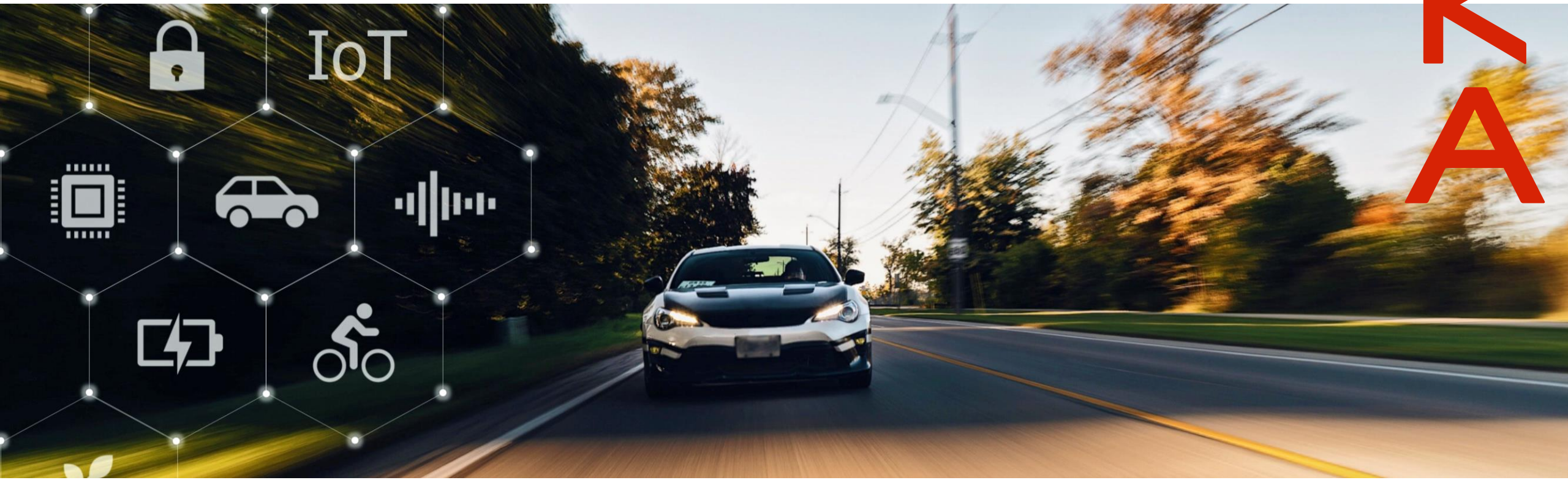
Hochschule Karlsruhe
University of
Applied Sciences

Institut für
Energieeffiziente Mobilität

Incident-Response-Management

An automotive perspective



Reiner Kriesten

Foto: Qijin Xu / Unsplash

Agenda

Short presentation Institute for Energy Efficient Mobility (IEEM)

Motivation

- The economic dimension of capable security incident management processes

Standards and regulation: An overview

- A localization in the V model and in current standardization and regulation

Technical implementations and evaluation

- From holistic detection to the appropriate response through a Vehicular SOC

Giving some further context

- Approaches for preventive and real-time monitoring of internal and 3rd party sources

Challenges & Outlook

IEEM – About us

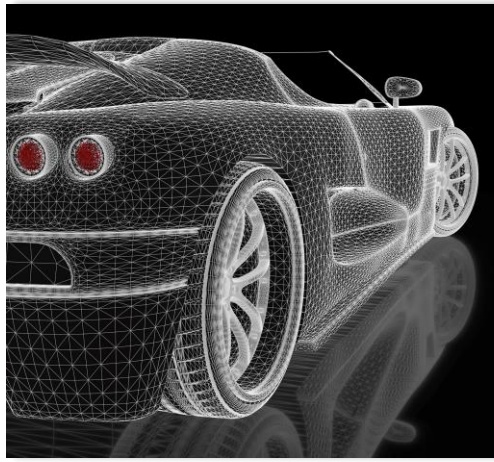
Institute for Energy Efficient Mobility (IEEM) – University of Applied Sciences Karlsruhe

- Foundation in 2012
- Institute management
  - Prof. Dr.-Ing. Reiner Kriesten (Sprecher)
  - Prof. Dr.-Ing. Philipp Nenninger (stellv. Sprecher)
  - Prof. Dr.-Ing. Dirk Feßler
  - Prof. Dr.-Ing. Peter Offermann
  - Prof. Dr.-Ing. Maurice Kettner
- around 20 employees: Betreuung einiger Doktoranden (10)
- Locations
  - Bruchsal:
    Büroeinrichtungen, Labore, Prüfstände, Forschungsfahrzeuge, Werkstatt & Hebebühne
  - Karlsruhe:
    Büroeinrichtungen, Labor, Rollenprüfstand

Research Areas

Security für Cyber-Physikalische und Automotive Systeme

- Modellierung CPS & Security-Artefakte
- Eigenes „automotive Opfernetzwerk“
- Penetrations- & modellbasierte Tests
- Schwachstellendatenbank
- Automotive Responsible Disclosure
- Threat- and Risk-Analyse (TARA & HARA)
- Security-Features: Firewall, IDPS
- Security für Autonomes Fahren (auch für HU)

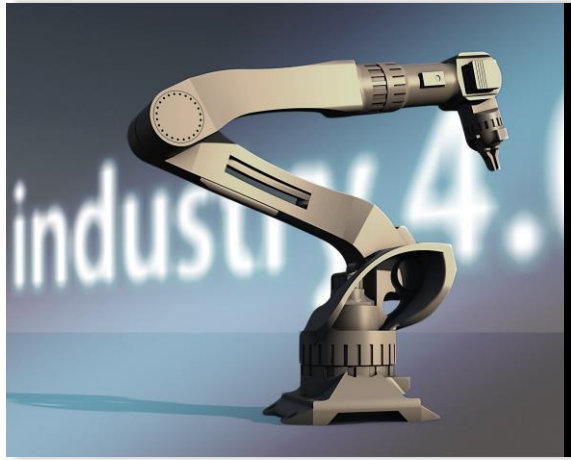


Modellbasierte Entwicklung & Rapid-Prototyping Systeme

- Unity-Applikation zur Entwicklung von ADAS (mit Anbindung realer Prototypen)
- Simulation E/E-Architektur & Offboard-Schnittstellen über Toolsuite (Opfernetzwerk)
- MATLAB/Simulink & weitere für z.B. Energie- & Reichweitenmanagement für E-Fahrzeuge & E-Bikes

Virtuelle Testfelder für Mobility & Industry

- Unity (ADAS & Fahrradsimulator)
- MATLAB/Simulink & CarMaker (System & Umwelt)
- Opfernetzwerk mit u.a. AUTOSAR
- Digitaler Zwilling: Virtualisiertes Multiinstanz-Leitsystem mit virtualisierter Steuerungsebene



Industrial IoT

- Automatisierung
- Digitale Zwillinge: virtuelle Abbilder von Anlagen mit ihren Steuerungseinheiten, Feldbussysteme, Schnittstellen sowie Sensoren und Aktoren
- Verfahren der Bilderkennung
- Künstliche Intelligenz, Maschinelles Lernen
- Pseudonymisierung & Anonymisierung
- Bots

Research Areas

Energieeffiziente Antriebe

- Alternative Kraftstoffe
- Wasserstoff
- Brennverfahren
- Innovative & alternative Zündsysteme
- Abgasemissionssensoren
- Klima- & Höhensimulation
- intelligentes Energie- und Reichweiten-management für E-Fahrzeuge und E-Bikes

Tomorrow-Bike

- Fahrradsimulator
- Energiemanagement für E-Bikes (Powertrain & Nebenverbraucher)
- Abstandssensor für Messung kritischer Überholvorgänge
- Fahrradreparaturstation
- Lastenräder

Smart City & Last Mile Logistics

- Urbane Logistik
- Letzte Meile
- Maschinenethik
- Wissenstransfer
- Bürgerbeteiligung/Partizipation
- Entwicklung von automatisierten, intelligenten Funktionen im automotiven & industriellen Bereich

Akademie & Schulungen

- Leitung Akademie
- Wissenstransfer
- Organisation von Veranstaltungen
- Wissensdatenbank, Webauftritt
- Gamification: z.B. virtueller Showroom
- Zertifizierte Lehrgänge & Studiengänge

Research Areas

Forschungskooperationen & studentische Projekte

SECURITY

SAVE Securing Automated Vehicles (Japan – Germany)

SecForCARs Security For Connected, Autonomous CARs

„Next Level“-Hauptuntersuchung
Forschungsvorhaben für mehr Verkehrssicherheit autonomer Fahrzeuge.

MYiTOPS
Ein internationales Projekt zu cyberphysischen Systemen (am IKKU-IEEM).

COMFORT

ADAS & Augmented Reality
Validierung von Advanced Driver Assistance Systems (ADAS) durch Augmented Reality.

ADAS-Sim Virtuelles Testfeld für Advanced Driver Assistance Systems (ADAS).

Testfeld Autonomes Fahren Reallabor für Mobilitätskonzepte zur Entwicklung zukunftsorientierter Lösungen für verschiedene Verkehrsträger.

Car2X CANoe Simulation von Car2X-Kommunikation.

ENERGY EFFICIENCY

VEHICLE Hybridisierung von Lithium-Ionen-Akkus mit Superkondensator. Ein Ansatz für den Betrieb von Reluktanzmotoren in Fahrzeugantrieben.

Easy E-Bike Erweitertes Reichweiten- und Energiemanagement

Sim-Bike
Fahrradsimulator

efeuAkademie Informationszentrum für autonome urbane Güterlogistik

Study2Smart E Das Kart mit elektrischem Antrieb und Fahrerassistenzfunktionen.

Profilregion Mobilitätssysteme Karlsruhe
Ressourcenschonende und bedarfsorientierte Mobilität

Motivation

The economic dimension of operational security incident management processes

Motivation

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."

Gene Spafford, 1989

This leads us to the assumption that a compromise is likely to occur regardless of preventive security posture. The impact has to be limited through (real-time) detection and response [1]

Motivation

Why should automotive industry take cybersecurity incidents seriously?

- Let's look at some numbers…

- Famous Jeep hack of Miller and Valasek which caused a stir in the media [2]
- Presented at Black Hat conference 2015, remote attack also successful
- Presentation to publicity: How great was the damage for the FCA group... and how could that be measured?
- Perhaps the share price provides insights…

Motivation

- Date of publication on Black Hat: Aug. 5, 2015
- The share price fell by over 21% within 3 weeks from hack publication for Fiat Chrysler

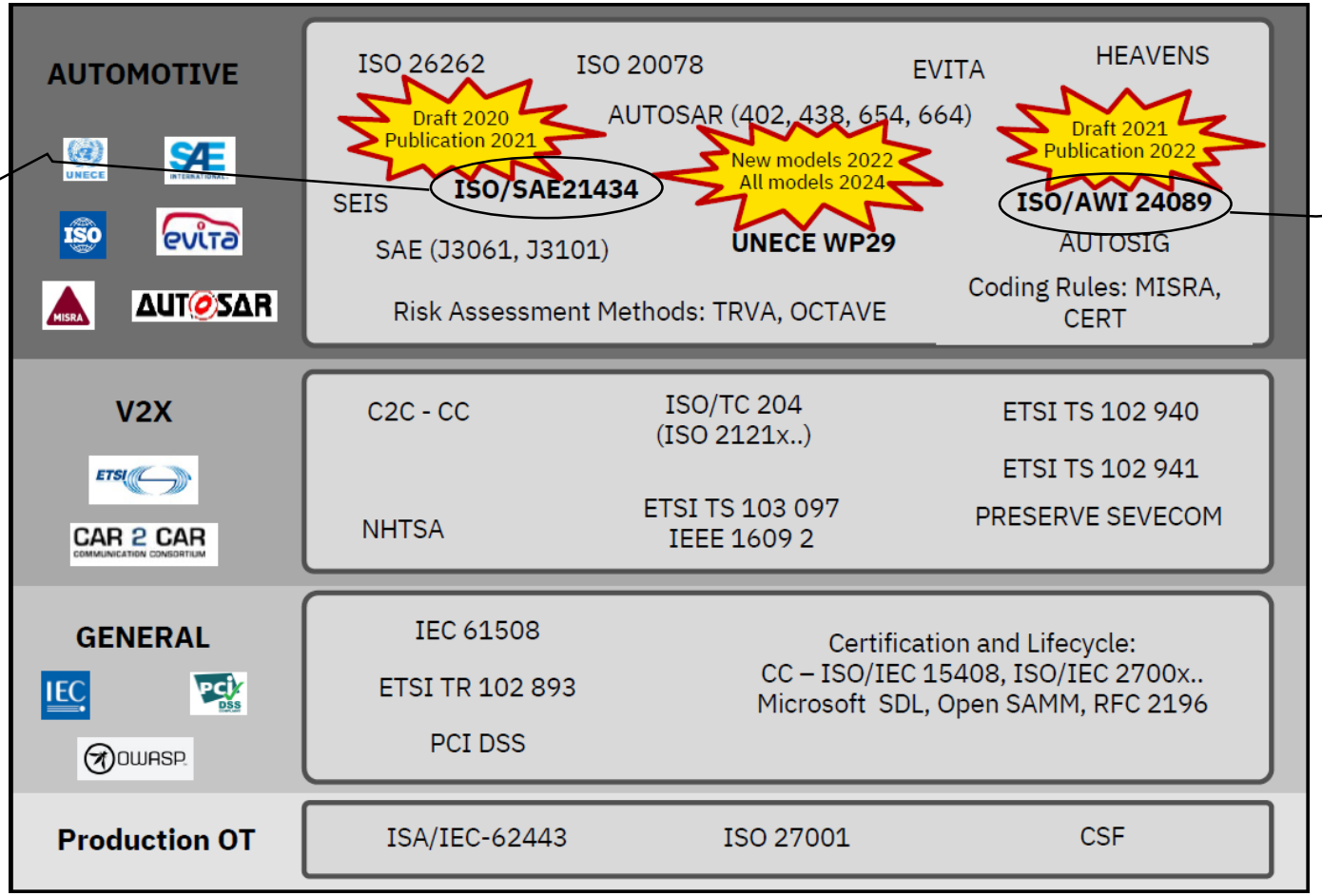
- It took until January 2017 (17 months) for the share price to recover...
- Coincidence?... Maybe! But maybe not…
- Research assumes existence of a root-cause ([4], [5], [6])

Standards and regulation: An overview

A localization in the lifecyle model and in current standardization and regulation

Standards & Guidance: Big Picture

ISO/SAE 21434 „Road vehicles – Cybersecurity engineering
-
Guidance on compliance with UN R155 (CSMS)



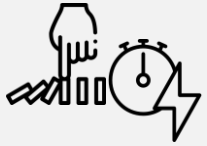
ISO DIS 24089 Road vehicles — Software update engineering
-
Guidance on compliance with UN R156 (SUMS)

Automotive Incident Response Management in Regulations

Link zu Florians Vulnerability Database and example pictures

UN R155 - approval of vehicles with regards to cyber security and its management system (CSMS)

Adequate consideration of cyber security (7.2.2.2)
Remark: ISO 21434 regulation in place since 2021



Response to cyber threats and vulnerabilities within a reasonable timeframe due to mitigations (7.2.2.3.) Remark: Automotive Vulnerability Disclosure Process?

Re-assessment of security measures in the light of new cyber threats and vulnerabilities (7.2.2.2.g)
Remark: vehicle lifetime 15-20 years

Management of dependencies with suppliers, service providers or sub-organizations (7.2.2.5.). Remark: Description of Systems-of-systems still research topic (e.g. SecForCars)

Provide relevant data to support analysis of attempted or successful cyber-attacks (7.2.2.2.h)
Remark: Common description language for cyber-attacks?

Report at least once a year the outcome of incident management activities to approval authority (7.4.1.) Remark: Common description language for cyber-attacks?

UN R156 - Approval of vehicles with regards to software update and its management system (SUMS)

SUMS related req.
- Process & documentation related req.

Technical req.

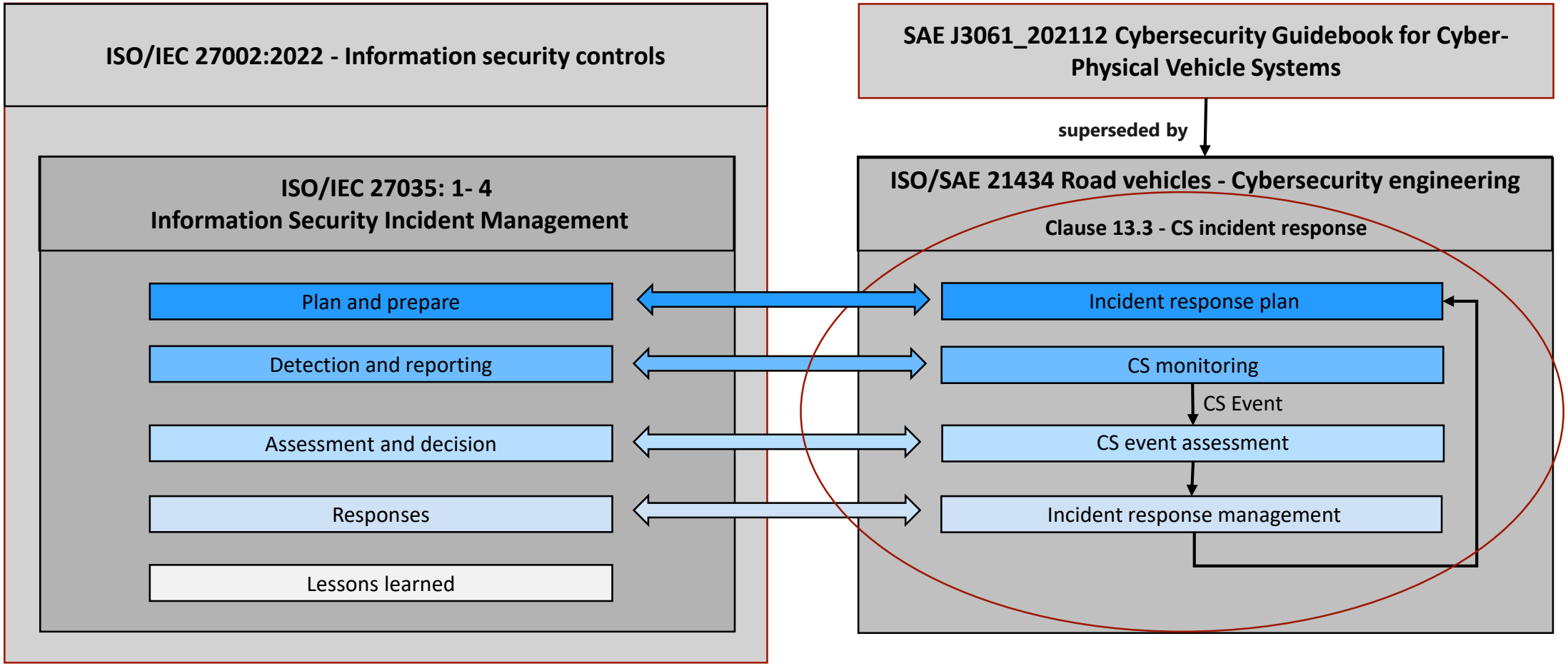
Automotive Incident Response Management in Regulations

Example of common attack description

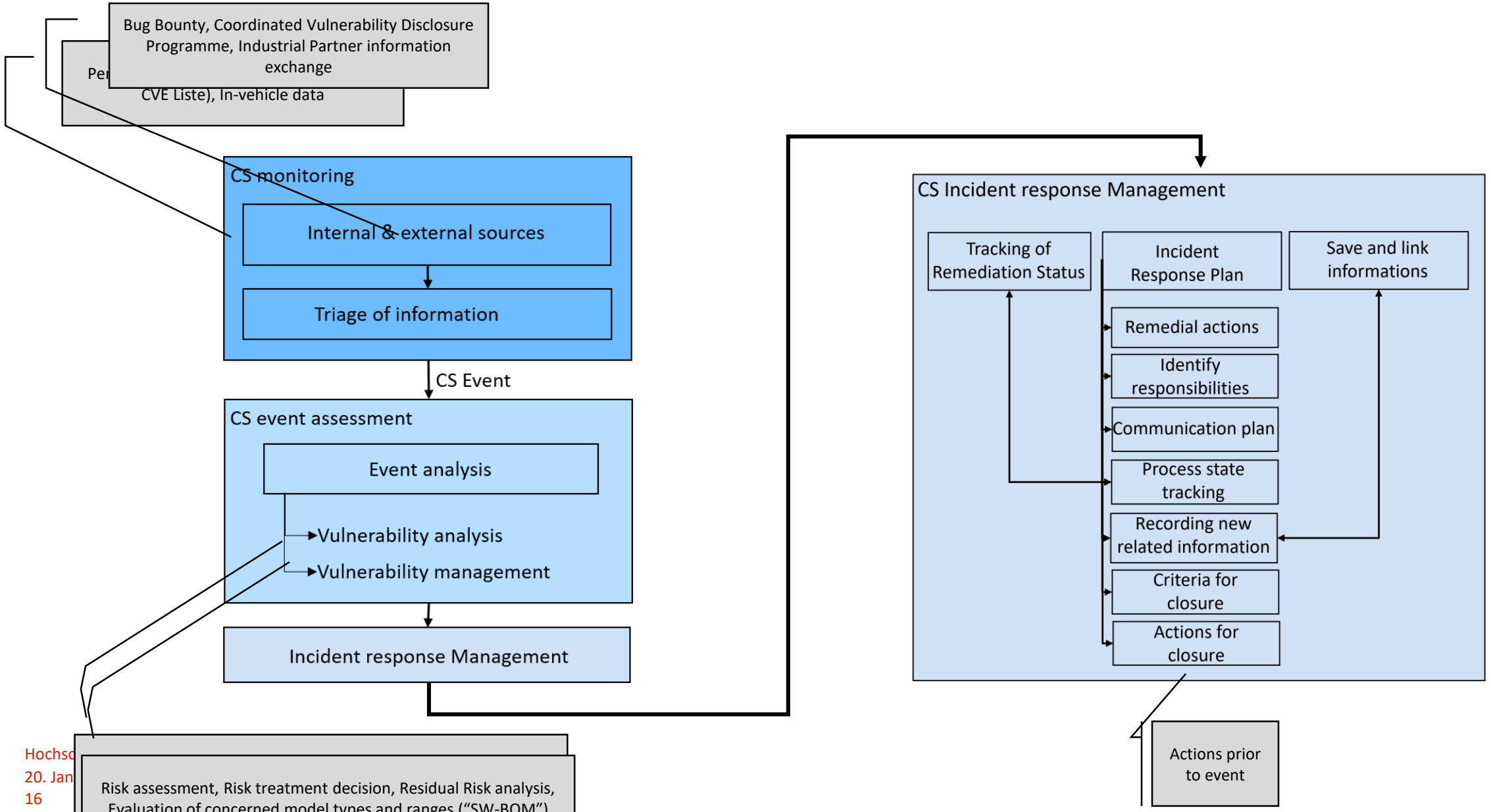
Category	Level 1	Level 2	Level 3
Description	Unauthorized flashing of malicious code on the engine ECU by using the diagnostic reprogramming routine		
Reference	Adventures in Automotive Networks and Control Units (C. Valasek et al.)		
Year	2013		
Attack Class	Tampering	Firmware Modification	None
Attack Base	Diagnostic Attack		
Attack Type	Real Attack		
Violated Security Property	Integrity		
Affected Asset	Information Security		
Vulnerability	CWE-693: Protection Mechanism Failure	CWE-287: Improper Authentication	Unauthorized reprogramming possible
Interface	OBD		
Consequence	Flashing of malicious code on ECU		
Attack Path	Downloading a new calibration update for ECU from manufacturer and Reverse Engineering of the Toyota Update Calibration Wizard (CUW). Monitoring the update process. Reverse Engineering update algorithm for calibration updates. Modification of calibration update. Reflashing of malicious update.		
Requirement	Required Access/Connection	OBD	None

Restriction	Security Feature	Access Control	Security Layer which is tied to the Calibration Version and allows only one time overwriting
Attack Level	Local Network		
Acquired Privileges	Full Control (Functional Component)		
Vehicle	Toyota Prius (Year of Construction: 2010)		
Component	Engine ECU	Engine Control Module	2 CPUs, NEC v850, Renesas M16/C
Tool	Software Tool	Vehicle Diagnostic Software	Toyota Calibration Update Wizard (CUW)
	Hardware Tool	Interface	J2534 PassThru Device (CarDAQPlus)
	Hardware Tool	Interface	ECOM cable
	Hardware Tool	Laptop/PC	Windows PC
	Software Tool	Communication Tool	EcomCat Application
Attack Motivation	Security Evaluation		
Entry in Vulnerability Database	None		
Rating	CVSS: 6,8		
Exploitability	CVSS Exploitability: 1,62		

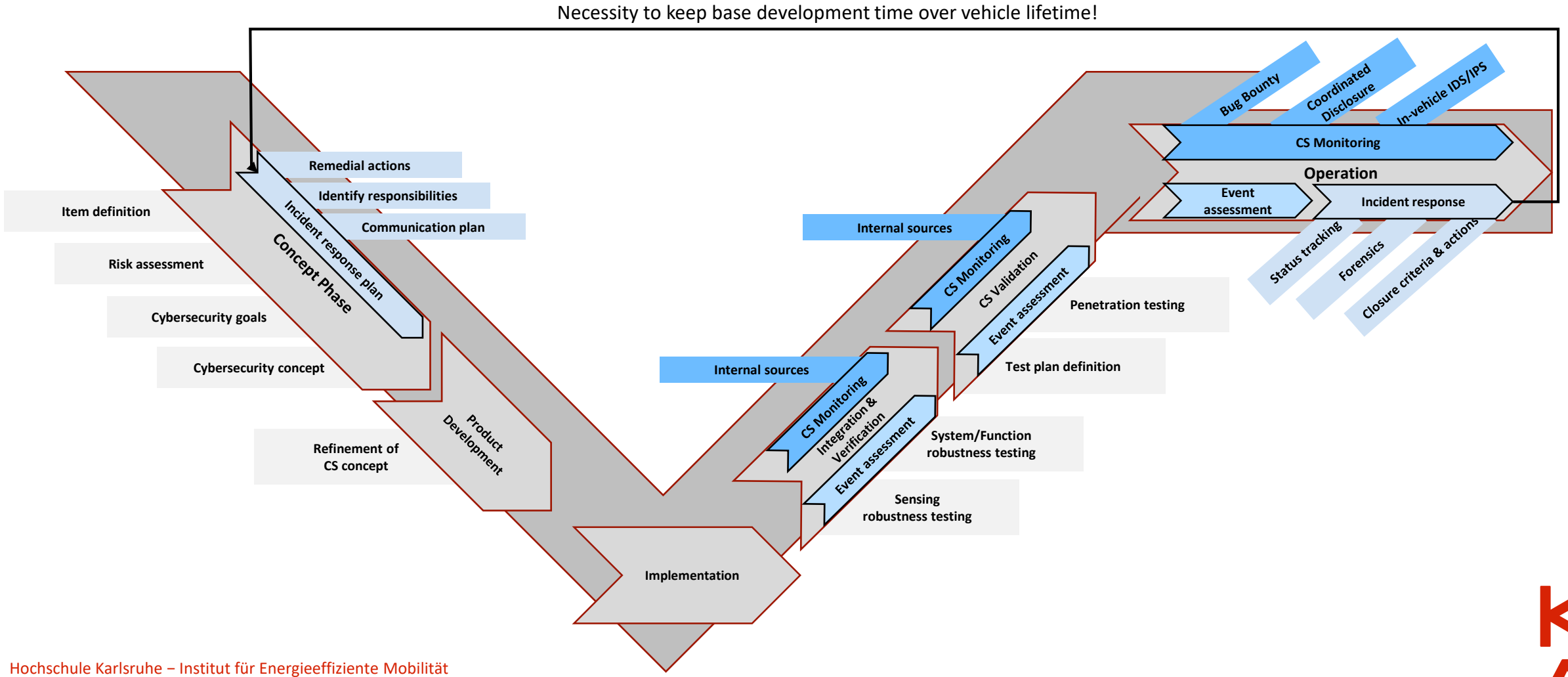
Standards & Guidance: Incident Response Management



Automotive incident response (ISO/SAE 21434)



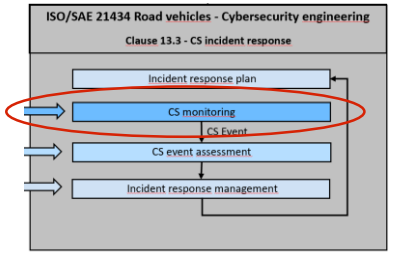
Automotive Incident Response in the vehicle lifecycle - V Model description (ISO/SAE 21434)



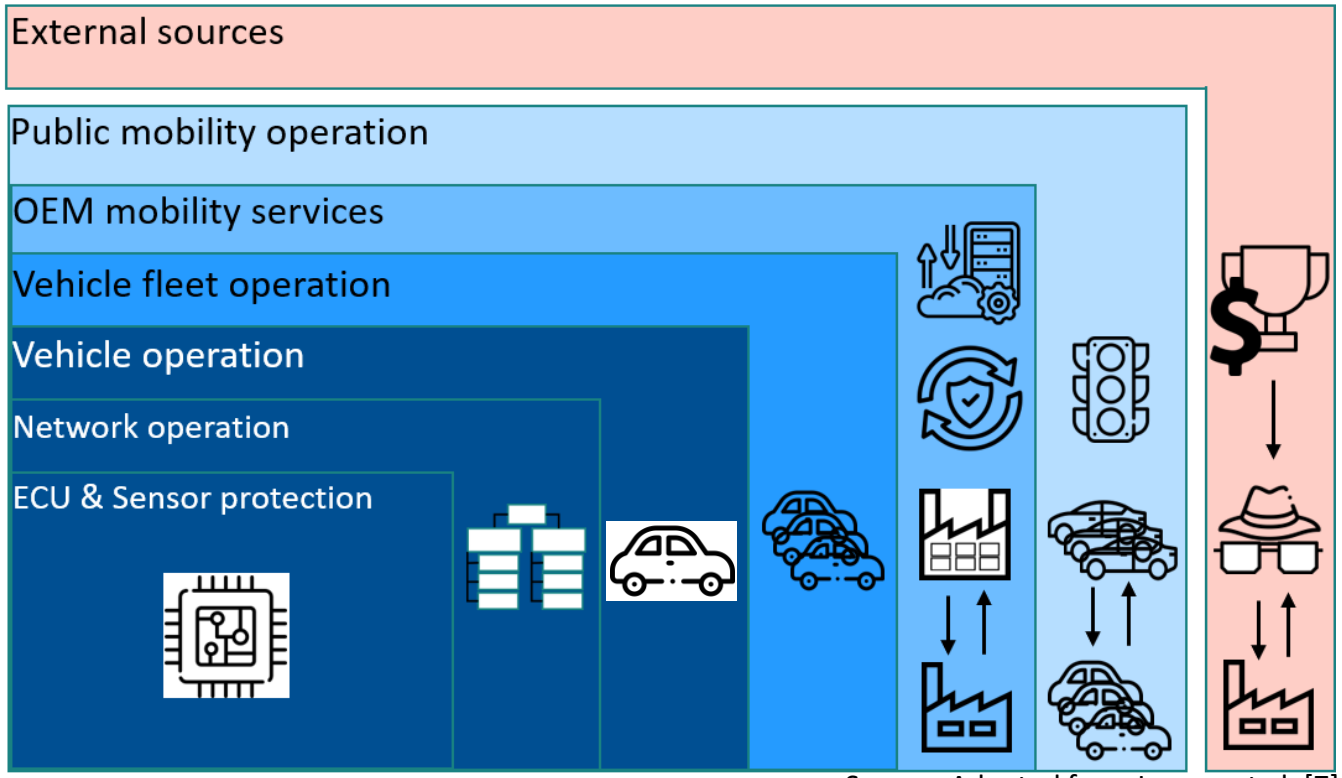
Technical implementations and evaluation

From holistic detection to the appropriate response through a Vehicular SOC

Monitoring dimensions in Systems-of-systems - An Holistic Approach is needed



Definition of system boundaries and layers of monitoring, analyzing and response, as well as technical measures for connected vehicles landscape



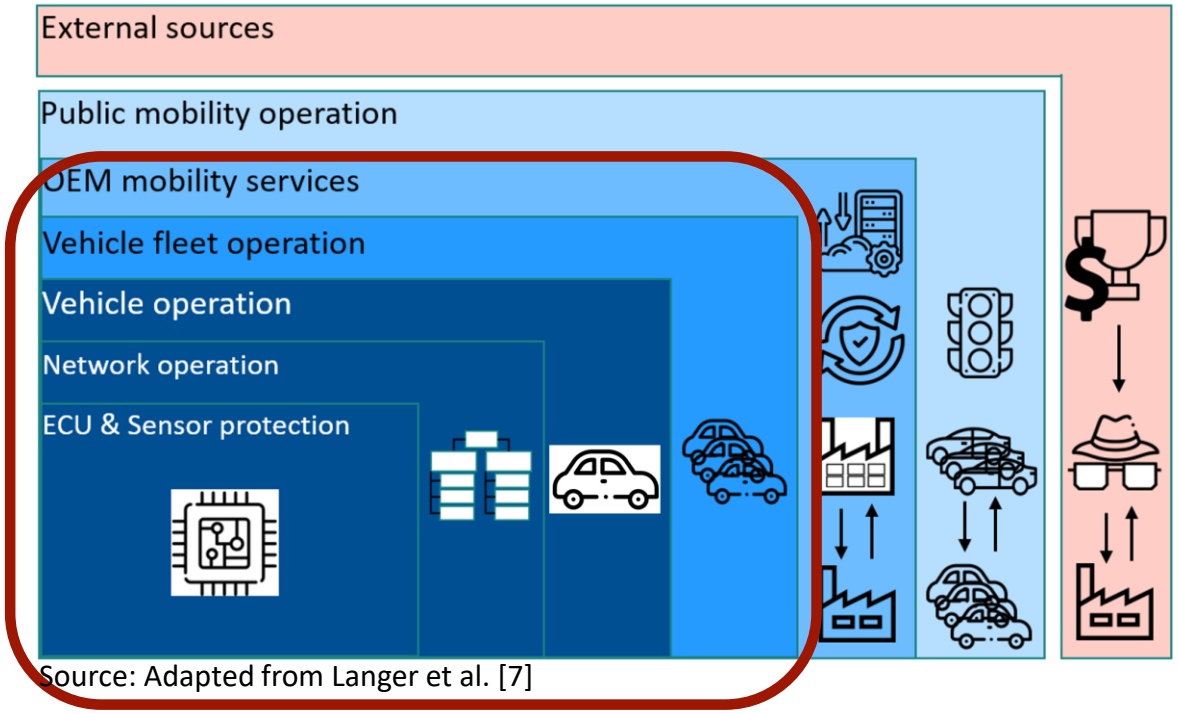
Source: Adapted from Langer et al. [7]

- Combine incident monitoring & response management for IT and OT systems
- Extend existing solutions for IT systems with in-vehicle detection
- Incentivize and offer open communication about vulnerabilities with third parties (e.g.: ethical hackers)
- Communication with industrial partners

Monitoring dimensions in Systems-of-systems

- Technical example Multilayer Intrusion Detection (Prevention) Systems

- Technical vehicle monitoring: ID(P)S, Firewall technologies, Vehicular honeypots ….
- State of the art of Vehicle Security Operation Center (VSOC)
  - monitoring systems boundary includes vehicle + (OEM/Tier) cloud solutions
  - PSIRTs (Product Security Information Response Teams) with regular information exchange within automotive industry
  - further vertical integration difficult to implement

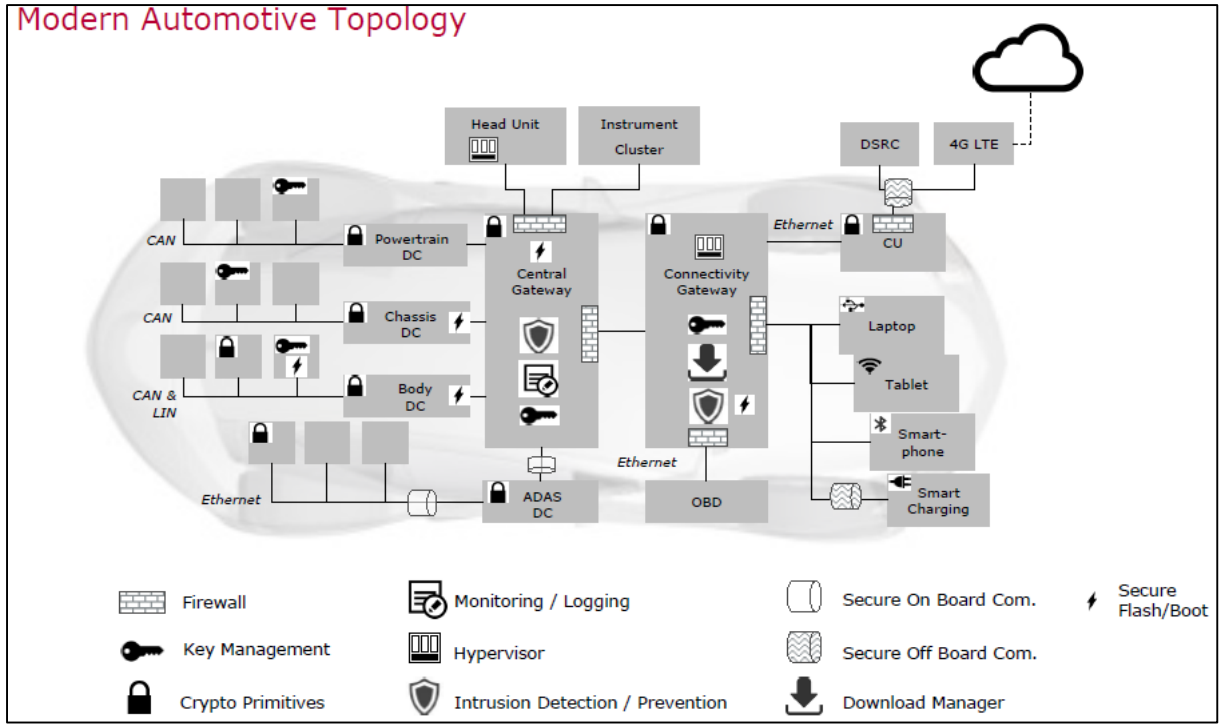


Source: Adapted from Langer et al. [7]

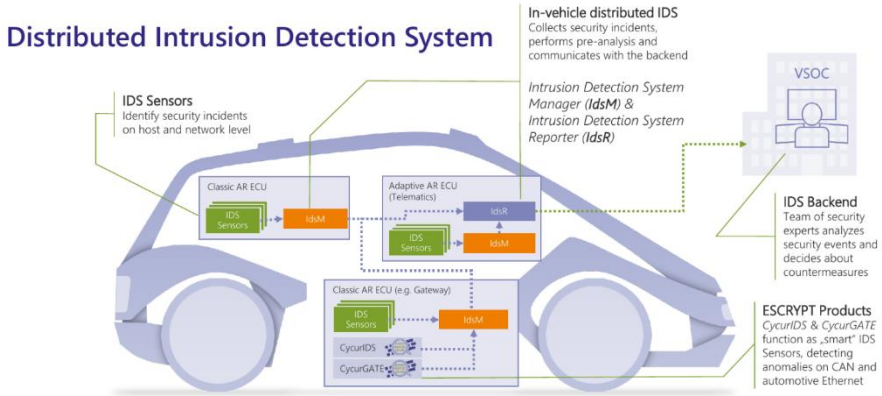
Monitoring dimensions in Systems-of-systems

- Technical example Multilayer Intrusion Detection (Prevention) Systems

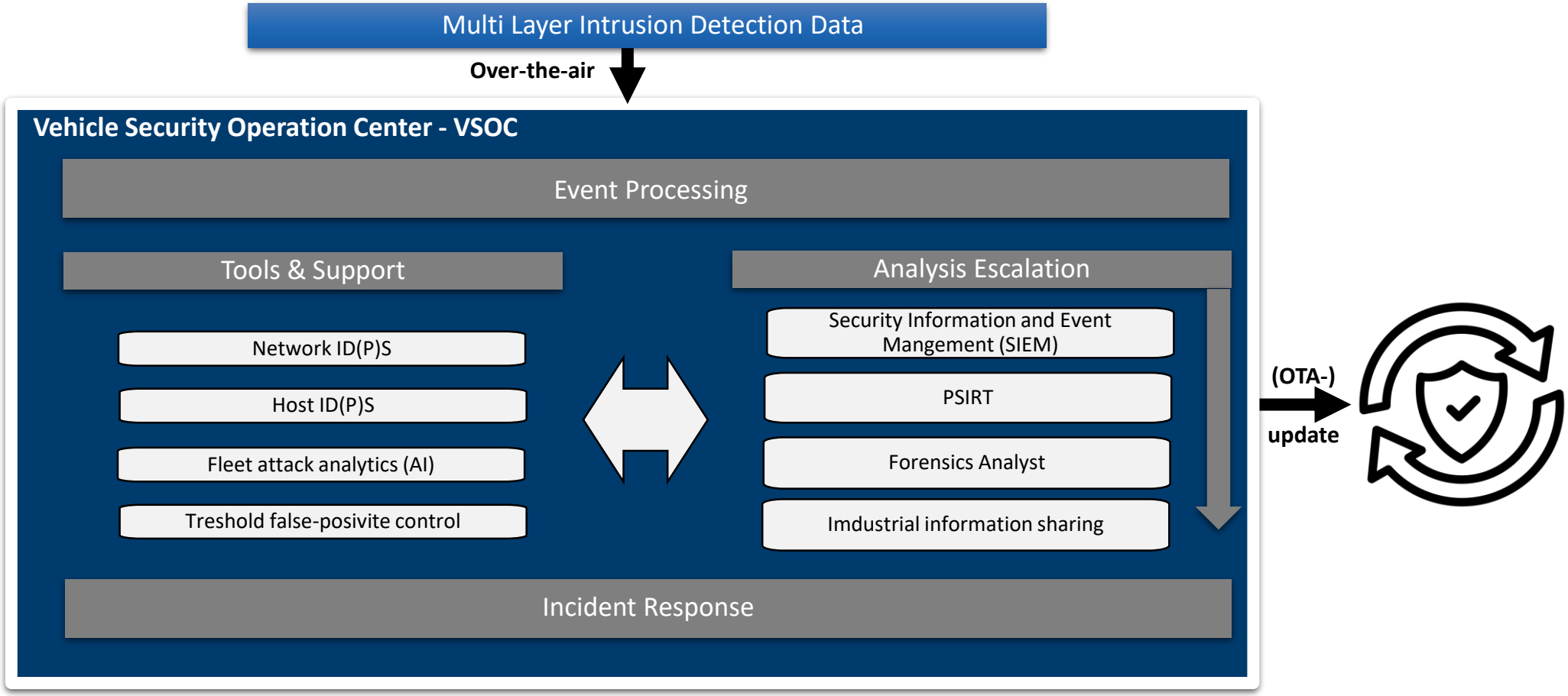
- Vehicular Security artefacts cover multiple approaches, see picture
- IDS systems need to be distributed
  a) over E/E-architecture of vehicle (*onboard view*)
  b) Over the fleet, access to cloud information database (*fleet/OEM view*)
- IDS approaches: network-based IDS versus host-base IDS
- Example attack monitoring:
  - Malicious diagnostics requests
  - Attacks over wireless interfaces (connectivity gateway, headunit)
  - Attacks over physical interfaces (infotainment, direct bus access, Debug access attempts)
- Attention: false positive alarms may be critical to reputation and vehicle availability



Source:S.Bayer, K. Hirata, D. KengoOka: Towards a Systematic Pentesting Framework for In-Vehicular CAN Networks, ESCRYPT, ESCAR EU, 2016



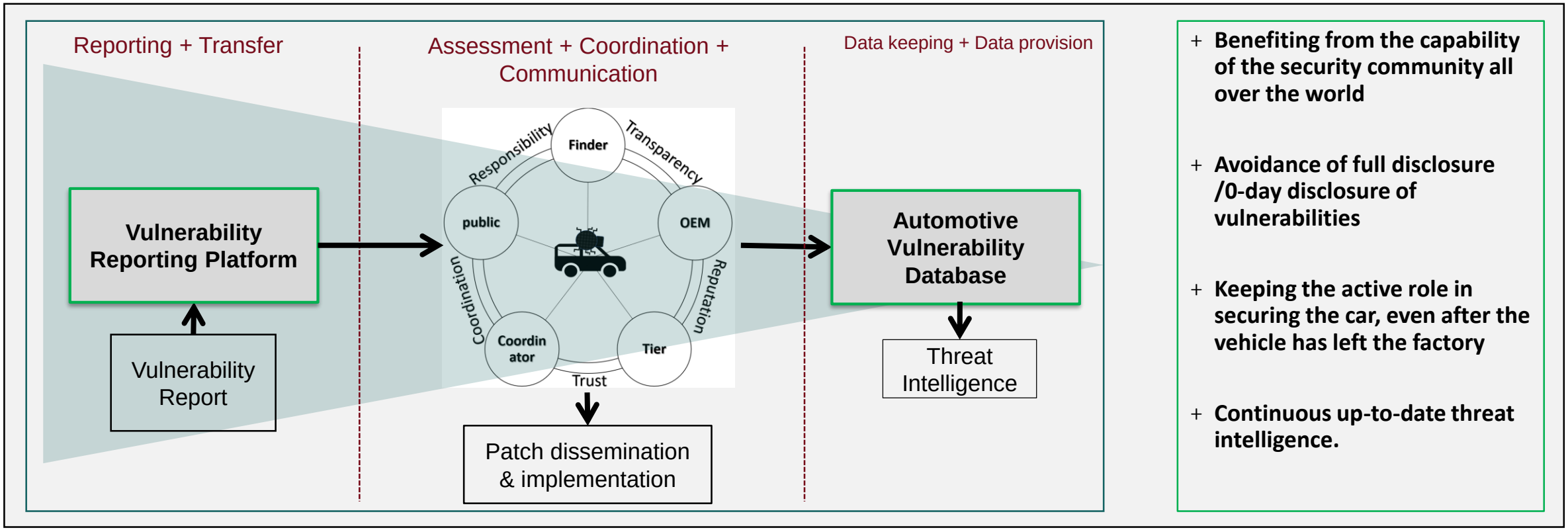
Monitoring dimensions in Systems-of-systems - Organisational setup of an VSOC for IDS processing



Giving some further context

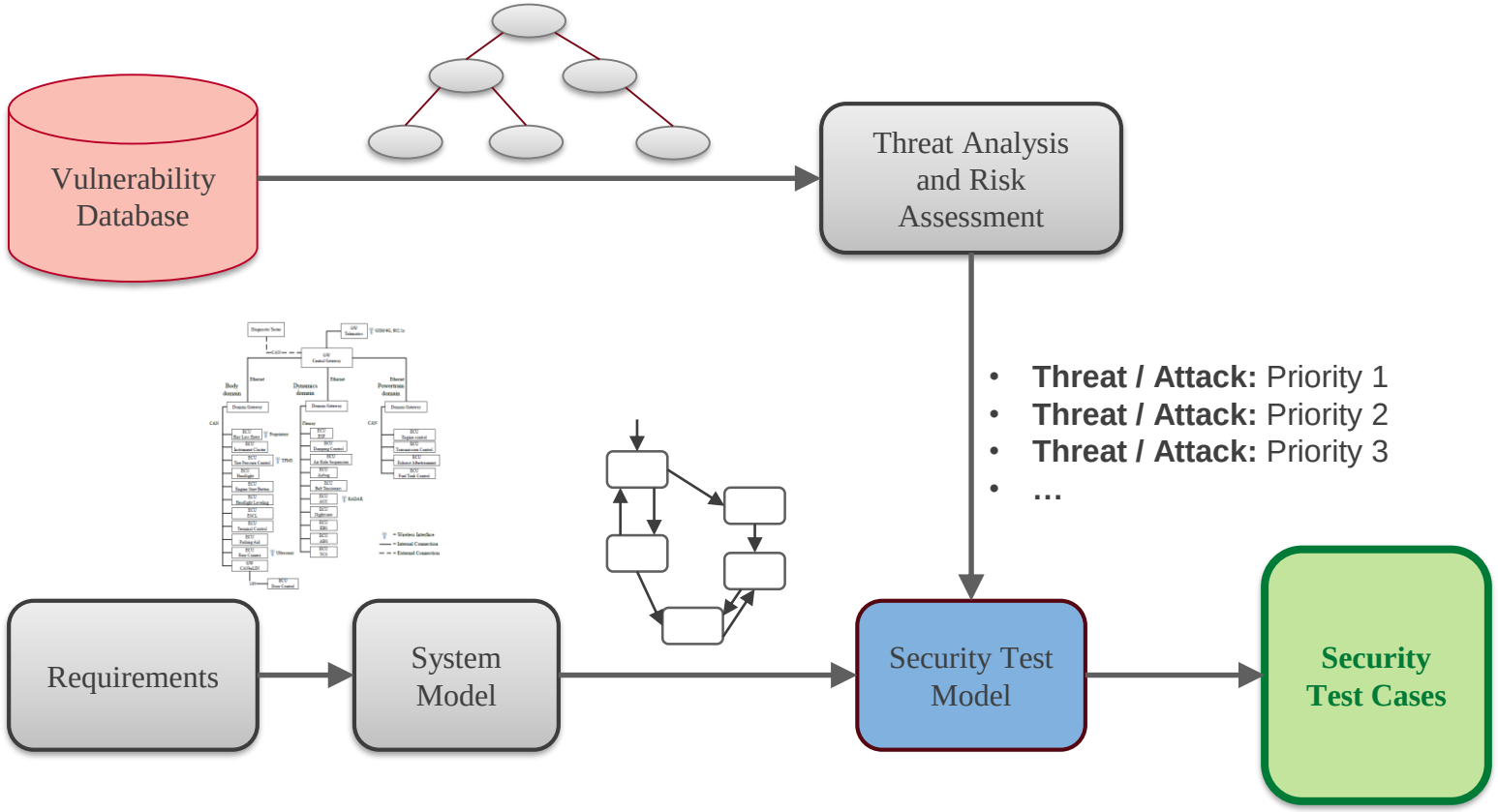
Approaches for peventive and real-time monitoring of internal and 3rd party sources

External Incident Detection: Coordinated Vulnerability Disclosure [8]



+ **Benefiting from the capability of the security community all over the world**
+ **Avoidance of full disclosure /0-day disclosure of vulnerabilities**
+ **Keeping the active role in securing the car, even after the vehicle has left the factory**
+ **Continuous up-to-date threat intelligence.**

Internal Incident Detection: Model-based security testing versus Penetration Testing [8]



Challenges & Outlook

Challenges & Outlook

- State of the art processes and development still to be developed in automotive security and its incident response management
  - In regard to technical development, see e.g. IDS-chain
  - In regard to holistic Systems-of-system analysis capability
  - In regard to the capability to manage incident response over lifetime from acquisition to decommissioning

- Cyber security engineering (CSE)versus Cyber security information management systems (CSMS)
  → Bring together IT- & vehicle security in cooperative cybersecurity operation processes

- Cyber security engineers with technical/physical expertise are increasing rarely to find, in contrast complexity rises fast → necessity of operational Incident Response Systems rises

- Integration of further vertical layers (public mobility, external sources) will rise

References

[1] Harde, G. (2018). Car Security Incident Response, Project report, Automotive Quality Institute

[2] Black Hat USA 2015: So wurde der Jeep gehackt | Offizieller Blog von Kaspersky

[3] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, accessed on 04.03.19

[4] Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software engineering*, *33*(8), 544-557.

[5] Spanos, G., Angelis, L., & Kosmidou, K. (2017). Is the Market Value of Software Vendors Affected by Software Vulnerability Announcements?. In *Strategic Innovative Marketing* (pp. 465-469). Springer, Cham.

[6] Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security*, *58*, 216-229.

[7] Langer, F. (2019). Establishing an Automotive Cyber Defense Center, IAV GmbH, Berlin, Germany

[8] Bolz, R., Rumez, M., Sommer, F., Dürrwang, J., & Kriesten, R. (2020). Enhancement of cyber security for cyber physical systems in the automotive field through attack analysis. In Proceedings of the Embedded World Conference.

[9] Reich, J., Metzker, E. (2021) Scalable Automotive Intrusion Detection Systems, Automotive Cybersecurity Symposium, Vector Informatik GmbH https://cdn.vector.com/cms/content/events/2021/vSES21/vSES21_Slides_05_Reich_IBM_Metzker_Vector.pdf

Hochschule Karlsruhe
University of
Applied Sciences

Institut für
Energieeffiziente Mobilität

www.h-ka.de/ieem

Quellen Icons

Stopwatch: flaticon.com; By Darius Dan

Schild: flaticon.com; By Freepik

Dominoeffekt: flaticon.com; By Freepik

Change Management: flaticon.com; By surang

Provide data: flaticon.com; By Smashicons

Give report: flaticon.com; By juicy_fish

Supplier dependencies: flaticon.com; By noomtah

CPU: flaticon.com; By Freepik

Car1: flaticon.com; By Freepik

Car2: flaticon.com; By monkik

Migration (Server Service): flaticon.com; By Eucalyp

Ampel: flaticon.com; By Freepik

Update: flaticon.com; By smashingstocks

Fabrik: flaticon.com; By Freepik