SYNSPACE experts in excellence

ISCN

Updates in Automotive SPICE© for Cybersecurity

A Multi-Level Approach to TARA

Attack Feasibility in Interference-Free Scenarios and the Trusted Zones Approach

Thomas Liedtke (PhD)

Prof. Richard Messnarz

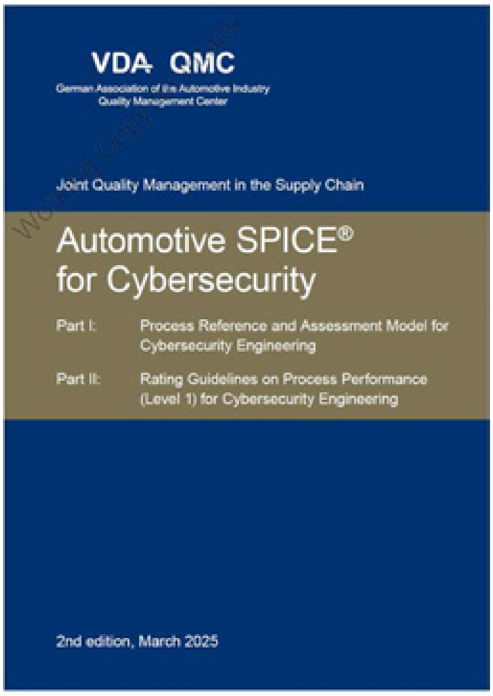
Presentation | RIGA | 15th September 2025

Online Technology Day

VDA – QMC | Automotive SPICE®

Online Technology Day – Cybersecurity Update

- Release of "Blue gold book" 2025, March, 2nd edition
- iNTACS Training material currently under update to be in line with PAM 2.0
- PAM 2.0 still contains some inconsistencies with the ISO/SAE 21434 standard



VDA QMC

German Association of the Automotive Industry
Quality Management Center

Joint Quality Management in the Supply Chain

Automotive SPICE®
for Cybersecurity

Part I: Process Reference and Assessment Model for Cybersecurity Engineering

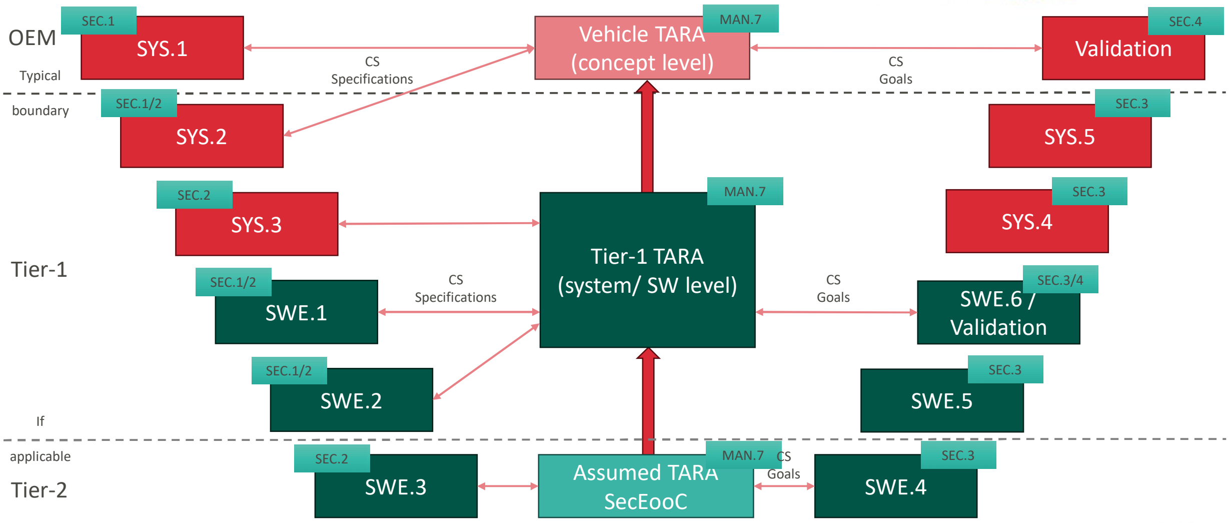
Part II: Rating Guidelines on Process Performance (Level 1) for Cybersecurity Engineering

2nd edition, March 2025

Risk Assessment is performed on different levels

Online Technology Day – Cybersecurity Update

Remember !



OEM

Typical boundary

Tier-1

If applicable

Tier-2

SEC.1 SYS.1

SEC.1/2 SYS.2

SEC.2 SYS.3

SEC.1/2 SWE.1

SEC.1/2 SWE.2

SEC.2 SWE.3

MAN.7 Vehicle TARA (concept level)

MAN.7 Tier-1 TARA (system/ SW level)

MAN.7 Assumed TARA SecEooC

SEC.4 Validation

SEC.3 SYS.5

SEC.3 SYS.4

SEC.3/4 SWE.6 / Validation

SEC.3 SWE.5

SEC.3 SWE.4

CS Specifications

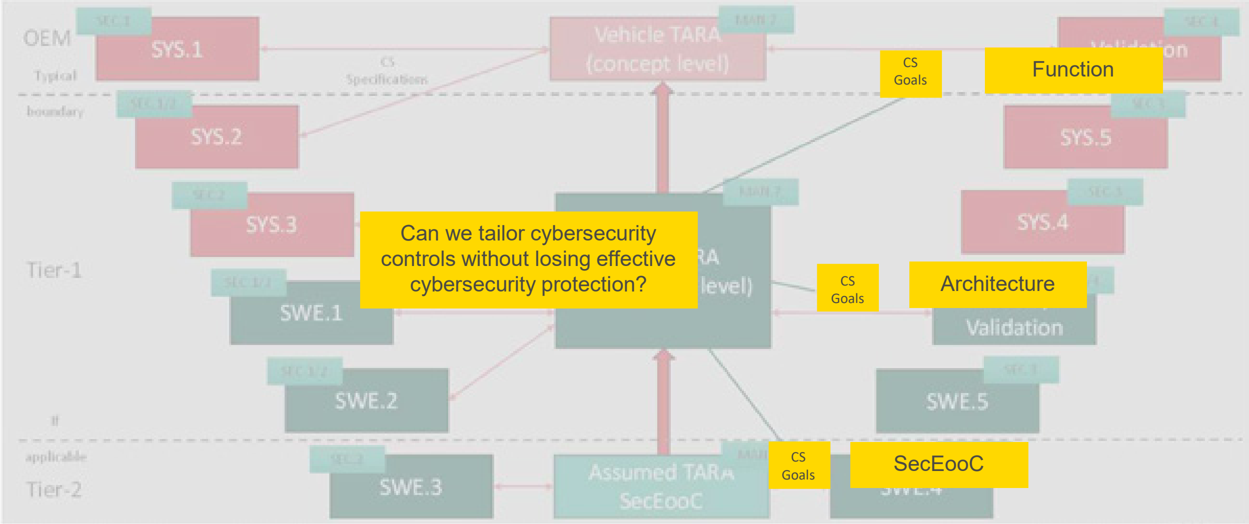
CS Goals

3 EuroSPI | Online Technology Day 2025 | © 2025 | Thomas Liedtke; Richard Messnarz | version 1v0

Criticality: internal

Tailoring of cybersecurity controls selected after identification of CS goals

Online Technology Day – Cybersecurity Update



Can we tailor cybersecurity controls without losing effective cybersecurity protection?

CS Goals — Function

CS Goals — Architecture

CS Goals — SecEooC

OEM

Typical boundary

Tier-1

If applicable

Tier-2

SYS.1 SYS.2 SYS.3 SWE.1 SWE.2 SWE.3

Vehicle TARA (concept level)

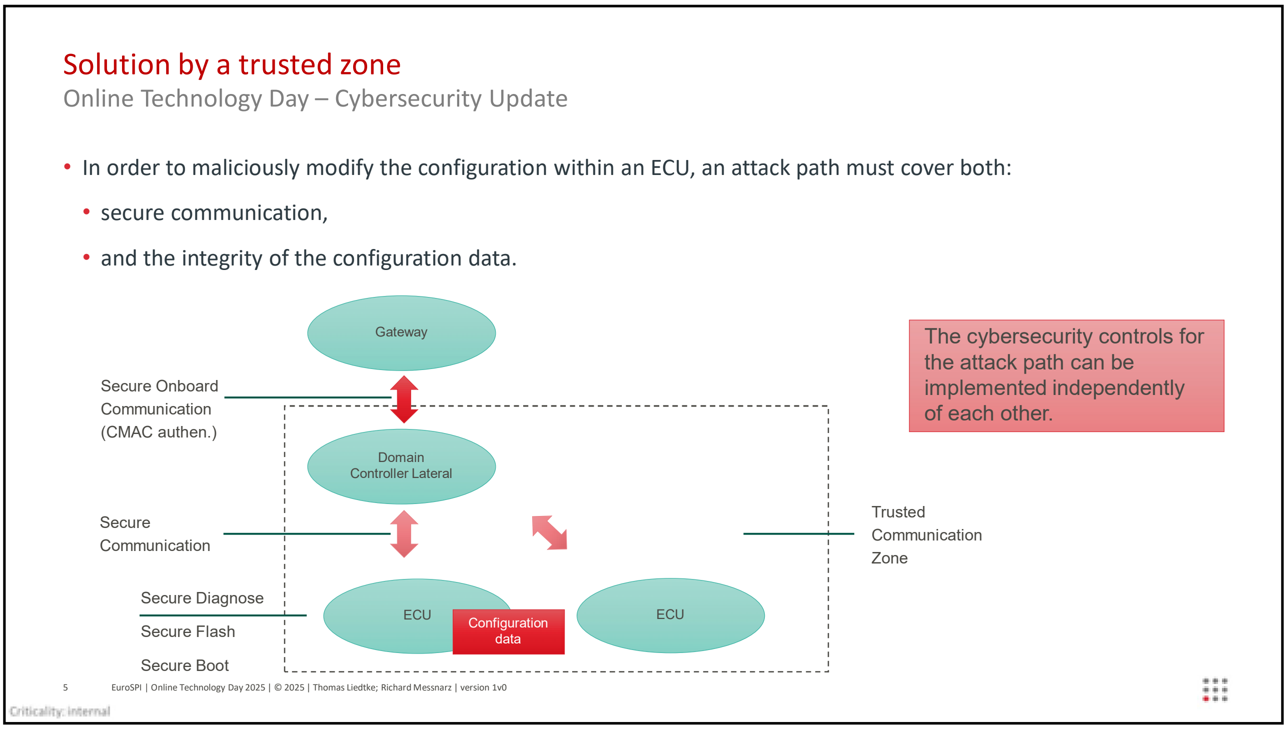
Assumed TARA SecEooC

Validation SYS.5 SYS.4 Validation SWE.5

CS Specifications

4 EuroSPI | Online Technology Day 2025 | © 2025 | Thomas Liedtke; Richard Messnarz | version 1v0

Criticality: internal



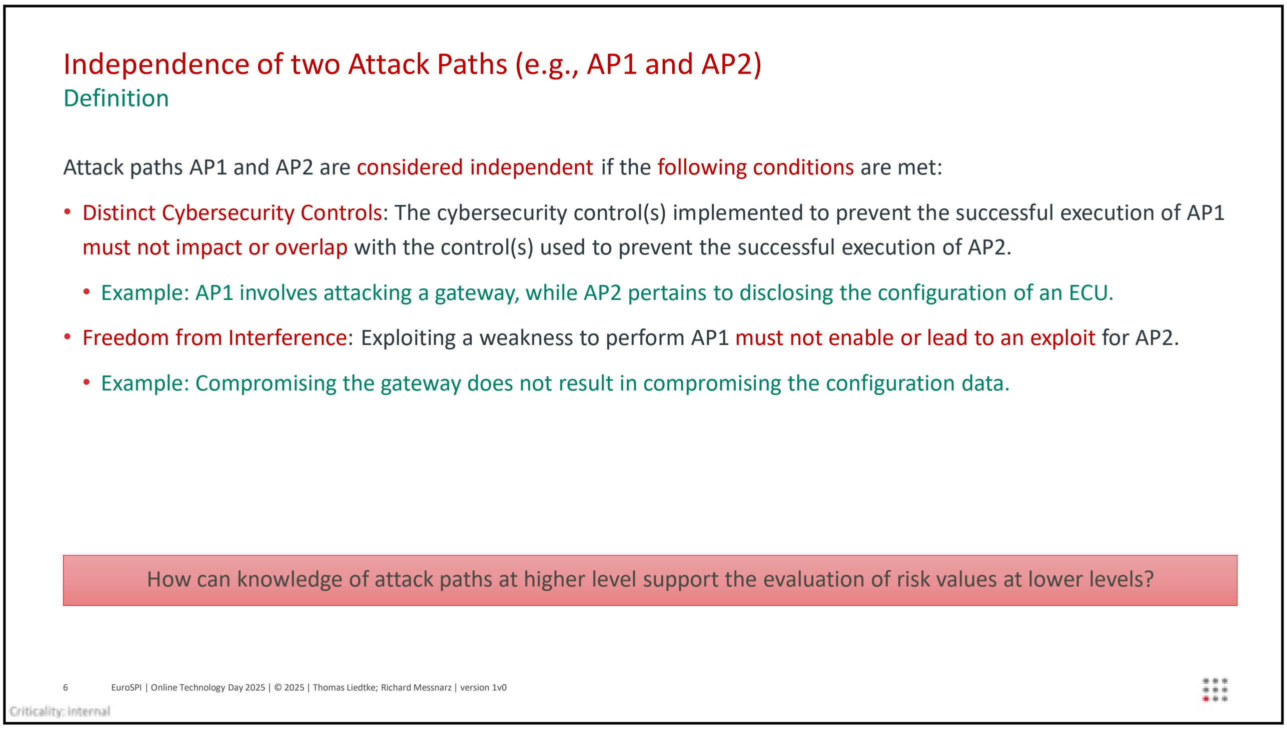
Solution by a trusted zone

Online Technology Day – Cybersecurity Update

- In order to maliciously modify the configuration within an ECU, an attack path must cover both:
  - secure communication,
  - and the integrity of the configuration data.

Gateway
Secure Onboard Communication (CMAC authen.)
Domain Controller Lateral
Secure Communication
Secure Diagnose
Secure Flash
Secure Boot
ECU
Configuration data
ECU
Trusted Communication Zone

The cybersecurity controls for the attack path can be implemented independently of each other.



Independence of two Attack Paths (e.g., AP1 and AP2)

Definition

Attack paths AP1 and AP2 are considered independent if the following conditions are met:

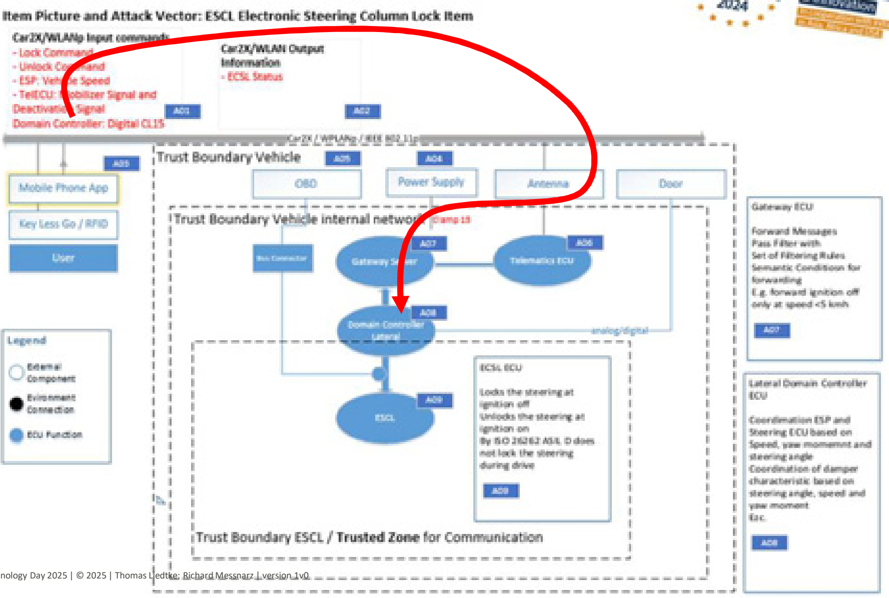
- Distinct Cybersecurity Controls: The cybersecurity control(s) implemented to prevent the successful execution of AP1 must not impact or overlap with the control(s) used to prevent the successful execution of AP2.
  - Example: AP1 involves attacking a gateway, while AP2 pertains to disclosing the configuration of an ECU.
- Freedom from Interference: Exploiting a weakness to perform AP1 must not enable or lead to an exploit for AP2.
  - Example: Compromising the gateway does not result in compromising the configuration data.

How can knowledge of attack paths at higher level support the evaluation of risk values at lower levels?

Architectural design of the Electronic Steering Column Lock ECU

Cybersecurity Item at Vehicle Level

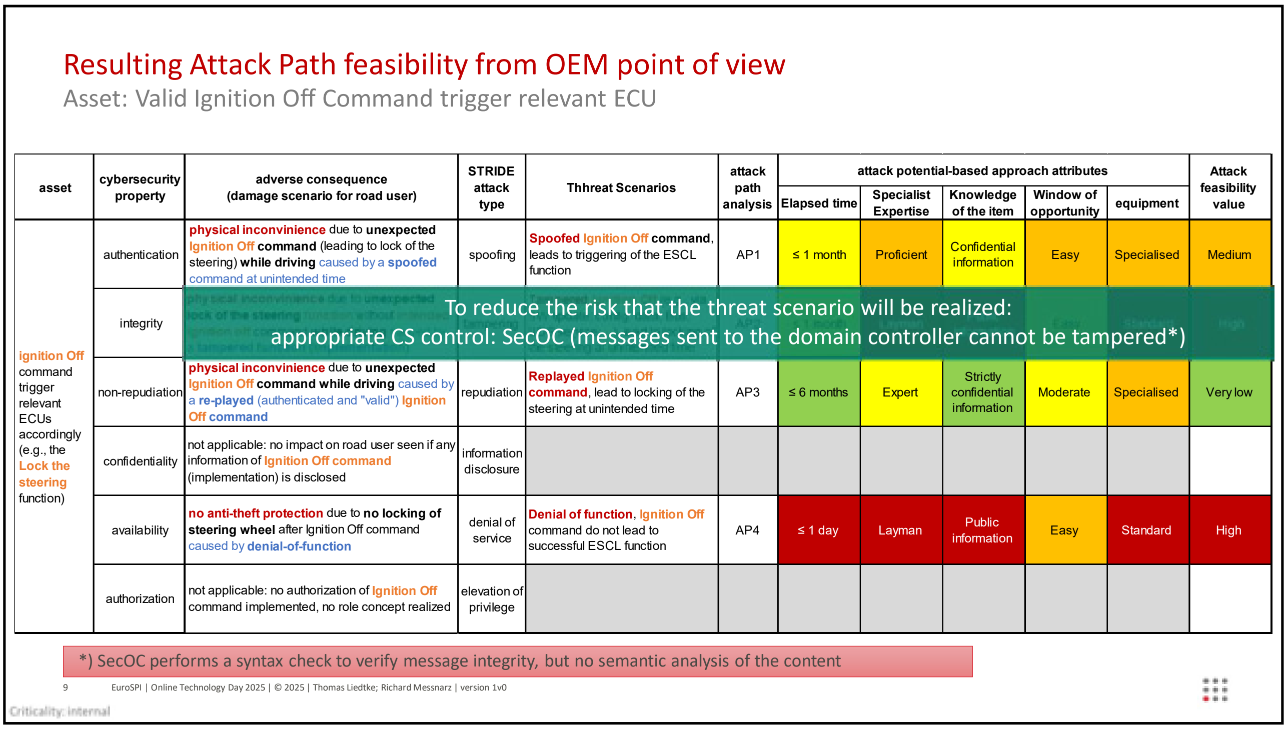
Remember !


Item Picture and Attack Vector: ESCL Electronic Steering Column Lock Item
Car2X/WLANp Input commands
- Lock Command
- Unlock Command
- ESP: Vehicle Speed
- TelECU: Imobilizer Signal and Deactivation Signal
Domain Controller: Digital CL15
A01
Car2X/WLAN Output Information
- ECSL Status
A02
Car2X / WPLANp / IEEE 802.11p
A03
Mobile Phone App
Key Less Go / RFID
User
Trust Boundary Vehicle
A05
A04
OBD
Power Supply
Antenna
Door
Trust Boundary Vehicle internal network
Clamp 15
Bus Connector
A07
Gateway Server
A06
Telematics ECU
A08
Domain Controller Lateral
analog/digital
A09
ESCL
ECSL ECU
Locks the steering at ignition off
Unlocks the steering at ignition on
By ISO 26262 ASIL D does not lock the steering during drive
A09
Trust Boundary ESCL / Trusted Zone for Communication
Legend
External Component
Evironment Connection
ECU Function
Gateway ECU
Forward Messages
Pass Filter with
Set of Filtering Rules
Semantic Condition for forwarding
E.g. forward ignition off only at speed <5 kmh
A07
Lateral Domain Controller ECU
Coordination ESP and Steering ECU based on Speed, yaw momemnt and steering angle
Coordination of damper characteristic based on steering angle, speed and yaw moment
Etc.
A08

Resulting Attack Path feasibility from OEM point of view

Asset: Valid Ignition Off Command trigger relevant ECU

asset	cybersecurity property	adverse consequence (damage scenario for road user)	STRIDE attack type	Threat Scenarios	attack path analysis	attack potential-based approach attributes					Attack feasibility value
						Elapsed time	Specialist Expertise	Knowledge of the item	Window of opportunity	equipment	
ignition Off command trigger relevant ECUs accordingly (e.g., the Lock the steering function)	authentication	**physical inconvinience** due to **unexpected** Ignition Off **command** (leading to lock of the steering) **while driving** caused by a **spoofed** command at unintended time	spoofing	**Spoofed** Ignition Off **command**, leads to triggering of the ESCL function	AP1	≤ 1 month	Proficient	Confidential information	Easy	Specialised	Medium
	integrity	**physical inconvinience** due to **unexpected lock of the steering** function without intended Ignition off command **while driving** caused by a **tampered function (implementation)**	tampering	**Tampered** Ignition Off (e.g., via SW update; config. data; Bus; UDS service; ...), lead to locking of the steering at unintended time	AP2	≤ 1 month	Layman	Public information	Easy	Standard	High
	non-repudiation	**physical inconvinience** due to **unexpected** Ignition Off **command while driving** caused by a **re-played** (authenticated and "valid") Ignition Off command	repudiation	**Replayed** Ignition Off **command**, lead to locking of the steering at unintended time	AP3	≤ 6 months	Expert	Strictly confidential information	Moderate	Specialised	Very low
	confidentiality	not applicable: no impact on road user seen if any information of Ignition Off command (implementation) is disclosed	information disclosure								
	availability	**no anti-theft protection** due to **no locking of steering wheel** after Ignition Off command caused by **denial-of-function**	denial of service	**Denial of function**, Ignition Off command do not lead to successful ESCL function	AP4	≤ 1 day	Layman	Public information	Easy	Standard	High
	authorization	not applicable: no authorization of Ignition Off command implemented, no role concept realized	elevation of privilege								



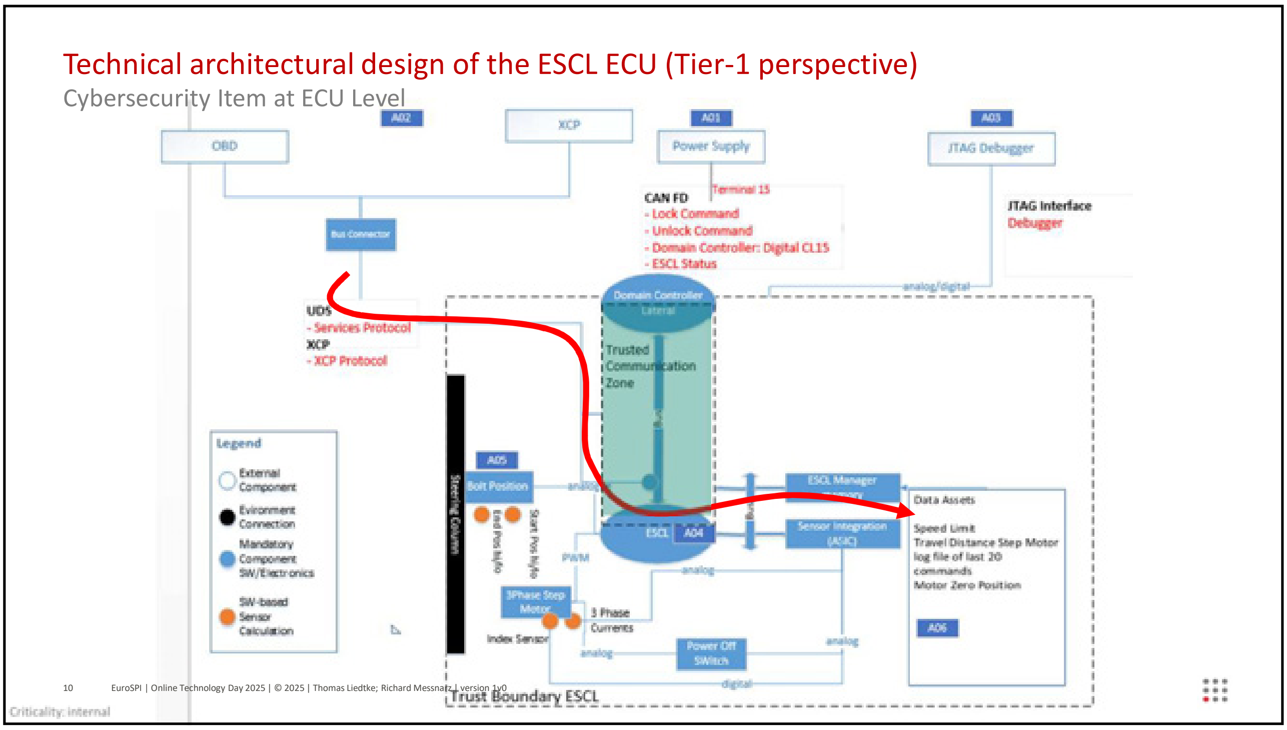
Resulting Attack Path feasibility from OEM point of view

Asset: Valid Ignition Off Command trigger relevant ECU

asset	cybersecurity property	adverse consequence (damage scenario for road user)	STRIDE attack type	Thhreat Scenarios	attack path analysis	attack potential-based approach attributes					Attack feasibility value
						Elapsed time	Specialist Expertise	Knowledge of the item	Window of opportunity	equipment	
ignition Off command trigger relevant ECUs accordingly (e.g., the Lock the steering function)	authentication	**physical inconvinience** due to **unexpected** Ignition Off **command** (leading to lock of the steering) **while driving** caused by a **spoofed** command at unintended time	spoofing	**Spoofed Ignition Off command**, leads to triggering of the ESCL function	AP1	≤ 1 month	Proficient	Confidential information	Easy	Specialised	Medium
	integrity	physical inconvinience due to unexpected lock of the steering function without intended Ignition off command while driving [illegible] a tampered function (implementation)	tampering	Tampered Ignition Off [illegible]	AP2	≤ 1 month	Layman	[illegible]	Easy	Standard	High
	non-repudiation	**physical inconvinience** due to **unexpected** Ignition Off **command while driving** caused by a **re-played** (authenticated and "valid") **Ignition Off command**	repudiation	**Replayed Ignition Off command**, lead to locking of the steering at unintended time	AP3	≤ 6 months	Expert	Strictly confidential information	Moderate	Specialised	Very low
	confidentiality	not applicable: no impact on road user seen if any information of **Ignition Off command** (implementation) is disclosed	information disclosure								
	availability	**no anti-theft protection** due to **no locking of steering wheel** after Ignition Off command caused by **denial-of-function**	denial of service	**Denial of function**, **Ignition Off** command do not lead to successful ESCL function	AP4	≤ 1 day	Layman	Public information	Easy	Standard	High
	authorization	not applicable: no authorization of **Ignition Off** command implemented, no role concept realized	elevation of privilege								

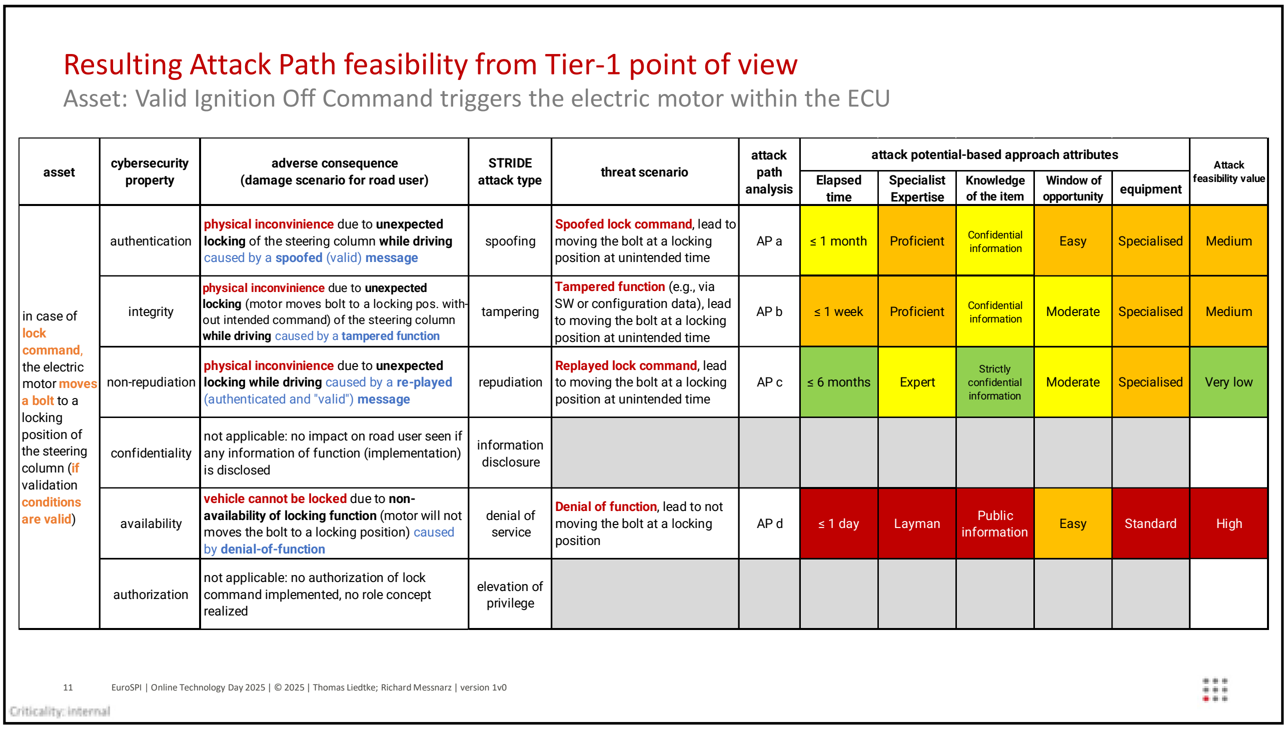
To reduce the risk that the threat scenario will be realized:
appropriate CS control: SecOC (messages sent to the domain controller cannot be tampered*)

*) SecOC performs a syntax check to verify message integrity, but no semantic analysis of the content



Technical architectural design of the ESCL ECU (Tier-1 perspective)

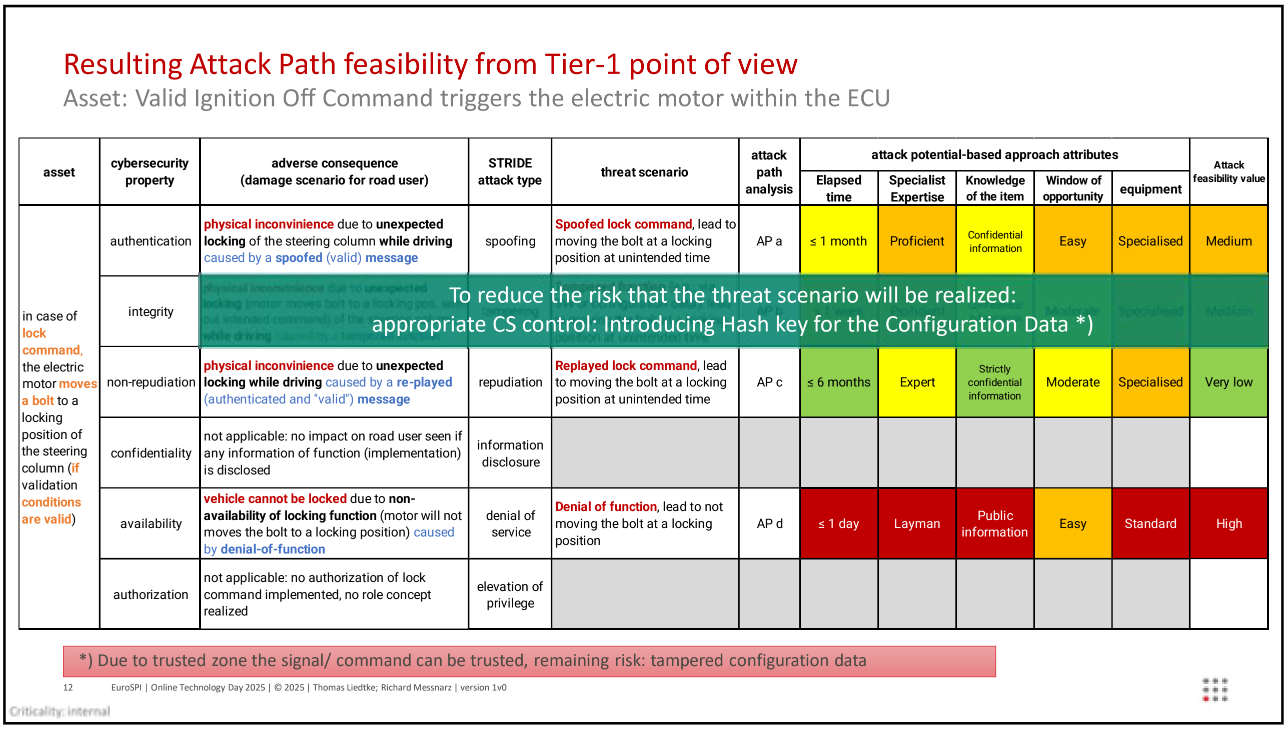
Cybersecurity Item at ECU Level



Resulting Attack Path feasibility from Tier-1 point of view

Asset: Valid Ignition Off Command triggers the electric motor within the ECU

asset	cybersecurity property	adverse consequence (damage scenario for road user)	STRIDE attack type	threat scenario	attack path analysis	attack potential-based approach attributes					Attack feasibility value
						Elapsed time	Specialist Expertise	Knowledge of the item	Window of opportunity	equipment	
in case of lock command, the electric motor moves a bolt to a locking position of the steering column (if validation conditions are valid)	authentication	physical inconvinience due to unexpected locking of the steering column while driving caused by a spoofed (valid) message	spoofing	Spoofed lock command, lead to moving the bolt at a locking position at unintended time	AP a	≤ 1 month	Proficient	Confidential information	Easy	Specialised	Medium
	integrity	physical inconvinience due to unexpected locking (motor moves bolt to a locking pos. with-out intended command) of the steering column while driving caused by a tampered function	tampering	Tampered function (e.g., via SW or configuration data), lead to moving the bolt at a locking position at unintended time	AP b	≤ 1 week	Proficient	Confidential information	Moderate	Specialised	Medium
	non-repudiation	physical inconvinience due to unexpected locking while driving caused by a re-played (authenticated and "valid") message	repudiation	Replayed lock command, lead to moving the bolt at a locking position at unintended time	AP c	≤ 6 months	Expert	Strictly confidential information	Moderate	Specialised	Very low
	confidentiality	not applicable: no impact on road user seen if any information of function (implementation) is disclosed	information disclosure								
	availability	vehicle cannot be locked due to non-availability of locking function (motor will not moves the bolt to a locking position) caused by denial-of-function	denial of service	Denial of function, lead to not moving the bolt at a locking position	AP d	≤ 1 day	Layman	Public information	Easy	Standard	High
	authorization	not applicable: no authorization of lock command implemented, no role concept realized	elevation of privilege								



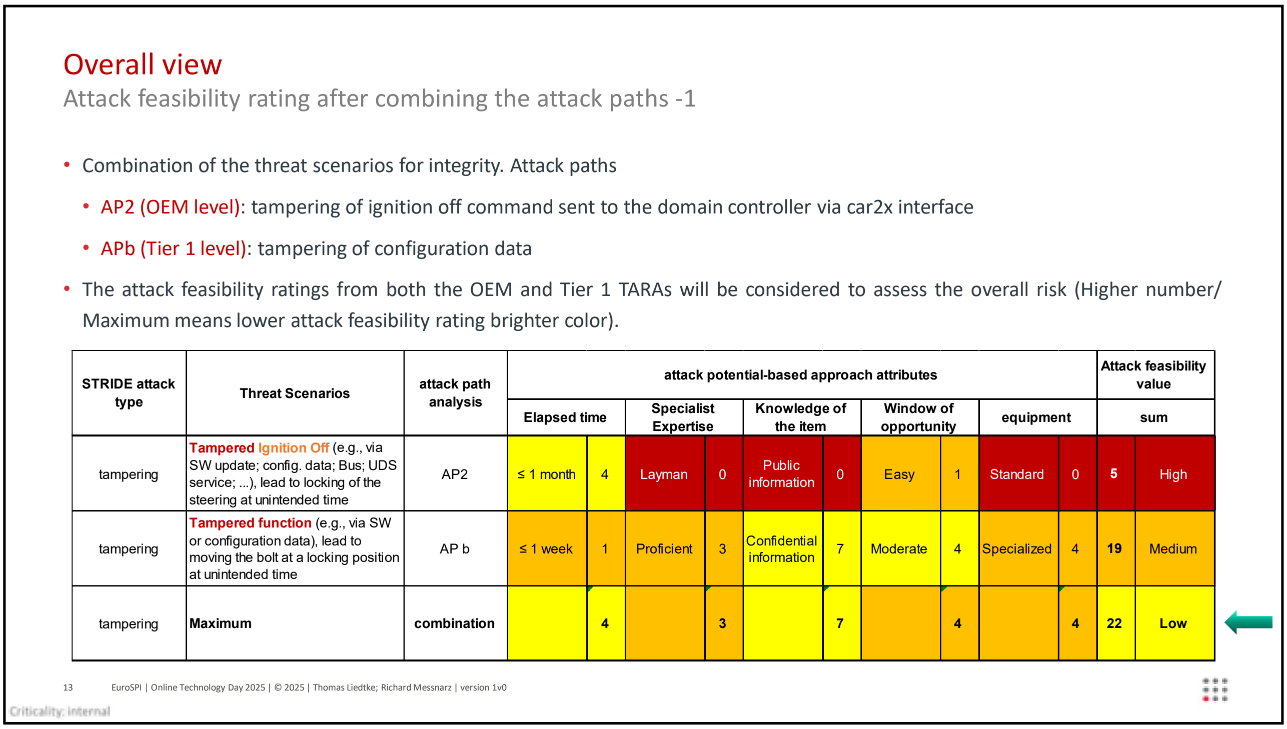
Resulting Attack Path feasibility from Tier-1 point of view

Asset: Valid Ignition Off Command triggers the electric motor within the ECU

asset	cybersecurity property	adverse consequence (damage scenario for road user)	STRIDE attack type	threat scenario	attack path analysis	attack potential-based approach attributes					Attack feasibility value
						Elapsed time	Specialist Expertise	Knowledge of the item	Window of opportunity	equipment	
in case of lock command, the electric motor moves a bolt to a locking position of the steering column (if validation conditions are valid)	authentication	physical inconvinience due to unexpected locking of the steering column while driving caused by a spoofed (valid) message	spoofing	Spoofed lock command, lead to moving the bolt at a locking position at unintended time	AP a	≤ 1 month	Proficient	Confidential information	Easy	Specialised	Medium
	integrity	physical inconvinience due to unexpected locking (motor moves bolt to a locking pos. with-out intended command) of the steering column while driving caused by a tampered function	tampering	Tampered function (e.g., via SW or configuration data), lead to moving the bolt at a locking position at unintended time	AP b	≤ 1 week	Proficient	Confidential information	Moderate	Specialised	Medium
	non-repudiation	physical inconvinience due to unexpected locking while driving caused by a re-played (authenticated and "valid") message	repudiation	Replayed lock command, lead to moving the bolt at a locking position at unintended time	AP c	≤ 6 months	Expert	Strictly confidential information	Moderate	Specialised	Very low
	confidentiality	not applicable: no impact on road user seen if any information of function (implementation) is disclosed	information disclosure								
	availability	vehicle cannot be locked due to non-availability of locking function (motor will not moves the bolt to a locking position) caused by denial-of-function	denial of service	Denial of function, lead to not moving the bolt at a locking position	AP d	≤ 1 day	Layman	Public information	Easy	Standard	High
	authorization	not applicable: no authorization of lock command implemented, no role concept realized	elevation of privilege								

To reduce the risk that the threat scenario will be realized:
appropriate CS control: Introducing Hash key for the Configuration Data *)

*) Due to trusted zone the signal/ command can be trusted, remaining risk: tampered configuration data



Overall view

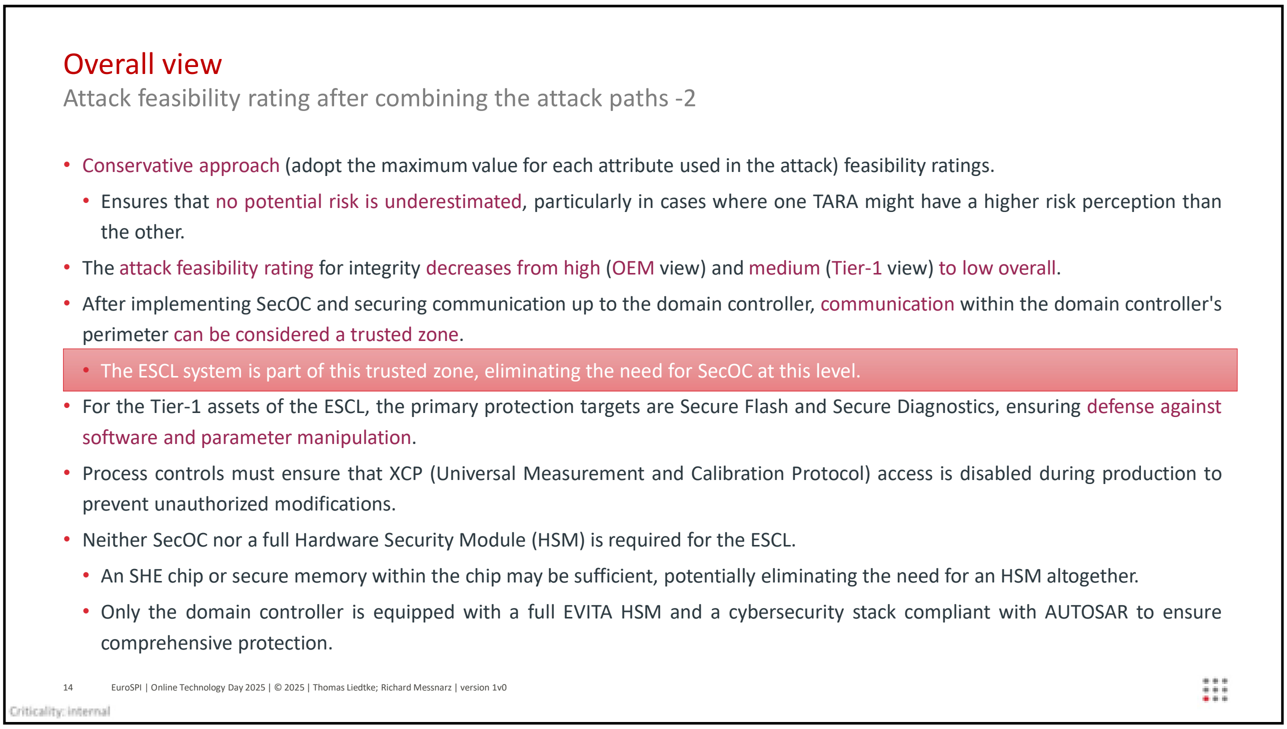
Attack feasibility rating after combining the attack paths -1

- Combination of the threat scenarios for integrity. Attack paths
  - AP2 (OEM level): tampering of ignition off command sent to the domain controller via car2x interface
  - APb (Tier 1 level): tampering of configuration data
- The attack feasibility ratings from both the OEM and Tier 1 TARAs will be considered to assess the overall risk (Higher number/ Maximum means lower attack feasibility rating brighter color).

STRIDE attack type	Threat Scenarios	attack path analysis	attack potential-based approach attributes										Attack feasibility value	
			Elapsed time		Specialist Expertise		Knowledge of the item		Window of opportunity		equipment		sum	
tampering	**Tampered Ignition Off** (e.g., via SW update; config. data; Bus; UDS service; ...), lead to locking of the steering at unintended time	AP2	≤ 1 month	4	Layman	0	Public information	0	Easy	1	Standard	0	**5**	High
tampering	**Tampered function** (e.g., via SW or configuration data), lead to moving the bolt at a locking position at unintended time	AP b	≤ 1 week	1	Proficient	3	Confidential information	7	Moderate	4	Specialized	4	**19**	Medium
tampering	**Maximum**	**combination**		**4**		**3**		**7**		**4**		**4**	**22**	**Low**

13 EuroSPI | Online Technology Day 2025 | © 2025 | Thomas Liedtke; Richard Messnarz | version 1v0

Criticality: internal



Overall view

Attack feasibility rating after combining the attack paths -2

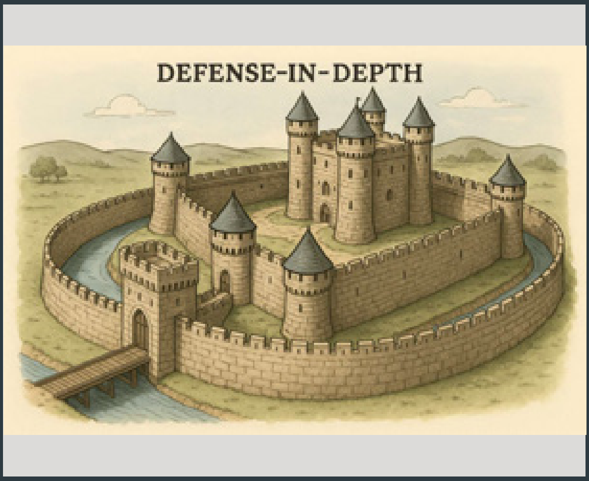
- Conservative approach (adopt the maximum value for each attribute used in the attack) feasibility ratings.
  - Ensures that no potential risk is underestimated, particularly in cases where one TARA might have a higher risk perception than the other.
- The attack feasibility rating for integrity decreases from high (OEM view) and medium (Tier-1 view) to low overall.
- After implementing SecOC and securing communication up to the domain controller, communication within the domain controller's perimeter can be considered a trusted zone.
  - The ESCL system is part of this trusted zone, eliminating the need for SecOC at this level.
- For the Tier-1 assets of the ESCL, the primary protection targets are Secure Flash and Secure Diagnostics, ensuring defense against software and parameter manipulation.
- Process controls must ensure that XCP (Universal Measurement and Calibration Protocol) access is disabled during production to prevent unauthorized modifications.
- Neither SecOC nor a full Hardware Security Module (HSM) is required for the ESCL.
  - An SHE chip or secure memory within the chip may be sufficient, potentially eliminating the need for an HSM altogether.
  - Only the domain controller is equipped with a full EVITA HSM and a cybersecurity stack compliant with AUTOSAR to ensure comprehensive protection.

14 EuroSPI | Online Technology Day 2025 | © 2025 | Thomas Liedtke; Richard Messnarz | version 1v0

Criticality: internal

Defense-in-depth

- ESCL functionality: Tier-1 suppliers can assume that higher-level systems (e.g., SecOC, communication gateway, domain controller) have cybersecurity controls in place.
- Overall defense strategy: These higher-level controls form part of the comprehensive security approach.
- Risk mitigation: Measures help reduce risks and prevent exploitation of ESCL assets.
- OEM & Tier-1 collaboration: A practical example of effective cooperation in cybersecurity.
- Defense-in-depth: Layered security measures at different system levels work together to counter potential threats.

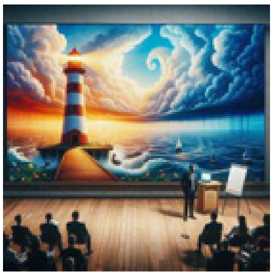


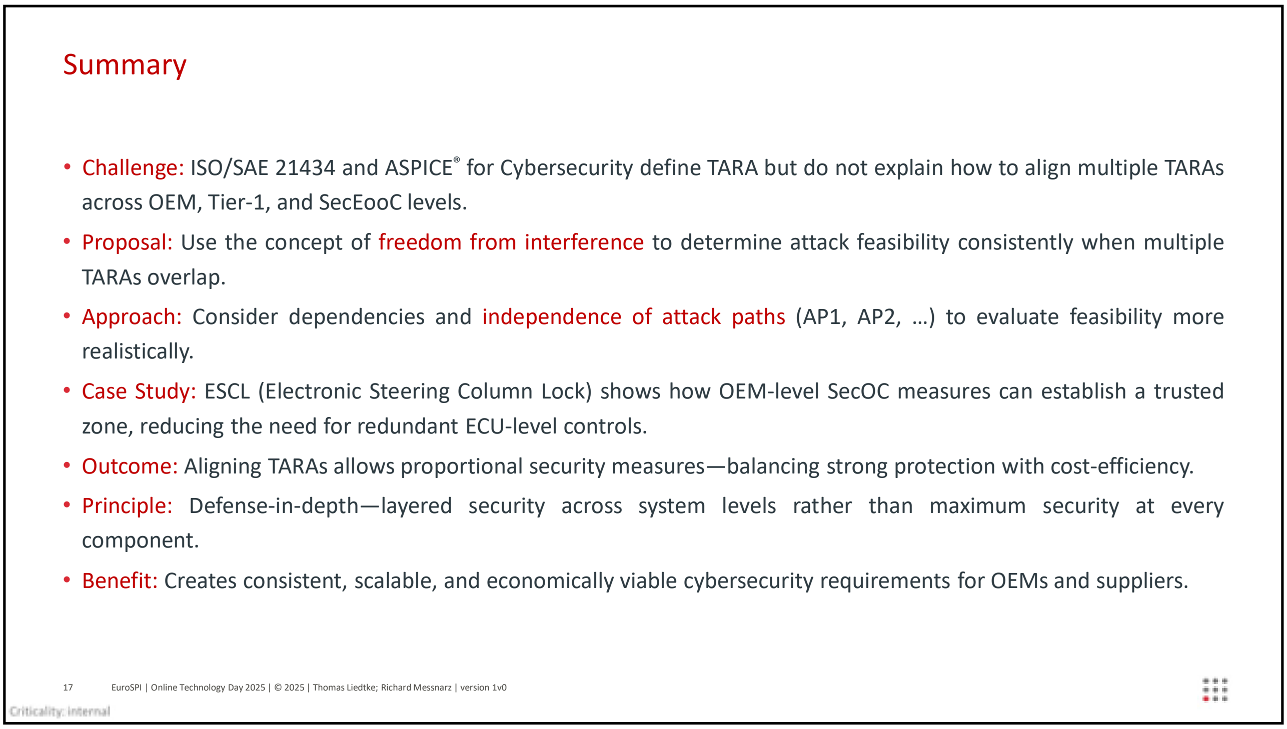
Defense-in-depth in the middle ages

Outlook

Balance between security efforts and associated costs

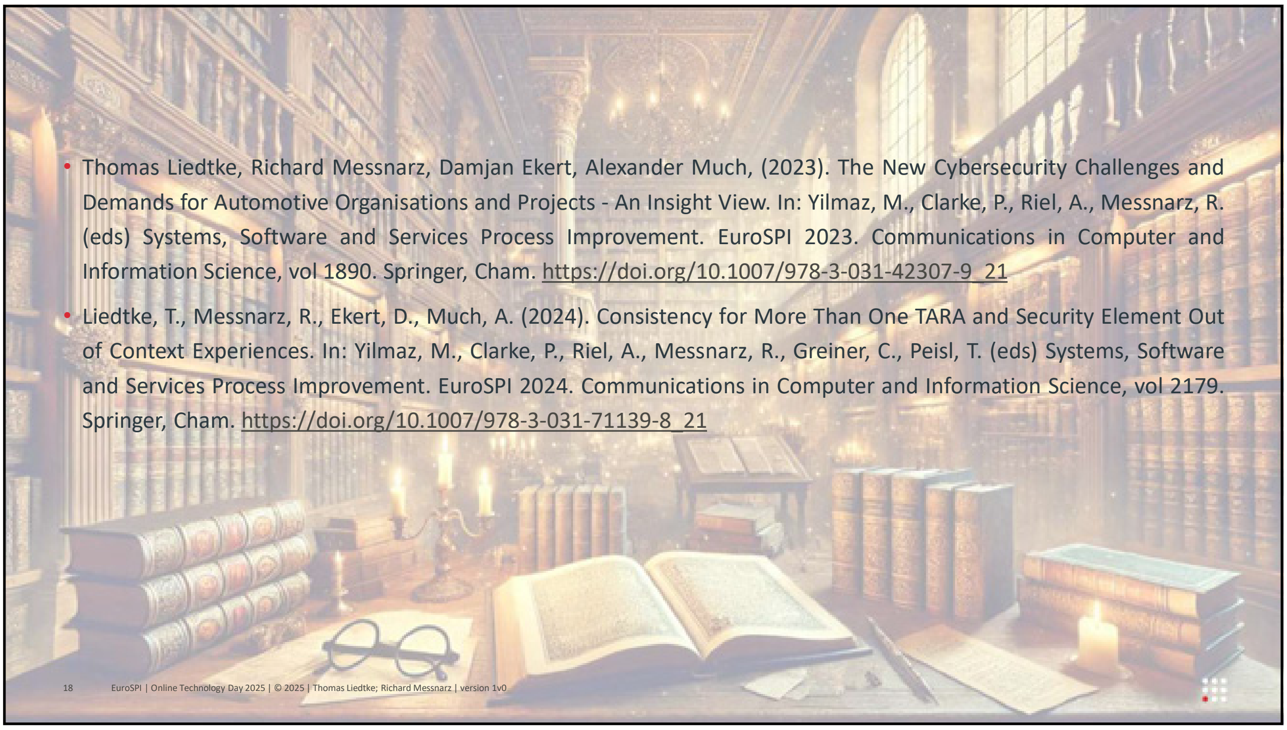
- The principle outlined above can be applied to define appropriate security requirements for suppliers, ensuring a proportionate balance between security efforts and associated costs:
- **Overestimating Security Requirements:**
  - Demanding an excessively high level of security (e.g., a very low attack feasibility) may result in disproportionate effort and costs without significantly enhancing the overall security level.
- **Underestimating Security Requirements:**
  - Conversely, requiring a security level that is too low may lead to an insecure product, exposing it to unacceptable risks.





Summary

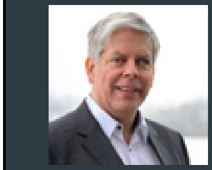
- Challenge: ISO/SAE 21434 and ASPICE® for Cybersecurity define TARA but do not explain how to align multiple TARAs across OEM, Tier-1, and SecEooC levels.
- Proposal: Use the concept of freedom from interference to determine attack feasibility consistently when multiple TARAs overlap.
- Approach: Consider dependencies and independence of attack paths (AP1, AP2, …) to evaluate feasibility more realistically.
- Case Study: ESCL (Electronic Steering Column Lock) shows how OEM-level SecOC measures can establish a trusted zone, reducing the need for redundant ECU-level controls.
- Outcome: Aligning TARAs allows proportional security measures—balancing strong protection with cost-efficiency.
- Principle: Defense-in-depth—layered security across system levels rather than maximum security at every component.
- Benefit: Creates consistent, scalable, and economically viable cybersecurity requirements for OEMs and suppliers.

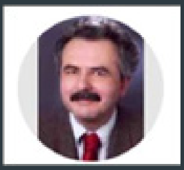


- Thomas Liedtke, Richard Messnarz, Damjan Ekert, Alexander Much, (2023). The New Cybersecurity Challenges and Demands for Automotive Organisations and Projects - An Insight View. In: Yilmaz, M., Clarke, P., Riel, A., Messnarz, R. (eds) Systems, Software and Services Process Improvement. EuroSPI 2023. Communications in Computer and Information Science, vol 1890. Springer, Cham. https://doi.org/10.1007/978-3-031-42307-9_21
- Liedtke, T., Messnarz, R., Ekert, D., Much, A. (2024). Consistency for More Than One TARA and Security Element Out of Context Experiences. In: Yilmaz, M., Clarke, P., Riel, A., Messnarz, R., Greiner, C., Peisl, T. (eds) Systems, Software and Services Process Improvement. EuroSPI 2024. Communications in Computer and Information Science, vol 2179. Springer, Cham. https://doi.org/10.1007/978-3-031-71139-8_21

19 EuroSPI | Online Technology Day 2025 | © 2025 | Thomas Liedtke; Richard Messnarz | version 1v0

Your Contact





SYNSPACE
experts in excellence

Thomas Liedtke (PhD)
Principal

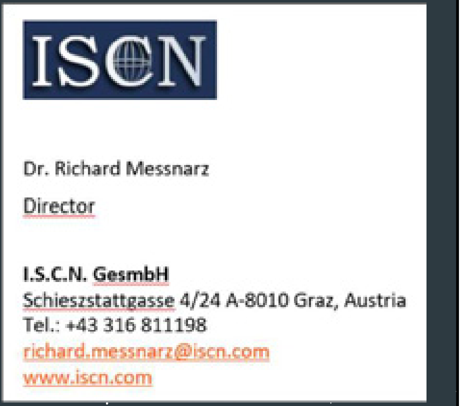
Mobil:	**+49 173 676 40 93**
E-Mail:	**thomas.liedtke@synspace.com**
Web:	**synspace.com**
LinkedIn:	**linkedin.com/in/thomas-liedtke-72a86b4a/**

Headquarter

SynSpace Group GmbH
Basler Landstr. 8
79111 Freiburg
Germany

Branch office

SynSpace Group GmbH
Birsigstr. 2
4054 Basel
Schweiz



ISCN

Dr. Richard Messnarz

Director

I.S.C.N. GesmbH
Schieszstattgasse 4/24 A-8010 Graz, Austria
Tel.: +43 316 811198
richard.messnarz@iscn.com
www.iscn.com