Deloitte.

SIP-Adus

Awareness training for cybersecurity of vehicles

14.11.2019

World Forum for Harmonization of Vehicle Regulations (WP.29)

Task Force on Cyber Security and OTA issues
TF CS/OTA

UNECE Cybersecurity

Resolution

Annex A: Regulation

CyberSec Engineering

Lifecycle Management

UNECE Software Update

Resolution

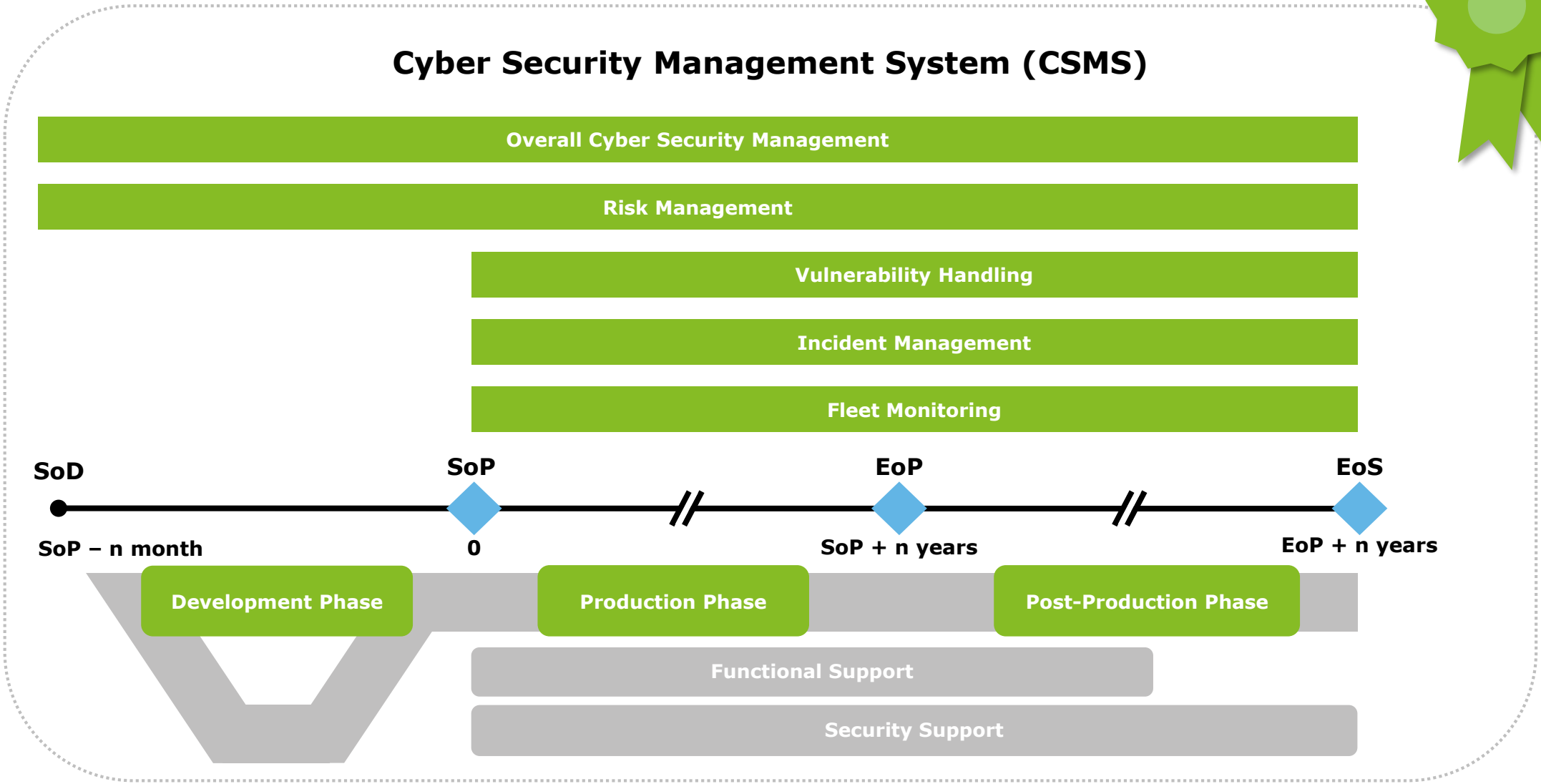
Annex A: Regulation

Annex B: Regulation

Technical Implementation

World Forum for Harmonization of Vehicle Regulations (WP.29)

Requirements for a Cyber Security Management System (CSMS)

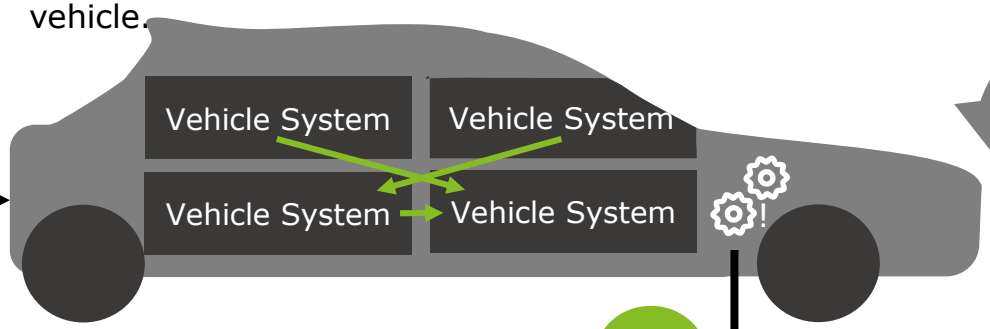


World Forum for Harmonization of Vehicle Regulations (WP.29)

Examples of requirements for a vehicle type approval

1. Implement appropriate security measures in the design of the vehicle and its systems

2. Demonstrate a risk assessment for the vehicle systems, the interactions of the different vehicle systems and the entire vehicle.

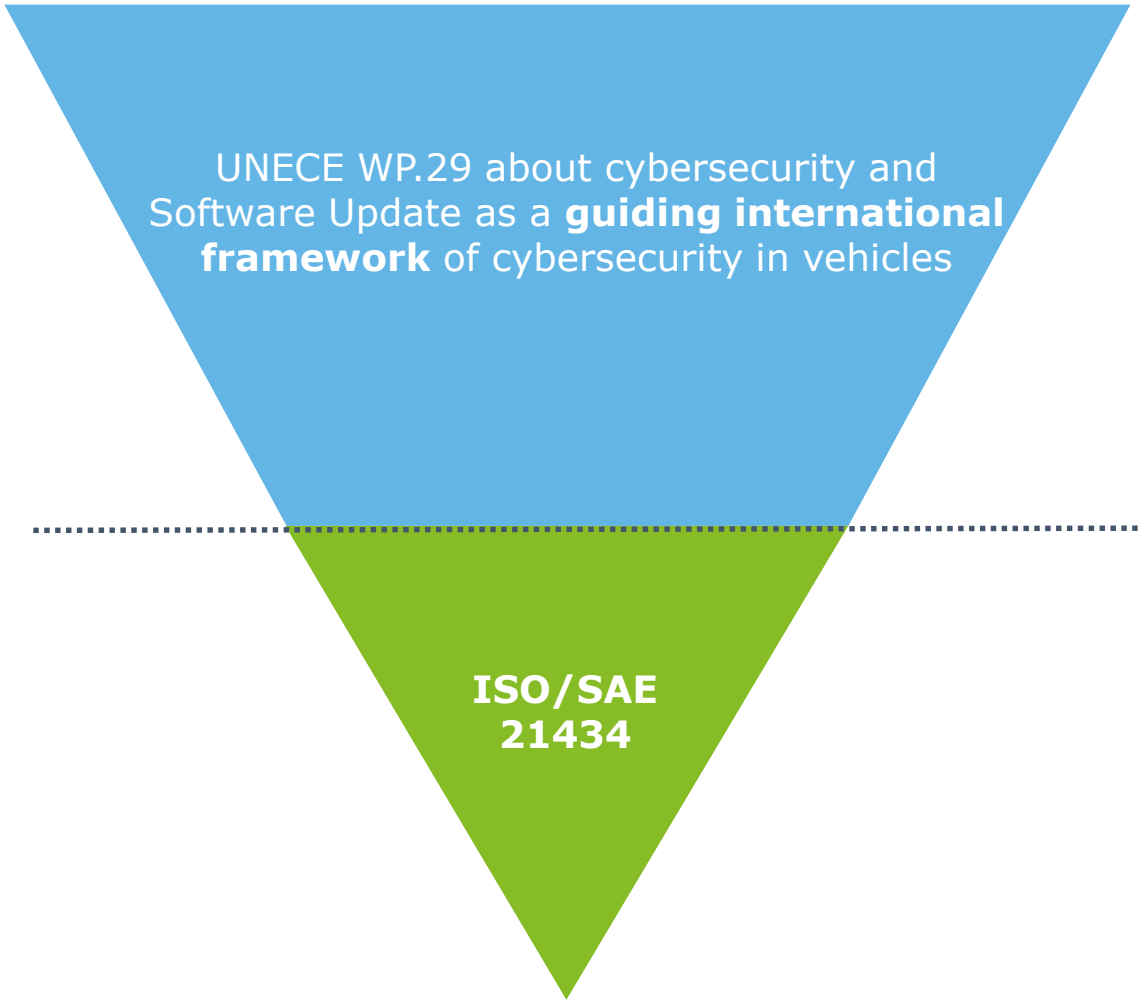


3. Verify the effectiveness of the security measures implemented and describe what testing has been performed incl. its outcome.

4. Demonstrate how risks to critical elements are assessed and mitigated.

5. Collect and verify as appropriate information required under this regulation, through the full supply chain. Maintain appropriate design and test information.

UNECE WP.29 and ISO/SAE 21434
Importance for vehicle homologation



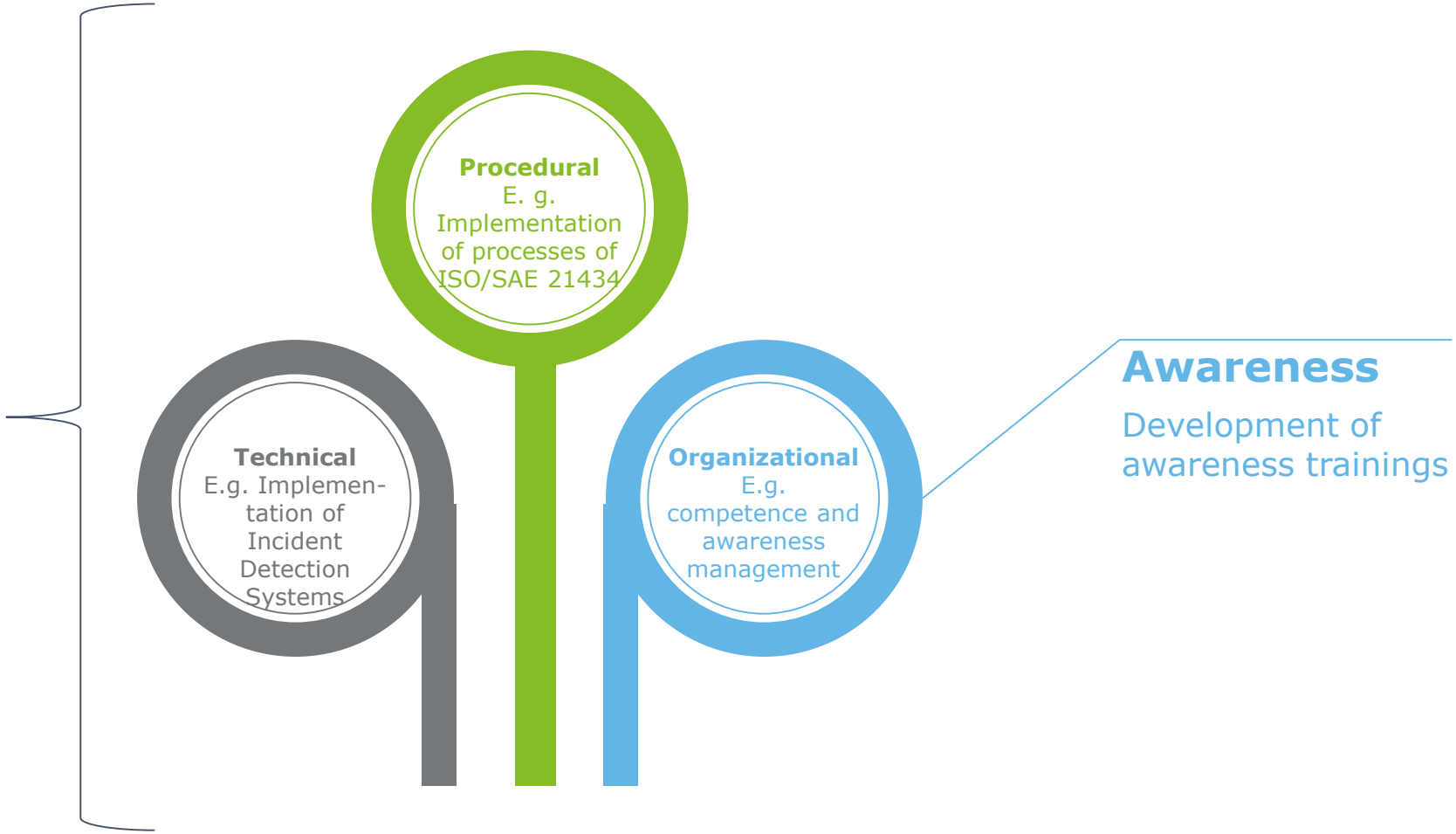
- UN Regulations are not applicable on a mandatory basis, but if a Contracting Party (C.P.) decides to apply a UN Regulation, the adoption becomes a binding act
- The Contracting Party which signed a Regulation may issue type approvals according to that Regulation and shall recognize the type approvals issued by all other Contracting Parties which signed the regulation, too.
- WP.29 provides a guiding international framework
- It does not give a detailed description how to achieve the requirements and recommendations

- Uniforms definitions of notions relevant to automotive security
- Specification of minimum requirements on cybersecurity engineering process and activities and a definition of criteria for assessment
- Description of the state of art of security engineering in automotive E/E development
- ISO/SAE 21434 describes how to achieve certain goals according to cybersecurity questions more detailed

Addressing cybersecurity

Realization of the requirements

Cybersecurity



Awareness

Development of awareness trainings

Addressing cybersecurity by raising awareness

Objectives for developing training modules

1. Rising awareness that cybersecurity can have an impact on functional safety.
2. Illustration of the type approval‘s dependence from cybersecurity.
3. Knowledge transfer of the content of the WP.29 and ISO/SAE 21434.
4. Examination whether it‘s necessary to establish new processes and procedures.
5. Examination whether it‘s necessary to establish new boards that carry out processes and procedures.
6. Prevention of possible future difficulties in communication between vehicle development employees and enterprise IT-risk management employees.

Development of 7 training modules

Addressing cybersecurity by raising awareness

Learning objectives for different stakeholder

Executive management	The executive level shall acknowledge the type approval now depending on cybersecurity.
Vehicle development	The vehicle development department shall understand the interdependence of cybersecurity, functional safety and data protection. They shall be able to adopt basic processes of information security into the vehicle development processes.
Enterprise IT-Risk Management	Enterprise IT-Risk Management shall get informed on vehicle engineering and data processing processes. They shall be able to adopt processes of information security into the vehicle development processes.
Aftersales / first level support	The aftersales department shall understand that safety relevant incidents can be caused by compromised cybersecurity.
All departments involved in vehicle cybersecurity processes	All departments involved in vehicle cybersecurity processes shall be able to realize relations of different areas of responsibilities to jointly address cybersecurity. For achieving this, they shall generate an approach of a possible structural adjustment of the organization.
All departments involved in incident management	Participants are able to apply their theoretical knowledge on vulnerability and incident handling into a simulated show case.

Training modules

1) Awareness training for the executive management

Executive management	The executive level shall acknowledge the type approval now depending on cybersecurity.

Assets and opportunities for attacks	**Required approach**	**Great topicality**	**Relevance**
Presentation of vehicle functions, interfaces and processed data in model ranges	Introduction to the methodical procedures of risk assessments	(Live-)Demonstration of a compromised vehicle	Illustration of financial impacts due to non-compliance with the WP.29 and ISO SAE 21434
For each model range: • Show vehicle functions and the way they are connected / existent interfaces • Show the processed data e. g. personal data, payment information … • Present possible attacks on interfaces, vehicle functions and scalability	• Scenario: automatic payment transaction while driving into a car park • Show how threat scenarios are developed: determination of attack path, impact rating, attack feasibility, risk assessment	• Prepare compromised vehicle in advance • Demonstrate in what ways an attack can impact vehicle functions	Explain relevance for executive management: • Introduction to UNECE WP.29, ISO/SAE 21434 and required processes • Illustrate financial impact on the organization if the type approval cannot be granted due to non-compliance with the requirements

Training modules
2) Awareness training for the vehicle development

Vehicle development	The vehicle development department shall understand the interdependence of cybersecurity, functional safety and data protection.

Relevance	**Assets and opportunities for attacks**	**Consequences of attacks**	**Great topicality**
Introduction to WP.29 and ISO SAE 21434 Relevance for type approval	Presentation of vehicle functions, interfaces and processed data in model ranges	Demonstration of an attack and impact on data flow and depending functions thereof	Presentation of past incidents

• Introduction to UNECE WP.29, ISO/SAE 21434 and required processes
• Explain that type approval is now depending on cybersecurity
• Illustrate financial impact on the organization if the type approval cannot be granted due to non-compliance with the requirements
	For each model range participants shall decide:
	• which vehicle functions are implemented, in what ways functions are connected / existent interfaces
	• Which data are being processed e. g. personal data, payment information …
		• Choose one specific model range and show attack via different attack vectors
		• Show consequences for data flow and depending vehicle function
		• Example: man-in-the-middle-attack
		  • data flow is not intermitted but redirected
		  • no impact on vehicle functions but compromise of data privacy
			• Show examples of past incidents
			• Illustrate what approach has been used
			• Explain that due to the fact that today attacks are possible there is need for action

Training modules

3) Awareness training for the vehicle development - basic processes of information security

Vehicle development	The vehicle development department shall be able to adopt basic processes of information security into the vehicle development processes.

Relevance of cybersecurity

Linkage between vehicles and IT

- Explain connection between the Internet of Things (IoT) and vehicles
- Demonstrate that vehicles are increasingly connected and gain more and more functions
- Therefore, system complexity is increasing, too

Approach of hackers

Introduction to motivations for attacking, security properties, types of attacks, attack vectors and feasibility

Introduce to:

- motivations of attackers for attacking
- type of attacks, e.g. Man-in-the-middle, Trojan, denial of service, …
- attack vectors: remote, adjacent, physical, local
- feasibility depending on attack vectors

How to avoid being hacked

Introduction to mitigations

Introduce to:

- Characteristics of measures as strength, collaboration, suitability
- Measures in the field of IT e. g. cryptography, firewalls, VPNs
- Measures in the field of vehicles e.g. architectural trends that enforce security

Training modules

4) Awareness training for the enterprise IT risk management

Enterprise IT-Risk Management

Enterprise IT-Risk Management shall get informed on vehicle engineering and data processing processes.
They shall be able to adopt processes of information security into the vehicle development processes.

Relevance of IT in vehicles

Linkage between vehicles and IT

- Explain connection between the Internet of Things (IoT) and vehicles
- Demonstrate that vehicles are increasingly connected and gain more and more functions
- Therefore, system complexity is increasing, too
- Introduction to vehicle parts, tasks, data flow, architecture and architectural trends
- Illustrate meaning for security of each subject

Consequences of attacks

Illustration of consequences for vehicle functions if the data flow is manipulated

- Explain vehicle functions and related data flow processes
- Illustrate consequences for vehicle functions and privacy if the data flow is manipulated and/or interrupts

How vehicles have been compromised in the past

Presentation of past incidents and explanation of the used approach

- Presentation of past incidents like the hacked jeep
- Explain course of action / how attackers were able to succeed → affected interfaces, systems, functions
- Illustrate complexity of the attack as well as impact / possible impact

Importance of protecting both, backend and vehicle

Explanation of linkage between vehicle and backend

- Explain the of linkage between vehicle and backend
- Illustrate possible consequences on functions if backend is compromised
- Illustrate possible consequences for the backend if vehicle is compromised
- Manipulation can have consequences in both directions

Training modules
5) Awareness training for aftersales staff

Aftersales / first level support	The aftersales department shall understand that safety relevant incidents can be caused by compromised cybersecurity.

Relevance of cybersecurity

Presentation of vehicle functions and services in model ranges: show dependence from proper data flow

For each model range:
- Show vehicle functions and services and their use
- Show the processed data e. g. personal data, payment information …
- Present possible consequences if data flow is interrupted or manipulated

Approach of hackers

Presentation of possible and past incidents

- Present possible attacks on interfaces, vehicle functions and scalability
- Present past incidents like the hacked jeep
- Explain course of action and consequences for vehicle functions

Learning outcome

Exercise to enhance learning outcome

Can misconducting vehicle functions be caused by compromised cybersecurity?
- Show different customer inquiries that state a misconducting vehicle
- The participants shall decide whether a manipulation could have caused this or if this is

- YES, forwarding is necessary!

Training modules

6) Awareness training for all departments involved in vehicle cybersecurity processes – rethinking the organizational structure

All departments involved in vehicle cybersecurity processes	All departments involved in vehicle cybersecurity processes shall be able to realize relations of different areas of responsibilities to jointly address cybersecurity. For achieving this, they shall generate an approach of a possible structural adjustment of the organization.

Regulation and processes

Introduction of UNECE, CSMS, ISO/SAE 21434, type approval, risk based approach

- Introduction to UNECE WP.29, ISO/SAE 21434 and required processes
- Explain that type approval is now depending on cybersecurity e.g. CSMS
- Show risk based approach: determination of threat scenarios, risk assessment
- Illustrate financial impact on the organization if the type approval cannot be granted due to non-compliance with the requirements

Importance of documentation

Transparent, complete documentation is important

- Explain that transparent and complete documentation is important for the certification of the CSMS
- Demonstrate that vulnerabilities that appeared years before can be fixed best if documentation from years before contains information on it

Incident Management

Which processes could be performed by which departments?

How to perform Incident Management for vehicle security incidents?

- Let IT Incident Management present their exact procedures
- LET product security present their exact procedures
- Collaboratively, develop ideas for a vehicle security incident management (composition, collaboration of different departments)

Workshop

Discussion of suitability of the organizational structure

- Discuss the suitability of the organizational structure for performing processes required for a type approval
- Discuss a possible restructuring
- Identify, if working groups need to be increased by stuff or by tasks or if they need to be reformed differently.
- Which positions need to collaborate?
- What kind of information needs to be exchanged and what processes require mutual agreements?

Training modules

7) Awareness training for all departments involved in incident management

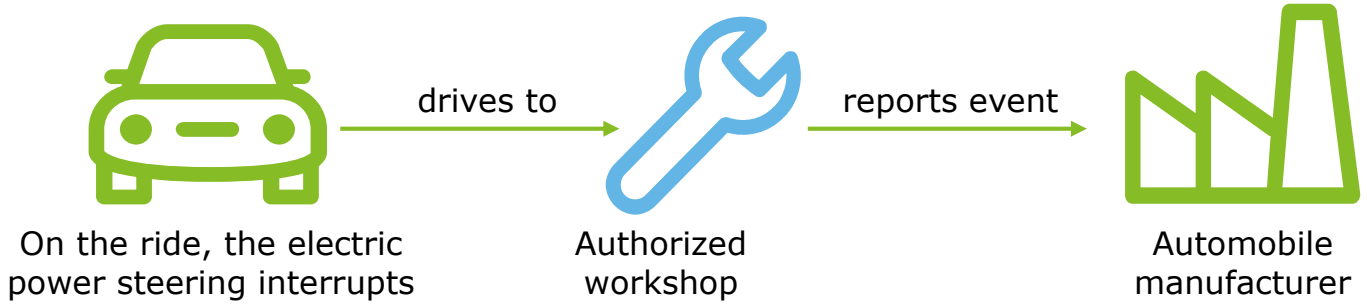
All departments involved in incident management	Participants are able to apply their theoretical knowledge on vulnerability and incident handling into a simulated show case.

Content: Exercise on how to proceed if there is an incident and how to induct decisions.

Knowledge transfer: Simulation

Preparations: Room/premises with necessary equipment
Distribution of roles according to roles as planned for standard operation
Further supporting roles: authorized workshop and supplier – can be communicated with trough telefone

Case study:



Training modules

7) Awareness training for all departments involved in incident management

All departments involved in incident management	Participants are able to apply their theoretical knowledge on vulnerability and incident handling into a simulated show case.

Provided material:

- A list with known existent vulnerabilities
- A list with suppliers and supplied components
- The documentation about the determination of risks for interfaces in the vehicle
- The documentation about the derived ´measures to mitigate risks for the interfaces
- The documentation about the vehicle architecture of the affected model range

Process & results:

- The documentation about the determination of risks for interfaces in the vehicle contains a vulnerability that hasn’t been handled before
- Scope of vulnerability shall be assessed
- Participants shall communicate with the authorized workshop to find out if there are further malfunctions
- Authorized workshop shall then give a clue to a misconducting component
- Participants shall find out with documentation that component comes from supplier
- Participants shall communicate with that supplier and agree on who is responsible for fixing the vulnerability

Deloitte.