Experiences with the ASPICE for Cybersecurity Assessment Model

EuroSPI TechDay, 29.8.2022

Suported by By SOQRATES Group https://soqrates.eurospi.net
and CyberENG project (co-funded by the the Erasmus+ program of the European Union)

Co-funded by
the European Union

We make your practical cybersecurity concept work

Presenters Researcher Profile

Dr R. Messnarz

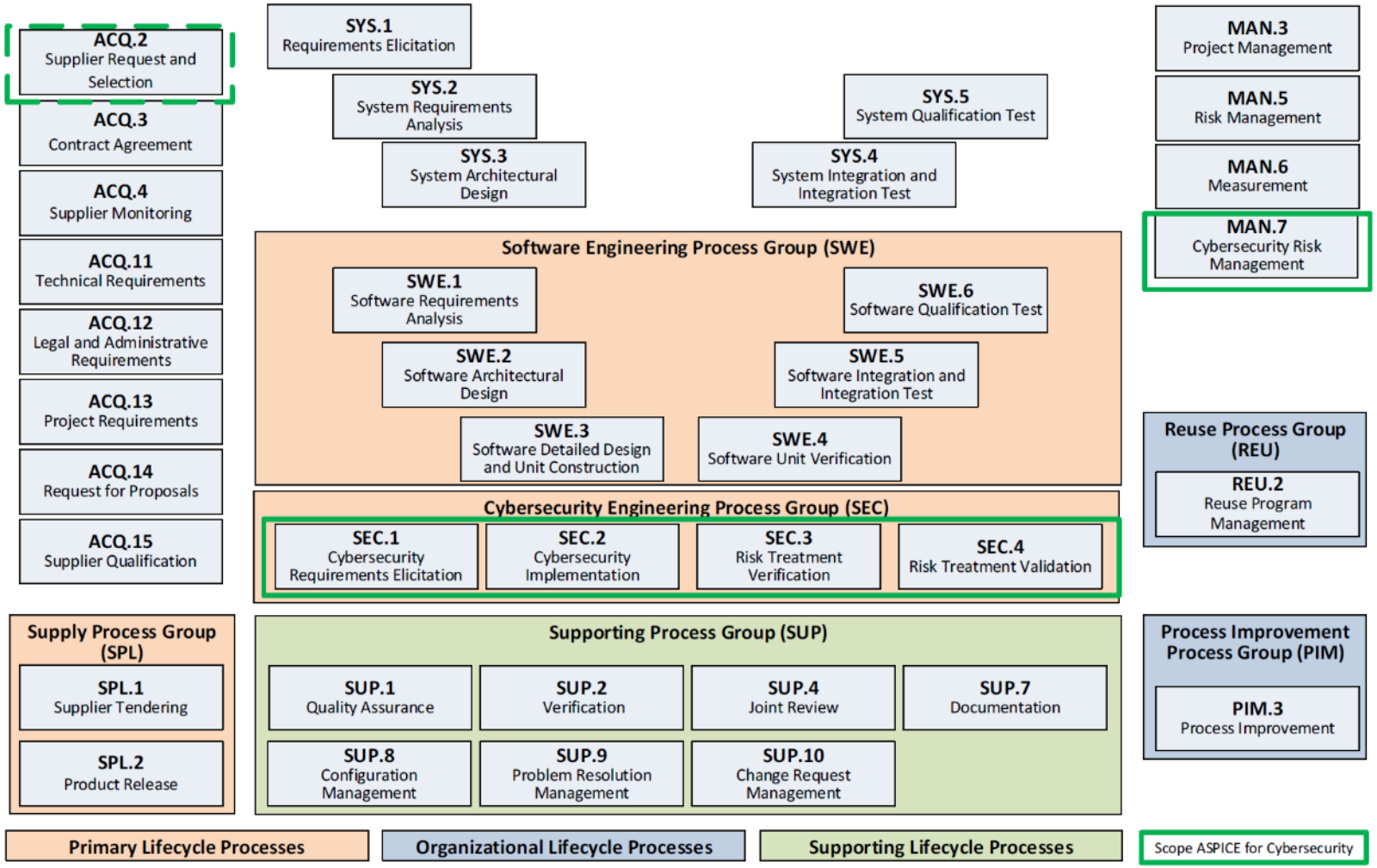
https://scholar.google.com/citations?user=v2xVlnwAAAAJ&hl=de&oi=ao

DI Damjan Ekert

https://scholar.google.com/citations?hl=en&user=4Sf3jdIAAAAJ

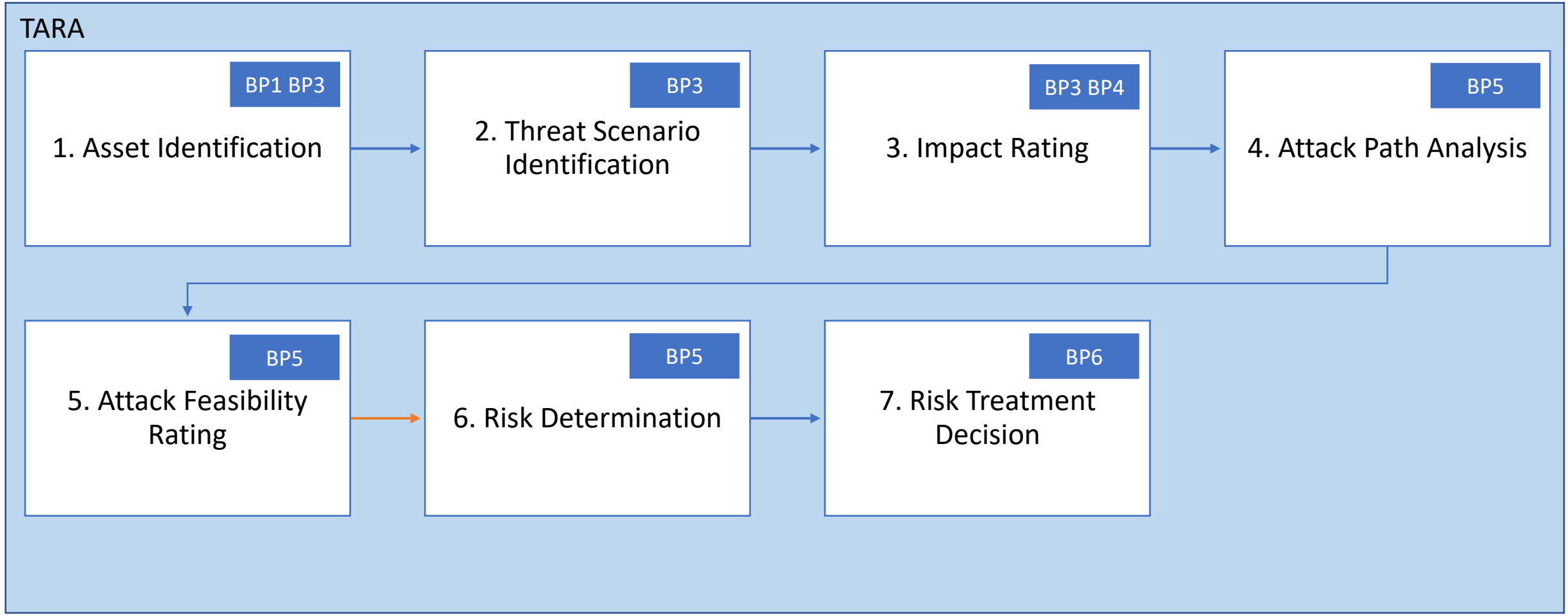
Process Landscape

Automotive SPICE for Cybersecurity released Feb 2021



Experience 1 (MAN.7 related)

MAN.7 Cybersecurity Risk management is based on the TARA workflow and has completely different set of ratings and attributes than MAN.5 Risk Management.



Experience 1 (see example impact rating below)

Asset ID	Asset Name	Description	Primary Stakeholder	Security Property	Damage Scenario	Safety Damage to Road User	Financial Damage to Road User	Operational Damage to Road User	Privacy & Legislation Damage to Road User	Financial Damage to Customer /OEM	Operational Damage to Customer /OEM	Privacy & Legislation Damage to Customer /OEM
A01.1	Lock Command via WLANp or V2X	Lock Command via WLANp or V2X (Lock function of ECSL)	Supplier	Authenticity	Life Threatening Accident due to locking the door and locking the steering system at speed and motor rpm > 10	Life-threatenir	Negligible	Severe	Negligible	Major	Severe	Negligible
				Integrity	Life Threatening Accident due to locking the door and locking the steering system at speed and motor rpm > 10	Life-threatenir	Negligible	Severe	Negligible	Major	Severe	Negligible
				Non-repudiation	Leaving no trail as an attacker due to deleting the ring buffer / log file of lock commands to hide the attack	No injury	Negligible	Moderate	Negligible	Moderate	Moderate	Negligible
				Confidentiality	Life Threatening Accident due to locking the door and locking the steering system at speed and motor rpm > 0	Life-threatenir	Negligible	Severe	Negligible	Major	Severe	Negligible
				Availability	The car will be stolen due to no locking of the car	No injury	Negligible	Severe	Negligible	Moderate	Severe	Negligible

MAN.7 requires a TARA method knowledge from the assessors. Assessors need to understand:

- Assets and Cybersecurity Properties and Damage Scenarios
- Impact rating of damage scenarios
- Attack feasibility rating of attack vectors

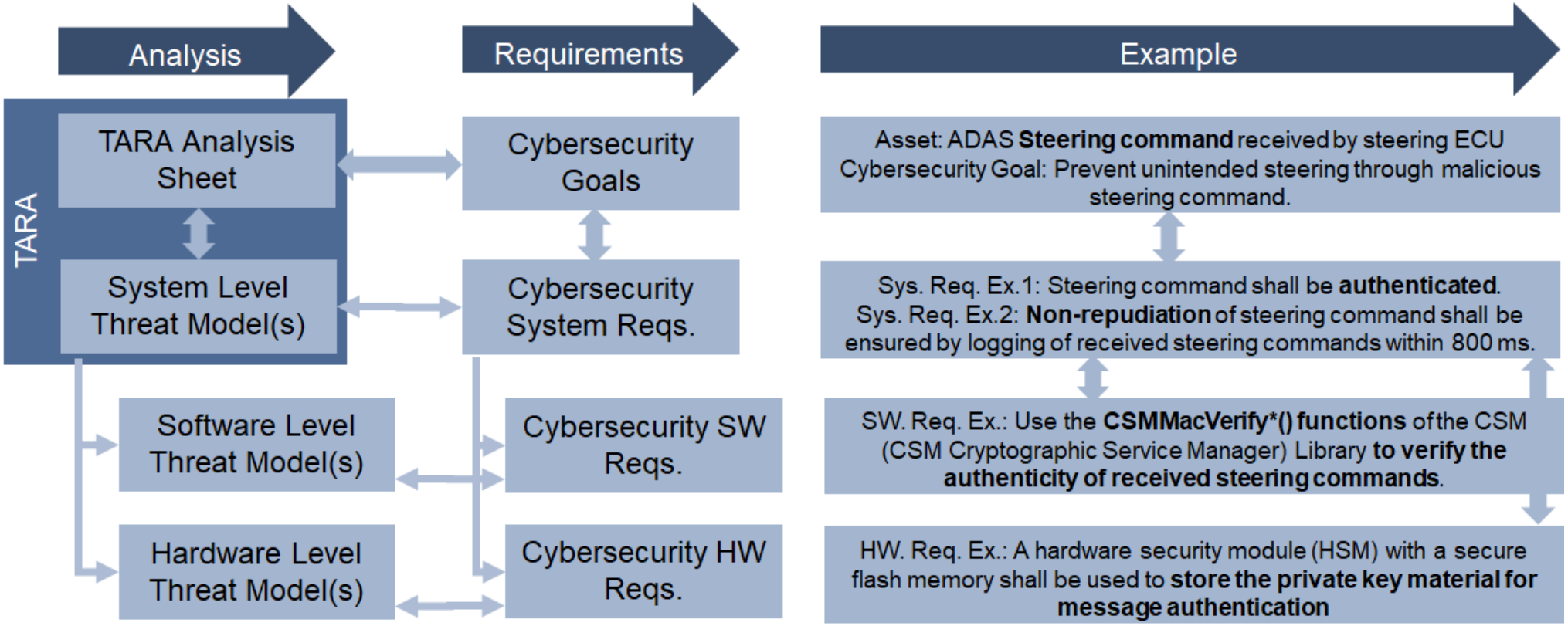
Experience 2 (SEC.x related)

Assessors need to know the basic cybersecurity related solution pattern.

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

Experience 3 (SEC.1 related)

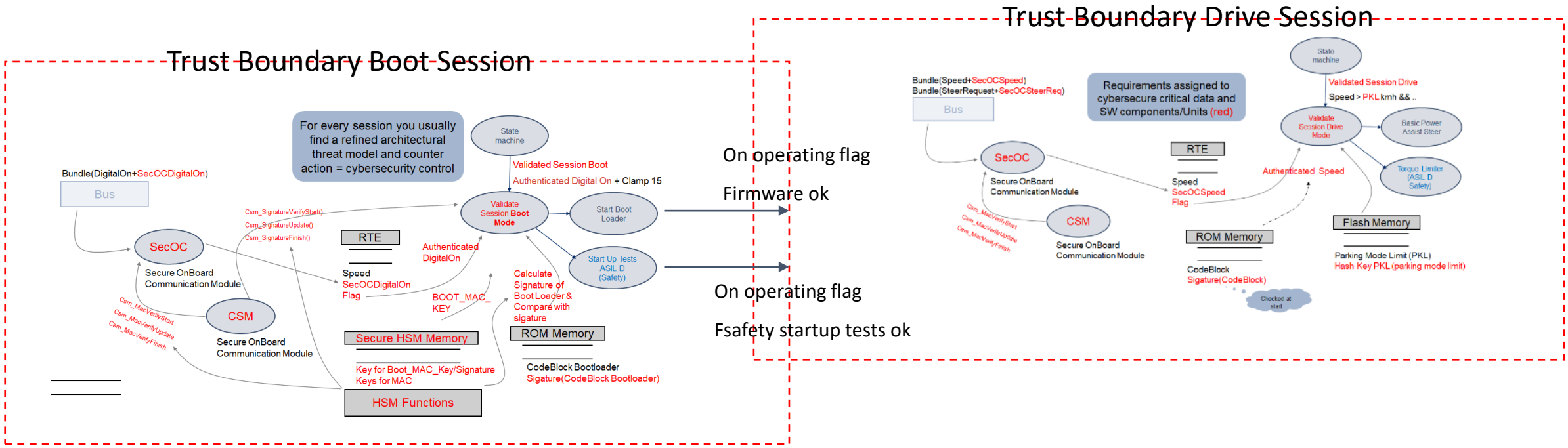
Assessors need to know that cybersecurity controls are derived from threat models and become cybersecurity requirements. And there are requirements at different levels.



Experience 4 (SEC.1 and SEC.2 related)

Assessors need basic knowledge about what additional design views will be necessary.

e.g. a threat model per state and transitions of states, cybersecurity controls marked red



Experience 5 (SEC.1 and SWE.1, SYS.2)

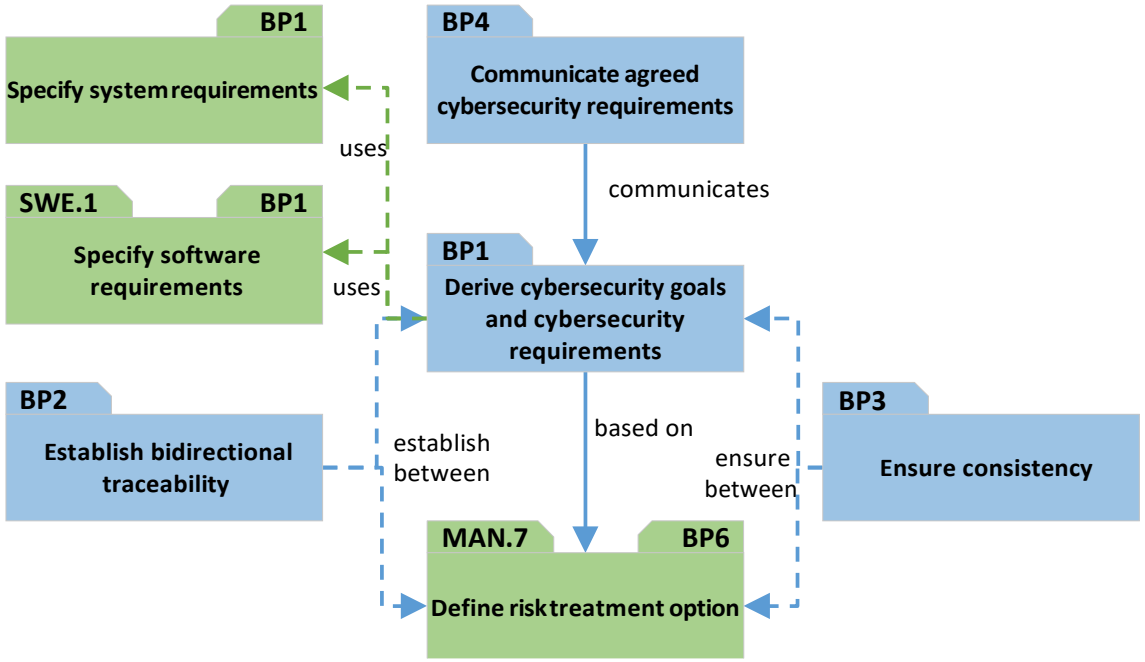
Assessors need to know the relationships between ASPICE and ASPICE for Cybersecurity to manage conflicts.

e.g.

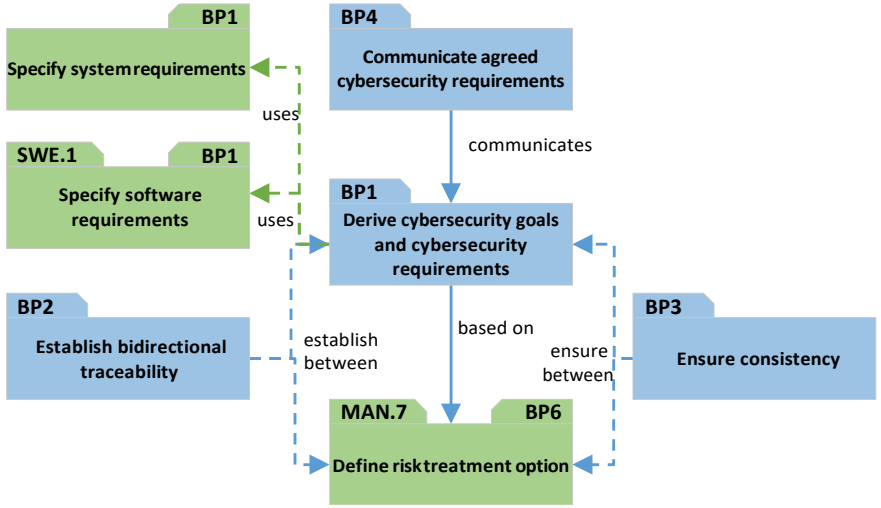
[SEC.1.RC.3] If BP1 for SYS.2 is downrated, this should be in line with the rating of the indicator BP1.

[SEC.1.RC.4] If BP1 for SWE.1 is downrated, this should be in line with the rating of the indicator BP1.

Since it is only “should” it allows different approaches.



Experience 5 (SEC.1 and SWE.1, SYS.2)



Since it is only “should” it allows different approaches.

(1) Do ASPICE assessment and e.g. achieve F on level 1 for SWE.1. Do some weeks later the ASPICE for Cybersecurity assessment and even if SEC.1 is rated P, you leave SWE.1 unchanged F.

(2) Do ASPICE assessment and e.g. achieve F on level 1 for SWE.1. Do just within the same assessment the ASPICE for Cybersecurity assessment and if SEC.1 is rated P, you return and correct the SWE.1 rating.

(3) Take more time and interview SYS.2 longer and enter SEC.1 parts in parallel. Take more time and interview SWE.1 longer and enter SEC.1 parts in parallel. And rate consistently

Conclusion and Outlook

- This experience change is just beginning, more needs to be shared.
- A technical background is helpful to understand the cybersecurity approach.
- Assessors need to read the UNECE 155, 156 norms and also learn the TARA which is included as an example in the appendix F,G,H of the ISO 21434 norm

Thanks

Thank you for cooperating with ISCN.

1. ISCN is INTACS certified training provider for Automotive SPICE assessor courses
2. ISCN is certified by VDA to hold provisional and competent ASPICE assessor courses

3. ISCN moderates the German task force SOQRATES (https://soqrates.eurospi.net) since 2003 where >20 Tier 1 collaborate on ASPICE, Safety and Security.

4. ISCN organises the EuroSPI conference since 1994 where e.g. VW is organising a workshop community, and VW, Rheinmetall AG, EB, MAGNA, AVL held key notes. http://www.eurospi.net

5. EuroSPI certificates are issued by EuroSPI Certificates & Services GmbH (www.eurospi.net) in cooperation with DRIVES and the Automotive Skills Alliance (ASA). The ASA was founded by the EU Blueprint Project Drives and ALBATTS with support from the European Automobile Manufacturers' Association (ACEA). https://www.eurospi.net. ISCN is founding member.

Thanks

ISCN
www.iscn.com

Thank you for cooperating with EuroSPI Certificates GmbH.

1. Academy – Courses and Training Platform
2. Certification – Exam system and cerrificates
3. EuroSPI Conference Series
4. Assessment Tool – ISO 330xx based