Hardware SPICE Extension for Automotive SPICE 3.1

Christian Schlager[3], Richard Messnarz[1(✉)], Harald Sporer[1], Armin Riess[2], Ralf Mayer[4], and Steffen Bernhardt[4]

[1] ISCN GesmbH, Graz, Austria
rmess@iscn.com
[2] BBraun, Melsungen, Germany
Armin.Riess@bbraun.com
[3] Magna ECS, St. Valentin, Austria
Christian.Schlager@magna.com
[4] BOSCH Engineering Gmbh, Gerlingen, Germany
ralf.mayer@de.bosch.com

Abstract. Automotive SPICE is an assessment model which is published and maintained by the VDA and the SPICE User Group (www.automotivespice.com). Version 3.1 has been published in Nov. 2017 and in Jan. 2018 a guideline for interpreting (Blue-Gold Book) ASPICE 3.1 has been published by the VDA. Also Automotive SPICE 3.1 in Annex D outlines that the plugin concept will foresee that a hardware and a mechanics SPICE assessment model will be integrated in the future. The SOQRATES working group (www.soqrates.de) which includes a group of leading Automotive suppliers developed a hardware SPICE model in 2016 – 2017 which can be plugged into Automotive SPICE 3.1 and used for hardware assessment. Also in the working party the ISO 26262 norm has been reviewed since product safety assessments according to the ISO 26262 functional safety norm include hardware assessment. All base practices of the hardware SPICE assessment model therefore have been extended with further checklists to include a functional safety scope. The paper describes the main elements of the hardware SPICE assessment model, how it can be plugged into Automotive SPICE 3.1, and where it is mainly used in the first trial projects.

Keywords: Automotive SPICE 3.1 · Functional safety · ISO 26262
Hardware assessment · Hardware SPICE

1 The Plug in Concept of Automotive SPICE 3.1

Figure 1 below illustrates the plugin concept in Automotive SPICE 3.1 [1]. The system V-model includes the processes SYS.1 Requirements Elicitation, SYS.2 System Requirements Analysis, SYS.3 System Architectural Design, SYS.4 System Integration and Integration Test, and SYS.5 System Qualification Test.

The software V-model includes the processes SWE.1 software requirements analysis, SWE.2 SW architectural design, SWE.3 SW detailed design and unit construction, SWE.4 software unit verification, SWE.4 software integration and integration test, SWE.5 SW qualification test.

X. Larrucea et al. (Eds.): EuroSPI 2018, CCIS 896, pp. 480–491, 2018.
https://doi.org/10.1007/978-3-319-97925-0_41

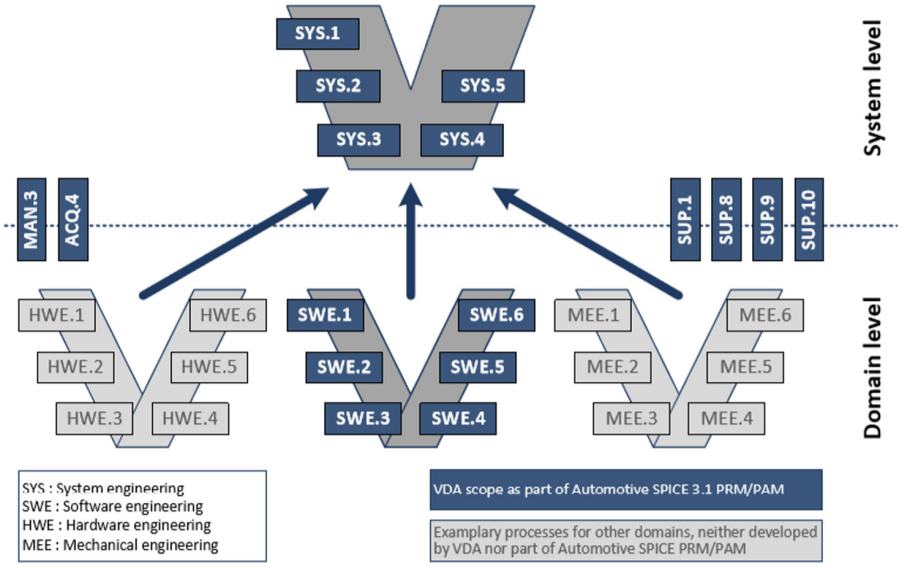

Fig. 1. The plugin concept of Automotive SPICE 3.1

Figure 2 below shows the traceability concept of Automotive SPICE which in Annex D describes the traceability concept for system and software level but still not for the hardware or mechanics level.

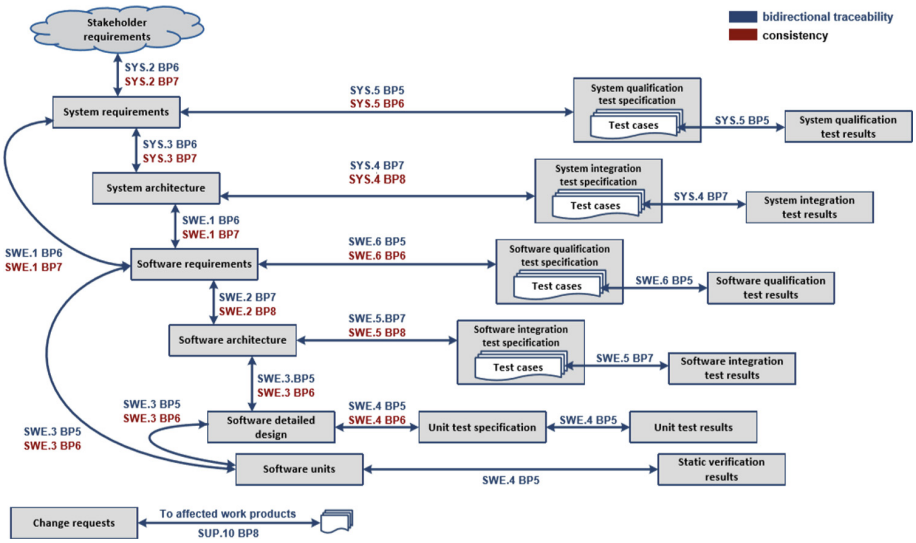

Fig. 2. Bidirectional traceability and consistency concept of ASPICE 3.1

Automotive SPICE 3.1 (see Fig. 1) does not contain a description and base practices for the HWE.1 to HWE.6 processes. However, Automotive SPICE 3.1 foresees a plug in model that can be used for an extended assessment including hardware. The SOQRATES working group developed a first version of this HWE.1 – HWE.6 processes and base practices.

HWE Spice includes the following processes

- HWE.1 Hardware Requirements Analysis
- HWE.2 Hardware Architectural Design
- HWE.3 Hardware Detailed Design
- HWE.4 Hardware Unit Verification
- HWE.5 Hardware Integration and Integration Test
- HWE.6 Hardware Qualification Test.

2 Research Method

The European Commission directive 2001/95/EC on General Product Safety and the decision 768/2008 of the European Parliament forced the Automotive industry -

- to report any safety critical issue to a publicly available database. These news are also used by journalists to report about large recall actions of Automotive manufacturers.
- to either solve the safety critical issue or to withdraw the products from the market.

Automotive manufacturers are not liable if they apply the state of the art in their developments and consider the safety norms appropriately. However, there is no clear definition of what a state of the art really is. Research papers might be used but they are not strong enough to withstand in court because you always find papers with contradictory views.

Therefore task forces like SOQRATES [7] (www.soqrates.de, formed in 2003 and with a large group of leading suppliers in Automotive) agreed a research method to define a state of the art. Best practices for analysis methods, design approaches, assessment model understanding etc. are compared among the group of the largest suppliers and joint best practices are agreed and published. This way these best practices are declared as a state of the art. This paper publishes such a consensus of a group of experts from leading suppliers in Automotive industry.

3 Extended Hardware SPICE Terminology

In Automotive SPICE the smallest part into which a software is decomposed is called SW unit. One of the research questions was: What is a hardware unit and the smallest part we will look at in an assessment?

The functional safety (ISO 26262) norm already included a hardware assessment and therefore the terminology of the ISO 26262 norm has been re-used. However, also the ISO 26262 norm did not define hardware unit, but hardware element and hardware

part. Below you find the terminology from the ISO 26262 as well as the hardware unit definition which was agreed in the SOQRATES working party.

HW Element (ISO 26262):

- ISO 26262: "system (1.129) or part of a system including components (1.15), hardware, software, hardware parts (1.55), and software units (1.125)" NOTE A component is a part of a system." The numbers 1.xx in this paragraph refer to definitions in part 1 of ISO 26262:2011.
- The top level of HWE in this scope
- HWE.1 requirements are related to this level
- HWE.2 describes the architecture of the element

HW Unit (New Definition):

- "A hardware unit is the smallest block of hardware to which a specific hardware sub-function can be assigned."
- HWE.2 describes an architecture, where the HW units of the HW element are defined
- HWE.3 describes the detailed design of these HW units, that consist of HW parts
- Example: Electrical power supply

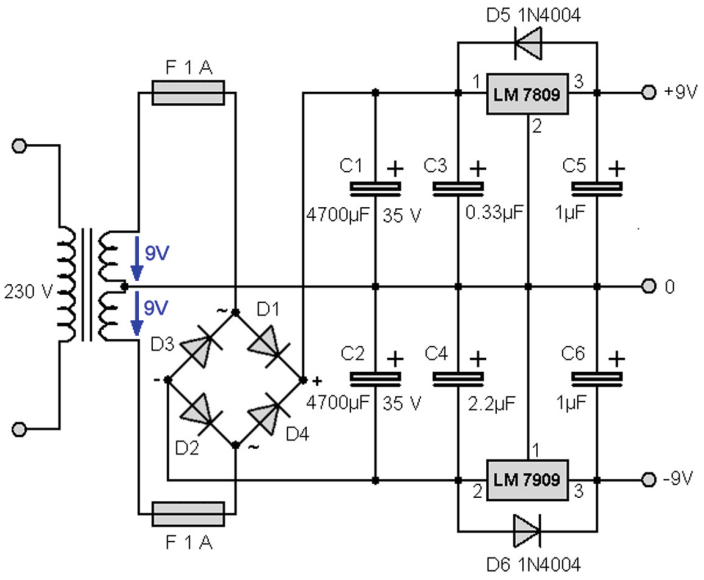

Fig. 3. Example of a hardware unit – electric power supply

In Fig. 3. Above the function of this module is to convert the 230 V to a circuit supply of 9 V. This includes different hardware parts and integrates them to a hardware unit. The hardware unit has a function which can be mapped onto unit testing including e.g. equivalence class test:

- Testing above 240 V, the fuses F1 shall fire, no voltage output
- Testing in 230 ± 10 V range, the system operates and delivers 9v

Hardware units can also include diagnose outputs such as a connection to an ADC that then writes the measured voltage to a register.

HW part (ISO 26262):

– Lowest level of HW
– Parts that are considered not to be sub-divided in this application scope
– E.g. a resistor or an IC.

4 Integrating Functional Safety Aspects in the Hardware Assessment Model

In ISO 26262 [2–4, 6, 8–13] two forms of assessment are done, a safety audit and a safety assessment. While the safety audit is a process assessment like Automotive SPICE the safety assessment is an assessment and evaluation of the product. Also the safety audit includes further aspects which need to be considered when assessing hardware.

Because ISO 26262:2011 assessments are used since years the members of the SOQRATES group expected an integration of both approaches. Therefore in the assessment model in chapter 5 of the paper safety related clauses are listed per Hardware SPICE base practice.

Below you find some specific work products which are additionally needed. The below is just an overview, more details have been described in previous safety related publications.

Safety Selects Parts that are Affected by a Safety Goal: All hardware parts that are affected by a safety goal inherit the ASIL (Automotive Safety integrity level, ASIL A – D) from the safety goal. E.g. In a steering system to not create more torque then demanded by the driver. The driver steering torque is measured by a torque sensor, and this torque is calculated by an ECU (Electronic Control Unit) and used to control an e-motor to provide this torque on the steering rack/system. Every hardware part in this functional chain and which is affected by the safety goal is marked with the proper ASIL A-D level. In steering the above mentioned safety goals is rated as ASIL – D. This includes e.g.

- The controller
- The torque sensor
- The connector from the torque sensor to the ASIC
- The ASIC/IC to convert the torque sensor
- The connection/bus between the ASIC and the controller
- The memory on the ECU
- The bridge to actuate the motor
- the bridge to connect to the motor and the IC to provide the phase currents.

Safety Looks at a FIT Rate: FIT stands for Failure in Time which is measured in hazardous errors occurring in 10^9 operating hours. 1 Fit is 10^{-9}, so one hazardous error in 10^9 operating hours. The higher the ASIL the higher the reliability of a hardware part has to become. And a safety goal rated ASIL D e.g. needs to achieve 10 FIT, which is 10^{-8}. 10^9 h observation time can easily be reached nowadays because cars are nowadays estimated with 10^4 h life time and a fleet of cars might by more than one million (10^6) using that component, making a total of $10^4 * 10^6 = 10^{10}$ h. When looking at single hardware units which are affected by the safety goal the ISO 26262 norm assumes around 100 such components in average and each having 10^{-10} h, so that $100 * 10^{-10} = 10^{-8}$ (meeting 10^{-8} ASIL – D goal).

Safety Uses Diagnostic Coverage to Reduce the FIT: The annex D of part 5 of the safety norm ISO 26262 includes guidance material to address 60%, 90%, or 99% diagnostic coverage. A simplified understanding is the following for signals:

- 60% - only values within range are accepted, so that the system only calculates with valid values.
- 90% - drift can be identified, so if the sensor starts to drift, the deviation can be detected. This usually requires a second separate channel and sensor to compare with.
- 99% - spiked and impact of oscillation is detected.
- 99.9% - together with the hardware manufacturer all known field issues are tested and the faults are detected.

The diagnostic coverage is then used to reduce the fit. E.g. if a controller has 400 FIT but in the architecture a second diverse controller is used to compare with the diagnostic coverage increases to 99%. If all known controller errors are detected (e.g. that both diverse controllers have not the same faults) the diagnostif coverage increases to 99.9%. The probability that the hazardous error is not detected is then decreasing to only 1 – 0.999 = 0.001. The 400 FIT are then reduced to 400 * 0.001 = 0.4 FIT.

Safety Looks at Single Point Faults and Latent Faults: The FIT rate is to be considered for single point and latent faults. A single point fault means that if a single hardware part is failing the hazardous error will appear. The latent fault means that the hardware part fails, the diagnose does detect the fault, and then the latent fault appears. The single point fault metric uses the FIT and the diagnose coverage as outlined above.

Safety Uses Decomposition Strategy: If you assign an ASIL – D to a hardware unit a design decision needs to be taken because

- mostly the hardware units/parts cannot be acquired at ASIL-D quality
- by using two different independent and diverse channels helps to increase the diagnostic coverage to 99.9% to get rid of the FIT.

Therefore in most ASIL ranked systems a decomposition into parallel independent parts/channels takes place.

Safety Uses an HSI – Hardware Software Interface: The HSI specifies safety critical hardware interfaces and assigns raw software variables (base software, physical

values, registers) and functional software variables. This allows to monitor and test safety critical physical and software parameters influencing the safe system behaviour.

Safety Expects an FMEDA - Failure Modes, Effects, and Diagnostic Analysis, and an FTA [5]: For each safety goal the affected hardware parts and their related diagnostic coverage are used to calculate a total FIT for single point faults. For each safety goal the affected hardware parts and their related diagnostic coverage are used to calculate a total FIT for latent point faults. There are many more such design strategies and they were integrated (using clauses from part 5 of ISO 26262) into the hardware SPICE assessment model.

5 The Hardware SPICE Assessment Model

Below you find an example HWE process as it is defined in the hardware SPICE assessment model. The whole model can be provided by the SOQRATES working party, under the condition that the materials are properly referenced and review input is provided back to the model developers in the SOQRATES group. This model then includes all 6 HWE processes with all base practices and ISO 26262 additional checklists. See example parts of the HWE.3 process below (the complete HWE.3 process is in the appendix (Table 1):

Table 1. Selected example of the HWE.3 Hardware Detailed Design Process

Process ID	HWE.3
Process name	Hardware Detailed Design
Process purpose	The purpose of the Hardware Detailed Design Process is to establish a detailed design for the hardware units
Process outcomes	As a result of successful implementation of this process: 1. A detailed design is developed that describes the composition of all hardware units into hardware parts and interfaces; 2. A detailed description of each hardware component and its interface is available; 3. The dynamic behaviour and resource consumption objectives of the hardware unit and software units related to the particular hardware unit are analysed; and 4. Consistency and bidirectional traceability are established between hardware requirements and hardware detailed design and consistency and bidirectional traceability are established between hardware architecture and the detailed hardware design 5. Hardware detailed design and the relationship to the hardware architectural design is agreed and communicated to all affected parties *Note: Definition of component detailed design includes development of verification criteria*

(*continued*)

Table 1. (*continued*)

Process ID	HWE.3
Base practices	**HWE.3.BP1: Develop hardware detailed design** Develop a hardware design, typically established through schematics, PCB design, layout, integrated circuit design, and similar artefacts, that represents a composition of all required hardware components, and that enables the fulfilment of the established functional and non-functional hardware requirements Develop criteria for verification of the detailed design. [Process Outcome 1] **HWE.3.BP2: Define/Refine interfaces of hardware units** Identify, specify/refine and document the internal and external interface(s) of each hardware component [Process Outcome 2] **HWE.3.BP3: Describe dynamic behaviour** Evaluate and document the timing and dynamic interaction of hardware components to meet the required dynamic behaviour of the system. If applicable include also the interaction with software or mechanic elements related to the particular hardware components Develop verification criteria according to the dynamic behaviour specified above. [Process Outcome 3, 4] *Note: Dynamic behaviour is determined by operating modes (e.g. start-up, shutdown, normal mode, calibration, diagnosis) as well as signal-based (timing, power-staging, transient behaviour of filters during switch operations, EMC, phase-/frequency response, required signal dynamics of amplifiers, power supply rejection/feed-through when changing loads, etc.)*
Output work products	04-00 Design - Hardware Design [Process Outcome 1, 2, 3, 4, 5] 13-19 Review record [Process Outcome 4, 5] 13-22 Traceability record [Process Outcome 5] 17-08 Interface requirement specification [Process Outcome 2]

For each base practice the companies in the working party SOQRATES assigned content of the ISO 26262 norm. This includes assignment of ISO 26262 clauses as well as additional questions that should be asked in case of a safety relevant development project. e.g. the additional questions asked by hardware safety exerts when joining the HWE SPICE assessment for **HWE.3.BP1: Develop hardware detailed design** are (Table 2):

Table 2. Example of additional safety related questions

• Can the individual elements/functional blocks be recognized in the PCB layout? • Do style guide/checklist exist for creating schematics (no flying pins, maximum amplification, blocking capacitors, termination of wires, high speed design vs. slew rates, clarity and comprehensibility) • Layout rules (manual vs. auto routing, use of signal constraints, minimum/maximum number of layers, impedance controlled layouts, parallel routing of differential signals, isochrone routing of time-critical signals of bus lines (timed routes); isolation and creeping distances; distances between not plated vias, pins in critrical areas e.g. measurement of I, U; proximity of blocking capacitors to ICs, connecting capacitors near to VCC or GND, IO protection, EMC/EMI filtering, thermal pads for higher power dissipation, separated GND/Power planes, Signal return path vs. layers) • Have mentioned guides been used (DRC, Checklist protocol) • Are the corresponding output files present (schematics, layout, Gerber-files, programming plans, ICT, …) • Are there assembly variants? Have they been marked and documented properly? • Have part tolerance been considered in part selection and layout? • Have special measures been done to safety critical areas? (e.g. by over-provisioning of parts? see ISO 26262-5:2011, 9.4.2.4: This requirement applies to ASIL C and D of the safety goal. A single-point fault occurring in a hardware part shall only be considered acceptable if dedicated measures are taken.) • Are connectors on the PCB and the future place sufficiently accessible?
• Have designs/outputs been placed under proper version/config control • Schematics • Layout/PCB • Assembly • Configuration-/calibration data • Variants • Labels • Housing • Material ID • Are verification criteria available

For example, the assignment of clauses for **HWE.3.BP1: Develop hardware detailed design** is shown below (Table 3):

Table 3. Example of ISO 26262 clauses assigned to a base practice

7.4.2.2 Non-functional causes for failure of a safety-related hardware part shall be considered during hardware detailed design, including the following influences, if applicable: temperature, vibrations, water, dust, EMI, noise factor, cross-talk originating either from other hardware parts of the hardware component or from its environment
7.4.2.3 The operating conditions of the hardware parts used in the hardware detailed design shall comply with the specification of their environmental and operational limits
7.4.2.4 Robust design principles should be considered

6 Expected Impact and Outlook

The AQUA [18, 19] (Knowledge alliance for Quality in Automotive engineering) integrates different norms and standards related to Functional safety, Automotive SPICE, APQP, Cybersecurity to manage the complexity of the systems and to achieve quality, safety, and security in the vehicle. AQUA created a new job role of a quality engineer that can integrate these methods and standards. AQUA will integrate the hardware SPICE into their educational program.

Major Tier 1 in SOQRATES [6] have co-developed to create a first version of the hardware SPICE plugin model. It can be used as a first draft to assess not inly the system and software but also the hardware in Automotive SPICE assessments. Since functional safety (ISO 26262 [2–4, 6, 8–13]) already does hardware assessment the hardware SPICE assessment model builds the bridge between the safety and the Automotive SPICE understanding.

7 The SPI Manifesto Revisited

The SPI manifesto [14–17] describes values and principles which need to be considered to make improvements work in an organisation. One of the approaches is to start with an assessment and to derive an improvement list. This is then used to set up an improvement program.

The principle "**Use dynamic and adaptable models as needed**" means that depending on the need of organisations specific models can be adapted. The hardware SPICE assessment model is such a new model which is needed in the Automotive domain.

The principle "**Base improvement on experience and measurements**" means that best practice experiences need to be shared and the usage must be tracked and measured. Since the model was developed in a group of Tier 1 in the SOQRATES working group the model development was based on such an experience and best practice sharing approach.

An additional principle proposed for the SPI manifesto is: "**Observe new trends and state of the art practices on the market and adopt**". The product liability law and the RAPEX (www.rapex.com) database changed the market because hazardous faults as well as legal violations in cars lead to a mandatory recall action and all cars must be repaired. This creates huge cost and thus new state of the art standards like functional safety, cybersecurity etc. became an important issue.

Acknowledgements. We are grateful to the members of the SOQRATES [6] working group who have contributed: Alastair Walker (LORIT), Alexander Much (Elektrobit), Frank König, Martin Dallinger, Thomas Wegner (ZF Friedrichshafen AG), Armin Riess (BBraun), Dietmar Kinalzyk (HELLA), Ralf Mayer (BOSCH Engineering), Gerhard Griessnig (AVL), Andreas Gruber (ZKW), Rainer Dreves, Ivan Sokic, Stephan Habel (Continental), Christian Schlager, Thomas Stiglhuber (Magna Powertrain ECS), Andreas Riel (ISCN/Grenoble INP), Helmut Zauchner, Christoph Karner (KTM), Andreas Gruber (ZKW), Georg Macher (AVL), Bernhard Sechser (Methodpark), Lutz Haunert (G&D), Damjan Ekert (ISCN), Richard Messnarz (ISCN).

We are also grateful to the European Commission which has funded some of the initiatives that funded the development of skills in the Automotive sector. ISCN is a member of AQUA (Knowledge Alliance for Quality in Automotive Engineering, 2013–2015) [18, 19], and AQU (Automotive Quality Universities, 2015–2017), and the BLUEPRINT project DRIVES (2018–2021).

References

1. Automotive SPICE 3.1, November 2017. www.automotivespice.com
2. ISO - International Organization for Standardization. ISO 26262 Road vehicles Functional Safety Part 1–10 (2011)
3. ISO - International Organization for Standardization. IEC 61508 Functional safety of electrical/electronic/programmable electronic safety-related systems
4. ISO - International Organization for Standardization. IEC 60812 Analysis techniques for system reliability - Procedure for failure mode and effects analysis (FMEA) (2006)
5. ISO - International Organization for Standardization. IEC 61025 Fault tree analysis (FTA), December 2006
6. ISO – International Organization for Standardization. ISO CD 26262-2018 2nd Edition Road vehicles Functional Safety (to appear)
7. SOQRATES, Task Forces Developing Integration of Automotive SPICE, ISO 26262 an d SAE J3061. http://soqrates.eurospi.net/
8. Messnarz, R., Kreiner, C., Riel, A.: Integrating automotive SPICE, functional safety, and cybersecurity concepts: a cybersecurity layer model. Softw. Qual. Prof. **18**(4), 13 (2016)
9. Messnarz, R., Kreiner, C., Riel, A., et al.: Implementing functional safety standards (SafEUr). Softw. Qual. Prof. **17**(3) (2015)
10. Macher, G., Sporer, H., Brenner, E., Kreiner, C.: Supporting cyber-security based on hardware-software interface definition. In: Kreiner, C., O'Connor, R.V., Poth, A., Messnarz, R. (eds.) EuroSPI 2016. CCIS, vol. 633, pp. 148–159. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44817-6_12
11. Macher, G., Messnarz, R., Kreiner, C., et al.: Integrated Safety and Security Development in the Automotive Domain, Working Group 17AE-0252/2017-01-1661, SAE International, June 2017
12. Redmill, F.: Understanding the use, misuse and abuse of safety integrity levels. In: Proceedings of the Eighth Safety-Critical Systems Symposium, Southampton, 8–10 February 2000. Springer, Heidelberg (2000)
13. Much, A.: Automotive security: challenges, standards and solutions. Softw. Qual. Prof. **18** (4), 4–12 (2016)
14. Korsaa, M., et al.: The SPI manifesto and the ECQA SPI manager certification scheme. J. Softw. Evol. Process **24**(5), 525–540 (2012)
15. Korsaa, M., et al.: The people aspects in modern process improvement management approaches. J. Softw. Evol. Process **25**(4), 381–391 (2013)
16. Messnarz, R., et al.: Social responsibility aspects supporting the success of SPI. J. Softw. Evol. Process **26**(3), 284–294 (2014)
17. Sanchez-Gordon, M.L., Colomo-Palacios, R., Amescua, A.: Towards measuring the impact of the SPI manifesto: a systematic review. In: Proceedings of European System and Software Process Improvement and Innovation Conference, pp. 100–110 (2013)

18. Messnarz, R., et al.: Integrating functional safety, automotive SPICE and Six Sigma – the AQUA knowledge base and integration examples. In: Barafort, B., O'Connor, R.V., Poth, A., Messnarz, R. (eds.) EuroSPI 2014. CCIS, vol. 425, pp. 285–295. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43896-1_26
19. Kreiner, C., et al.: Automotive knowledge alliance AQUA – integrating automotive SPICE, Six Sigma, and functional safety. In: McCaffery, F., O'Connor, R.V., Messnarz, R. (eds.) EuroSPI 2013. CCIS, vol. 364, pp. 333–344. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39179-8_30