technology provider for the European Certification and Qualification Association



- ✓ Accredited iNTACS™ training provider for Automotive SPICE®



- ✓ Moderator of the German SOQRATES initiative, where 23 leading Germany companies share knowledge concerning process improvement in the field of Functional Safety, Cybersecurity, Traceability...