



Consistency for
more than one
TARA - new content
of **Automotive**
SPICE for
Cybersecurity



European System, Software &
Service Process Improvement
& Innovation

In cooperation with initiatives
in Asia, Africa and USA

Online Technology Day

6th of September 2024

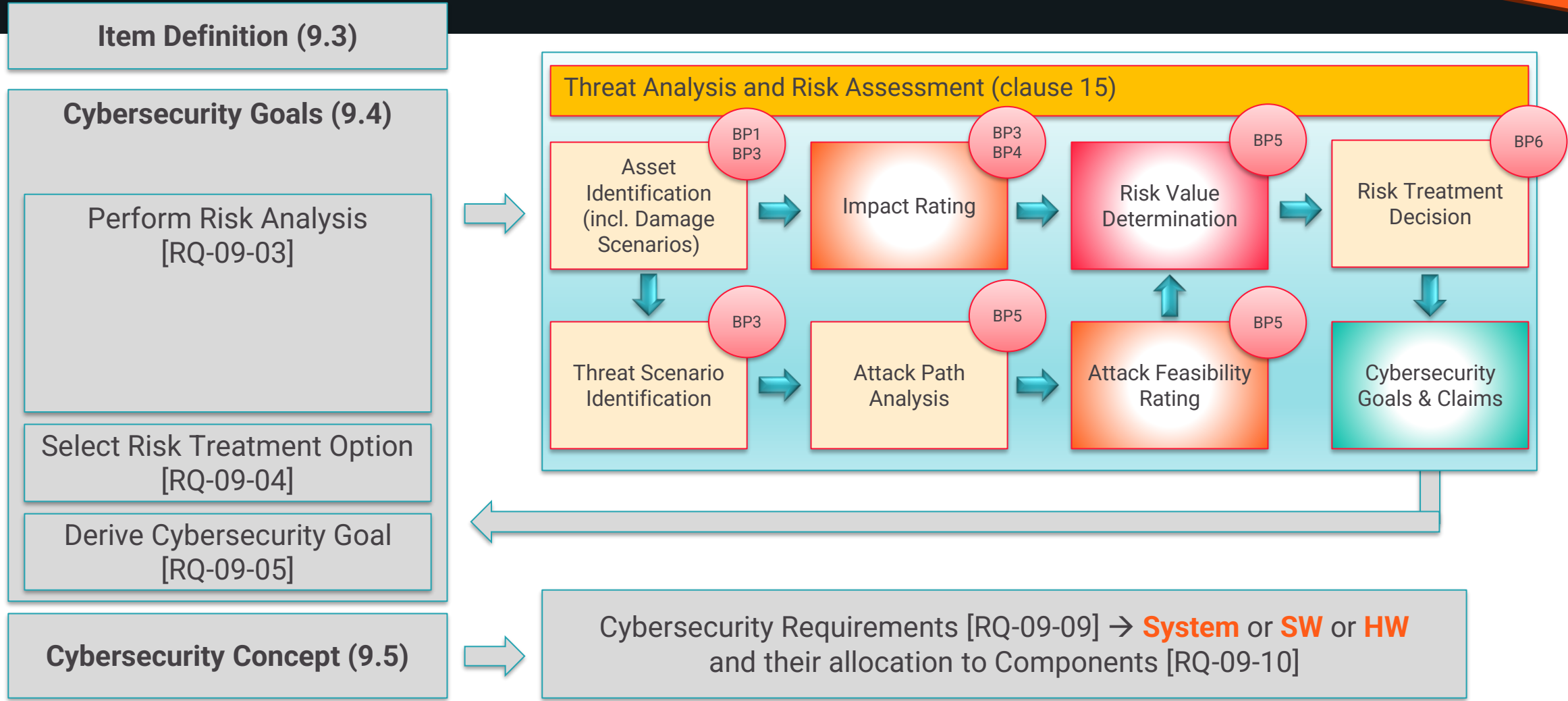
Thomas Liedtke (PhD)

Dr. Richard Messnarz



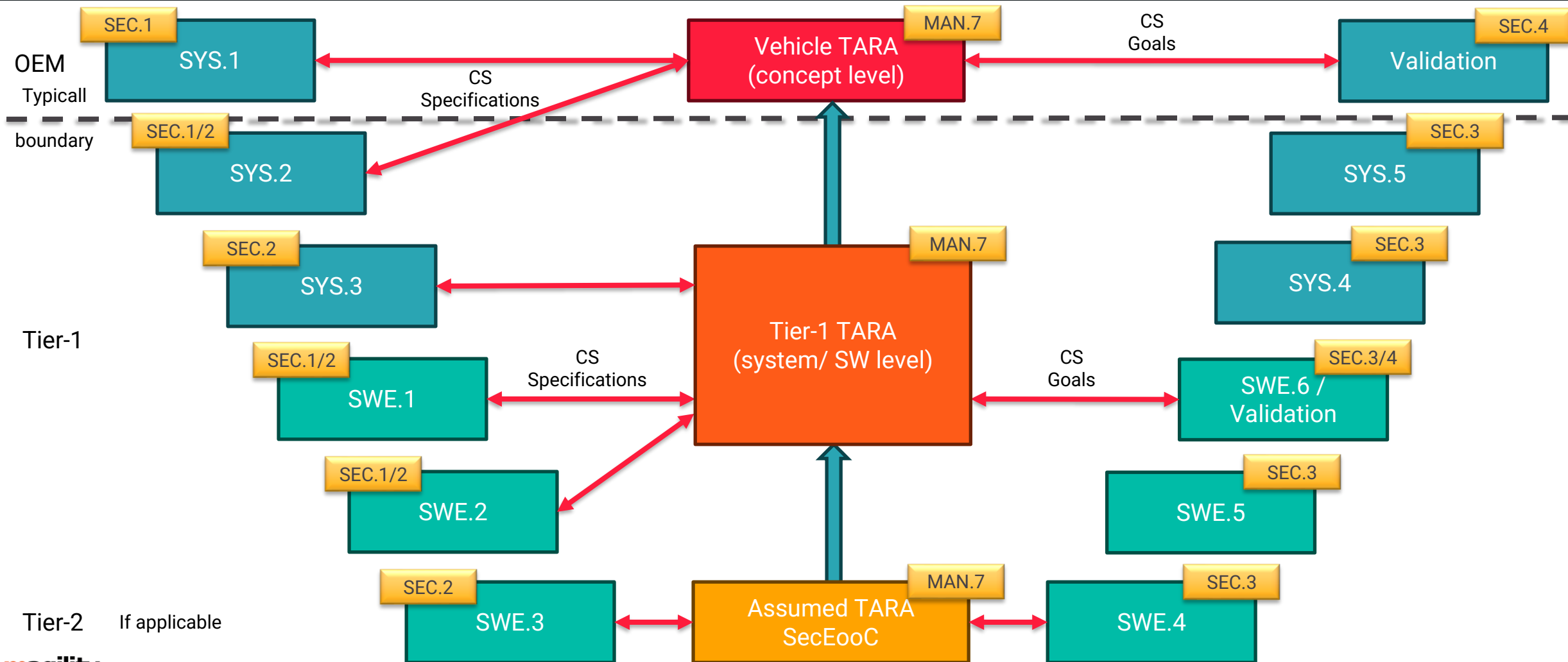
ISO/SAE 21434-clause 15: Threat analysis and risk assessment – Mapping to Automotive SPICE® MAN.7-BPs

Introduction and Items at Different Level



TARA looks at the same cybersecurity item at different levels of detail

Introduction and Items at Different Level



Identification of Damage Scenario and Impact (System Level; Tier-1)

Tier 1 level architectural TARA

asset	cybersecurity property	adverse consequence (damage szenario for road user)	impact rating (S, F, O, P)				justification
			safety	financial	operability	privacy	
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 inconvenience due to unexpected locking of the steering column while driving caused by a spoofed (valid) message	severe	severe	severe	negligible	S: assumed scenario: severe accident on a highway F: total loss of the vehicle O: vehicle cannot be used anymore P: no personal data affected
	integrity	physical inconvenience due to unexpected locking (motor moves a bolt to a locking position without intended lock command) of the steering column while driving caused by a tampered function (implementation)	severe	severe	severe	negligible	
	non-repudiation	physical inconvenience due to unexpected locking while driving caused by a re-played (authenticated and "valid") message	severe	severe	severe	negligible	
	confidentiality	not applicable: no impact on road user seen if any information of function (implementation) is disclosed					
	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	negligible	moderate	negligible	negligible	F: cost for repair moderate O: vehicle cannot be protected from theft
	authorization	not applicable: no authorization of lock command implemented, no role concept realized					

Identification of Damage Scenario and Impact (System Level; Tier-1)

Tier 1 level architectural TARA

asset	cybersecurity property	adverse consequence (damage scenario for road user)	impact rating (S, F, O, P)				justification
			safety	financial	operability	privacy	
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 inconvenience due to unexpected locking of the steering column while driving caused by a spoofed (valid) message	severe	severe	severe	negligible	S: assumed scenario: severe accident on a highway F: total loss of the vehicle O: vehicle cannot be used anymore P: no personal data affected
	integrity	physical inconvenience due to unexpected locking (motor moves a bolt to a locking position without intended lock command) of the steering column while driving caused by a tampered function (implementation)	severe	severe	severe	negligible	
	non-repudiation	physical inconvenience due to unexpected locking while driving caused by a re-played (authenticated and "valid") message	severe	severe	severe	negligible	
	confidentiality	not applicable: no impact on road user seen if any information of function (implementation) is disclosed					
	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	negligible	moderate	negligible	negligible	F: cost for repair moderate O: vehicle cannot be protected from theft
	authorization	not applicable: no authorization of lock command implemented, no role concept realized					

Derivation of Cybersecurity Requirements

Tier 1 level architectural TARA

impact rating (S, F, O, P)				threat scenario	attack path analysis	Total Value	Attack feasibility value	Risk value			
safety	financial	operability	privacy					safety	financial	operability	privacy
severe	severe	severe	negligible	Spoofer lock command , lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	15	Medium	4	4	4	1
severe	severe	severe	negligible	Tampered function (e.g., via SW or configuration data), lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	42	Very low	2	2	2	1
severe	severe	severe	negligible	Replayed lock command , lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	5	High	5	5	5	1
negligible	moderate	negligible	negligible	Denial of function , lead to not moving the bolt at a locking position	attacker action 1 attacker action 2 ...	1	High	1	3	1	1

Derivation of Cybersecurity Requirements

Tier 1 level architectural TARA

Cybersecurity Goal

impact rating (S, F, O, P)				threat scenario	attack path analysis	Total Value	Attack feasibility value	Risk value			
safety	financial	operability	privacy					safety	financial	operability	privacy
severe	severe	severe	negligible	Spoofted lock command , lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	15	Medium	4	4	4	1
severe	severe	severe	negligible	Tampered function (e.g., via SW or configuration data), lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	42	Very low	2	2	2	1
severe	severe	severe	negligible	Replayed lock command , lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	5	High	5	5	5	1
negligible	moderate	negligible	negligible	Denial of function , lead to not moving the bolt at a locking position	attacker action 1 attacker action 2 ...	1	High	1	3	1	1



Risk treatment	Cybersecurity Goal (negative passive)/ Cybersecurity Claim	Cybersecurity Control (general principle to be selected)	Cybersecurity Requiements (specific)
reduce	CS G1: Steering lock shall not react/work triggered by a malicious/ spoofted lock command	Message / command Authentication	RQ 1: The lock command shall be authenticated using a Message Authentication Code (MAC)
reduce	CS G2: Steering lock shall not react/work triggered by a tampered lock command	Message / command Encryption (SecOC)	RQ 2: The lock command shall encrypted (symmetric encryption: AES-128)
reduce	CS G3: Steering lock shall not react/work triggered by a replayed lock command	Message / command Authentication (MAC) and time stamp	RQ 3: The lock command shall include a freshness counter to avoid replay attacks
n.a.			
transfer	CS C1: supplier cannot avoid flooding of communication channels by themselves	n.a.	n.a.
n.a.			

Cybersecurity Claim

Derivation of Cybersecurity Requirements

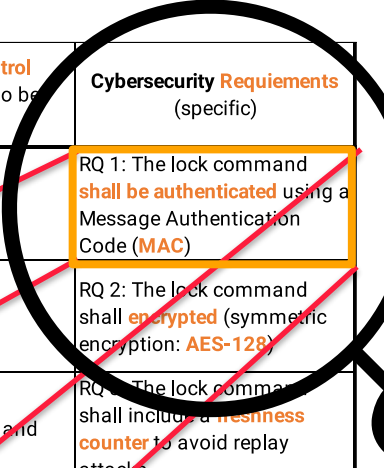
Tier 1 level architectural TARA

impact rating (S, F, O, P)				threat scenario	attack path analysis	Total Value	Attack feasibility value	Risk value			
safety	financial	operability	privacy					safety	financial	operability	privacy
severe	severe	severe	negligible	Spoofted lock command , lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	15	Medium	4	4	4	1
severe	severe	severe	negligible	Tampered function (e.g., via SW or configuration data), lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	42	Very low	2	2	2	1
severe	severe	severe	negligible	Replayed lock command , lead to moving the bolt at a locking position at unintended time	attacker action 1 attacker action 2 ...	5	High	5	5	5	1
negligible	moderate	negligible	negligible	Denial of function , lead to not moving the bolt at a locking position	attacker action 1 attacker action 2 ...	1	High	1	3	1	



Risk treatment	Cybersecurity Goal (negative passive)/ Cybersecurity Claim	Cybersecurity Control (general principle to be selected)	Cybersecurity Requiements (specific)
reduce	CS G1: Steering lock shall not react/work triggered by a malicious/ spoofted lock command	Message / command Authentication	RQ 1: The lock command shall be authenticated using a Message Authentication Code (MAC)
reduce	CS G2: Steering lock shall not react/work triggered by a tampered lock command	Message / command Encryption (SecOC)	RQ 2: The lock command shall encrypted (symmetric encryption: AES-128)
reduce	CS G3: Steering lock shall not react/work triggered by a replayed lock command	Message / command Authentication (MAC) and time stamp	RQ 3: The lock command shall include a freshness counter to avoid replay attacks
n.a.			
n.a.			n.a.
n.a.			

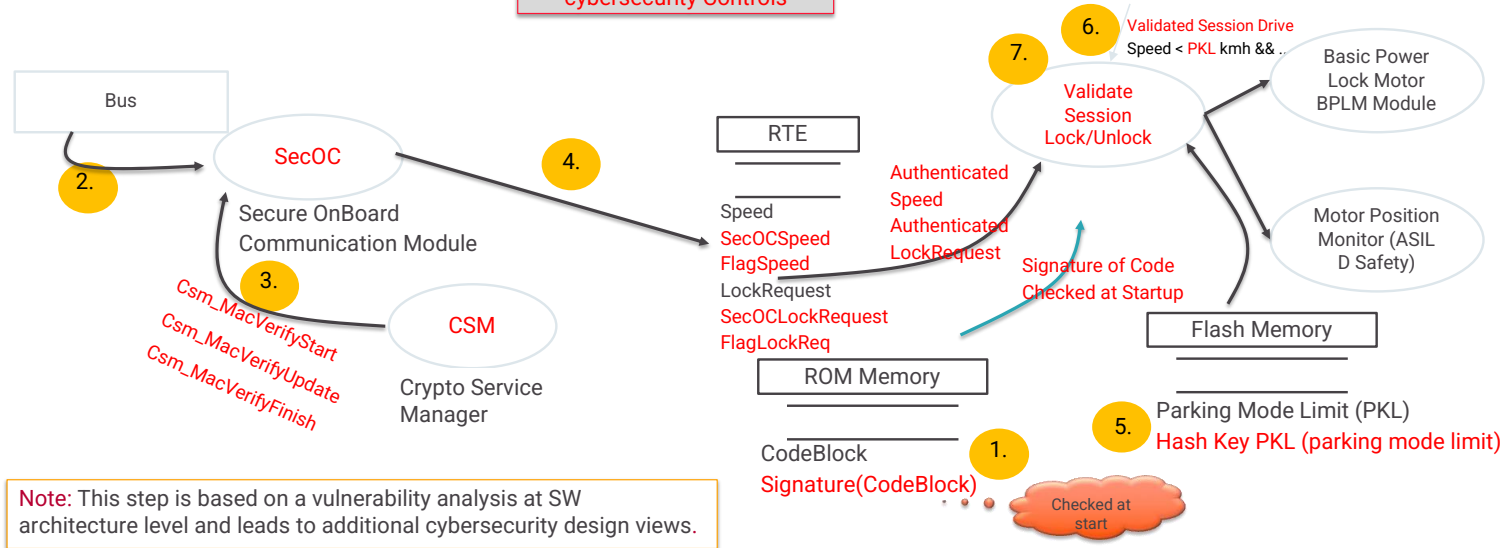
RQ 1: "The lock command shall be authenticated using a Message Authentication Code (MAC)."



Specification of Software Requirements

Tier 1 level architectural TARA

Red letters: Added cybersecurity Controls




Note: This step is based on a vulnerability analysis at SW architecture level and leads to additional cybersecurity design views.

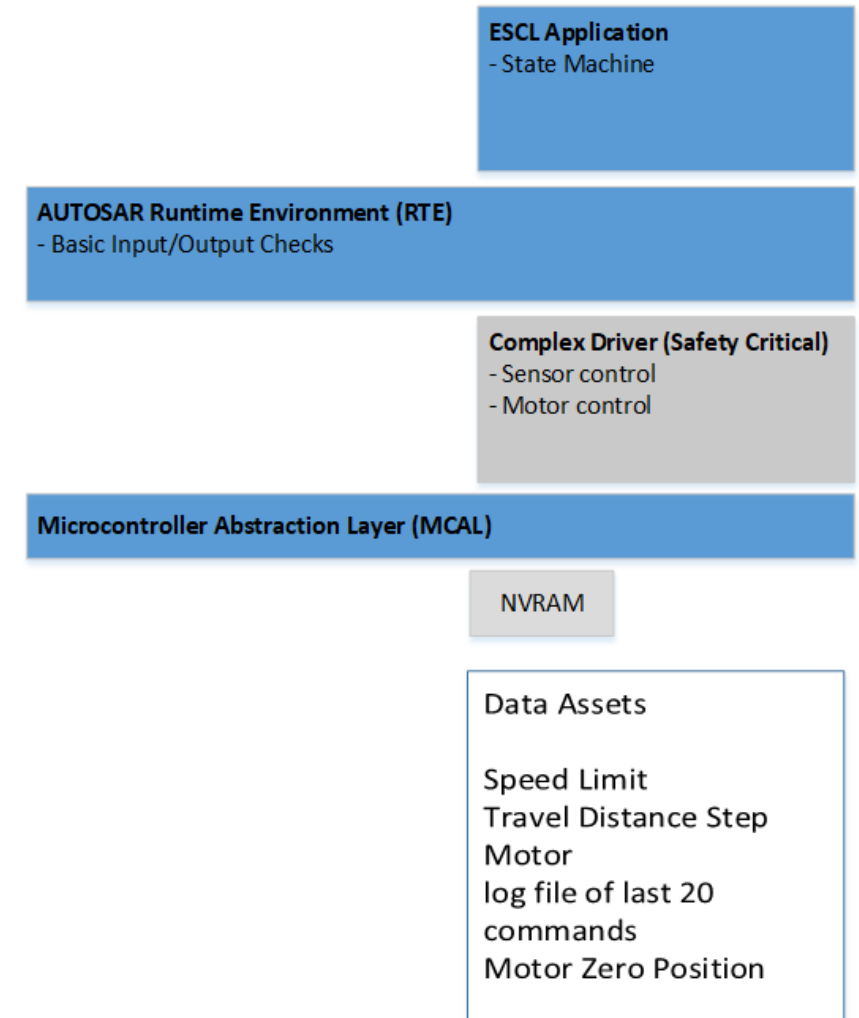
IF (speedlimit parameter **valid** && speed **valid** && LockRequest **valid**) && (speed < speedlimit) THEN call BPLM::Mlock

Cybersecurity Control in SW Architecture	Software Component	Software Cybersecurity Requirements for SW Implementation
		IF (speedlimit parameter valid && speed valid && LockRequest valid) && (speed < speedlimit) THEN call BPLM::Mlock
Authenticate Speed and Lock/Unlock Request and Validate the Lock and Unlock Session	SessionVAL_LockUnlock.c	IF (speedlimit parameter invalid speed invalid LockRequest invalid) THEN call BPLM::SafeState
	SecOC.c	IF (speed > speedlimit && LockRequest valid) THEN call BPLM::SafeState
		Configure Autosar SecOC and assign the AES-256 algorithm to the MAC (Message Authentication Code)

Software Module Level SecEooC (Security Element out of Context) concept

Software Module Level SecEooC concept

- Tier 1 can outsource SW libraries and specific functions to third party suppliers.
- Example boundaries at SecEooC level 
 - ESCL state manager
 - Complex device driver (CDD) for the motor control as a software function. (lib)
 - If contributed by a third party a vulnerability analysis at module level is necessary.
 - → **separate TARA** or **enter the results** of the vulnerability analysis **to the Tier 1 TARA**
- Example: **processor** with the MCAL SW (Microcontroller Controller Abstraction Layer).
 - Comes with an **integration manual**: guidance about assumed assets, attack vectors, threat types, already built in and configuration guide for security controls, operational environment, and **assumptions of use and configuration**.





Dr. Thomas Liedtke

Senior Cyber Security Expert

Magility Cyber Security GmbH

Heinrich-Otto-Str 71 | Wendlingen am Neckar

Tel.: +49 173-676-4093

thomas.liedtke@magility-mcs.com

www.magility-mcs.com



Dr. Richard Messnarz

Director

I.S.C.N. GesmbH

Schiezstattgasse 4/24 A-8010 Graz, Austria

Tel.: +43 316 811198

richard.messnarz@iscn.com

www.iscn.com



A modern office interior with glass walls, desks, and computers. The office is bright and spacious, with large windows and a clean, minimalist design. The floor is a light-colored wood or laminate, and the ceiling has recessed lighting. The overall atmosphere is professional and contemporary.

Your contact to magility cyber security

Magility Cyber Security GmbH | Heinrich-Otto-Str. 71 |
73240 Wendlingen am Neckar | Germany

+49 177 698 2021 | contact@magility-mcs.com | www.magility-mcs.com

Disclaimer

Magility Cyber Security GmbH

Liability for contents

As a service provider, we are responsible for our own content on these pages in accordance with § 7 Para. 1 of the German Telemedia Act (TMG). However, according to §§ 8 to 10 TMG, we are not obliged as a service provider to monitor transmitted or stored third-party information or to investigate circumstances that indicate illegal activity. Obligations to remove or block the use of information in accordance with general laws remain unaffected by this. However, liability in this regard is only possible from the point in time at which a concrete infringement of the law becomes known. If we become aware of any such infringements, we will remove the relevant content immediately.

Although the greatest possible care has been taken in the preparation of this presentation, we cannot accept any liability for the completeness, up-to-dateness or correctness of the information contained therein. The information in this documentation is provided for information purposes only and should not be construed as an offer or public advertisement soliciting the use of services.

Liability for any damage or loss claimed on the basis of the information contained in this documentation is excluded.

Liability for links

If there are links to external websites in our presentation, we have no influence on their contents. We do not assume any liability for external contents. The responsibility for the contents of linked pages always lies with the respective provider and operator of the pages. Constant monitoring of the content of linked pages is not reasonable as long as there are no concrete indications of a violation of the law. If such become known, we will remove such links immediately.

Copyright

The contents and works created by Magility Cyber Security on these pages are subject to German copyright law. Duplication, processing, distribution and any kind of exploitation outside the limits of copyright law require the written consent of the respective author or creator. Downloads and copies of this site are only permitted for private, non-commercial use.

Insofar as the contents of this site were not created by the operator, the copyrights of third parties are respected. In particular, third-party content is marked as such. Should you nevertheless become aware of a copyright infringement, please inform us accordingly. If we become aware of any infringements, we will remove such content immediately.

No part of the content of this document may be used for other purposes, distributed to persons or companies outside the receiving company or reproduced, edited or disseminated in any other way without the prior express written permission of Magility Cyber Security. The text and graphics obtained in the presentation are for illustrative and reference purposes only.

This document, all information relating to this document and any attachment to this document are confidential and proprietary to Magility Cyber Security GmbH. All contents of this document are copyright ©Magility Cyber Security GmbH. All rights reserved.

Managing Director: Dino Munk | Magility Cyber Security GmbH | European Metropolitan Region Stuttgart
Heinrich-Otto-Str. 71 | 73240 Wendlingen am Neckar | Germany
E-Mail: dino.munk@magility.com | Tel. +49 177 698 2021
Stuttgart | HRB-Nummer 78 4630
www.magility-mcs.com



magility
together. cyber. secure.