# Impact of the New A-SPICE Appendix for Cybersecurity on the Implementation of ISO26262 for Functional Safety

Noha Moselhy(✉) and Yasser Ali

Valeo, Cairo, Egypt
{noha.moselhy,Yasser.ali}@valeo.com

**Abstract.** In the world of automotive industry, the usage of network communications and cloud services is an unavoidable need, which jeopardizes the vehicle systems to cyber-attacks, causing loss of money, vital information, or may be safety hazards. Hence, just as safety became a critical part of the development in the late 20th century, the automotive domain started to consider cyber-security as an integral part of the development of modern vehicles, which led the VDA to release the new A-SPICE appendix for Cybersecurity. For years, the co-design of automotive solutions depended on the integration of ISO26262 standard for Functional Safety with the SAE J3061 cybersecurity-guide-book SAE [International, a global standards development organization and professional association of engineers and technical experts in the aerospace, automotive, and commercial-vehicle industries]. In this paper, a demonstration will be presented through a case study performed with a certain methodology to illustrate the impact of the new Automotive SPICE standard for Cybersecurity on the implementation of ISO26262 standard for Functional Safety.

**Keywords:** Automotive SPICE for cybersecurity · SAE J3061 · ISO26262 · Automotive software · Improved implementation of functional safety work products

## 1 Introduction

Cybersecurity plays a vital role in the development of connected cars. Remote hacking of cars and cyber-attacks via system penetration or network based scanning resulted in famous accidents that jeopardize the safety of many souls. In the past, vehicle vulnerability would only arise from malfunction of one or more of the internal car systems, but today, it is not enough to implement safety mechanisms without considerations of security factors from the external environment of the vehicle.

As a result, the automotive industry became aware of such challenges, and started to introduce guidelines for the development of both safety and security-based solutions. Furthermore, the possible integration between the two standards remained a critical research topic in hopes that one day we will have one single process workflow for the implementation of a software solution that is compliant to both Functional Safety as

M. Yilmaz et al. (Eds.): EuroSPI 2021, CCIS 1442, pp. 122–136, 2021.
https://doi.org/10.1007/978-3-030-85521-5_9

described in the ISO26262, as well as Cyber-Security as described in the SAE J3061 Guide-Book.

Today, a new factor was introduced to the equation by the German Association of the Automotive Industry VDA; which the “Automotive SPICE for Cybersecurity”, giving not only guidelines for technical implementation of such systems, but also a tool for Automotive SPICE assessors to evaluate the development process of the Cybersecurity components (System or Software) versus the expectations of the standards.

In the course of this paper, we will present how the base practices of the new Automotive SPICE processes for Cybersecurity impact the implementation of ISO26262 standard work products.

This paper is organized as follows: [1] Description of the paper background, [2] A detailed Case Study to drive the improvement of functional safety work products compliance to automotive SPICE appendix for Cybersecurity, [3] Observation & findings, [4] Results, and finally [5] Conclusion of the work.

### 1.1 Scope

This paper addresses the automotive tier 1 suppliers in general and automotive software suppliers who are providing software solutions in the automotive field in specific. Currently, most of the OEMs require suppliers to be certified to Automotive SPICE as a prerequisite for becoming and remaining a supplier in the OEM’s database or being considered for future business. Extending this requirement to include compliance to Automotive SPICE for Cybersecurity is a natural expectation.

### 1.2 Background and Approaches

The need to integrate both safety and security engineering standard approaches into one practical process has been under study for many years now. In September of the year 2017, Georg Macher, a researcher from Graz University of Technology submitted one of the latest papers on the topic under the title: “Automotive SPICE, Safety and Cybersecurity Integration” in the “International Conference on Computer Safety, Reliability, and Security” – with others [6].

The paper addressed studies, standards and work groups who covered relevant topics such as various safety assessments techniques (e.g.: Failure Mode and effect analysis (FMEA), Fault Tree Analysis (FTA)), cyber-security implementation guiding principles (e.g.: SAE J3061[9]), as well as the different approaches previously used to describe the integration between Safety and Cybersecurity (e.g.: SoQrates Security AK [11], IEC 62443 [12])… etc.

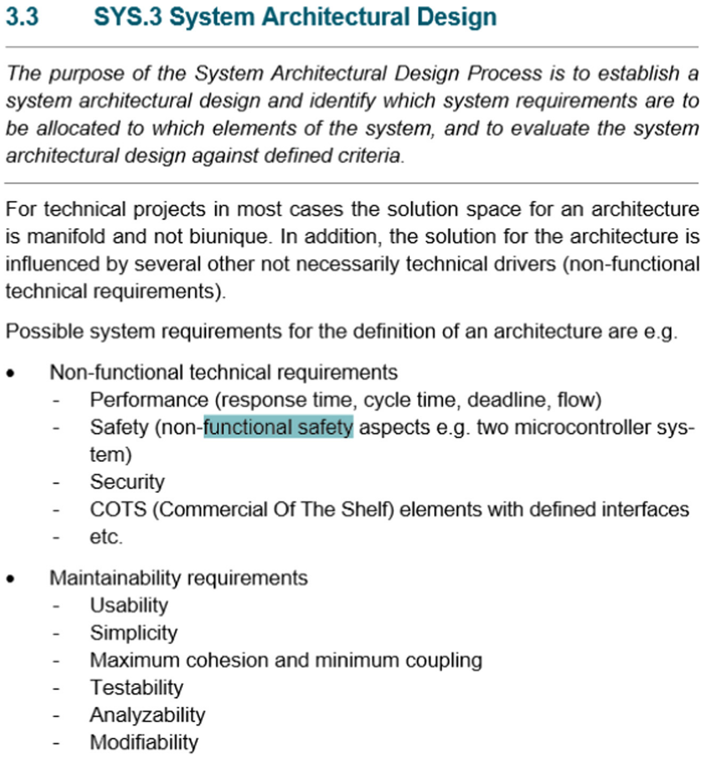
The paper also addressed newly created assessment models back then that aimed at evaluating the functional safety processes inside the automotive industry (e.g.: SS 7740 [13]) and were based on the Automotive SPICE standardized capability levels.

The presented case study was based on a safety critical system scenario (electronic steering system) that is implemented according to the ISO26262 [7] and is subject to cybersecurity threats, moving towards how the implementation of this system can be evaluated by an automotive SPICE assessor. The suggested A-SPICE assessment of the system in question was based on one approach, which assumes that both functional safety and cybersecurity criteria can be appended to A-SPICE process practices as notes, or extra base practices.

That is, if the base practice 1 of "SYS.3 SYSTEM ARCHITECTURAL DESIGN" is speaking about the need to "Define System architectural design", the additional notes from Functional Safety would speak about the definition of "Technical Safety Concept", while the note from cybersecurity can ask if there are any traceable cybersecurity requirements in the upstream of this architecture.

Being one of the latest comprehensive papers on the topic, the study did not tackle other assessment approaches that handled Safety aspects as separate – yet complementary - process areas to the existing process areas of Automotive SPICE. In addition, the mapping between automotive SPICE process practices, cybersecurity activities, and safety work products has not been analyzed in the first place.

With the popularity of the VDA Guidelines for the Automotive SPICE 1st Edition (also released in 2017 and known as the A-SPICE blue book), it became evident that Safety aspects are treated as notes or explanations on existing automotive SPICE process practices, up until now (see Fig. 1 Example of Automotive SPICE guideline referral to Safety aspects).



### 3.3 SYS.3 System Architectural Design

*The purpose of the System Architectural Design Process is to establish a system architectural design and identify which system requirements are to be allocated to which elements of the system, and to evaluate the system architectural design against defined criteria.*

For technical projects in most cases the solution space for an architecture is manifold and not biunique. In addition, the solution for the architecture is influenced by several other not necessarily technical drivers (non-functional technical requirements).

Possible system requirements for the definition of an architecture are e.g.

- Non-functional technical requirements
  - Performance (response time, cycle time, deadline, flow)
  - Safety (non-functional safety aspects e.g. two microcontroller system)
  - Security
  - COTS (Commercial Of The Shelf) elements with defined interfaces
  - etc.
- Maintainability requirements
  - Usability
  - Simplicity
  - Maximum cohesion and minimum coupling
  - Testability
  - Analyzability
  - Modifiability

**Fig. 1.** Example of automotive SPICE guideline referral to Safety aspects (SYS.3)

Today, and after the release of the draft Automotive SPICE appendix for Cybersecurity with completely separate processes; the need to re-evaluate the mapping of the new "SEC" process group to safety aspects, and analyze its impact on the implementation of the traditional Functional Safety work products became critical.

### 1.3 Relationship with the EUROSPI Manifesto

Based on the principle "Use dynamic and adaptable models as needed" from EURO Software Process improvement (EURO SPI) Manifesto [2], which aims to drive organizations improvements for software development processes through applying a combination of process models.

Also, based on the principal "Apply risk management" that enforces the organizations to consider and follow the risk based thinking methodology which is aligned with the global direction of the IATF 16949–2016 requirements that were derived in line with ISO 9001–2015 requirements.

Accordingly, the following solution was suggested to improve the organization's ability to develop Functional Safety work products that are compliant with the new cybersecurity process model extension of A-SPICE for system and software development processes in the project.

## 2 Case Study Methodology and Scope

A case study has been applied on a certain software project with ASiL critical components and a Cybersecurity deliverable commitment, to determine the impact of releasing the new Automotive SPICE appendix for Cybersecurity on the compliance level of the project ISO26262 work products, such that, the project "Safety Relevant" work products were assessed using A-SPICE version 3.1 and were re-inspected again using the A-SPICE appendix for Cybersecurity to see if they will obtain the same compliance level with the same gaps identified.

First, a sample of Functional Safety work product descriptions were created (templates, guidelines…) to be applied in the selected software project for the purpose of this case study according to ISO26262 mandated list of work products. The ASiL work products delivered by this project were following the provided samples.

Then that project was initially assessed by Automotive SPICE Process assessment model version 3.1 targeting capability level 2 for the VDA scope process areas, and was found compliant (without consideration of the Cybersecurity appendix).

Later, the same project with the same set of Functional Safety work products was re-inspected using the Automotive SPICE appendix for Cybersecurity, to find that there are new gaps introduced on the previously created sample of ASiL work products that we recommend should now to be covered, especially in a project with Cybersecurity requirements.

The study methodology followed in this paper work was based on following steps as per [Fig. 2]:

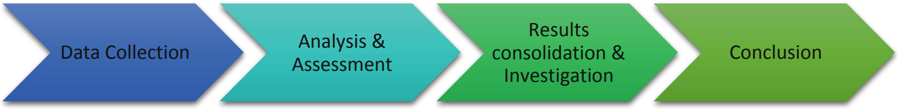


**Fig. 2.** Steps of this case study methodology

- **Data Collection**: In this step:
  - The Functional Safety work products that are mandated by ISO26262 according to different ASiL levels were listed, and their applicability on the Project under the case study has been decided based on the Product ASiL level (refer to Table 1).
  - The applicable ISO26262 work products were developed within the project ASiL activities according to the defined descriptions.
  - The project work products were first assessed against Automotive SPICE version 3.1 (excluding the Cybersecurity appendix), and was found compliant with capability level two (refer to Table 2) in spite of the CS deliverables.

**Table 1.** List of Functional Safety work products investigated

| ISO26262 work product | Abbreviation | Applicability in the Project (Y/N) | Purpose |
|---|---|---|---|
| Safety development plan | SaDP | Y | A project management artifact, to describe the activities & work products as defined in ISO2626 with respect to the related ASIL functions |
| Hazard assessment & risk analysis (HARA) | HARA | Y | Is mentioned in Part-3 of ISO 26262. with a purpose to identify the malfunctions that could possibly lead to system hazards and assess their associated risks |
| Functional safety concept | FSC | Y | The safety concept describes how functional safety will be achieved mainly at vehicle system level |

(*continued*)

**Table 1.** (*continued*)

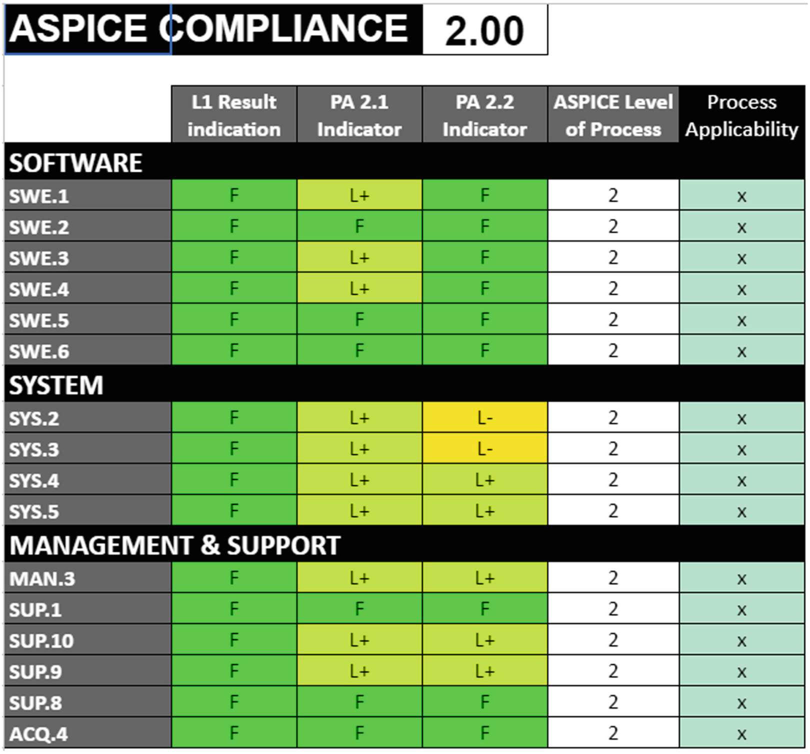
| ISO26262 work product | Abbreviation | Applicability in the Project (Y/N) | Purpose |
|---|---|---|---|
| Technical safety concept | TSC | Y | The technical safety concept describes how functional safety will be achieved when the component is operating (architectural level) |
| Safety test strategy | -- | Y | The safety test strategy plans the activities to verify the functional safety requirements and technical safety requirements in a consistent way |
| Failure mode & effect analysis | -FMEA | -N | FMEDA is a functional approach used to analyze component architecture and to systematically evaluate propagation of the possible internal failures to the outputs of the component |
| Software safety design analysis/ critical path analysis | SDA/CPA | Y | The safety analysis must consider the propagation of failures between software modules and verify that they are mitigated by safety mechanisms |
| Safety verification report | SVR | Y | The Safety verification report ensures the coverage of all the safety requirements defined in the TSaC |

(*continued*)

**Table 1.** (*continued*)

| ISO26262 work product | Abbreviation | Applicability in the Project (Y/N) | Purpose |
|---|---|---|---|
| Safety case | SaC | Y | Safety case communicates a clear, comprehensive and defensible argument that the system is acceptably safe to be operated. It is the sum of the deliverables issued following the application of the safety process |
| Software tools qualification | SWTQR | Y | The objective is to provide evidence for tool suitability for use in product development in compliance with ISO26262 |

**Table 2.** CL2 ASPICE Profile for the first assessment of the Project before ASPICE CS appendix Release



ASPICE COMPLIANCE 2.00

| | L1 Result indication | PA 2.1 Indicator | PA 2.2 Indicator | ASPICE Level of Process | Process Applicability |
|---|---|---|---|---|---|
| **SOFTWARE** | | | | | |
| SWE.1 | F | L+ | F | 2 | x |
| SWE.2 | F | F | F | 2 | x |
| SWE.3 | F | L+ | F | 2 | x |
| SWE.4 | F | L+ | F | 2 | x |
| SWE.5 | F | F | F | 2 | x |
| SWE.6 | F | F | F | 2 | x |
| **SYSTEM** | | | | | |
| SYS.2 | F | L+ | L- | 2 | x |
| SYS.3 | F | L+ | L- | 2 | x |
| SYS.4 | F | L+ | L+ | 2 | x |
| SYS.5 | F | L+ | L+ | 2 | x |
| **MANAGEMENT & SUPPORT** | | | | | |
| MAN.3 | F | L+ | L+ | 2 | x |
| SUP.1 | F | F | F | 2 | x |
| SUP.10 | F | L+ | L+ | 2 | x |
| SUP.9 | F | L+ | L+ | 2 | x |
| SUP.8 | F | F | F | 2 | x |
| ACQ.4 | F | F | F | 2 | x |

- **Analysis and Assessment:** In this step, the same list of project work products were then re-inspected against Automotive SPICE **including** the Cybersecurity appendix. and were found compliant yet a new set of gaps were identified.
- **Results consolidation and investigation:** In this step, results and obtained data of the inspection from the previous step are consolidated. An investigation was carried out to determine the differences between the work product samples before and after impact of the new Automotive SPICE process group for Cybersecurity (SEC).
- **Conclusion:** In this step a final recommendation is given based on application of the new proposed CS practices on the project.

## 3 Case Study Observations and Results Consolidation

A case study was conducted to study the impact of the BPs, outcomes, and work products of the new Automotive SPICE process group for Cybersecurity on the output work products of ISO26262 as implemented in the previously ASIL assessed software project with Cybersecurity scope.

The case study aimed at recording the observations about the differences between the work products before and after A-SPICE CS scope application in a readable format for researchers.

The following Table 3 demonstrates the project output list of Functional Safety work products investigated mapped to their relevant SEC process areas:

**Table 3.** List of functional safety work products investigated vs. relevant SEC process areas

| ISO26262 Work product | Abbreviation | Relevant cybersecurity (CS) process area |
|---|---|---|
| Safety development plan | SaDP | MAN.7 CS risk management |
| Hazard assessment & risk analysis | HARA | SEC.1 CS requirements elicitation |
| Functional safety concept | FSC | SEC.1 CS requirements elicitation |
| Technical safety concept | TSC | SEC.2 CS implementation |
| Safety test strategy | -- | SEC.3 CS risk treatment verification<br>SEC.4 CS risk Treatment Validation |
| Failure mode & effect analysis | -FMEA | MAN.7 CS risk management |
| Safety design analysis | SDA | SEC.2 CS implementation |
| Safety verification report | SVR | SEC.3 CS risk treatment verification<br>SEC.4 CS risk treatment validation |
| Safety case | SaC | MAN.7 CS risk management<br>SEC.3 CS risk treatment verification<br>SEC.4 CS risk treatment validation |
| Software tools qualification | SWTQR | MAN.7 CS risk management |

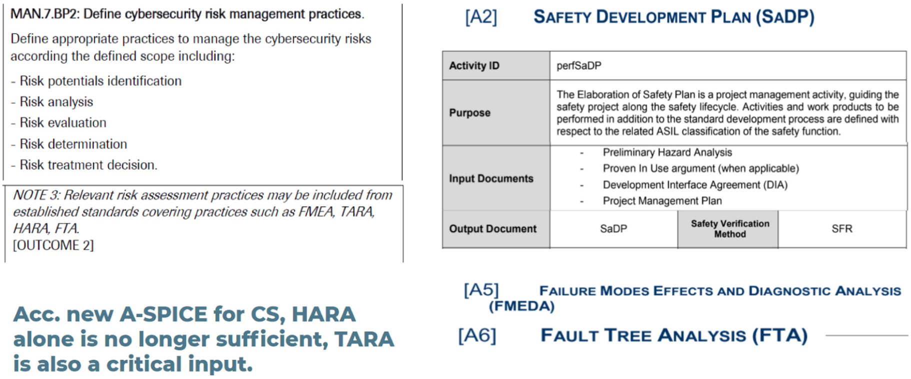
The below set of illustrations show the suggested improvements to be applied in the future to each of the ISO26262 work products from the study perspective, as a result of applying the new methodology suggested by the ASPICE appendix for CS on the project work products:

### 3.1 Safety Development Plan (SaDP)

In ISO26262 the safety development plan is a project management activity, which defines the safety activities and work products to be performed in that project.

When comparing it to MAN.7 BP2, it has been shown that the definition of the appropriate practices to manage the cybersecurity risks can be added as a chapter inside the safety development plan.

Also the inputs for the Safety Development Plan (SaDP) will need to take into consideration the Threat Assessment and Remediation Analysis (TARA) analysis for example, instead of the Hazards Analysis and Risk Assessment (HARA) only as before (see Fig. 3).



MAN.7.BP2: Define cybersecurity risk management practices.

Define appropriate practices to manage the cybersecurity risks according the defined scope including:

- Risk potentials identification
- Risk analysis
- Risk evaluation
- Risk determination
- Risk treatment decision.

*NOTE 3: Relevant risk assessment practices may be included from established standards covering practices such as FMEA, TARA, HARA, FTA.*
[OUTCOME 2]

Acc. new A-SPICE for CS, HARA alone is no longer sufficient, TARA is also a critical input.

[A2] SAFETY DEVELOPMENT PLAN (SADP)

| | | | |
|---|---|---|---|
| Activity ID | perfSaDP | | |
| Purpose | The Elaboration of Safety Plan is a project management activity, guiding the safety project along the safety lifecycle. Activities and work products to be performed in addition to the standard development process are defined with respect to the related ASIL classification of the safety function. | | |
| Input Documents | - Preliminary Hazard Analysis<br>- Proven In Use argument (when applicable)<br>- Development Interface Agreement (DIA)<br>- Project Management Plan | | |
| Output Document | SaDP | Safety Verification Method | SFR |

[A5] FAILURE MODES EFFECTS AND DIAGNOSTIC ANALYSIS (FMEDA)

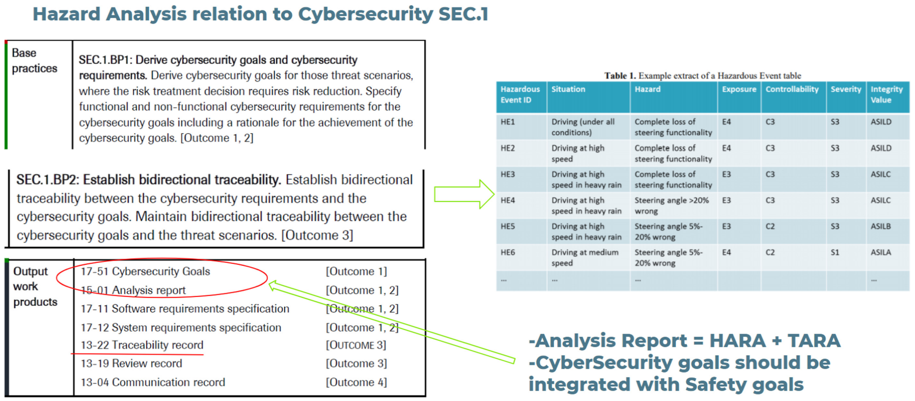
[A6] FAULT TREE ANALYSIS (FTA)

**Fig. 3.** Impact on SaDP from SPICE for CS BP's & outcomes, plus suggested improvements

### 3.2 Hazard Analysis and Risk Assessment (HARA)

As shown in Fig. 4 below, the Cybersecurity goals and analysis report can be integrated with the Hazard Analysis and Risk Assessment (HARA) report to meet the criteria for SEC.1 BP1.

Security-Aware Hazard and Risk Analysis Method [SAHARA] has been introduced in this paper [5] before to fulfill such an approach [Combining between both HARA/TARA].



Hazard Analysis relation to Cybersecurity SEC.1

| | |
|---|---|
| Base practices | **SEC.1.BP1: Derive cybersecurity goals and cybersecurity requirements.** Derive cybersecurity goals for those threat scenarios, where the risk treatment decision requires risk reduction. Specify functional and non-functional cybersecurity requirements for the cybersecurity goals including a rationale for the achievement of the cybersecurity goals. [Outcome 1, 2] |

**SEC.1.BP2: Establish bidirectional traceability.** Establish bidirectional traceability between the cybersecurity requirements and the cybersecurity goals. Maintain bidirectional traceability between the cybersecurity goals and the threat scenarios. [Outcome 3]

| | | |
|---|---|---|
| Output work products | 17-51 Cybersecurity Goals | [Outcome 1] |
| | 15-01 Analysis report | [Outcome 1, 2] |
| | 17-11 Software requirements specification | [Outcome 1, 2] |
| | 17-12 System requirements specification | [Outcome 1, 2] |
| | 13-22 Traceability record | [OUTCOME 3] |
| | 13-19 Review record | [Outcome 3] |
| | 13-04 Communication record | [Outcome 4] |

**Table 1.** Example extract of a Hazardous Event table

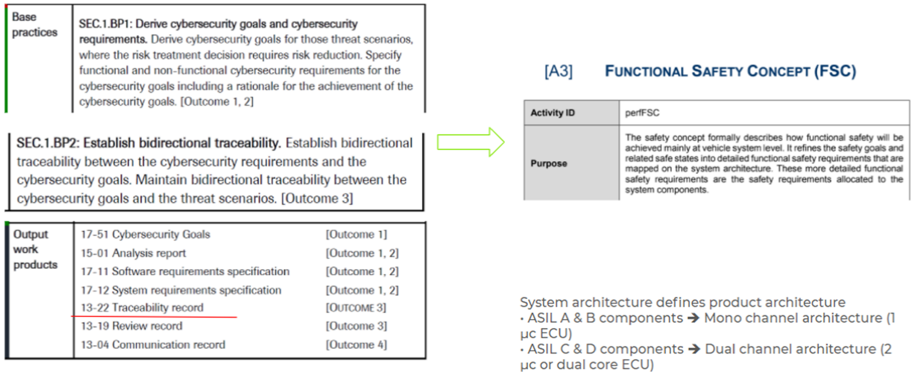
| Hazardous Event ID | Situation | Hazard | Exposure | Controllability | Severity | Integrity Value |
|---|---|---|---|---|---|---|
| HE1 | Driving (under all conditions) | Complete loss of steering functionality | E4 | C3 | S3 | ASILD |
| HE2 | Driving at high speed | Complete loss of steering functionality | E4 | C3 | S3 | ASILD |
| HE3 | Driving at high speed in heavy rain | Complete loss of steering functionality | E3 | C3 | S3 | ASILC |
| HE4 | Driving at high speed in heavy rain | Steering angle >20% wrong | E3 | C3 | S3 | ASILC |
| HE5 | Driving at high speed in heavy rain | Steering angle 5%-20% wrong | E3 | C2 | S3 | ASILB |
| HE6 | Driving at medium speed | Steering angle 5%-20% wrong | E4 | C2 | S1 | ASILA |
| ... | ... | ... | | | | ... |

-Analysis Report = HARA + TARA
-CyberSecurity goals should be integrated with Safety goals

**Fig. 4.** Impact on Hazard Analysis from SPICE for CS BP's & outcomes, plus suggested improvements

## 3.3 Functional Safety Concept (FSC)

Cybersecurity requirements can be embedded inside the functional safety concept and to be mapped to cybersecurity goals as they both serve the same concept of maintaining the safety and security of the product and those using it (see Fig. 5 below). A traceability record should be maintained as well.



| | |
|---|---|
| Base practices | **SEC.1.BP1: Derive cybersecurity goals and cybersecurity requirements.** Derive cybersecurity goals for those threat scenarios, where the risk treatment decision requires risk reduction. Specify functional and non-functional cybersecurity requirements for the cybersecurity goals including a rationale for the achievement of the cybersecurity goals. [Outcome 1, 2] |

**SEC.1.BP2: Establish bidirectional traceability.** Establish bidirectional traceability between the cybersecurity requirements and the cybersecurity goals. Maintain bidirectional traceability between the cybersecurity goals and the threat scenarios. [Outcome 3]

| | | |
|---|---|---|
| Output work products | 17-51 Cybersecurity Goals | [Outcome 1] |
| | 15-01 Analysis report | [Outcome 1, 2] |
| | 17-11 Software requirements specification | [Outcome 1, 2] |
| | 17-12 System requirements specification | [Outcome 1, 2] |
| | 13-22 Traceability record | [OUTCOME 3] |
| | 13-19 Review record | [Outcome 3] |
| | 13-04 Communication record | [Outcome 4] |

[A3] FUNCTIONAL SAFETY CONCEPT (FSC)

| | |
|---|---|
| **Activity ID** | perfFSC |
| **Purpose** | The safety concept formally describes how functional safety will be achieved mainly at vehicle system level. It refines the safety goals and related safe states into detailed functional safety requirements that are mapped on the system architecture. These more detailed functional safety requirements are the safety requirements allocated to the system components. |

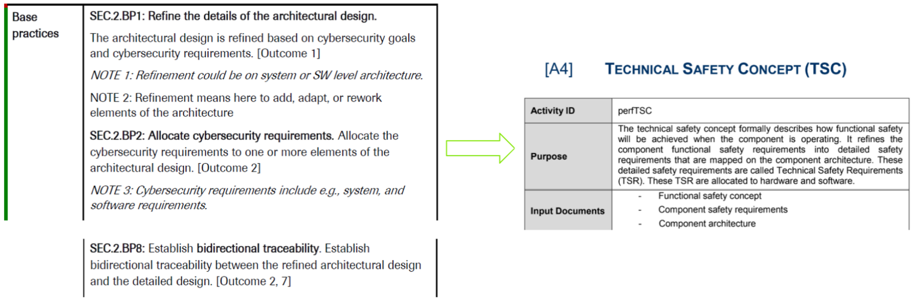
System architecture defines product architecture
- ASIL A & B components ➔ Mono channel architecture (1 µc ECU)
- ASIL C & D components ➔ Dual channel architecture (2 µc or dual core ECU)

**Fig. 5.** Impact on FSC from SPICE for CS BP's & outcomes, plus suggested improvements

## 3.4 Technical Safety Concept (TSC)

As stated in SEC.2 BP1, the refinement of cybersecurity requirements is quite similar to the purpose of the refinement of the technical safety requirements in the Technical Safety Concept "TSaC" both can happen in the same document "TSaC".

The allocation of the cybersecurity related requirements to system / software layers is then essential, as stated in SEC.2 BP2 (see Fig. 6):



| | |
|---|---|
| Base practices | **SEC.2.BP1: Refine the details of the architectural design.**<br>The architectural design is refined based on cybersecurity goals and cybersecurity requirements. [Outcome 1]<br>*NOTE 1: Refinement could be on system or SW level architecture.*<br>NOTE 2: Refinement means here to add, adapt, or rework elements of the architecture<br>**SEC.2.BP2: Allocate cybersecurity requirements.** Allocate the cybersecurity requirements to one or more elements of the architectural design. [Outcome 2]<br>*NOTE 3: Cybersecurity requirements include e.g., system, and software requirements.* |

SEC.2.BP8: Establish **bidirectional traceability**. Establish bidirectional traceability between the refined architectural design and the detailed design. [Outcome 2, 7]

[A4] TECHNICAL SAFETY CONCEPT (TSC)

| | |
|---|---|
| Activity ID | perfTSC |
| Purpose | The technical safety concept formally describes how functional safety will be achieved when the component is operating. It refines the component functional safety requirements into detailed safety requirements that are mapped on the component architecture. These detailed safety requirements are called Technical Safety Requirements (TSR). These TSR are allocated to hardware and software. |
| Input Documents | - Functional safety concept<br>- Component safety requirements<br>- Component architecture |

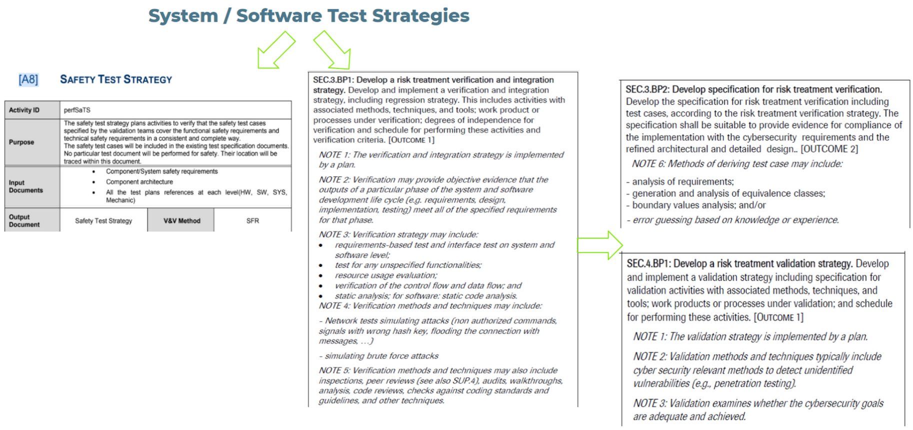
**Fig. 6.** Impact on TSC from SPICE for CS BP's & outcomes, plus suggested improvements

## 3.5 Safety Test Strategy

The project test strategy (System or Software) should include all test methods that will be applied on a certain solution or product.

Since most ASiL projects already have a safety test strategy (as indicated by ISO26262) which guides the working team on the needed activities to verify and validate certain safety requirements, another extension can be added for cybersecurity related tests as shown in SEC.3 BP1 and SEC.4 BP1.

The purpose of this will be to include in one place an explanation for the overall strategy of testing, with all its aspects (Safety/Security) for the given solution – see Fig. 7.



System / Software Test Strategies

[A8] SAFETY TEST STRATEGY

| | | | |
|---|---|---|---|
| Activity ID | perfSaTS | | |
| Purpose | The safety test strategy plans activities to verify that the safety test cases specified by the validation teams cover the functional safety requirements and technical safety requirements in a consistent and complete way.<br>The safety test cases will be included in the existing test specification documents. No particular test document will be performed for safety. Their location will be traced within this document. | | |
| Input Documents | • Component/System safety requirements<br>• Component architecture<br>• All the test plans references at each level(HW, SW, SYS, Mechanic) | | |
| Output Document | Safety Test Strategy | V&V Method | SFR |

**SEC.3.BP1: Develop a risk treatment verification and integration strategy.** Develop and implement a verification and integration strategy, including regression strategy. This includes activities with associated methods, techniques, and tools; work product or processes under verification; degrees of independence for verification and schedule for performing these activities and verification criteria. [OUTCOME 1]

*NOTE 1: The verification and integration strategy is implemented by a plan.*

*NOTE 2: Verification may provide objective evidence that the outputs of a particular phase of the system and software development life cycle (e.g. requirements, design, implementation, testing) meet all of the specified requirements for that phase.*

*NOTE 3: Verification strategy may include:*
- *requirements-based test and interface test on system and software level;*
- *test for any unspecified functionalities;*
- *resource usage evaluation;*
- *verification of the control flow and data flow; and*
- *static analysis; for software: static code analysis.*

*NOTE 4: Verification methods and techniques may include:*

*- Network tests simulating attacks (non authorized commands, signals with wrong hash key, flooding the connection with messages, ...)*

*- simulating brute force attacks*

*NOTE 5: Verification methods and techniques may also include inspections, peer reviews (see also SUP.4), audits, walkthroughs, analysis, code reviews, checks against coding standards and guidelines, and other techniques.*

**SEC.3.BP2: Develop specification for risk treatment verification.** Develop the specification for risk treatment verification including test cases, according to the risk treatment verification strategy. The specification shall be suitable to provide evidence for compliance of the implementation with the cybersecurity requirements and the refined architectural and detailed design.. [OUTCOME 2]

*NOTE 6: Methods of deriving test case may include:*

- analysis of requirements;
- generation and analysis of equivalence classes;
- boundary values analysis; and/or
- *error guessing based on knowledge or experience.*

**SEC.4.BP1: Develop a risk treatment validation strategy.** Develop and implement a validation strategy including specification for validation activities with associated methods, techniques, and tools; work products or processes under validation; and schedule for performing these activities. [OUTCOME 1]

*NOTE 1: The validation strategy is implemented by a plan.*

*NOTE 2: Validation methods and techniques typically include cyber security relevant methods to detect unidentified vulnerabilities (e.g., penetration testing).*

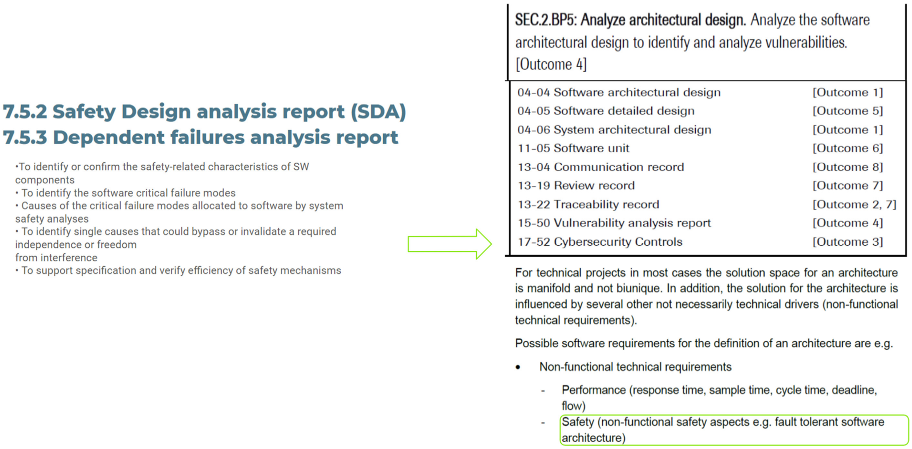
*NOTE 3: Validation examines whether the cybersecurity goals are adequate and achieved.*

**Fig. 7.** Impact on Safety Test Strategy from SPICE for CS BP's & outcomes, plus suggested improvements

## 3.6 Safety Design Analysis (SDA)

ISO26262 Safety Design Analysis (SDA) shall take the Cybersecurity Vulnerability Report (CSVR) into consideration while analyzing Cybersecurity components of the solution (e.g.: network based scans) in order to check if further safety mechanisms need to be implemented (see Fig. 8 below).

- Functional Safety manager shall participate in the analysis of the defined Cybersecurity controls to be able to advise if more controls need to be implemented.
- A few activities should be added to the solution architecture (system/ software) to ensure compliance to A-SPICE for Cybersecurity (e.g.: Vulnerability analysis report).
- A-SPICE guideline shall refer to the need of system vulnerabilities analysis.



7.5.2 Safety Design analysis report (SDA)
7.5.3 Dependent failures analysis report

•To identify or confirm the safety-related characteristics of SW components
• To identify the software critical failure modes
• Causes of the critical failure modes allocated to software by system safety analyses
• To identify single causes that could bypass or invalidate a required independence or freedom from interference
• To support specification and verify efficiency of safety mechanisms

**SEC.2.BP5: Analyze architectural design.** Analyze the software architectural design to identify and analyze vulnerabilities. [Outcome 4]

| | |
|---|---|
| 04-04 Software architectural design | [Outcome 1] |
| 04-05 Software detailed design | [Outcome 5] |
| 04-06 System architectural design | [Outcome 1] |
| 11-05 Software unit | [Outcome 6] |
| 13-04 Communication record | [Outcome 8] |
| 13-19 Review record | [Outcome 7] |
| 13-22 Traceability record | [Outcome 2, 7] |
| 15-50 Vulnerability analysis report | [Outcome 4] |
| 17-52 Cybersecurity Controls | [Outcome 3] |

For technical projects in most cases the solution space for an architecture is manifold and not biunique. In addition, the solution for the architecture is influenced by several other not necessarily technical drivers (non-functional technical requirements).

Possible software requirements for the definition of an architecture are e.g.

- Non-functional technical requirements
  - Performance (response time, sample time, cycle time, deadline, flow)
  - Safety (non-functional safety aspects e.g. fault tolerant software architecture)

**Fig. 8.** Impact on SDA from SPICE for CS BP's & outcomes, plus suggested improvements

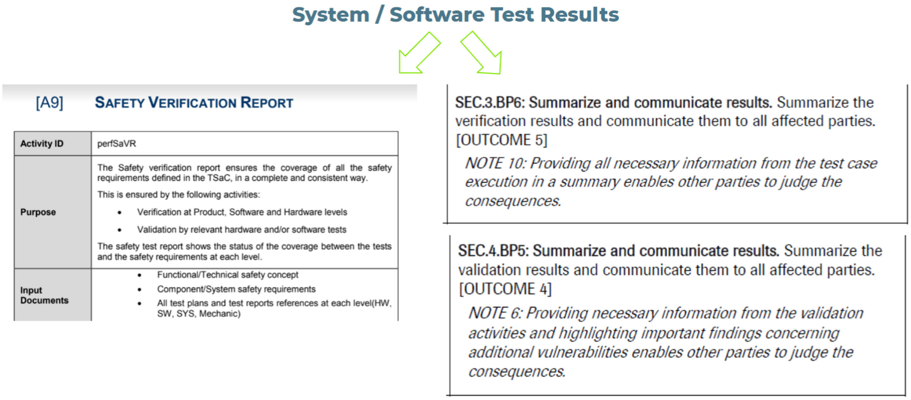
## 3.7 Safety Verification Report (SVR)

The purpose of Safety Verification Report (SVR) as defined in ISO26262 is to ensure that all requirements defined in the Technical Safety Concept (TSaC) are consistent and have been verified on both system and software levels.

In order to align with A-SPICE for Cybersecurity, the SVR shall consider the practices SEC.3 BP6 and SEC.4 BP5 coming from Cybersecurity testing processes.

That is, the test results coming from the verification of cybersecurity related requirements shall be embedded also within the same SVR of the project.

By this integration of verification reports, we will not only ensure that safety related requirements are consistent and covered but also that cybersecurity requirements have been verified as well and are in line with the overall solution goals (refer to Fig. 9 below).



System / Software Test Results

[A9] SAFETY VERIFICATION REPORT

| | |
|---|---|
| Activity ID | perfSaVR |
| Purpose | The Safety verification report ensures the coverage of all the safety requirements defined in the TSaC, in a complete and consistent way.<br>This is ensured by the following activities:<br>• Verification at Product, Software and Hardware levels<br>• Validation by relevant hardware and/or software tests<br>The safety test report shows the status of the coverage between the tests and the safety requirements at each level. |
| Input Documents | • Functional/Technical safety concept<br>• Component/System safety requirements<br>• All test plans and test reports references at each level(HW, SW, SYS, Mechanic) |

**SEC.3.BP6: Summarize and communicate results.** Summarize the verification results and communicate them to all affected parties. [OUTCOME 5]

*NOTE 10: Providing all necessary information from the test case execution in a summary enables other parties to judge the consequences.*

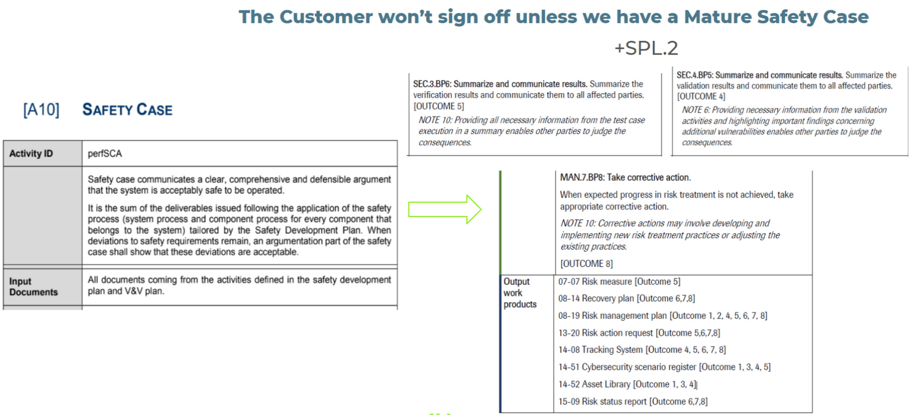
**SEC.4.BP5: Summarize and communicate results.** Summarize the validation results and communicate them to all affected parties. [OUTCOME 4]

*NOTE 6: Providing necessary information from the validation activities and highlighting important findings concerning additional vulnerabilities enables other parties to judge the consequences.*

**Fig. 9.** Impact on SVR from SPICE for CS BP's & outcomes, plus suggested improvements

## 3.8 Safety Case (SaC)

In the end of an ASiL project, the safety case is the sum of all deliverables of the safety process, we can add to it the related cybersecurity deliverables to present a cybersecurity compliant product as well (see Fig. 10 below).



The Customer won't sign off unless we have a Mature Safety Case

+SPL.2

[A10] SAFETY CASE

| | |
|---|---|
| Activity ID | perfSCA |
| | Safety case communicates a clear, comprehensive and defensible argument that the system is acceptably safe to be operated.<br>It is the sum of the deliverables issued following the application of the safety process (system process and component process for every component that belongs to the system) tailored by the Safety Development Plan. When deviations to safety requirements remain, an argumentation part of the safety case shall show that these deviations are acceptable. |
| Input Documents | All documents coming from the activities defined in the safety development plan and V&V plan. |

**SEC.3.BP6: Summarize and communicate results.** Summarize the verification results and communicate them to all affected parties. [OUTCOME 5]

*NOTE 10: Providing all necessary information from the test case execution in a summary enables other parties to judge the consequences.*

**SEC.4.BP5: Summarize and communicate results.** Summarize the validation results and communicate them to all affected parties. [OUTCOME 4]

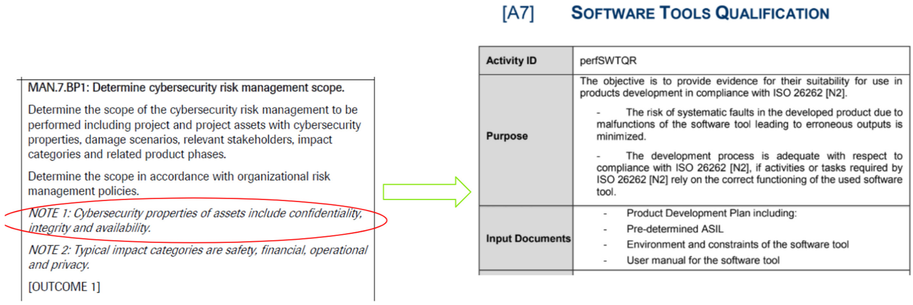
*NOTE 6: Providing necessary information from the validation activities and highlighting important findings concerning additional vulnerabilities enables other parties to judge the consequences.*

| | |
|---|---|
| | MAN.7.BP8: Take corrective action.<br>When expected progress in risk treatment is not achieved, take appropriate corrective action.<br>*NOTE 10: Corrective actions may involve developing and implementing new risk treatment practices or adjusting the existing practices.*<br>[OUTCOME 8] |
| Output work products | 07-07 Risk measure [Outcome 5]<br>08-14 Recovery plan [Outcome 6,7,8]<br>08-19 Risk management plan [Outcome 1, 2, 4, 5, 6, 7, 8]<br>13-20 Risk action request [Outcome 5,6,7,8]<br>14-08 Tracking System [Outcome 4, 5, 6, 7, 8]<br>14-51 Cybersecurity scenario register [Outcome 1, 3, 4, 5]<br>14-52 Asset Library [Outcome 1, 3, 4]<br>15-09 Risk status report [Outcome 6,7,8] |

**Fig. 10.** Impact on the Safety Case from SPICE for CS BP's & outcomes, plus suggested improvements

## 3.9 Software Tools Qualifications Report (SWTQR)

As stated in MAN.7 BP1: Properties of assets should be defined. On the other hand, in ISO26262 we are talking about a tools qualification activity. Both serve the same concept " Qualification and Characterization " and can be embedded in one Work Product also (Fig. 11 below).



MAN.7.BP1: Determine cybersecurity risk management scope.

Determine the scope of the cybersecurity risk management to be performed including project and project assets with cybersecurity properties, damage scenarios, relevant stakeholders, impact categories and related product phases.

Determine the scope in accordance with organizational risk management policies.

*NOTE 1: Cybersecurity properties of assets include confidentiality, integrity and availability.*

*NOTE 2: Typical impact categories are safety, financial, operational and privacy.*

[OUTCOME 1]

[A7] SOFTWARE TOOLS QUALIFICATION

| | |
|---|---|
| **Activity ID** | perfSWTQR |
| **Purpose** | The objective is to provide evidence for their suitability for use in products development in compliance with ISO 26262 [N2].<br>- The risk of systematic faults in the developed product due to malfunctions of the software tool leading to erroneous outputs is minimized.<br>- The development process is adequate with respect to compliance with ISO 26262 [N2], if activities or tasks required by ISO 26262 [N2] rely on the correct functioning of the used software tool. |
| **Input Documents** | - Product Development Plan including:<br>- Pre-determined ASIL<br>- Environment and constraints of the software tool<br>- User manual for the software tool |

**Fig. 11.** Impact on SWTQR from SPICE for CS BP's & outcomes, plus suggested improvements

## 4 Study Results

The case study and inspection done above has shown that multiple ISO26262 Work Products and activities are impacted by the newly published Automotive SPICE® for Cybersecurity in the same environment, given the same inputs, and development circumstances.

The before and after evaluations of our safety critical project show that new gaps have been identified on each output work product of the ISO26262 in light of the new release of Automotive SPICE appendix for Cybersecurity.

Whether these new gaps will certainly impact the project overall compliance (capability level) to Automotive SPICE or not is a topic that needs to be further addressed and studied once the Automotive SPICE appendix for Cybersecurity has been officially released into a final edition, with a clear clarification in the VDA guidelines about the relation between its goals, practices, and outcomes and those of the original PAM v3.1 for Automotive SPICE.

## 5 Conclusion and Recommendations for Future Work

Cybersecurity has become a serious concern in the automotive domain in recent years due to the increasing integration of computers and connectivity in modern vehicles.

In this paper, we share our experience of applying the guidance in the newly published Automotive SPICE® for Cybersecurity in the light of the currently established ISO26262 work products.

The case study introduces an evaluation and extra guidance on how to expand the implementation of the already-existing ISO26262 activities and work products to comply with the cybersecurity practices, outcomes, or work products as essential inputs for ASiL Projects to be in line with Automotive SPICE®.

Each work product of them needs to include extra activities/inputs in order to fulfill the cybersecurity goals of a certain solution and comply with the new Automotive SPICE appendix for cybersecurity.

This imposes a conclusion of the following:

- Functional Safety work products are impacted by the newly released standard appendix of Automotive SPICE for Cybersecurity.

- The possibility to expand the ISO26262 activities within a project to embrace both safety and security aspects in the long run.
- The practices for safety and security development can be smoothly integrated underneath the umbrella of Automotive SPICE.
- A Software project with Functional Safety components and Cybersecurity constraints needs to integrate a unified solution to facilitate safe and secure communication within the whole system with minimal overhead.

We believe that these experiences and suggestions need to be shared with the automotive safety and security community to push forward automotive cybersecurity and to improve the standard in the long run.

## References

1. Automotive SPICE®: Process Reference Model, Process Assessment Model Version 3.1, November 1 2017. http://www.automotivespice.com/
2. SPI MANIFESTO [Version A.1.2.2010]
3. www.iatfglobalozsversight.org [IATF 16949 global website, retrieved: Jan 2019]
4. Automotive SPICE pocket guide version 3 by Kuglermaag, Jan 2019
5. SAHARA: A Security-Aware Hazard and Risk Analysis Method Georg Macher∗, Harald Sporer∗, Reinhard Berlach∗, Eric Armengaud and Christian Kreine ∗Institute for Technical Informatics, Graz University of Technology, AUSTRIA
6. Macher, G., Much, A., Riel, A., Messnarz, R., Kreiner, C.: Automotive SPICE, safety and cybersecurity integration. In: Tonetta, S., Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2017. LNCS, vol. 10489, pp. 273–285. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-66284-8_23
7. ISO - International Organization for Standardization. ISO 26262 Road vehicles Functional Safety Part 1–10 (2011)
8. ISO - International Organization for Standardization. ISO/IEC 15408. In: van Tilborg, H.C.A., Jajodia, S., (eds.) Encyclopedia of Cryptography and Security. 2nd Edn. Springer, Heidelberg (2011)
9. Vehicle Electrical System Security Committee: SAE J3061 Cybersecurity Guidebook for Cyber-Physical Automotive Systems. http://standards.sae.org/wip/j3061/
10. Using SAE J3061 for Automotive Security Requirement Engineering. Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P.: Austrian Institute of Technology, Austria2TTTech Computertechnik AG, Austria3TTControl GmbH, Austria4Vienna University of Technology, Department of Computer Engineering
11. SOQRATES Task Forces Developing Integration of Automotive SPICE, ISO 26262 and SAE J3061. http://soqrates.eurospi.net/
12. ISO: International Organization for Standardization: IEC 62443 - Industrial Communication Networks Network and System Security (2009)
13. ISO: International Organization for Standardization: SS 7740 Road Vehicles Functional Safety Process Assessment Model (2012)