The ASPICE for Cybersecurity - Updates in the latest materials (e.g. TARA for vehicle servers)

Dr. Thomas Liedtke

Dr. Richard Messnarz

Agenda

The ASPICE for Cybersecurity - Updates in the latest materials (e.g. TARA for vehicle servers)

1 | Status Training Material

2 | TARA for vehicle servers

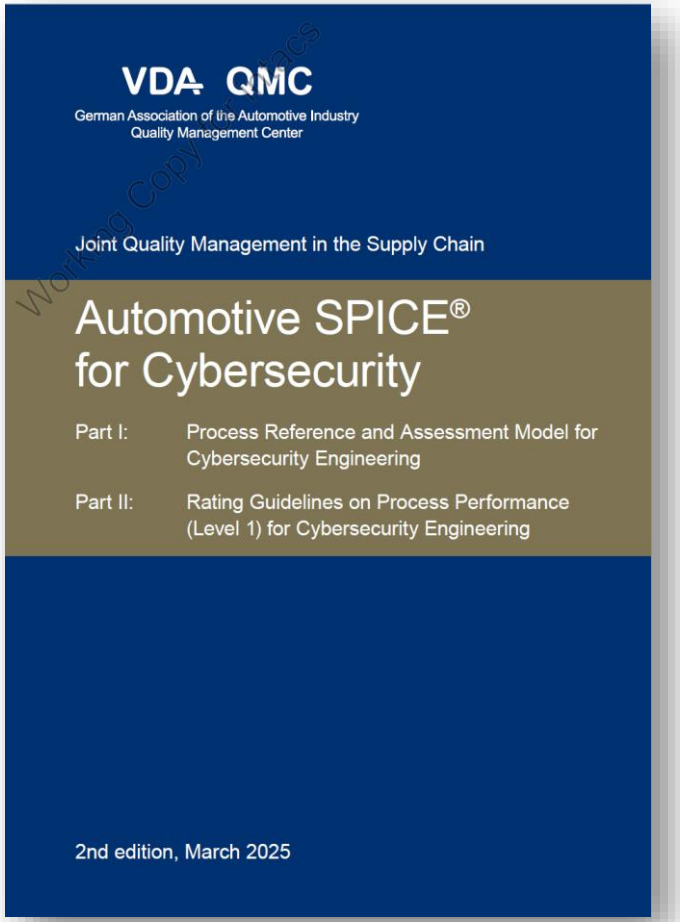
3 | Summary

EURO SPI 2026
European System, Software & Service Process Improvement & Innovation
in cooperation with initiatives in Asia, Africa and USA

VDA – QMC | Automotive SPICE®

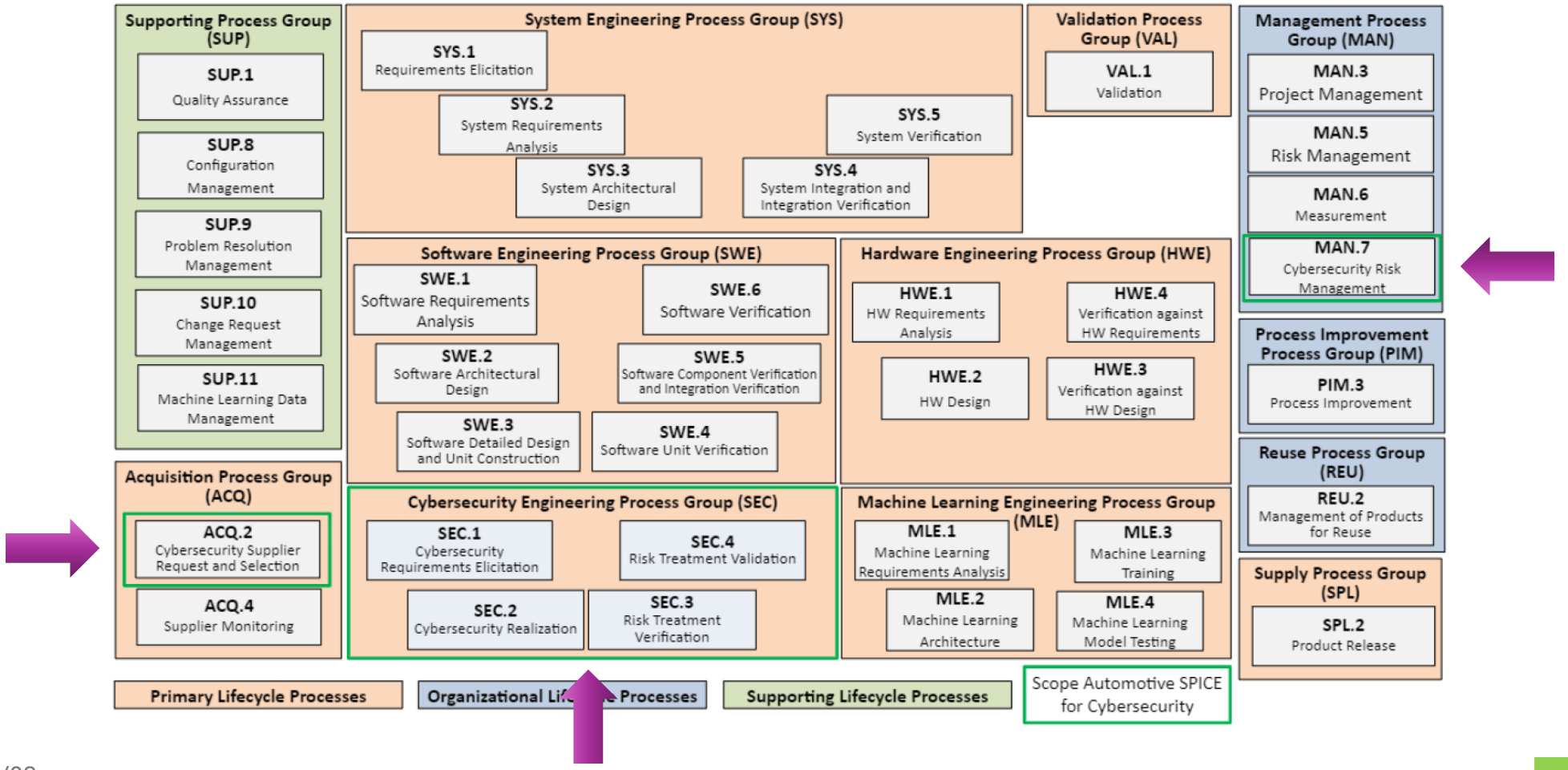
1 | Status Training Material

- Release of “Blue gold book” 2025, March, 2nd edition
  - Many alignments with ISO/SAE 21434 (e.g., wording)
- iNTACS Training material updated to be in line with PAM 2.0
- Latest version of training material: **3v1**
- Next improvement (reworking feedback) ongoing



Remember

1 | Status Training Material



Agenda

The ASPICE for Cybersecurity - Updates in the latest materials (e.g. TARA for vehicle servers)

1 | Status Training Material

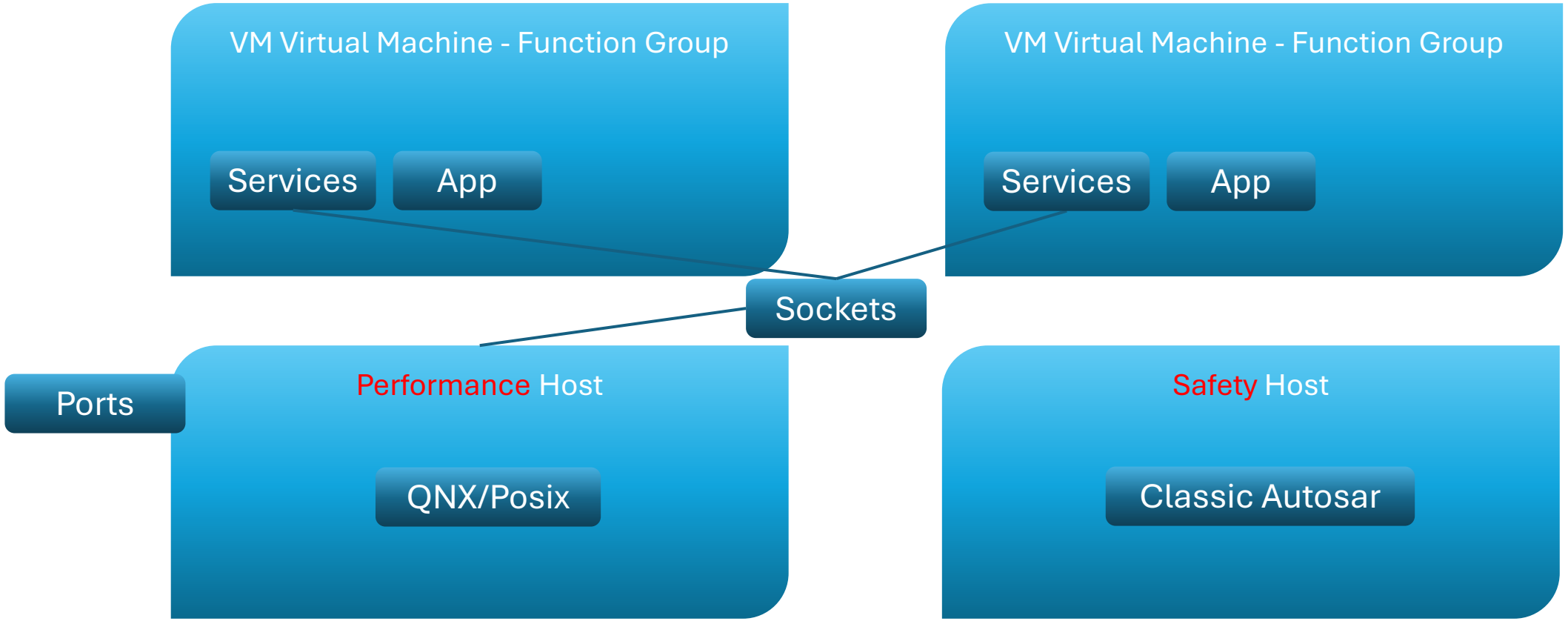
2 | TARA for vehicle servers

3 | Summary

Service based Architecture

2 | TARA for vehicle servers

- Services and Apps are registered in the **V**irtual **M**achines (**VM**) into different function groups.
- Each service is assigned to a port.



SOA (Service-Oriented-Architecture)

2 | TARA for vehicle servers

- Way how the cybersecurity software architects are modelling the attack vectors looks different (e.g., compared to our paper in the last years)
- It's becoming more like the IT/ OT world
- SOA based attack vectors are modelled to attack service ports and services

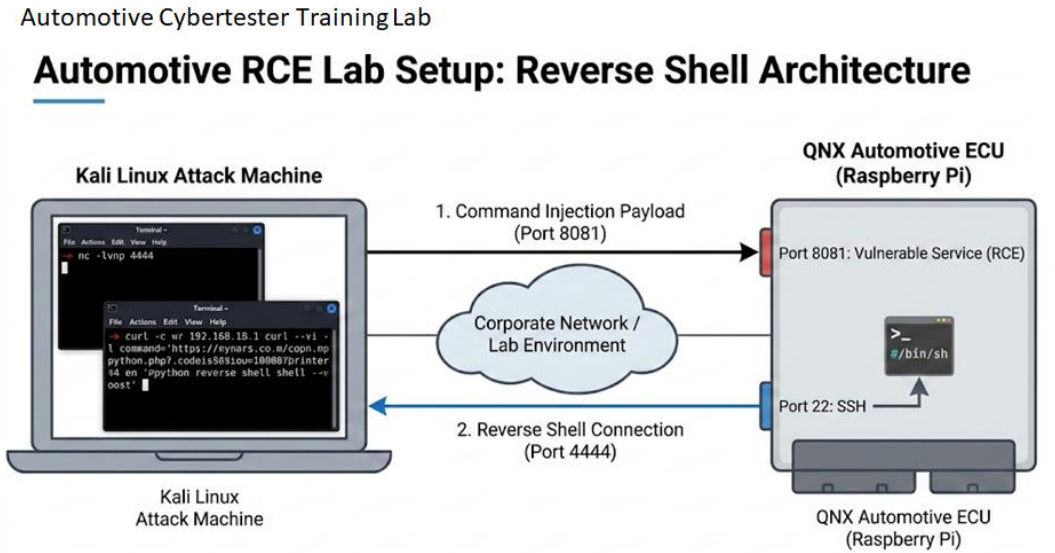
Performance Host apps are running like

- sensor-fusion for Highly Autonomous Drive)
- electric vehicle optimisation app which integrates up to 500 various parameters to control the e-motor and related electric systems
- Multimedia and internet services, with a MMX QNX multimedia port.
- ADAS services using the sensor fusion and sending commands to the ECUs.
- Telemetry services report vehicle data to generate diagnostic data of the fleet.
- …

SOA Attack vector

2 | TARA for vehicle servers

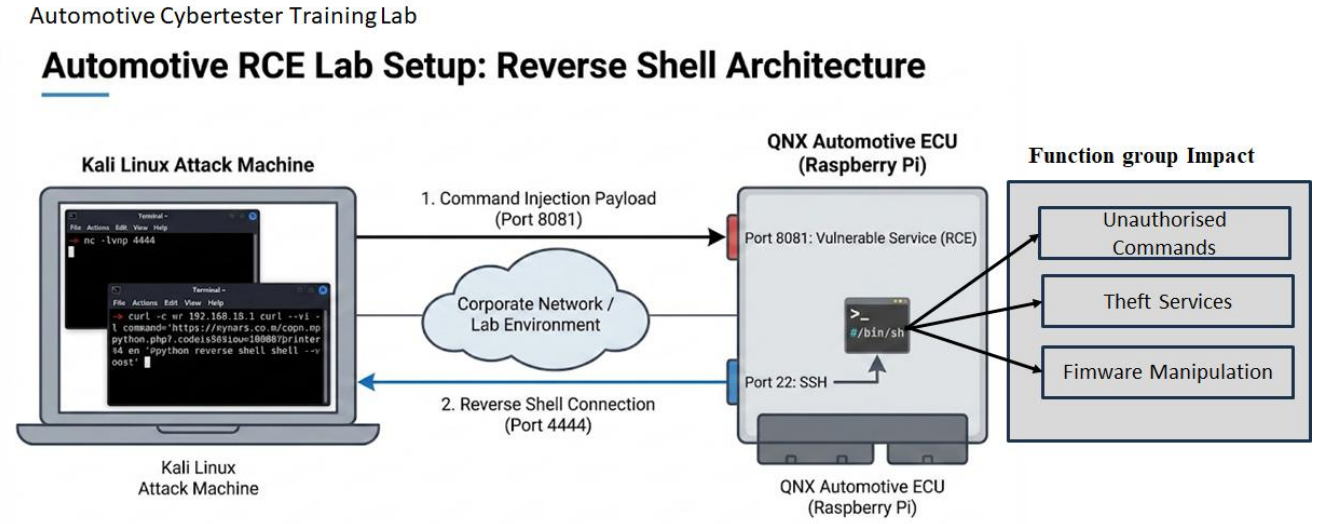
- Access by an attack platform from outside of the vehicle over the Internet via port 4444 on the attack platform and port 22 ssh on the QNX server. The attacker has shell access.
- Steps:
  - Vehicle user downloads an app from the Internet which contains a malicious code which can be executed from outside via the port 8081 (Internet).
  - This malicious code opens a ssh port 22 connection to the attack platform on port 4444 and starts a bin/sh command shell (the program includes code to execute commands on the OS).



Attack path to trigger the damage scenario compromising underlying assets are different

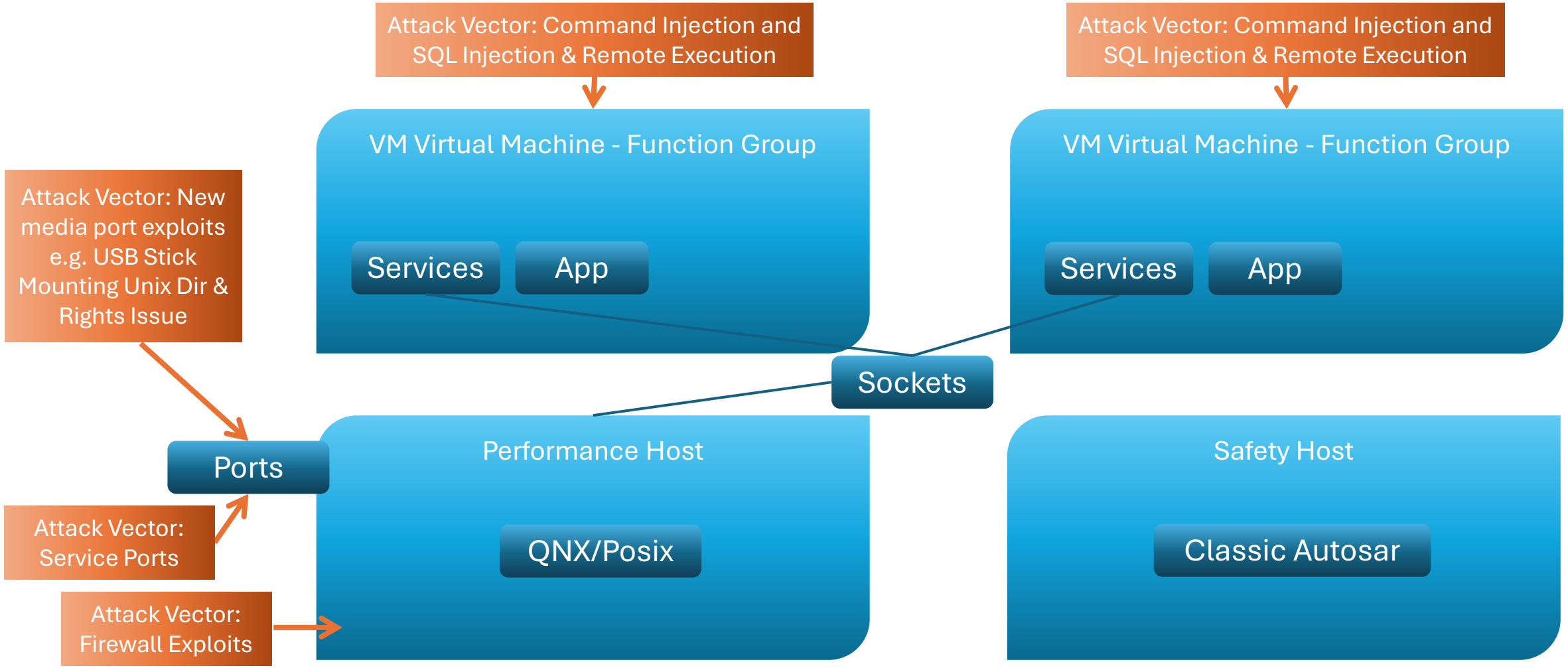
2 | TARA for vehicle servers

- Complete Vehicle Control
- Remote Tracking and Hijacking
- Safety Critical Failures
- Data Theft and Privacy Breach
- Firmware Manipulation
- Backend System Compromise



Cybersecurity Item at Vehicle Level with attack vectors

2 | TARA for vehicle servers



Threat Analysis and Risk Assessment

2 | TARA for vehicle servers

TARA final steps

- After identification of attack paths, feasibility of the attack paths has to be rated.
- Having rated damage scenario severity and attack feasibility risk value can be determined according to the matrix given in ISO/SAE 21434

Cybersecurity Goals and Controls

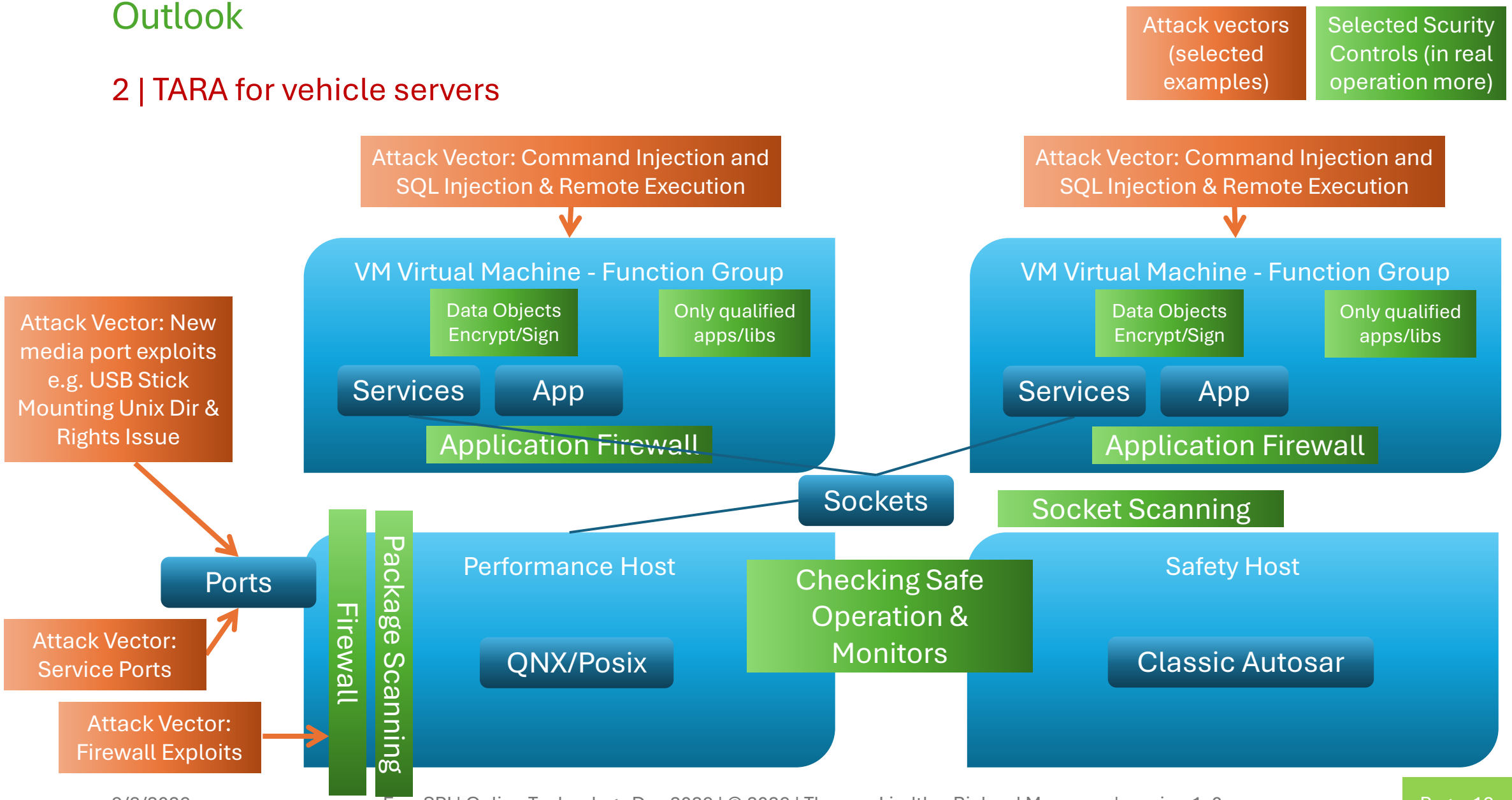
- After decision to reduce the risk related cybersecurity goal can be stated as

“skids out of control of the vehicle due to tampered service requests shall not happen”

Cybersecurity Controls have to be defined, such as firewall settings, package scanning, application firewall, whitelisting, signing of apps, registration and authentication of services etc.

Outlook

2 | TARA for vehicle servers



Agenda

The ASPICE for Cybersecurity - Updates in the latest materials (e.g. TARA for vehicle servers)

1 | Status Training Material

2 | TARA for vehicle servers

3 | Summary

Key Findings – Cybersecurity of HPC / SOA Architectures

2 | TARA for vehicle servers

- TARA remains applicable:
  - The function-oriented ISO/SAE 21434 approach can be applied to service-oriented/HPC architectures with only minor modifications.
- Attack paths change significantly:
  - HPC architectures introduce new attack surfaces and techniques, e.g. command injection, reverse shells, service manipulation and privilege escalation.
- Cybersecurity goals remain largely unchanged:
  - The focus is still on ensuring the safe and correct operation of vehicle functions.
- Security controls need to evolve:
  - Service authentication, application whitelisting, container isolation, secure service discovery and Zero Trust become increasingly important.
- TARA must cover new architectural assets:
  - Services, applications, virtual machines, containers, communication ports and service registries need to be considered.
- Skills, standards & assessments must evolve:
  - Existing training, assessment models and best practices need to address SOA/HPC architectures, including the combined consideration of safety and cybersecurity.
- → **Bottom line:** The approach we have developed over the past few years now also supports the SDV and AIDV Vehicles versions.

Key differences between ECU-based architectures and modern HPC-based vehicle server architectures

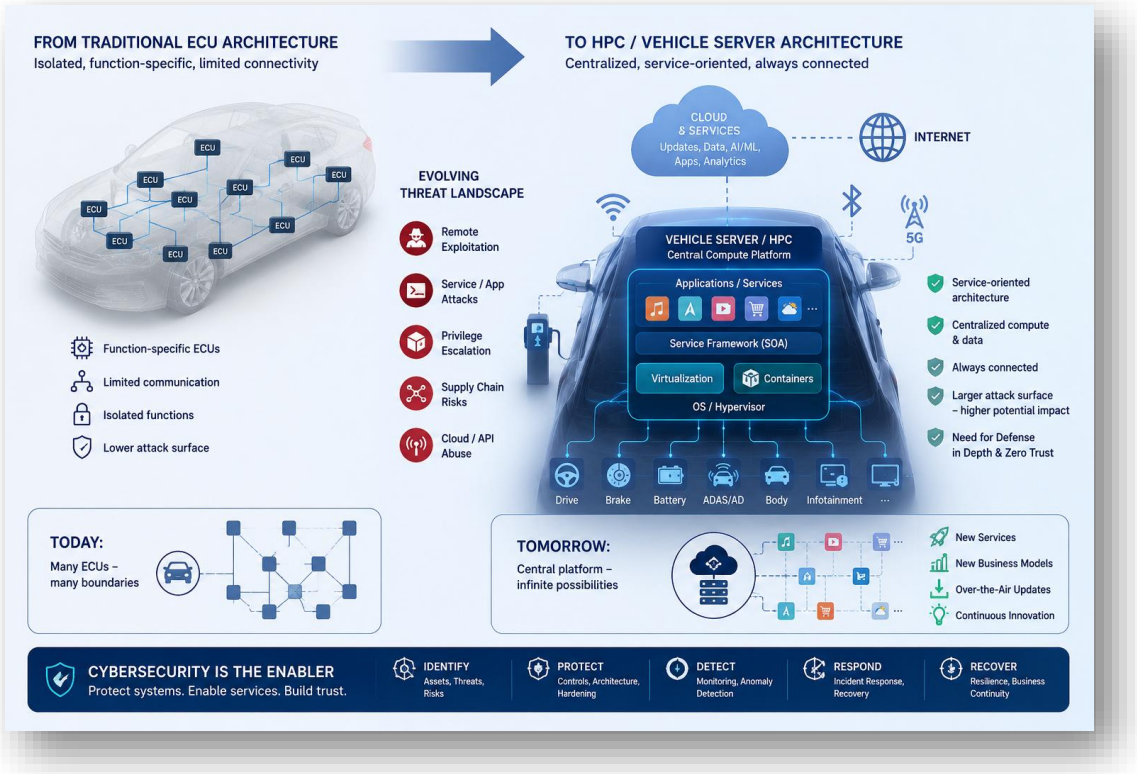
7 | Summary

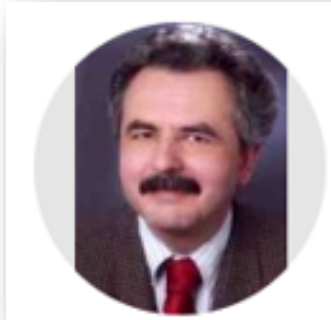
Aspect	Classical ECU	Vehicle Server
Primary Assets	ECUs, Vehicle Functions	Services, Applications, Vehicle Functions
Entry Points	CAN, LIN, Physical Access	Internet, Telematics, App Interface
Architecture	AUTOSAR Classic	Adaptive AUTOSAR / SOA
Attack Surface	Primarily Internal Vehicle Networks	Internet Facing Services
Typical Attack Techn.	CAN Injection, Firmware Manipulation	Command Injection, RCE, Reverse Shell
Trust Boundary	ECU Perimeter	Service and Application Perimeter
Security Controls	Secure Boot, Secure Flashing	Service Authentication, Container Isolation, Zero Trust
TARA Focus	ECU and Function Protection	Service and Function Protection

Outlook

7 | Summary

- Vehicle server platforms will become the primary software development platform, with applications and SOA-based services increasingly driving vehicle functionality.
- Increasing connectivity to cloud and Internet infrastructure will expand the attack surface, making robust cybersecurity controls essential.
- Best-practice sharing and new engineering skills will be critical, covering assets, threats, attack vectors, verification/validation, and protection of server architectures.





Dr. Thomas Liedtke
Consultant

+49 173 676 40 93
thomas@tliedtke.onmicrosoft.com
https://www.linkedin.com/in/thomas-liedtke/

Dr. Richard Messnarz
Director

I.S.C.N. GesmbH
Karl Morre Straße 86 A-8020 Graz, Austria
Tel.: +43 316 811198
E-Mail: rmess@iscn.com
Web: www.iscn.com