First Experiences with the Automotive SPICE for Cybersecurity Assessment Model

TechDay 30.8. , and EuroSPI, 1.-3.9.2021

Suported by By SOQRATES Group https://soqrates.eurospi.net

We make your practical cybersecurity concept work

Presenter Researcher Profile

https://scholar.google.com/citations?user=v2xVlnwAAAAJ&hl=de&oi=ao

Motivation

PAM 4.0

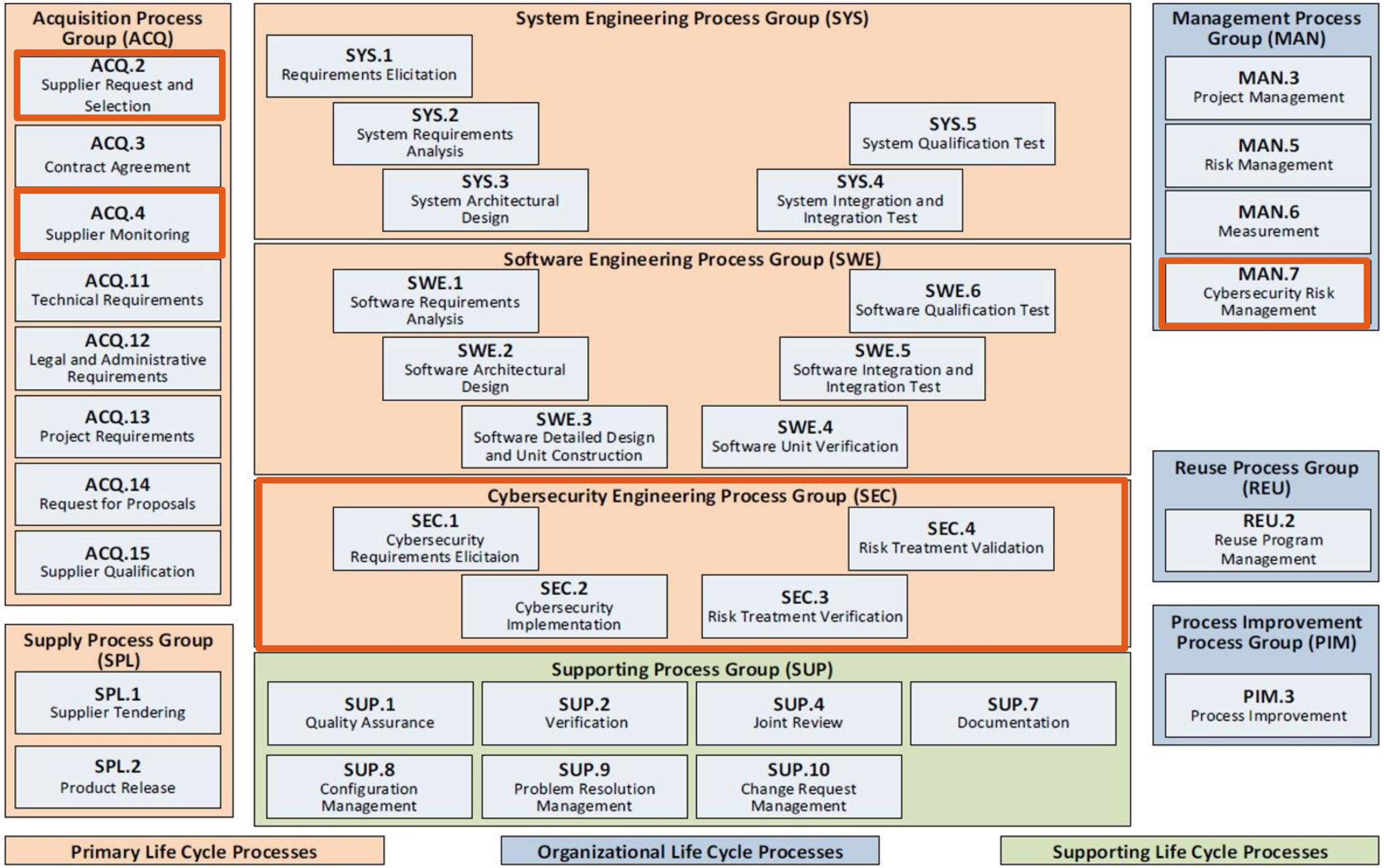
- Automotive SPICE for Cybersecurity, 1st Edition, Feb. 2021, VDA QMC Working Group 13, Feb. 2021
- New SEC.1-SEC.4, MAN.7 etc. processes
- An understanding of expected results in assessments required

DRIVES (www.project-drives.eu, 2018 – 2021)

- Skills set for a cybersecurity engineer
- Skills set for a cybersecurity manager
- Skills set for a cybersecurity tester

SOQRATES (https://soqrates.eurospi.net , working group)

- Best practices exchange of implementation on a method basis
- ECQA Certified Cybersecurity Engineer Training Development



Acquisition Process Group (ACQ)

- ACQ.2 Supplier Request and Selection
- ACQ.3 Contract Agreement
- ACQ.4 Supplier Monitoring
- ACQ.11 Technical Requirements
- ACQ.12 Legal and Administrative Requirements
- ACQ.13 Project Requirements
- ACQ.14 Request for Proposals
- ACQ.15 Supplier Qualification

Supply Process Group (SPL)

- SPL.1 Supplier Tendering
- SPL.2 Product Release

System Engineering Process Group (SYS)

- SYS.1 Requirements Elicitation
- SYS.2 System Requirements Analysis
- SYS.3 System Architectural Design
- SYS.4 System Integration and Integration Test
- SYS.5 System Qualification Test

Software Engineering Process Group (SWE)

- SWE.1 Software Requirements Analysis
- SWE.2 Software Architectural Design
- SWE.3 Software Detailed Design and Unit Construction
- SWE.4 Software Unit Verification
- SWE.5 Software Integration and Integration Test
- SWE.6 Software Qualification Test

Cybersecurity Engineering Process Group (SEC)

- SEC.1 Cybersecurity Requirements Elicitaion
- SEC.2 Cybersecurity Implementation
- SEC.3 Risk Treatment Verification
- SEC.4 Risk Treatment Validation

Supporting Process Group (SUP)

- SUP.1 Quality Assurance
- SUP.2 Verification
- SUP.4 Joint Review
- SUP.7 Documentation
- SUP.8 Configuration Management
- SUP.9 Problem Resolution Management
- SUP.10 Change Request Management

Management Process Group (MAN)

- MAN.3 Project Management
- MAN.5 Risk Management
- MAN.6 Measurement
- MAN.7 Cybersecurity Risk Management

Reuse Process Group (REU)

- REU.2 Reuse Program Management

Process Improvement Process Group (PIM)

- PIM.3 Process Improvement

Primary Life Cycle Processes

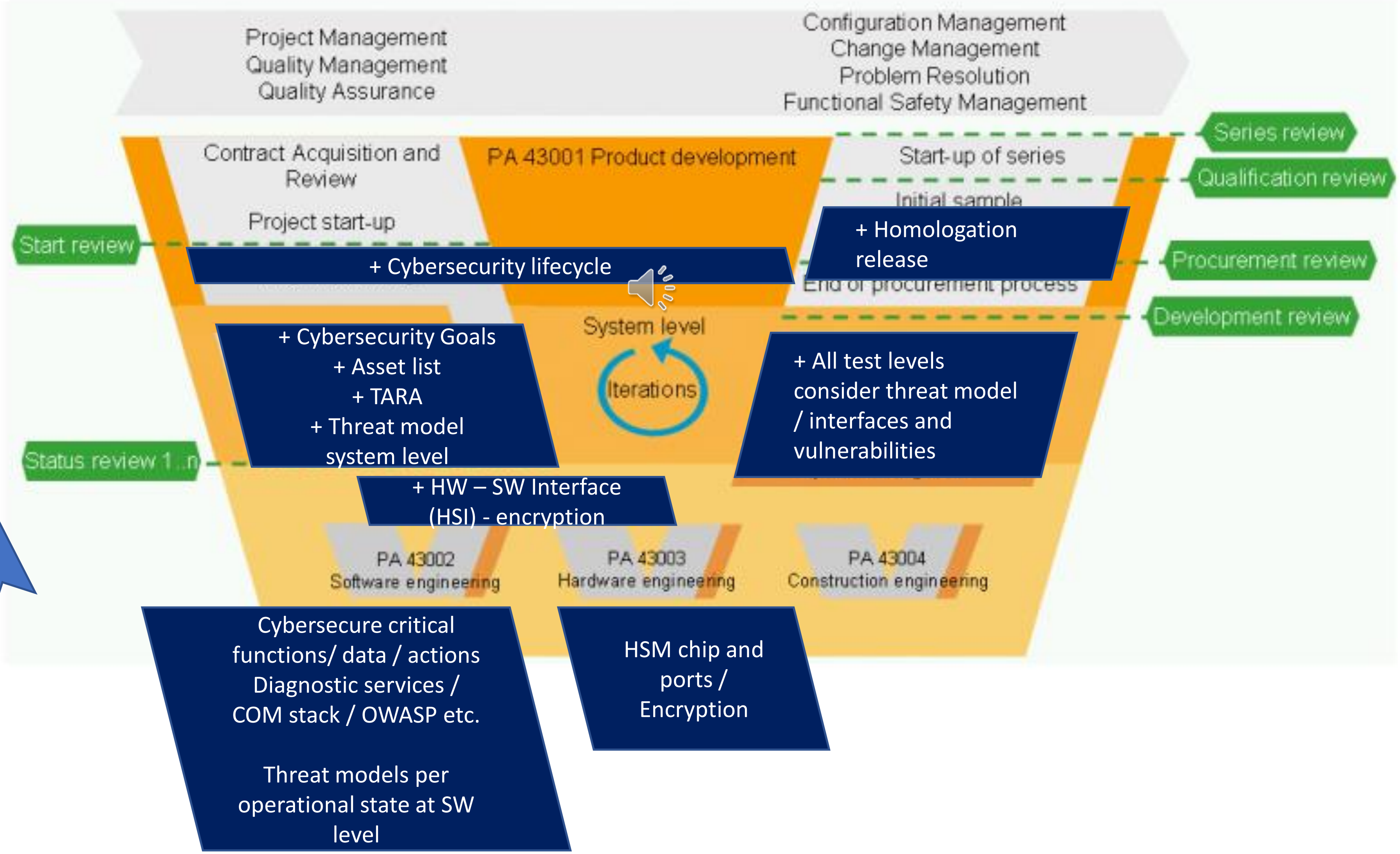
Organizational Life Cycle Processes

Supporting Life Cycle Processes

Strategy based on V model and learning by doing

- ASPICE extension
- KGAS chapter about cybersecurity
- Best practices templates

Learning by exercise



+ Cybersecurity lifecycle

+ Homologation release

+ Cybersecurity Goals
+ Asset list
+ TARA
+ Threat model system level

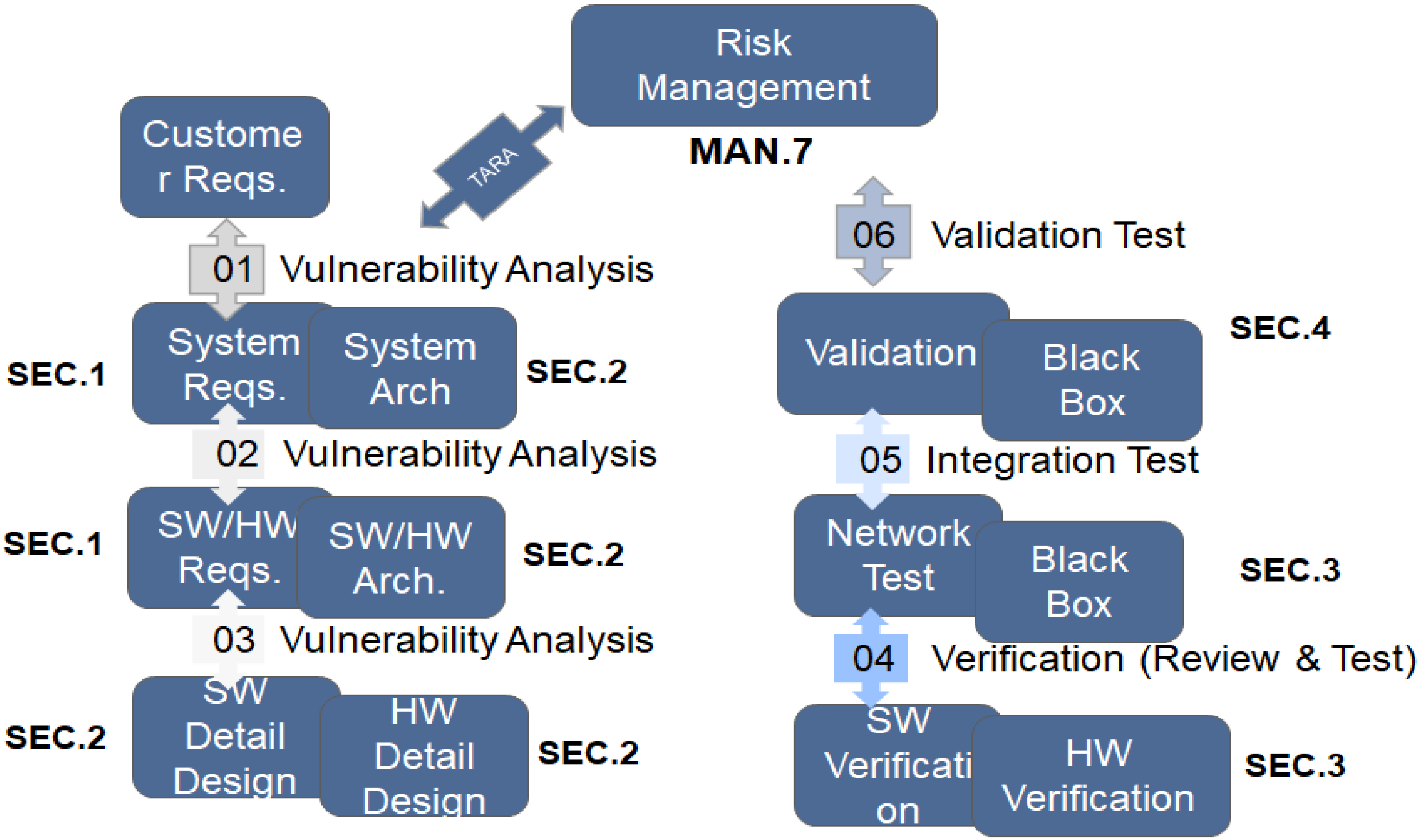
+ All test levels consider threat model / interfaces and vulnerabilities

+ HW – SW Interface (HSI) - encryption

Cybersecure critical functions/ data / actions Diagnostic services / COM stack / OWASP etc.

Threat models per operational state at SW level

HSM chip and ports / Encryption



Risk Management

MAN.7

TARA

Customer Reqs.

01 Vulnerability Analysis

SEC.1 System Reqs.

System Arch SEC.2

02 Vulnerability Analysis

SEC.1 SW/HW Reqs.

SW/HW Arch. SEC.2

03 Vulnerability Analysis

SEC.2 SW Detail Design

HW Detail Design SEC.2

06 Validation Test

Validation

Black Box SEC.4

05 Integration Test

Network Test

Black Box SEC.3

04 Verification (Review & Test)

SW Verification

HW Verification SEC.3

System Level

- ✓ 01 Block Diagram (Item)
- ✓ 01 Asset List
- ✓ 01 Tech Stack
- ✓ 01 Critical Function Blocks
- ✓ 01 Threat Model Level 0
- ✓ 01 TARA
- ✓ 01 System Requirements

SW/HW Level

- ✓ 02 Refined System Functions Block Diagram
- ✓ 02 Operational Modes Analysis
- ✓ 02 Threat Model Level 1 for each operational mode
- ✓ 02 SW Requirements / HW Requirements

SW/HW Detailed Design

- ✓ 03 Cybersecurity critical Functions
- ✓ 03 Cybersecurity Critical Data
- ✓ 03 SW Unit Design and Specification
- ✓ 03 HSM Architecture, Config. And Communication

Source: Automotive SPICE® https://learn.drives-compass.eu/
EU Blueprint for Automotive, Steering Board Members ACEA and CLEPA, ISCN WP Leader DRIVES Learning Portal

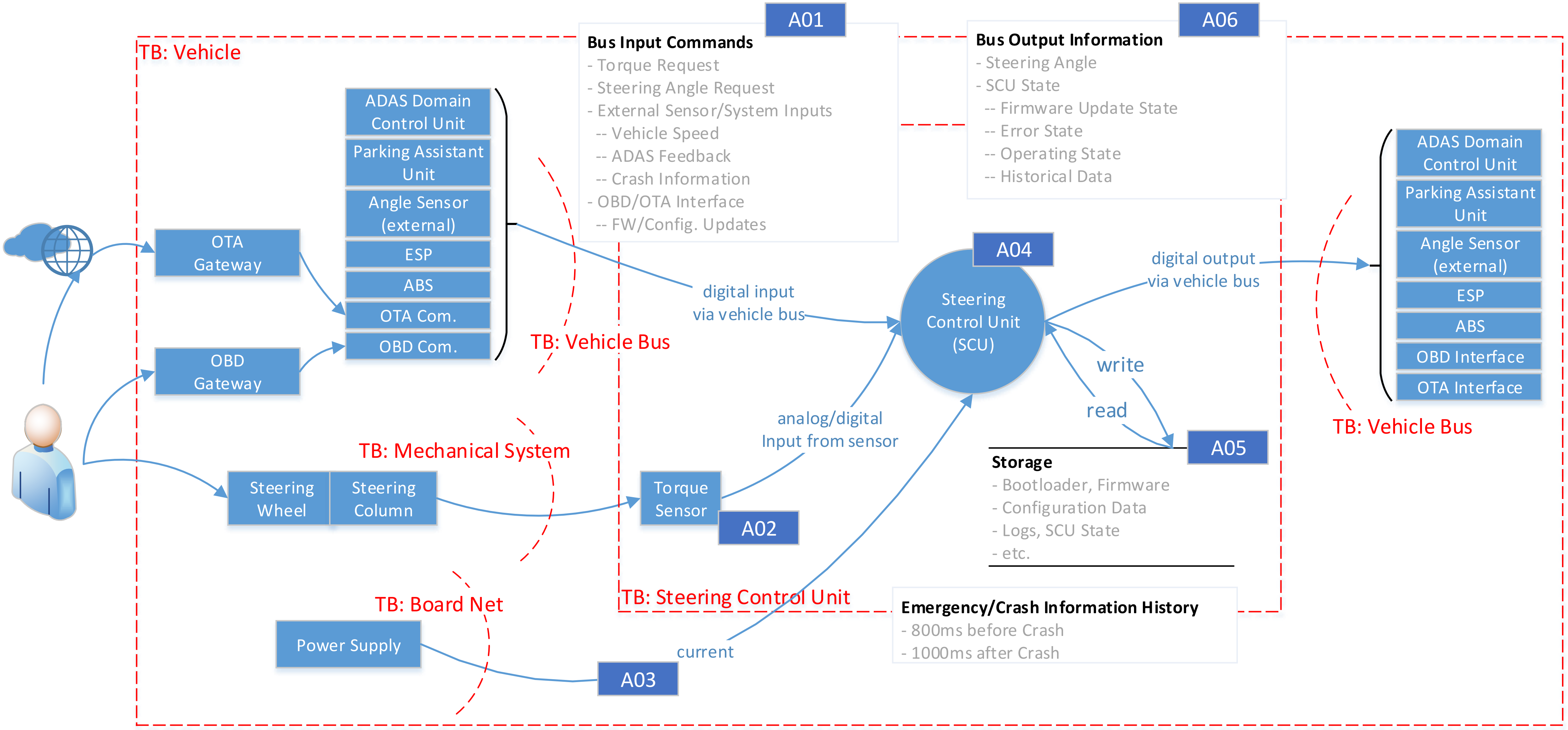
Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Vulnerability Analysis System Level**

- 01 Block Diagram (Item)
  - Cybersecurity item analysis and model
- 01 Asset List
  - Identified assets that can be attacked. A best practice template with attributes for rating an asset has been established.
- 01 Tech Stack
  - If a partner had already experience with cybersecurity a technology stack model was used where the implemented modules for cybersecurity are shown on each layer (HSM – Hardware Security Module, vHSM as part of MCAL, SecOC, Crypto Service Manager, Secure Bootloader, etc.)
- 01 Critical Function Blocks
  - Functions that can be influenced from cybersecure critical interfaces are marked and counter measures considered.
- 01 Threat Model Level 0
  - Usually this is either a model following STRIDE [46] or a data flow schema at high level showing the complete system and all its interfaces to surrounding components.

Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Vulnerability Analysis System Level**

- 01 TARA
  - Threat and risk analysis following the guidelines in the ISO 21434 and delivering assets, potential attacks, damage scenarios, impact analysis and impact level, threat analysis and threat level and a security level (combination of impact level and threat level by a defined risk graph).
- 01 System Requirements
  - A TARA results in cybersecurity goals (high level requirements) which are broken down to system requirements.
  - In requirements analyse the state-of-the-art methods like STRIDE [46] gives us a solution pattern, each attack form has a defined mitigation pattern (see Figure 7).

Example Level 0 Threat Model of the Steering Control Unit



TB: Vehicle

A01

Bus Input Commands
- Torque Request
- Steering Angle Request
- External Sensor/System Inputs
-- Vehicle Speed
-- ADAS Feedback
-- Crash Information
- OBD/OTA Interface
-- FW/Config. Updates

A06

Bus Output Information
- Steering Angle
- SCU State
-- Firmware Update State
-- Error State
-- Operating State
-- Historical Data

ADAS Domain Control Unit
Parking Assistant Unit
Angle Sensor (external)
ESP
ABS
OTA Com.
OBD Com.

OTA Gateway

OBD Gateway

TB: Vehicle Bus

digital input via vehicle bus

A04

Steering Control Unit (SCU)

digital output via vehicle bus

ADAS Domain Control Unit
Parking Assistant Unit
Angle Sensor (external)
ESP
ABS
OBD Interface
OTA Interface

TB: Vehicle Bus

write

read

A05

Storage
- Bootloader, Firmware
- Configuration Data
- Logs, SCU State
- etc.

analog/digital Input from sensor

TB: Mechanical System

Steering Wheel

Steering Column

Torque Sensor

A02

TB: Board Net

Power Supply

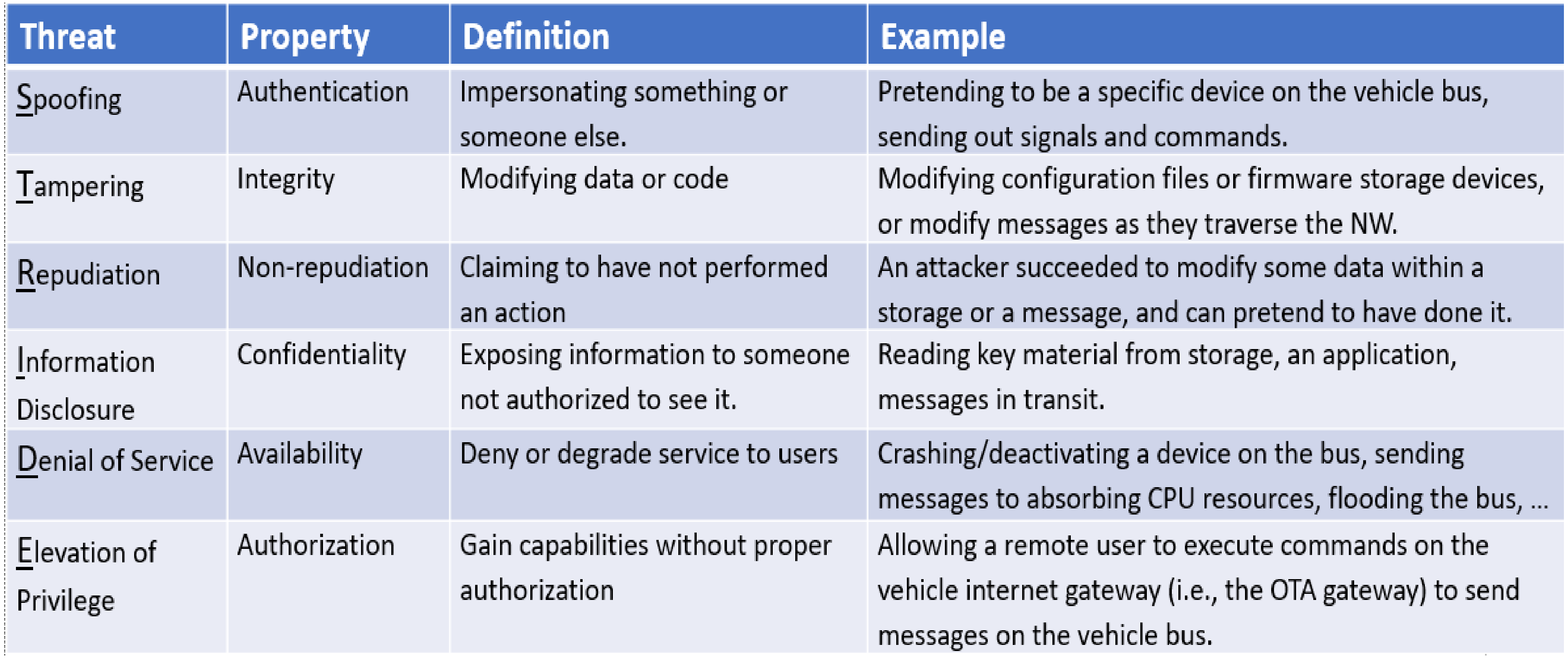
A03

current

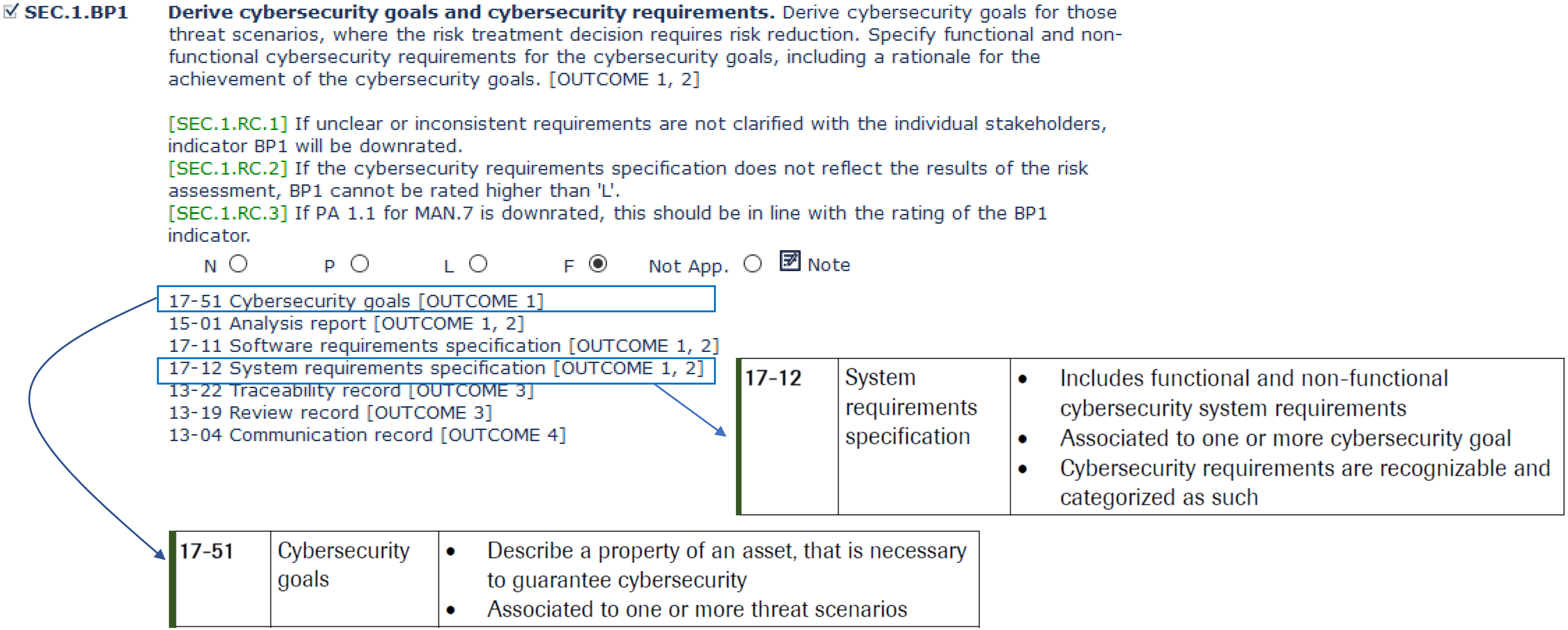
TB: Steering Control Unit

Emergency/Crash Information History
- 800ms before Crash
- 1000ms after Crash

Set of cybersecurity properties



Threat	Property	Definition	Example
Spoofing	Authentication	Impersonating something or someone else.	Pretending to be a specific device on the vehicle bus, sending out signals and commands.
Tampering	Integrity	Modifying data or code	Modifying configuration files or firmware storage devices, or modify messages as they traverse the NW.
Repudiation	Non-repudiation	Claiming to have not performed an action	An attacker succeeded to modify some data within a storage or a message, and can pretend to have done it.
Information Disclosure	Confidentiality	Exposing information to someone not authorized to see it.	Reading key material from storage, an application, messages in transit.
Denial of Service	Availability	Deny or degrade service to users	Crashing/deactivating a device on the bus, sending messages to absorbing CPU resources, flooding the bus, …
Elevation of Privilege	Authorization	Gain capabilities without proper authorization	Allowing a remote user to execute commands on the vehicle internet gateway (i.e., the OTA gateway) to send messages on the vehicle bus.



☑ **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]

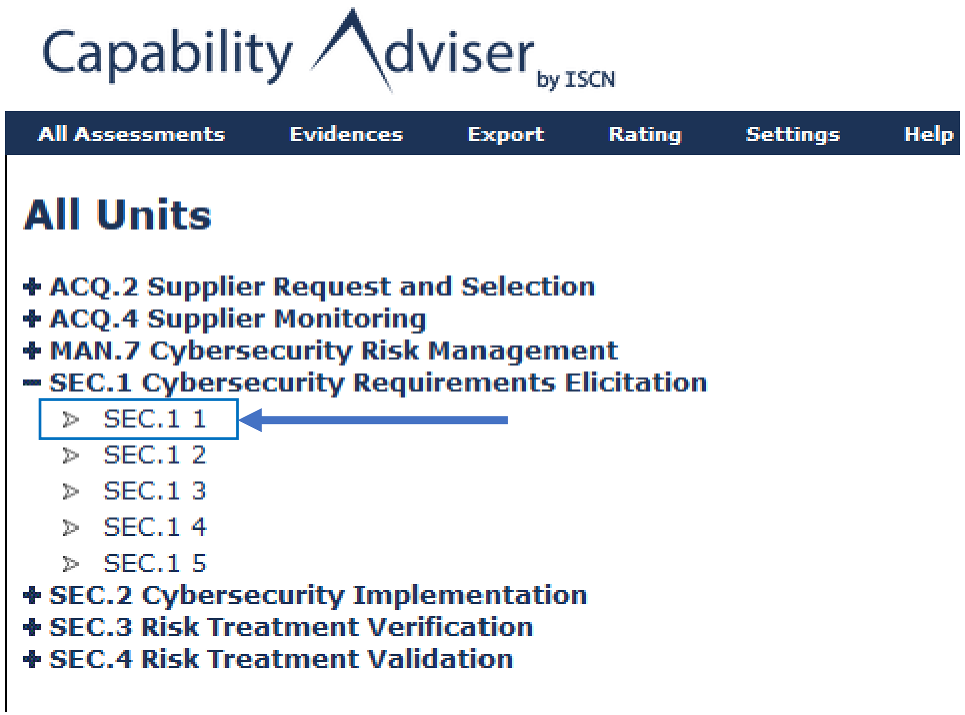
[SEC.1.RC.1] If unclear or inconsistent requirements are not clarified with the individual stakeholders, indicator BP1 will be downrated.
[SEC.1.RC.2] If the cybersecurity requirements specification does not reflect the results of the risk assessment, BP1 cannot be rated higher than 'L'.
[SEC.1.RC.3] If PA 1.1 for MAN.7 is downrated, this should be in line with the rating of the BP1 indicator.

N ○ P ○ L ○ F ● Not App. ○ Note

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]

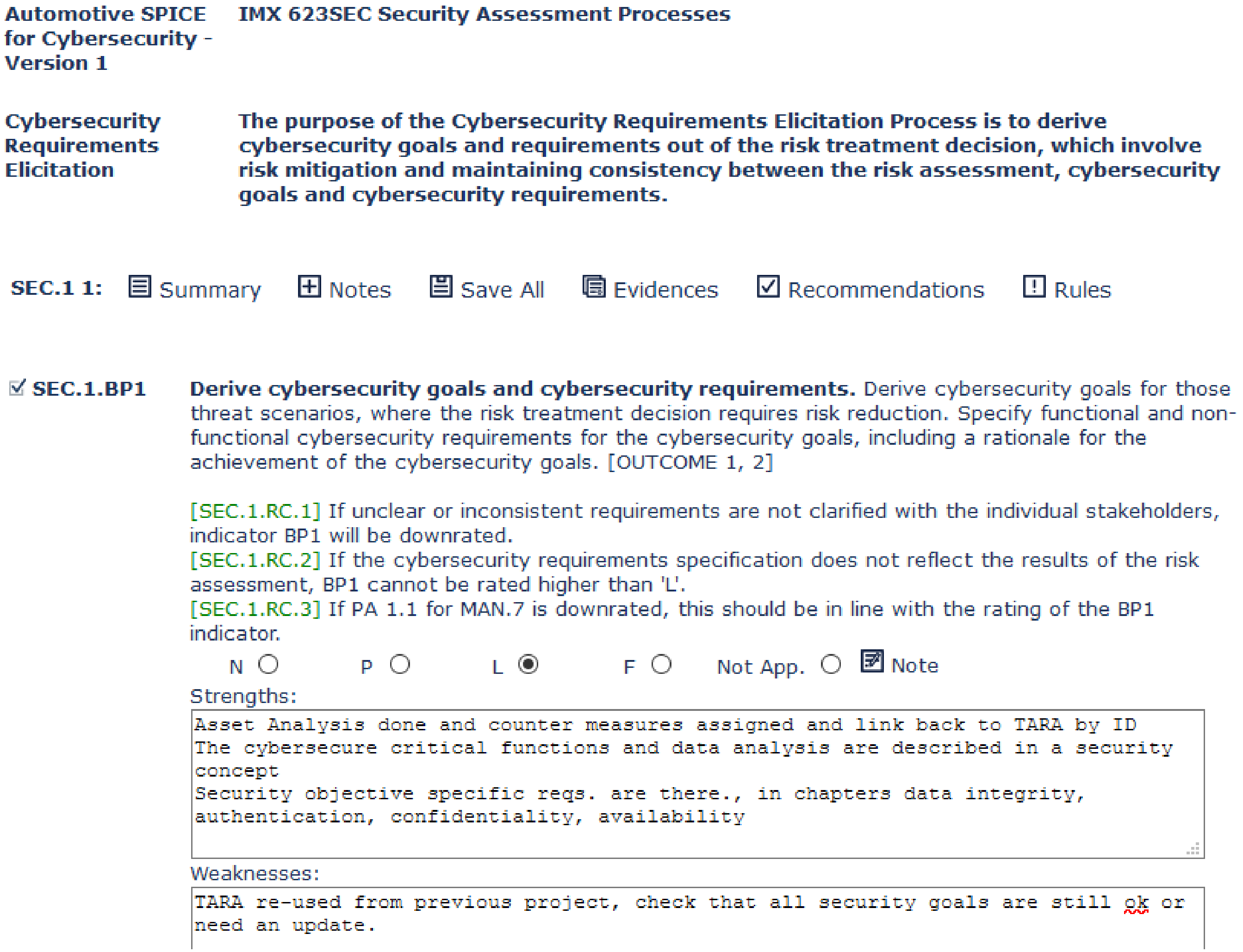
17-12	System requirements specification	• Includes functional and non-functional cybersecurity system requirements • Associated to one or more cybersecurity goal • Cybersecurity requirements are recognizable and categorized as such

17-51	Cybersecurity goals	• Describe a property of an asset, that is necessary to guarantee cybersecurity • Associated to one or more threat scenarios



All Units

- ✚ ACQ.2 Supplier Request and Selection
- ✚ ACQ.4 Supplier Monitoring
- ✚ MAN.7 Cybersecurity Risk Management
- ━ SEC.1 Cybersecurity Requirements Elicitation
  - ▷ SEC.1 1
  - ▷ SEC.1 2
  - ▷ SEC.1 3
  - ▷ SEC.1 4
  - ▷ SEC.1 5
- ✚ SEC.2 Cybersecurity Implementation
- ✚ SEC.3 Risk Treatment Verification
- ✚ SEC.4 Risk Treatment Validation



Automotive SPICE for Cybersecurity - Version 1	**IMX 623SEC Security Assessment Processes**
Cybersecurity Requirements Elicitation	**The purpose of the Cybersecurity Requirements Elicitation Process is to derive cybersecurity goals and requirements out of the risk treatment decision, which involve risk mitigation and maintaining consistency between the risk assessment, cybersecurity goals and cybersecurity requirements.**

☑ **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.RC.1] If unclear or inconsistent requirements are not clarified with the individual stakeholders, indicator BP1 will be downrated.
[SEC.1.RC.2] If the cybersecurity requirements specification does not reflect the results of the risk assessment, BP1 cannot be rated higher than 'L'.
[SEC.1.RC.3] If PA 1.1 for MAN.7 is downrated, this should be in line with the rating of the BP1 indicator.

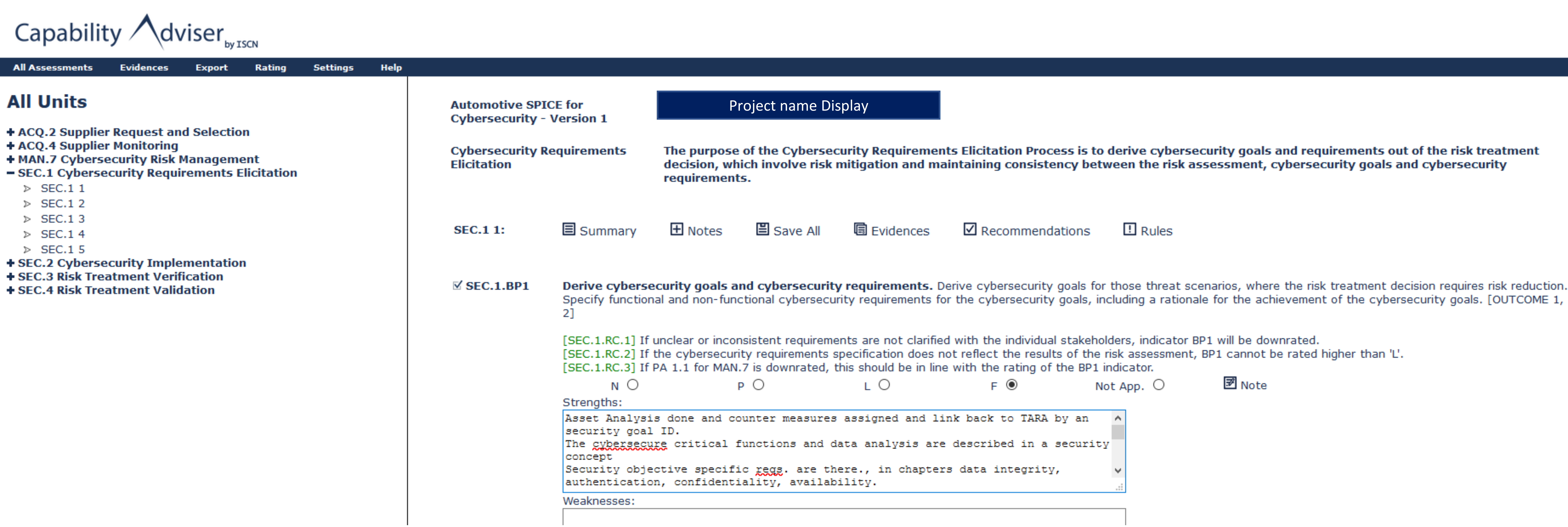
N ○ P ○ L ● F ○ Not App. ○ Note

Strengths:

```
Asset Analysis done and counter measures assigned and link back to TARA by ID
The cybersecure critical functions and data analysis are described in a security
concept
Security objective specific reqs. are there., in chapters data integrity,
authentication, confidentiality, availability
```

Weaknesses:

```
TARA re-used from previous project, check that all security goals are still ok or
need an update.
```



All Units

- ✚ ACQ.2 Supplier Request and Selection
- ✚ ACQ.4 Supplier Monitoring
- ✚ MAN.7 Cybersecurity Risk Management
- − SEC.1 Cybersecurity Requirements Elicitation
  - ▷ SEC.1 1
  - ▷ SEC.1 2
  - ▷ SEC.1 3
  - ▷ SEC.1 4
  - ▷ SEC.1 5
- ✚ SEC.2 Cybersecurity Implementation
- ✚ SEC.3 Risk Treatment Verification
- ✚ SEC.4 Risk Treatment Validation

Automotive SPICE for Cybersecurity - Version 1 — Project name Display

Cybersecurity Requirements Elicitation

The purpose of the Cybersecurity Requirements Elicitation Process is to derive cybersecurity goals and requirements out of the risk treatment decision, which involve risk mitigation and maintaining consistency between the risk assessment, cybersecurity goals and cybersecurity requirements.

SEC.1 1:

☑ **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]

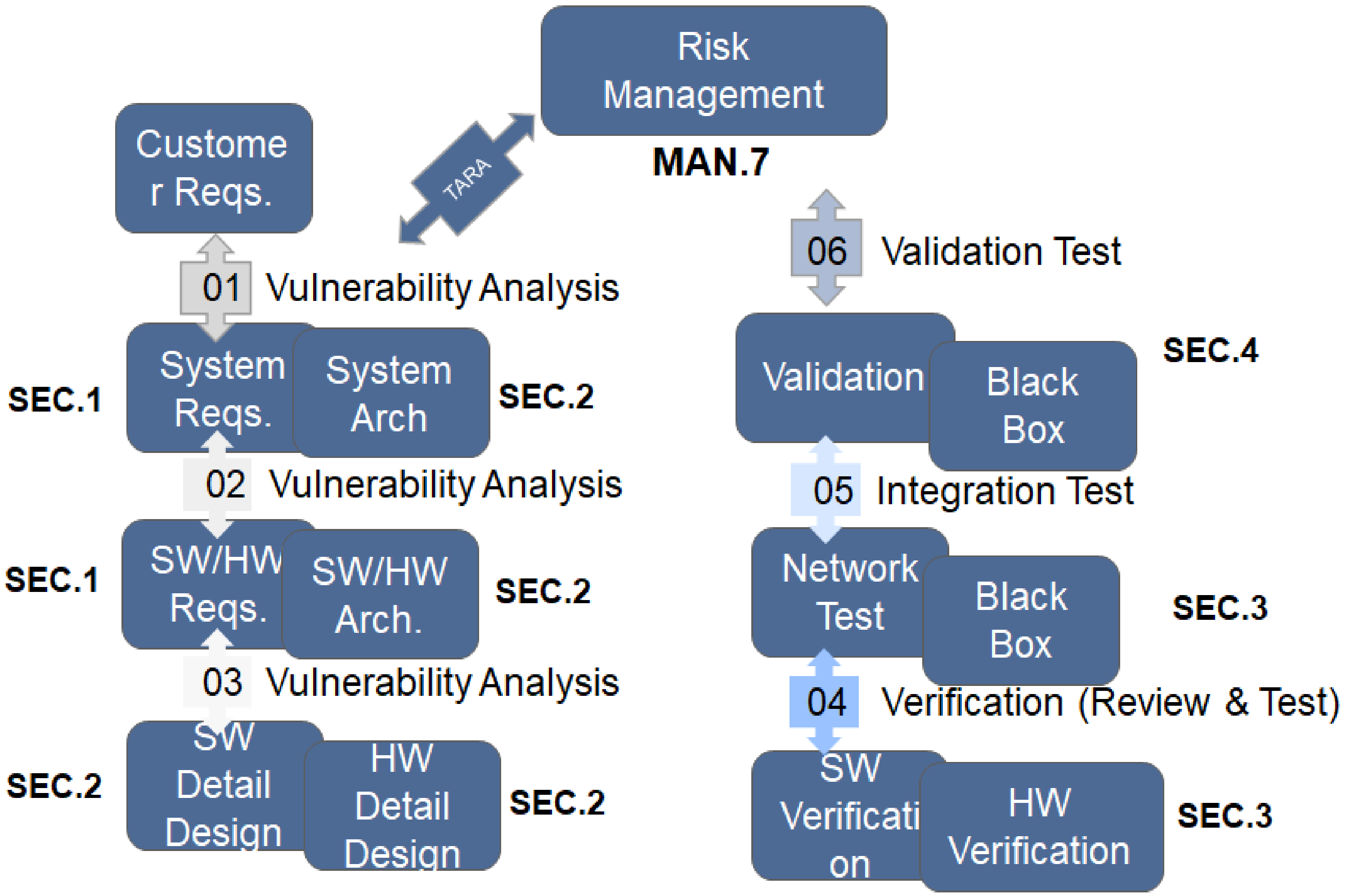
[SEC.1.RC.1] If unclear or inconsistent requirements are not clarified with the individual stakeholders, indicator BP1 will be downrated.
[SEC.1.RC.2] If the cybersecurity requirements specification does not reflect the results of the risk assessment, BP1 cannot be rated higher than 'L'.
[SEC.1.RC.3] If PA 1.1 for MAN.7 is downrated, this should be in line with the rating of the BP1 indicator.

N ○ P ○ L ○ F ● Not App. ○

Strengths:

```
Asset Analysis done and counter measures assigned and link back to TARA by an
security goal ID.
The cybersecure critical functions and data analysis are described in a security
concept
Security objective specific reqs. are there., in chapters data integrity,
authentication, confidentiality, availability.
```

Weaknesses:



Risk Management

MAN.7

TARA

Customer Reqs.

01 Vulnerability Analysis

SEC.1 System Reqs. | System Arch SEC.2

02 Vulnerability Analysis

SEC.1 SW/HW Reqs. | SW/HW Arch. SEC.2

03 Vulnerability Analysis

SEC.2 SW Detail Design | HW Detail Design SEC.2

06 Validation Test

Validation | Black Box SEC.4

05 Integration Test

Network Test | Black Box SEC.3

04 Verification (Review & Test)

SW Verification | HW Verification SEC.3

System Test

- ✓06 New EOL Test Bench
- ✓06 Penetration Test / Test Team Cooperation
- ✓06 New Scenarios in Vehicle Testing
- ✓06 Cybersecurity Case/ Validation Report

SW Integration / Network Test

- ✓ 05 Network Test Suite
- ✓ 05 Types of Network Test Cases
- ✓ 05 Attack Types Tested
- ✓ 02 Typical OEM Test Cooperation

SW Unit Verification

- ✓ 04 MISRA Addendum
- ✓ 04 CERT
- ✓ 04 Security bad practices list MITRE
- ✓ 04 OWASP
- ✓ 04 Code Inspection

Source: Automotive SPICE® https://learn.drives-compass.eu/
EU Blueprint for Automotive, Steering Board Members ACEA and CLEPA, ISCN WP Leader DRIVES Learning Portal

Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Verification System/SW Integration Level**

- 05 Network Test Suite
  - This is a diagnostic test suite which automatically performs tests and reports cybersecurity coverage. Usually this test suite is provided by the customer. If now the existing HIL set up needs to be updated.
- 05 Types of Network Test Cases
  - Test case types are usually structured by the MITRE attack patterns catalogue (https://attack.mitre.org).
  - Test cases examples: e.g. sending unauthorised command, sending command at wrong time, overlading bus with messages and ECU shall filter, trying to access critical data without secure diagnostic session, etc.
- 05 Attack Types Tested
  - AS a measure of coverage all attack types according to the MITRE attack patterns catalogue must be covered (usually applied as review criteria by the working group partners).
- 05 Typical OEM Test Cooperation
  - Car manufacturers which have invested into an SSA (Secure Service Architecture) usually provide a tool set zo be used: e.g. Network Test Suite in case of Daimler AG, FAT Tool Suite in case of BMW Group, etc.

Experiences so far

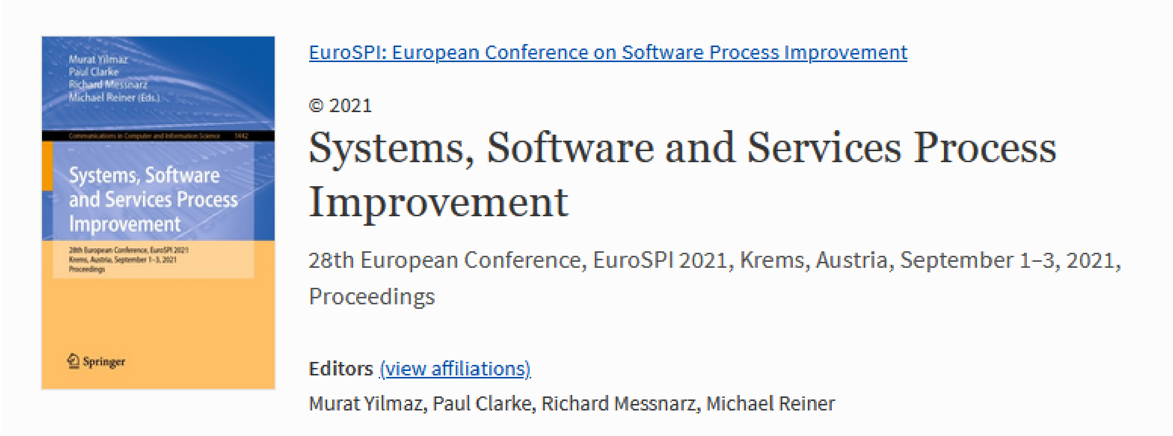
- Typical supporting and management processes still need a cybersecurity related mapping as well. And it was felt that this is still missing.
  - e.g. MAN.3 Project Management: Asking for a cybersecurity plan. Asking for role assignment of cybersecurity manager, cybersecurity engineer. Also checking meetings related to cybersecurity and status reports. MAN.7 is very much related to the TARA and contents of TARA based risk management, still the set up of a cybersecurity case is a cybersecurity project manager task as well.
  - e.g. SUP.8 configuration management and including the cybersecurity related work products in the configuration item list and including a cybersecurity baseline report and status report.
  - e.g. SUP.9 including incident reporting for cybersecurity related problems and impact analysis including a TARA update.
  - e.g. SUP.10 including to mark change requests cybersecure relevant and impact analysis including a TARA update.

Experiences so far

- Also in the assessment it was not so easy to separate SEC.1 Cybersecurity requirements elicitation from SYS.2 system requirements analysis and SWE.1 software requirements analysis.
- e.g. if you see a requirements specification including functional, non-functional, safety and cybersecurity requirements in the interview. Are we then rating two processes based on the same evidence. This in fact happened in the interviews, and as assessor you had to jump between SEC1. And SYS.2 and SWE.1.

Reference

https://link.springer.com/book/10.1007/978-3-030-85521-5


Murat Yilmaz
Paul Clarke
Richard Messnarz
Michael Reiner (Eds.)
Communications in Computer and Information Science 1442
Systems, Software and Services Process Improvement
28th European Conference, EuroSPI 2021
Krems, Austria, September 1–3, 2021
Proceedings
Springer

EuroSPI: European Conference on Software Process Improvement

© 2021

Systems, Software and Services Process Improvement

28th European Conference, EuroSPI 2021, Krems, Austria, September 1–3, 2021, Proceedings

Editors (view affiliations)

Murat Yilmaz, Paul Clarke, Richard Messnarz, Michael Reiner

Citation:

Messnarz R. et al. (2021) **First Experiences with the Automotive SPICE for Cybersecurity Assessment Model**. In: Yilmaz M., Clarke P., Messnarz R., Reiner M. (eds) Systems, Software and Services Process Improvement. EuroSPI 2021. Communications in Computer and Information Science, **vol 1442. Springer, Cham. https://doi.org/10.1007/978-3-030-85521-5_35**

Appendix

Further Work Products from Practice Mapped onto V-Model

Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Vulnerability Analysis SW/HW Level**

- 02 Refined System Functions Block Diagram
  - Refined cybersecurity item
- 02 Operational Modes Analysis
  - All cybersecurity experienced partners were creating a set of threat models and followed a design strategy to draw the threat models. The design strategy broke the system down into operational states based on the state machine. For each operational state a threat model and a refinement of the TARA has been done.
- 02 Threat Model Level 1 for each operational mode
  - The level 1 threat models include
  - One model still at systems level and includes the cybersecurity critical interfaces, SW functions, and cybersecurity critical data that can be attacked at systems level.
  - A model per operational state of the system showing the cybersecurity critical interfaces, SW functions, and cybersecurity critical data that can be attacked at a specific operational state. Some call that model per state a threat model level 2 already.
- 02 SW Requirements / HW Requirements
  - Based on the threat models level 1 system requirements are refined to cybersecurity software and hardware requirements for the system.

Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Vulnerability Analysis Detailed Design Level**

- 03 Cybersecurity critical Functions
  - List of cybersecurity critical functions impacted by the cybersecurity critical software and hardware requirements.
  - Counter actions to be programmed using cybersecurity libraries (Secure On-Board Communication, Cryptography Service Manager, etc.) to implement cybersecurity objectives like authentication, non-repudiation, authorization, integrity, availability, confidentiality.
- 03 Cybersecurity Critical Data
  - List of cybersecurity critical data impacted by the cybersecurity critical software and hardware requirements.
  - Counter actions to be programmed using cybersecurity libraries (Secure On-Board Communication, Cryptography Service Manager, etc.) to implement cybersecurity objectives like authentication, non-repudiation, authorization, integrity, availability, confidentiality.
- 03 SW Unit Design and Specification
  - Detailed requirements for single SW units broken down from cybersecurity related software requirements.
  - Coding follows cybersecurity related coding guidelines
- 03 HSM Architecture, Config. And Communication
  - Architecture of the HSM (Hardware Security Module) and service calls to the HSM. Configuration of HSM in Autosar 4.3.

Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Verification – Unit Level**

- 04 MISRA Addendum
  - Additional cybersecurity related coding rules from 2016 (MISRA C:2012 Amendment 1 April 2016)
- 04 CERT
  - CERT as additional cybersecurity related coding rules (ISO/IEC TS 17961:2013 C-Secure)
- 04 Security bad practices list MITRE
  - Cybersecurity Attack and Mitigation Patterns
  - https://attack.mitre.org
- 04 OWASP
  - The Open Web Application Security Project (owasp.org), in case the supplier develops an ECU connected to the internet / WLAN / Car2X, etc.
- 04 Code Inspection
  - Reviews applying an extended cybersecurity related checklist and rule set

Typical Work Products from Practice Example (for all see the SPRINGER CCIS 1442 paper) – **Validation – System/SW Level**

- 06 New EOL Test Bench
  - Suppliers in most cases needed a new test bench where the flashing of new keys for the EOL (End Of Line) Test is simulated.
- 06 Penetration Test / Test Team Cooperation
  - The norm requires a penetration test by an external cybersecurity expert team. Here usually only the general level of specification is provided and
  - 06 New Scenarios in Vehicle Testing
  - Vehicle testing required new scenarios in car set up. E.g. the test driver needs to flash new keys before the driving tests are starting.
- 06 Cybersecurity Case/ Validation Report
  - A cybersecurity manager needs to document the cybersecurity case by proving that 100% of cybersecure relevant requirements at all levels are tested and passed. In case of deviations the deviations must appear in the release statement and the impact is to be analysed and documented.

✓ 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

intacs.info
International Assessor Certification Scheme™

- ✓ Accreditated iNTACS™ training provider for Automotive SPICE®

SoQrates
SOFTWARE
OFFENSIVE
BAYERN

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