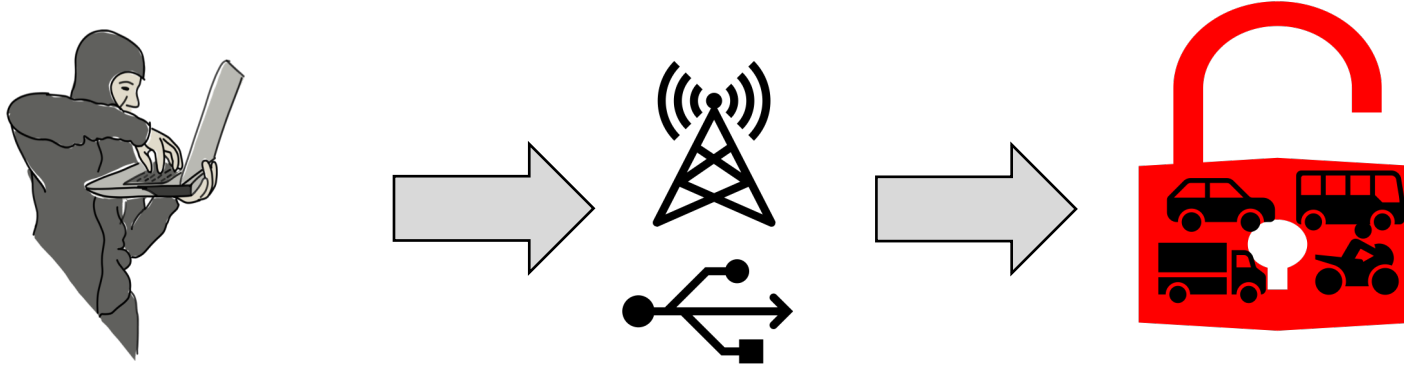


Automotive SPICE for Cybersecurity

(May 2021)

Achim Hoenow

Motivation



What do you expect from your government?

1. Car manufacturer must do cyber security preventions
2. In case of a cyber security incident (can be a safety issue)
 - a) You get a fix very soon from car manufacturer
 - b) You can return your car and get your money back

Automotive SPICE for Cybersecurity

Agenda



- 1 Cyber Security and Car Homologation**
- 2 Cyber Security SPICE – Top Level Architecture**
- 3 Executing Cyber Security SPICE Assessment**
- 4 Supply Chain**
- 5 Summary**

Cyber Security and Car Homologation Situation



UN ECE Press Release June 24th, 2020: [\(Link\)](#)

The two new UN Regulations, adopted by UNECE's World Forum for Harmonization of Vehicle Regulations, require that measures be implemented across 4 distinct disciplines:

1. Managing **vehicle cyber risks**
2. Securing vehicles by design to mitigate risks **along the value chain**;
3. Detecting and responding to **security incidents** across vehicle fleet;
4. Providing **safe and secure software updates** and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "Over-the-Air" (O.T.A.) updates to on-board vehicle software.

The regulations will apply to passenger cars, vans, trucks and buses. They will enter into force in January 2021.

All of these will be audited by national technical services or homologation authorities.

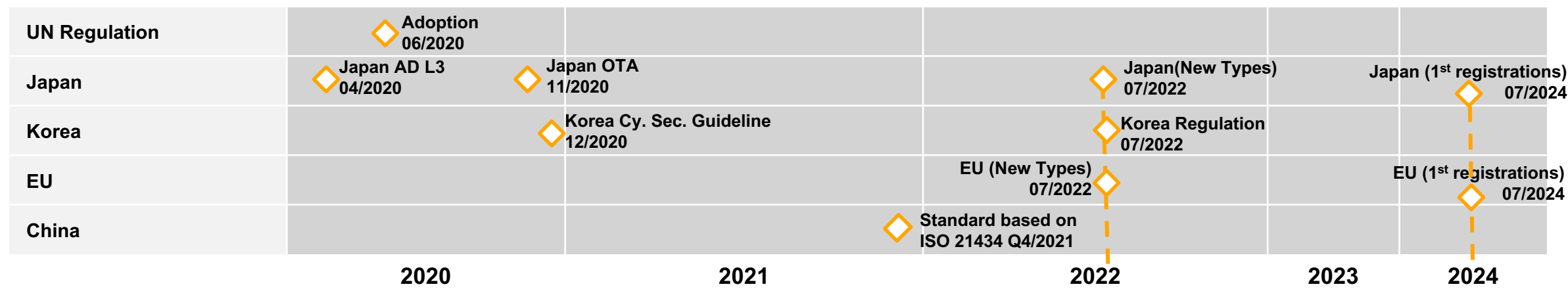
Cyber Security and Car Homologation Situation



***Japan** has indicated that it plans to apply these regulations upon entry into force.*

*The **Republic of Korea** has adopted a stepwise approach, introducing the provisions of the regulation on Cybersecurity in a national guideline in the second half of 2020, and proceeding with the implementation of the regulation in a second step.*



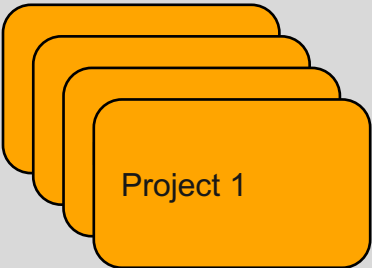

*In the **European Union**, the new regulation on cyber security will be mandatory for all new vehicle types from **July 2022** and will become mandatory for all new vehicles produced from **July 2024**.*



Cyber Security and Car Homologation

UN ECE and International Standards



Homologation approval		Standards	Status
Audit (organization)  CSMS- Corporate wide measurement and management of Cybersecurity  Company CSMS certificate		Homologation: UN ECE adoption agreement based in ISO 21434	released
		ISO Standard: ISO 21434 Cybersecurity Final Draft since Q1/2020	delayed release Q3 / 2021
Assessment (project)  Project 1  Automotive Cyber Security SPICE Assessment		Audit: VDA Cybersecurity Management System - Red Band November 2020	released
		Audit: International standard ISO PAS 5112	Draft: 03/2021 Public: 07/2021
		Assessment: Automotive Cybersecurity SPICE Assessment	Draft: released Release: 07/2021

Cyber Security and Car Homologation

UN ECE and International Standards



Homologation approval

Audit (organization)

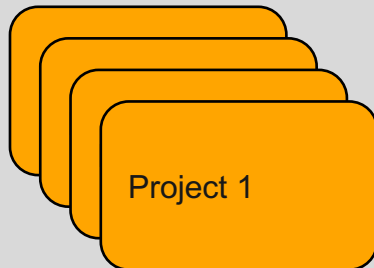
CSMS- **Corporate** wide
measurement and
management of
Cybersecurity



Passed Cyber Security Management System certification

- Supplier **certification done by certification bodies**

Assessment (project)



Passed Automotive **Cyber Security Assessment**

- Automotive **SPICE Assessment for non cyber security** project part (VDA Scope)
- Automotive **SPICE Assessment of cyber security** part (SEC Scope)

Cyber Security SPICE – Top Level Architecture

Basic requirements for Cyber Security SPICE



- Add on to Automotive SPICE assessment
- Must be executed in < 2,5 days if VDA Scope assessment has been done already
 - ideal for cyber security upgrades of legacy products
- Traceability to ISO 21434
 - Process related requirements of ISO 21434 are covered by ACSMS audit and ASPICE for cyber security
- Guidance for a homologation relevant rating (passed, not passed) on basis of a capability profile

Cyber Security SPICE – Top Level Architecture

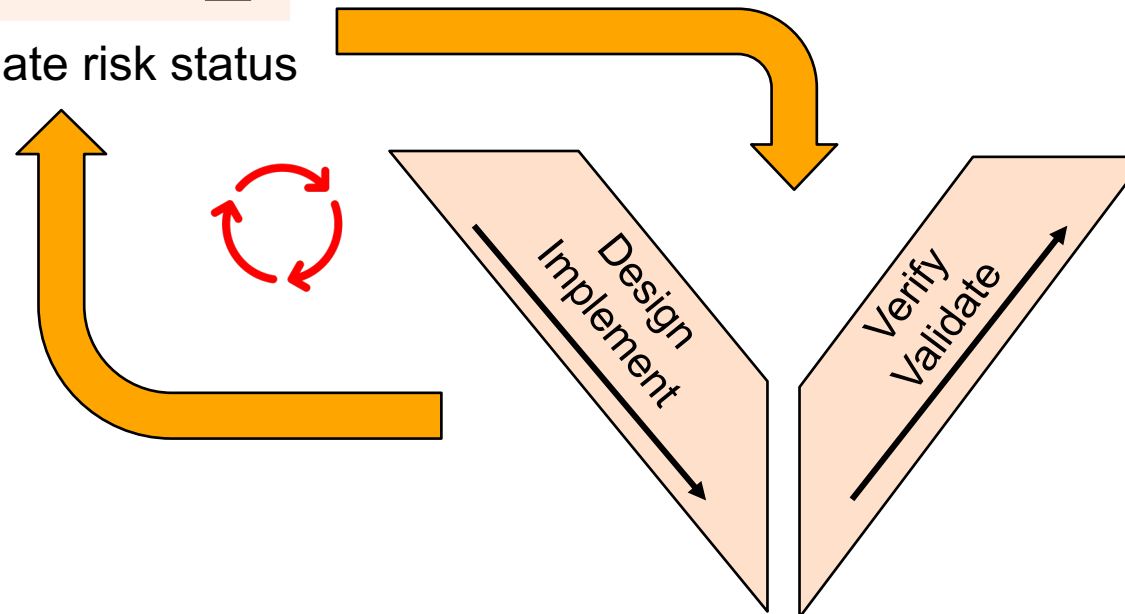
Managing cyber security risks

Cyber Security Risk Management	Risk Treatment
Security compliant process for risk assessment Relevant risk assessment practices may be included from established standards covering practices such as FMEA, TARA, HARA.	Accept ✓
	Avoid <input type="checkbox"/>
	Reduce <input type="checkbox"/>

- (1) Update functionality, implement new features
(2) Plan and execute additional cyber security tests

(3) Re-evaluate risk status

(4) No “higher” cyber security risk:
Release ✓



Cyber Security SPICE – Top Level Architecture

Managing cyber security risks



MAN.7 Risk Management

**Cyber Security
Engineering Processes
(SEC)**

SEC.1 Cyber Security
Requirements Elicitation

SEC.4 Risk Treatment
Validation

SEC.2 Cyber Security
Implementation

SEC.3 Risk Treatment
Verification

ACQ.2 Supplier Request
and Selection

ACQ.4 Supplier
Monitoring

Executing Cyber Security SPICE Assessment

Scoping

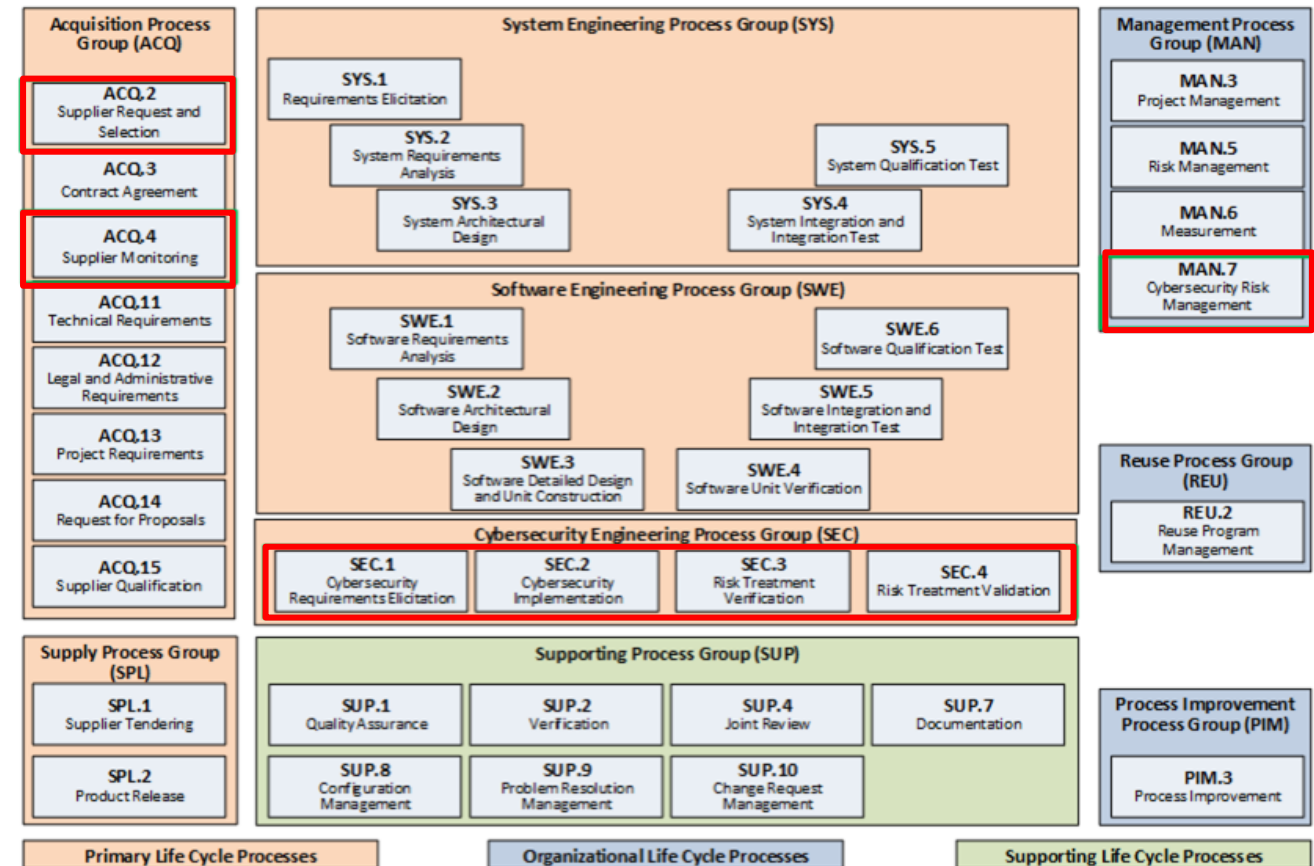


Assessment Purpose:

- Cyber Security Capability Determination

Processes:

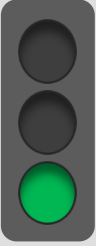
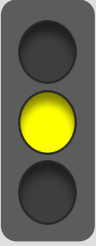
- VDA Scope for non cy. security project part
- SEC Scope for cy. security project part
- ACQ.2 and ACQ.4 if cy. security relevant components are purchased



Source: Yellow Volume VDA Automotive SPICE® for Cybersecurity

Executing Cyber Security SPICE Assessment Rating



 Passed	VDA Scope	Level	MAN.3	SUP.1	SUP.8	SUP.9	SUP.10	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6
		PA1.1	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
		PA2.1	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		PA2.2	NA	NA	NA	L	L	L	L	L	L	L	L	L	L	L	L
	SEC Scope	Level	MAN.7	SEC.1	SEC.2	SEC.3	SEC.4	ACQ.2	ACQ.4								
		PA1.1	F	F	F	F	F	F	F								
		PA2.1	NA	NA	NA	NA	NA	NA	NA								
		PA2.2	L	L	L	L	L	NA	NA								
 Passed with conditions	VDA Scope	Level	MAN.3	SUP.1	SUP.8	SUP.9	SUP.10	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6
		PA1.1	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
		PA2.1	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		PA2.2	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
	SEC Scope	Level	MAN.7	SEC.1	SEC.2	SEC.3	SEC.4	ACQ.2	ACQ.4	“Improvement measures are agreed between lead assessor and assessed organization at the end of the assessment to close the corresponding gaps within an appropriate time frame.” <i>Source: Yellow Volume VDA Automotive SPICE® for Cybersecurity</i>							
		PA1.1	L	L	L	L	L	L	L								
		PA2.1	NA	NA	NA	NA	NA	NA	NA								
		PA2.2	L	L	L	L	L	NA	NA								

Supply Chain

Cyber Security relevant Components



Supply Chain	Products
OEM	Car, OTA Updates, Web-Services, etc.
TIER1	ECU, Software, Hardware, Web-Services, etc.
TIER2-N	Active Components and their Firmware: Microcontroller, Memory, Sensors, ASICS, Switching Devices, Modules, Radio Semiconductors, etc. Software: Hardware Related Software, Basic Software, Application Software

Summary

Motivation

Cyber Security SPICE – Top Level Architecture

Managing Cyber Security

Executing Cyber Security SPICE Assessment

Scoping

Assessment

- Cyber

Processes

- VDA S
- SEC S
- ACQ.2
- compo

(4) No "H
Rele

Executing Cyber Security SPICE Assessment

Rating

	VDA Scope	Level	MAN.3	SUP.1	SUP.8	SUP.9	SUP.10	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6
		PA1.1	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
		PA2.1	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		PA2.2	NA	NA	NA	L	L	L	L	L	L	L	L	L	L	L	L
		Level	MAN.7	SEC.1	SEC.2	SEC.3	SEC.4	ACQ.2	ACQ.4								
		PA1.1	F	F	F	F	F	F	F								
		PA2.1	NA	NA	NA	NA	NA	NA	NA								
		PA2.2	L	L	L	L	L	NA	NA								
	SEC Scope	Level	MAN.3	SUP.1	SUP.8	SUP.9	SUP.10	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6
		PA1.1	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
		PA2.1	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		PA2.2	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		Level	MAN.7	SEC.1	SEC.2	SEC.3	SEC.4	ACQ.2	ACQ.4								
		PA1.1	L	L	L	L	L	L	L								
		PA2.1	NA	NA	NA	NA	NA	NA	NA								
		PA2.2	L	L	L	L	L	NA	NA								
	VDA Scope	Level	MAN.3	SUP.1	SUP.8	SUP.9	SUP.10	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6
		PA1.1	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
		PA2.1	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		PA2.2	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		Level	MAN.7	SEC.1	SEC.2	SEC.3	SEC.4	ACQ.2	ACQ.4								
		PA1.1	L	L	L	L	L	L	L								
		PA2.1	NA	NA	NA	NA	NA	NA	NA								
		PA2.2	L	L	L	L	L	NA	NA								
	SEC Scope	Level	MAN.3	SUP.1	SUP.8	SUP.9	SUP.10	SYS.2	SYS.3	SYS.4	SYS.5	SWE.1	SWE.2	SWE.3	SWE.4	SWE.5	SWE.6
		PA1.1	L	L	L	L	L	L	L	L	L	L	L	L	L	L	L
		PA2.1	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		PA2.2	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
		Level	MAN.7	SEC.1	SEC.2	SEC.3	SEC.4	ACQ.2	ACQ.4								
		PA1.1	L	L	L	L	L	L	L								
		PA2.1	NA	NA	NA	NA	NA	NA	NA								
		PA2.2	L	L	L	L	L	NA	NA								

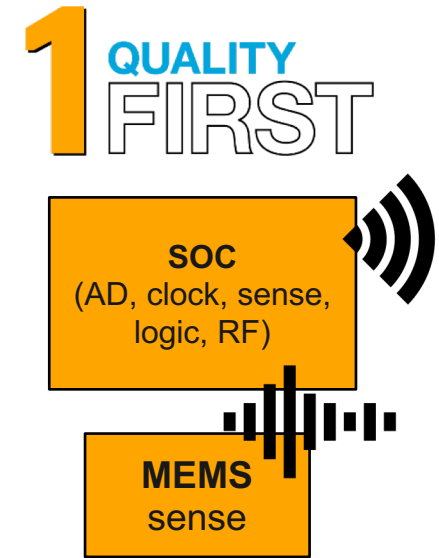
"Improvement measures are agreed between lead assessor and assessed organization at the end of the assessment to close the corresponding gaps within an appropriate time frame."

Source: Yellow Volume VDA Automotive SPICE® for Cybersecurity

Backup

Cyber Security Assessment – TPMS Example

Overview



Project: *“Make existing Tire Pressure Management Sensor Cybersecurity safe”*

SEC.1: Initial Cybersecurity Concept (at project start):

- **Threat scenario:** Receiver gets corrupted signal “wheel damage – stop immediately”
- **Cybersecurity Requirement:** Use encryption for secure transfer of TPMS signal to receiver
- **Cyber Security Release Criteria:**
 - Signal cannot be hacked, so that another sender can not send out corrupted message, receiver shall not accept wrong signal.

Cyber Security Assessment – TPMS Example

Development Steps



MAN.7 / Cyber Security Risk Management



Run Cyber Security Risk Management to identify and analyze attacks and risks:

- **Identified risks and their risk treatment implementation and verification are**
 1. High risk on corrupted/hacked signal:
 - RTI/new requirement: Build in encryption on sender and receiver
 - RTV/new requirement: Stress test on signal receiving, PEN Test, Hacking Test
 2. Low risk that crypto key can be read out of TPMS or Sender: No RTI necessary
 3. Low risk TPMS MEMS destruction
- **Update on Cybersecurity concept:** Add low risk vulnerability “Crypto key can be read out of TPMS” and TPMS MEMS destruction

Cyber Security Assessment – TPMS Example

Development Steps



SEC.2 / RTI



- **Add new system requirements:**
 - RTI/new requirement: Build in encryption on sender and receiver
 - RTV/new requirement: Stress test on signal receiving, PEN Test, Hacking Test
- Update system test criteria
- **Update System Architecture**
 - Crypto Module on sender and receiver
 - Crypto sequence between sender and receiver
- Break down system requirements to **software requirements and software architecture** and update software requirements and software architecture
- Update software test criteria
- Create/Update **Software Design**
- Create/Update **Software Code**

Cyber Security Assessment – TPMS Example

Development Steps



SEC.3 / RTV

- **Update system and software test specification**
- White box testing (unit testing, static code analysis, cybersecurity tests on module level)
- **Software integration and verification tests** including cybersecurity tests
 - Stress test on signal receiving
- System integration and validation tests **including cybersecurity tests**
 - PEN Test
 - Hacking Test