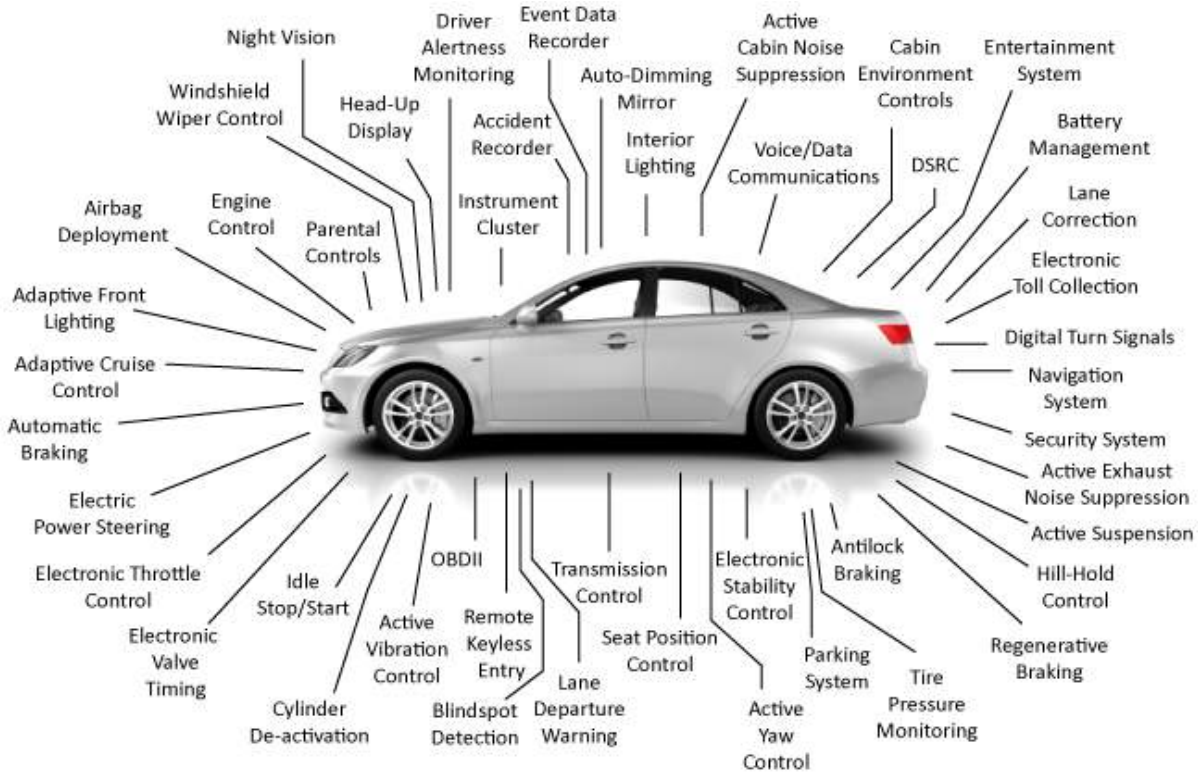
DEKRA
Cybersecurity for Connected Cars

A perspective from Standardization and Certification process

A cyber safe world

Cybersecurity Competence Center

Electronics/computers in modern cars



Source: The Clemson University Vehicular Electronics Laboratory

Threats in the connected vehicle

Malicious firmware updates
- Through USB, CD, SD card
- Through OBD port
- Via OTA process

Attack from downloaded applications

Attack from mobile device applications

Man-in-the-middle attack

Attack to the vehicle internal bus (injection/capture)

Compromised actuators controlled by malicious software

Sniffing of user data and passwords through screens and keypads, transmitted to outside world

Attack on certificate and key stores

Malware delivered through encoded music

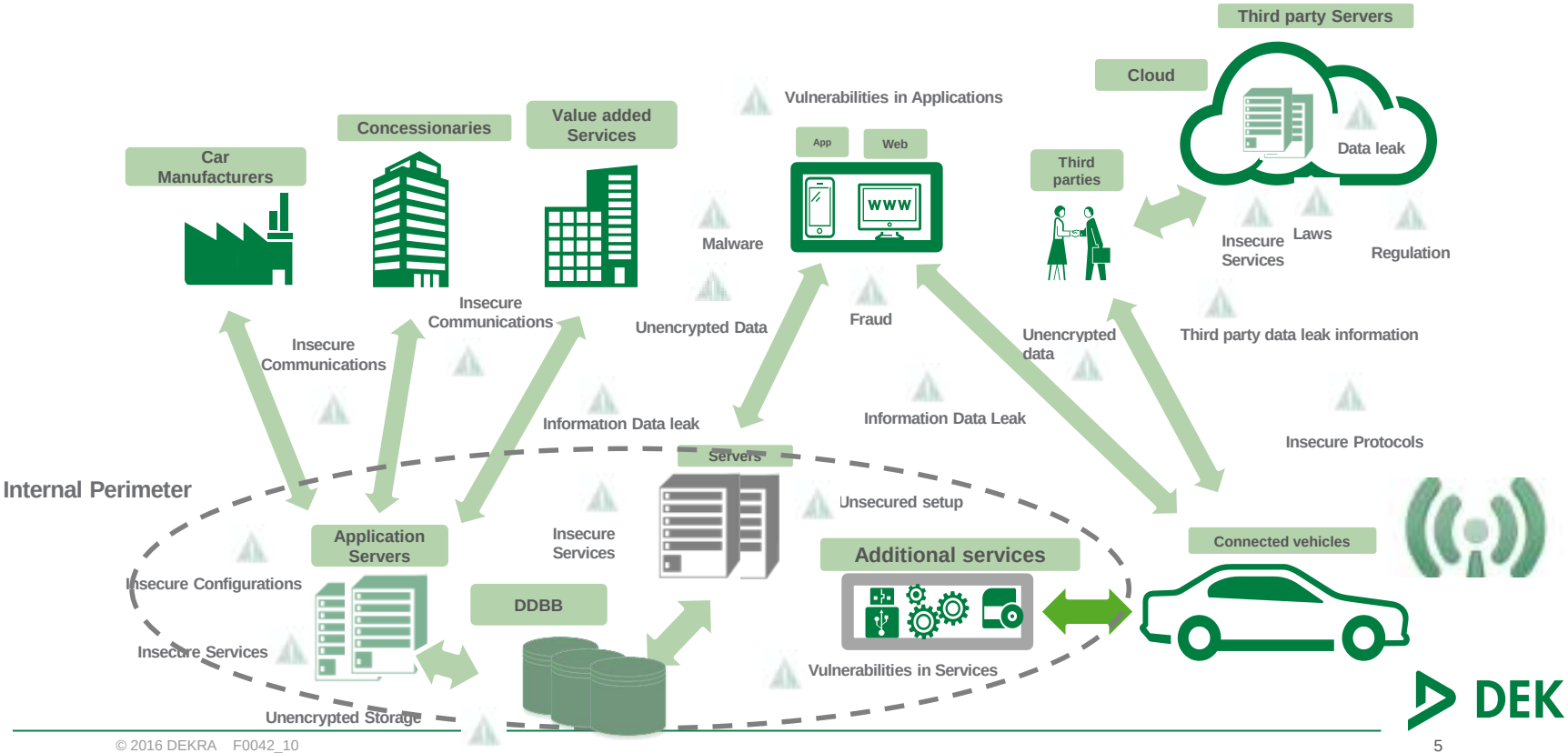
Open source software vulnerabilities

Any part of the electronic system can be an attack point

CYBERSECURITY RISK

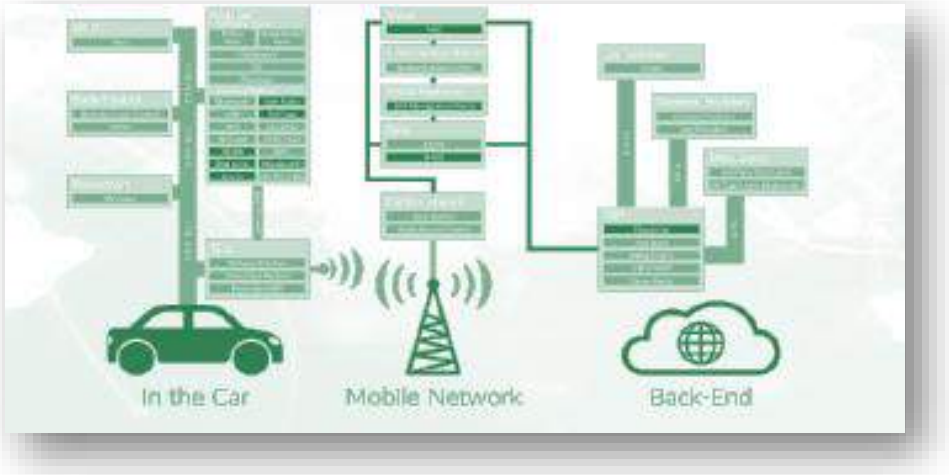
CAR ECOSYSTEM IS GETTING BIGGER

Cybersecurity Risks



Threats in the connected vehicle ecosystem

There are over 50 attacks points in the eco system of a connected vehicle

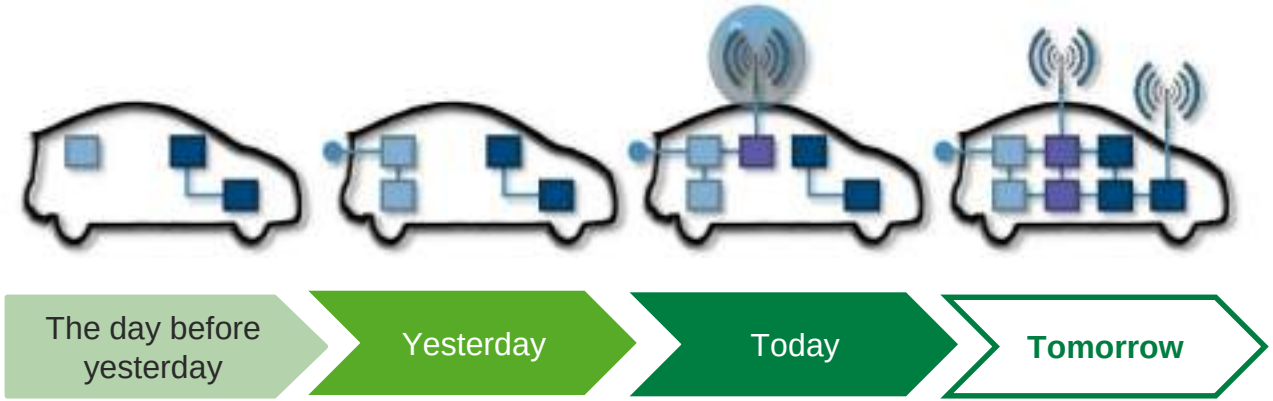


Any part of the Eco System can be an attack point

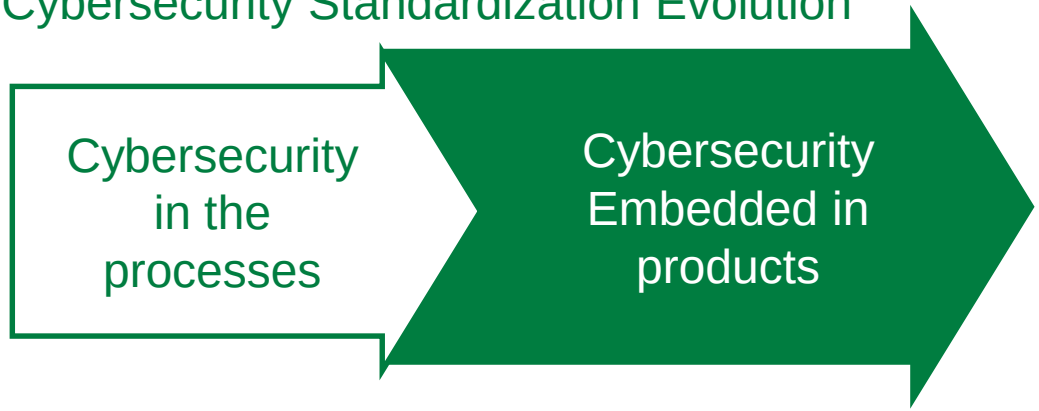
Cybersecurity evolution in vehicles

The day before yesterday	Yesterday	Today	**Tomorrow**
▪ No Cybersecurity requirements	▪ Cybersecurity in internal processes ▪ ISO 27000	▪ Cybersecurity in process development	▪ Cybersecurity embedded in final product ▪ SAE J3061 ▪ WAVE 1609.2 ▪ FIPS 140 ▪ ISO 15408

Cybersecurity evolution in vehicles



Cybersecurity Standardization Evolution



Cybersecurity Evolution

Auditing / Certifying Cybersecurity

TODAY

- Certification is the process to verify the implementation of some security controls
- Value of an independent 3rd-party
- Security consultants and Security auditors have a conflict of interest.

TOMORROW

- Formal Product Security Evaluation
- Pentesting

Pentesting procedures

- Pentesting will be part of the product development process
- Security Evaluators bring early detection of new vulnerabilities

Cybersecurity Evolution

Auditi
Cy

ROW
Security

- Certificatio
  verify the i
  security co
- Value of a
- Security c
  auditors ha

e product

arly detection of new

Somebody will do it some day !!

Better be the first to try it !!

DEKRA

Cybersecurity Evolution

Auditing / Certifying Cybersecurity

TODAY

- Certification is the process to verify the implementation of some security controls
- Value of an independent 3rd-party
- Security consultants and Security auditors have a conflict of interest.

TOMORROW

- Formal Product Security Evaluation
- Pentesting

Pentesting procedures

- Pentesting will be part of the product development process
- Security Evaluators bring early detection of new vulnerabilities

Formal Product Security Evaluation

- ISO 15408 - Evaluation Assurance Level (EAL)
- Specific Protection Profiles for each component
- Different Security Levels for different components

Product Security Evaluation
Implementing Common Criteria (ISO 15408) evaluation and certification

Key points:

- Consistent product security evaluation
- Systematic vulnerability identification and common patterns attacks
- Comparable results thought specific protection profiles

Approach:

- 7 Evaluation Assurance Levels (EAL) for security requirements
- Define a protection profile for each kind of product / component under evaluation
- It is possible to define general protection profiles for international recognition of certificates
- Evaluation include pentesting procedures for new vulnerabilities identification

Benefits:

- Evaluation procedures brings security improvements to final product
- Certification based on new specific Protection profiles for car components allows international recognized certification

Tailored protection profiles combined with **systematic vulnerabilities identification** and **common attacks patterns** bring most powerful tools for security improvement and security assurance

DEKRA

Formal product security evaluation procedures

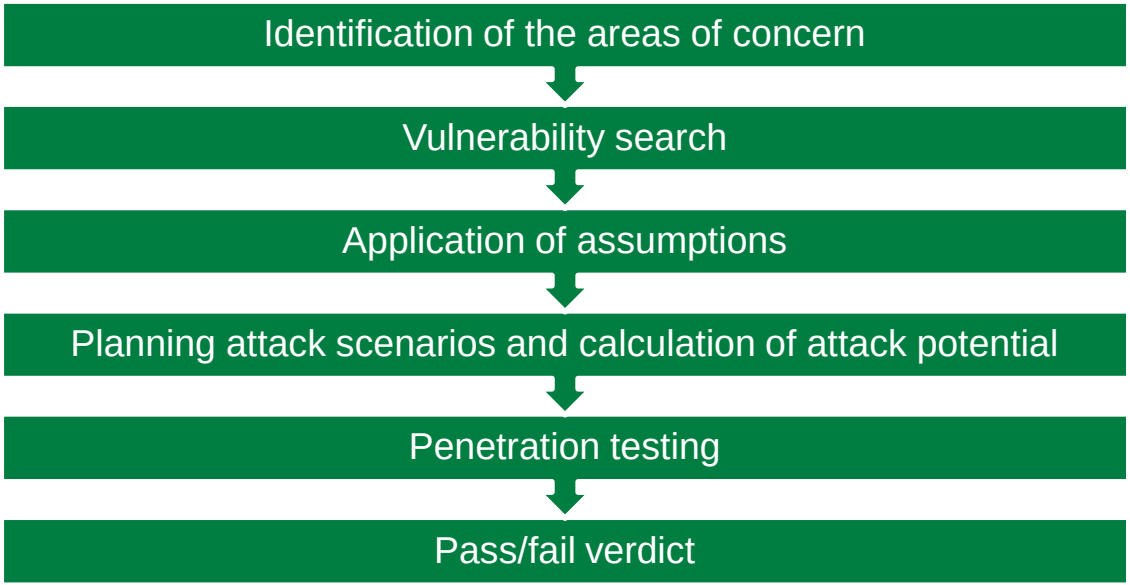
ISO 15408 Common Criteria – Evaluation Assurance Levels

- The Evaluation Assurance Level (**EAL1** through **EAL7**) of an IT product or system is a numerical grade assigned following the completion of a Common Criteria (CC) security evaluation.
- The increasing assurance levels reflect added assurance requirements that must be met to achieve CC certification.
- The intent of the higher levels is to provide higher confidence that the system's principal security features are reliably implemented.
- The **EAL** level does not measure the security of the system itself, it simply states at what level the system was tested.
- The higher EALs involve more detailed documentation, analysis, and testing than the lower ones.
- Assurance levels:

EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Functionally Tested	Structurally Tested	Methodically Tested and Checked	Methodically Designed, Tested and Reviewed	Semi formally Designed and Tested	Semi formally Verified Design and Tested	Formally Verified Design and Tested

Product Security Evaluation with ISO 15408

Flow of the ISO 15408 vulnerability assessment



Common Criteria ISO 15408 – Vulnerability Assessment

Class AVA: Vulnerability assessment

- The purpose of the vulnerability assessment activity is to determine the exploitability of flaws or weaknesses in the TOE in the operational environment.
- This determination is based upon analysis of the evaluation evidence and a search of publicly available material by the evaluator and is supported by evaluator penetration testing.

Example: Evaluation of Methodical Vulnerability Analysis (AVA_VAN.4)

- The objective of this sub-activity is to determine whether the TOE, in its operational environment, has vulnerabilities exploitable by attackers possessing Moderate attack potential.
- A methodical vulnerability analysis is performed by the evaluator to ascertain the presence of potential vulnerabilities.
- The evaluator performs penetration testing, to confirm that the potential vulnerabilities cannot be exploited in the operational environment for the TOE.
- Penetration testing is performed by the evaluator assuming an attack potential of Moderate.

CALCULATION EXAMPLE OF ATTACK POTENTIAL

Factor		Value
Elapsed time	Two weeks or less	2
Specialist expertise	Expert	6
Knowledge of evaluation target	Public	0
Window of opportunity	Unlimited access	0
Equipment	Specialized (modified tool)	4
Total (attack potential)		12

Test Validation

Security validation method:

- Security test, Penetration Test, Attack simulation
- Shall be planned at the beginning of the project
- Need specialized HW & SW tools and methods

Example: Goals for an ECU evaluation:

- Take control of the execution flow of ECU for arbitrary code execution
- Inject arbitrary CAN/LIN frames to attack ECU and other connected systems
- Demonstrate the ability to use link (USB, Bluetooth, Wifi,...) to attack ECU
- Demonstrate the ability to reach the PSA infrastructure through TCU access.

Identified vulnerability	Impact	Priority	Criticity	Difficulty
Login prompt available on serial port	DICP			Technician
Alternative root account without credentials	DICP	Critical	Very High	Technician
Firewall rules misconfiguration	DICP	Medium	Medium	Technician
Log interface on serial port	C	Weak	Weak	Technician
Debug interface available	C	Weak	Weak	N / A
Insufficient WiFi keys complexity	C P	Weak	Weak	Technician
WiFi keys stored in plain text	C P	Medium	Medium	Technician
Bypass of the update image signature	DICP	Critical	Very High	

DEFINING THE LEVEL OF EXPLOITABILITY	LEVEL
Exploitation of this vulnerability requires few resources and skills. The operation is technically affordable without special knowledge	
Exploitation of this vulnerability requires the resources and skills of a person with technical knowledge. This operation may require the use of tools or various documentations.	Technician
Exploitation of this vulnerability requires the skills of a hacker. This requires a thorough knowledge in SSI.	Hacker

ISO 15408 CC protection profiles

PROTECTION PROFILES (PP)

- A Protection Profile (PP) is a document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC). As the generic form of a Security Target (ST), it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements.
- A PP is a combination of threats, security objectives, assumptions, security functional requirements (SFRs), security assurance requirements (SARs) and rationales.
- A PP specifies generic security evaluation criteria to substantiate vendors' claims of a given family of information system products. Among others, it typically specifies the Evaluation Assurance Level (EAL), a number 1 through 7, indicating the depth and rigor of the security evaluation, usually in the form of supporting documentation and testing, that a product meets the security requirements specified in the PP.
- The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have agreed to cooperate on the development of validated U.S. government PPs.

VALIDATED PPS

Security devices with PPs

Validated US Government PP

- Anti-Virus
- Key Recovery
- Certificate Management
- Tokens
- DBMS
- Firewalls
- Operating System
- IDS/h

Validated Non-U.S. Government PP

- Smart Cards
- Remote electronic voting systems
- Trusted execution environment

ISO 15408 CC protection profiles

PROTECTION PROFILES (PP)

Dekra Cybersecurity Offering
Product Security Evaluation

PRODUCT SECURITY EVALUATION SERVICES

Packetized Security evaluation services:

- IoT devices and cloud ecosystem
- Smartphone and mobile applications
- SCADA system security evaluation
- IACS devices and OT networks
- Electronic PLCs (Achilles Certification)
- Medical Devices

Customized product Security evaluations

- Formal Security Assessment
- Penetration Testing, manually conducted by our team of cybersecurity professionals
- Covering the device itself and its whole ecosystem

PENETRATION TEST

BINARY ANALYSIS

STATIC CODE ANALYSIS

DYNAMIC RUNTIME ANALYSYS

FIRMWARE ANALYSIS

REVERSE ENGINEERING

DEKRA

EXPERT KNOWLEDGE IN CYBERSECURITY

Our group of cybersecurity evaluation engineers has extensive knowledge on the specific technologies with more than 10 years of experience on product security evaluation and pentesting, with a continuous research of security vulnerabilities and with strong technical background in:

PENTESTING

- Identify attacks surfaces.
- Identify vulnerabilities.
- Attack hardware Interfaces.
- Attacking communication protocols.
- Attacking surfaces environment (device hosts, cloud services, …).

CODE ANALISYS

- Embedded device static code analysis.
- Dynamic code analysis.
- Finding code security Flaws
- Compliance with main standards (MISRA, MISRA C, CWE,CERT C, …)

VULNERABILITY ASSESMENT

- Systematic analysis of Vulnerability identification
- Security assessment of authentication and access control, and privacy.
- Vulnerability assessment in web applications
- Vulnerability assessment in cloud interfaces and mobile interfaces

FIRMWARE ANALYSIS

- Firmware analysis and extraction.
- Finding and exploiting logic flaws.
- Extracting and running binaries.
- Bypassing stack protections.
- Mounting firmware in File systems.
- Firmware modification/persistance

DEKRA CYBERSECURITY EXPERTS

Our cybersecurity team counts with most reputed technical security certifications

TECHNICAL CERTIFICATIONS

- **OSCP**: Offensive Security Certified Professional
- **CEH**: Certified Ethical Hacker
- **Lead Auditor ISO 27001:** Information security Management
- **Reverse Engineering and Exploit Development**
- **Acunetix v10** User Test certification
- **Penetration Testing** With Kali
- Assembly Language and Shellcoding on Linux (SLAE)

PARTICIPATION AS EXPERTS IN INTERNATIONAL COMMITTEES

Our engineers works regularly with international standardization committees where International standards for cybersecurity are developed:

ISO/SAE AWI 21434: Cybersecurity engineering for Road Vehicles.

- Defining guidelines to implement security in the automotive industry products that has strong safety and security requirements.

IEC/SC65C/WG13: Cybersecurity in Industrial Networks.

- Developing standard 62443 series for security for industrial automation and control systems (IACS),
- Standard 62443-4-1.Security requirements for product development
- Standard 62443-4-2. Security technical requirements for IACS components

CONTACT INFORMATION

Joaquín Torrecilla
Chief Technology Officer

DEKRA Testing and Certification, S.A.U.

Parque Tecnológico de Andalucía
Severo Ochoa, 2 & 6 | 29590 | Málaga | Spain
Phone: +34 952 61 98 48
joaquin.torrecilla@dekra.com

Thank you

BACK UP SLIDES

Common Criteria – Vulnerability Analysis

Vulnerability Analysis Workflow VAW

PARAMETERS:

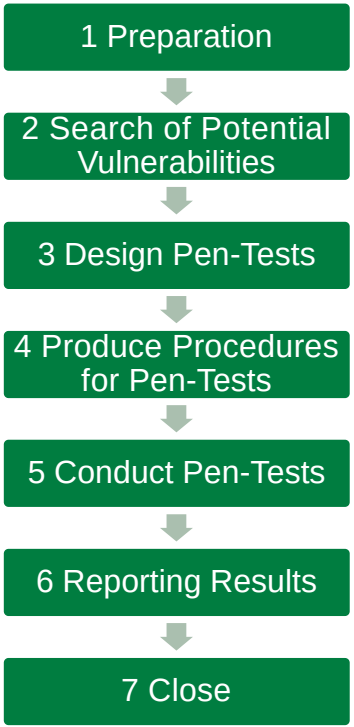
Developer VA: Yes, No

Vulnerability Identification:

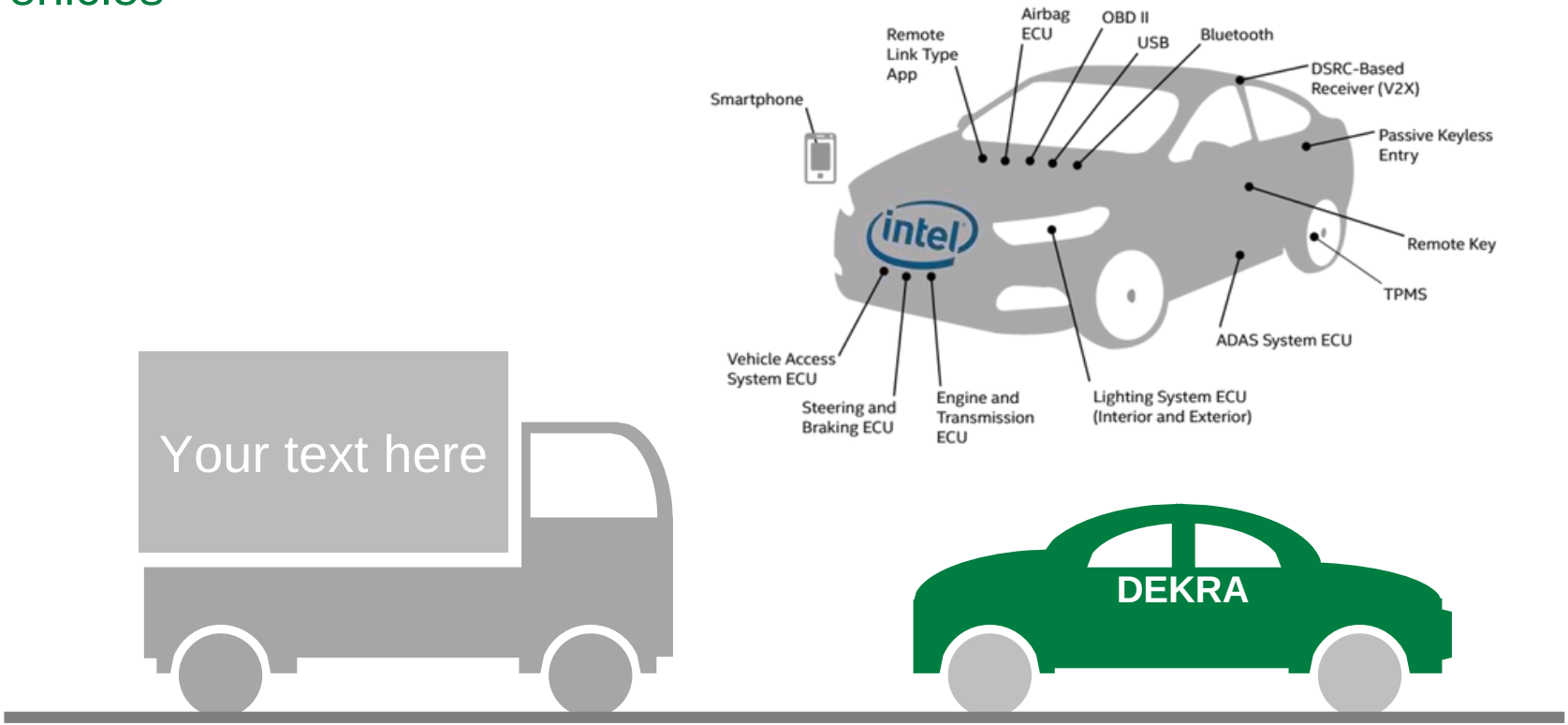
a. Source

b. Type of Search - Attack Potential:

PHASES



Vehicles



A Classification of Security Evaluation Services

Type	Description	Procedure	Comments
Penetration Testing	Exploit potential vulnerabilities in a product. Find unknown vulnerabilities	Individual analysis based on experts' knowledge and capabilities. Proprietary methodology.	
Security Assessment	Identify potential vulnerabilities through testing. Check for known vulnerabilities.	Defined evaluation procedures, with specific test details specified for each evaluation.	May include evaluation of SDLC (software development life-cycle).
Conformance testing	Check for conformance against a defined standard.	Defined evaluation and test procedures. Highly automated. Pass/fail results.	Only applicable to an specific class of product or interface.

Intensity applied

Insights gained

Evolution of Cybersecurity

Process Security is evolving to Product Security

Product security has new challenges

Components with external textboxes

- Text
- Text
- Text

- Text
- Text
- Text

- Text
- Text
- Text

- Text
- Text
- Text

- Text
- Text
- Text

- Text
- Text
- Text

- Text
- Text
- Text

- Text
- Text
- Text

Arbitrage

Lorem ipsum

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

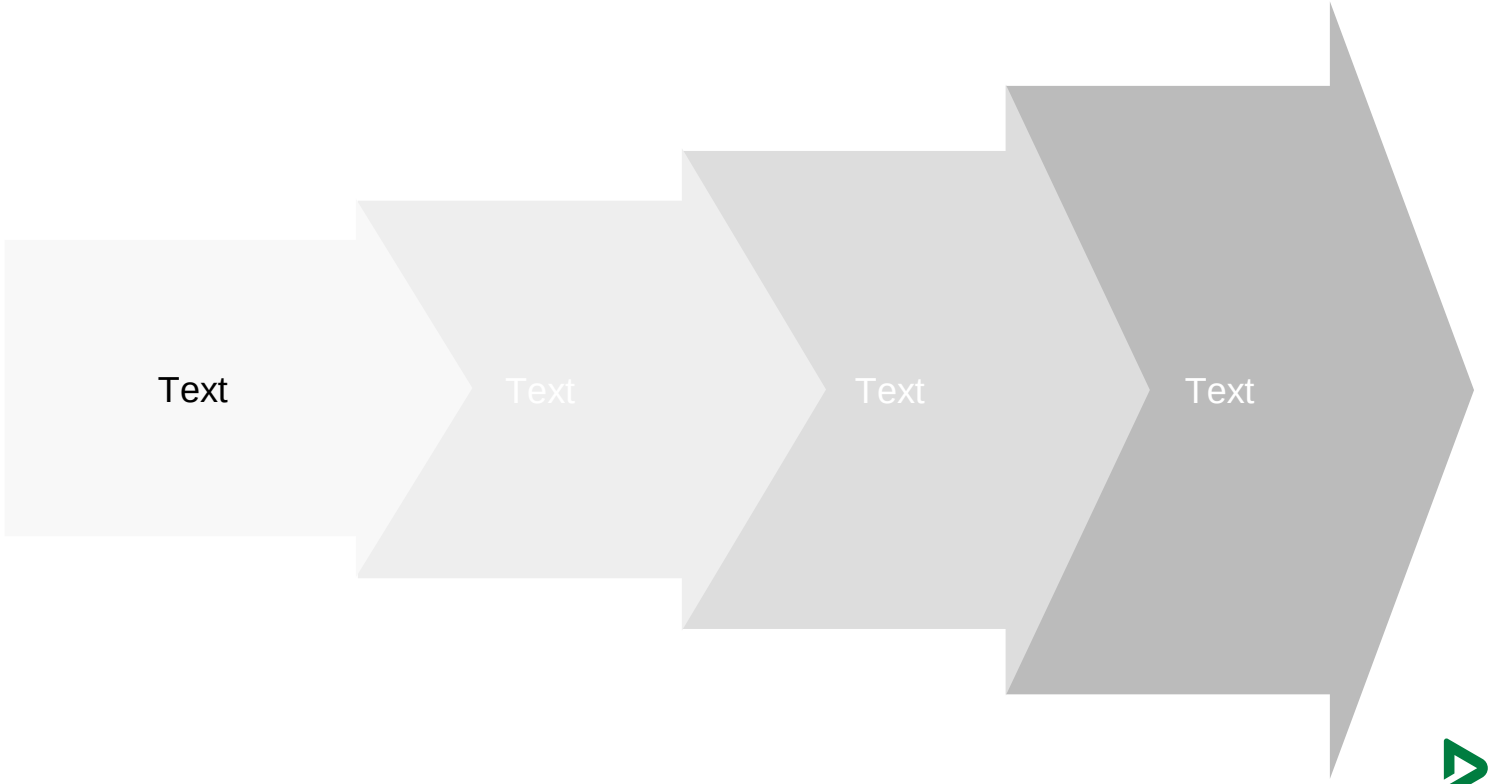
Lorem ipsum dolor sit amet

+ Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aliquam eget scelerisque turpis.
- Nam ut erat quis purus sagittis convallis eget eu tellus.

Recommendation

DEKRA

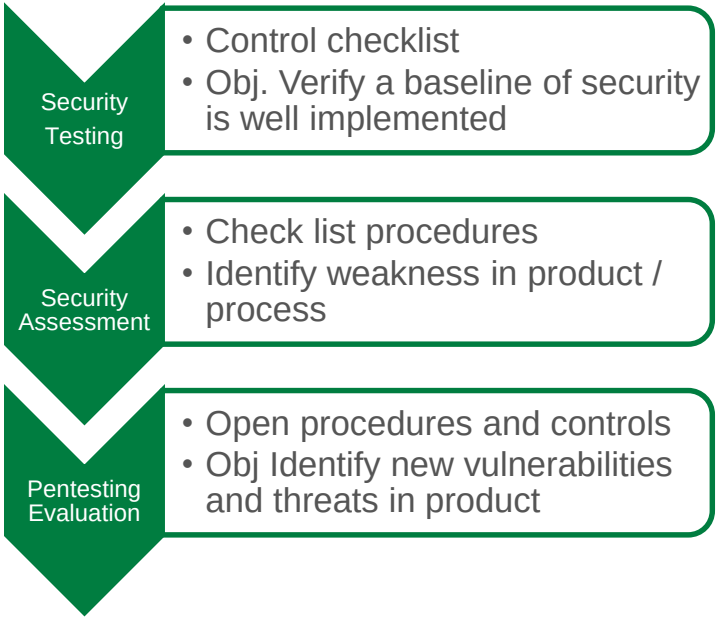
Arrow 2



TODAY

Security auditors verify the security controls implemented.

TOMORROW
New approach security audit

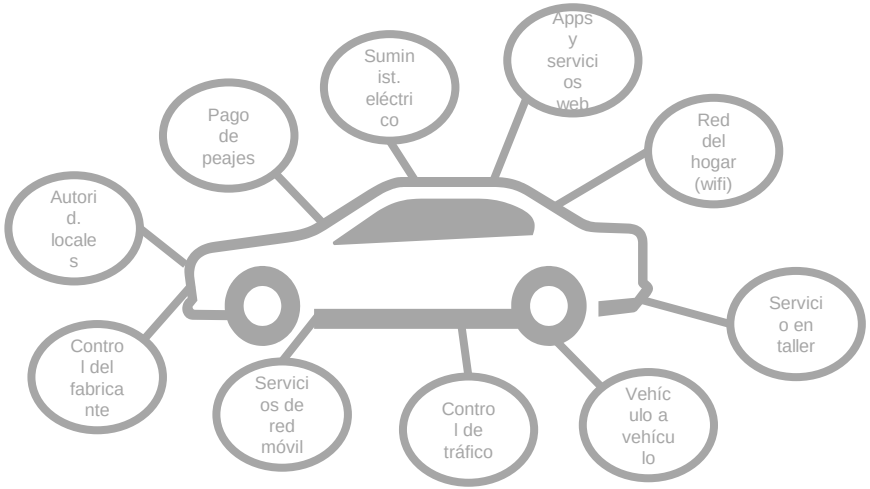


Evaluation procedures are critical to develop better products

CYBER RISK IN CONNECTED VEHICLES

Suministradores + Fabricantes

- Conectividad:
  - Corto, medio y largo alcance
  - Participantes: fabricantes, distribuidores, talleres, seguros, autoridades, otros clientes, etc.
  - Diseño basados en estándar
- Resistencia frente a ataques de interceptación, localización, disrupción (DoS)
- Afectación a la conducción asistida y autónoma
- Datos del cliente y privacidad
- Seguridad a y desde los terceros
- Protección de apps y webs

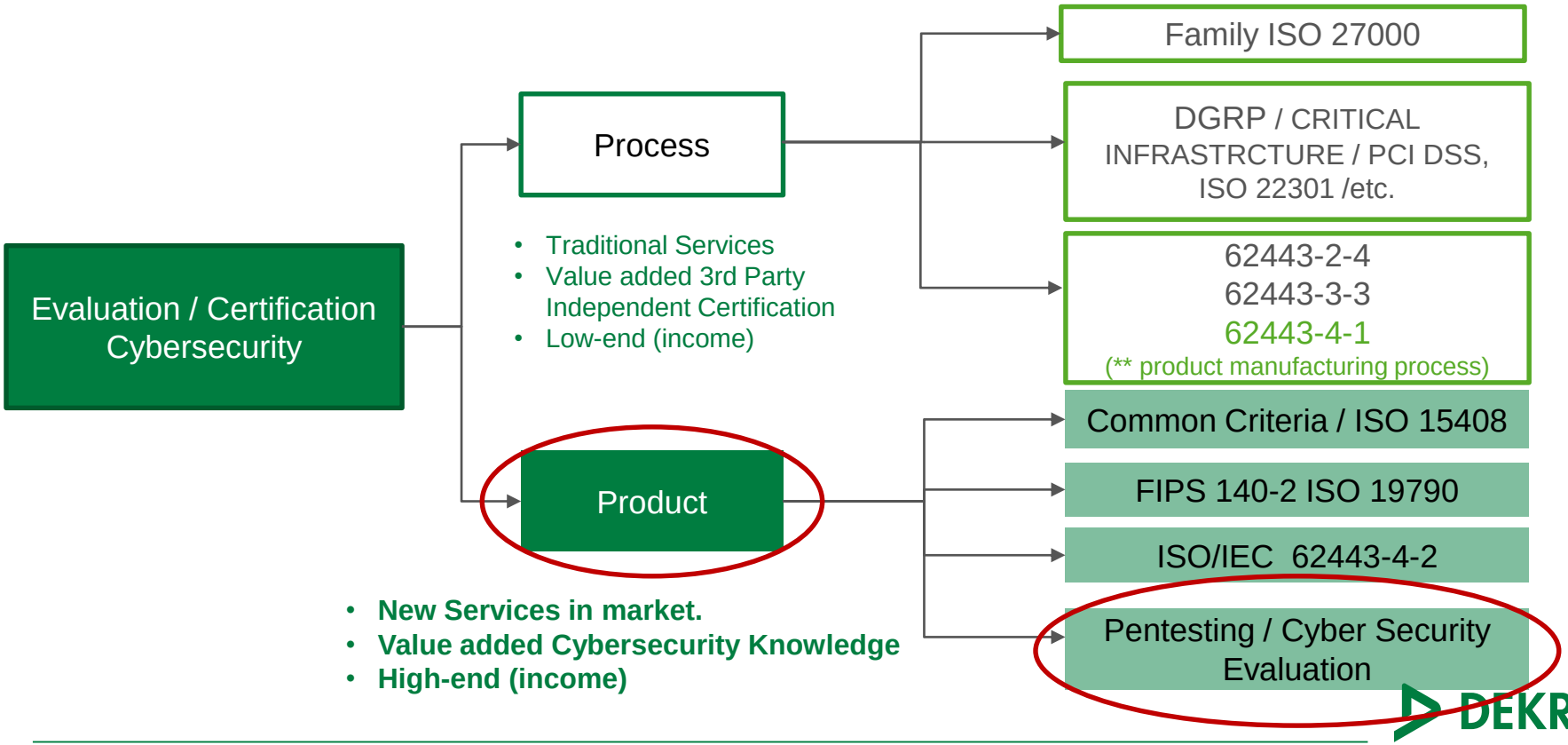


Análisis de vectores de ataque

Canales y acceso inalámbrico	V2Inet: GSM/IoT/WiFi …
	V2V: DSCR, VANET…
	V2X: bluetooth, desbloqueo …
Canales y acceso físico	

Introduction

Actual Status Cybersecurity Services in Certification / Evaluation



ekgfjgjr

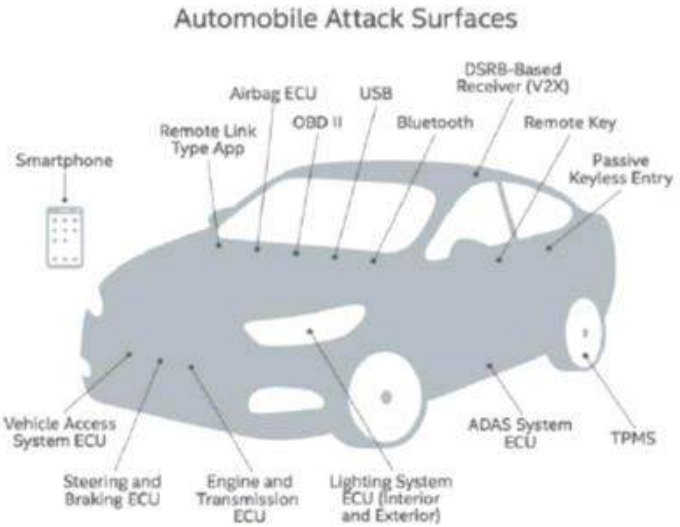


Image credit: Silicon Valley Business Journal

- CarIT Security as a standard?

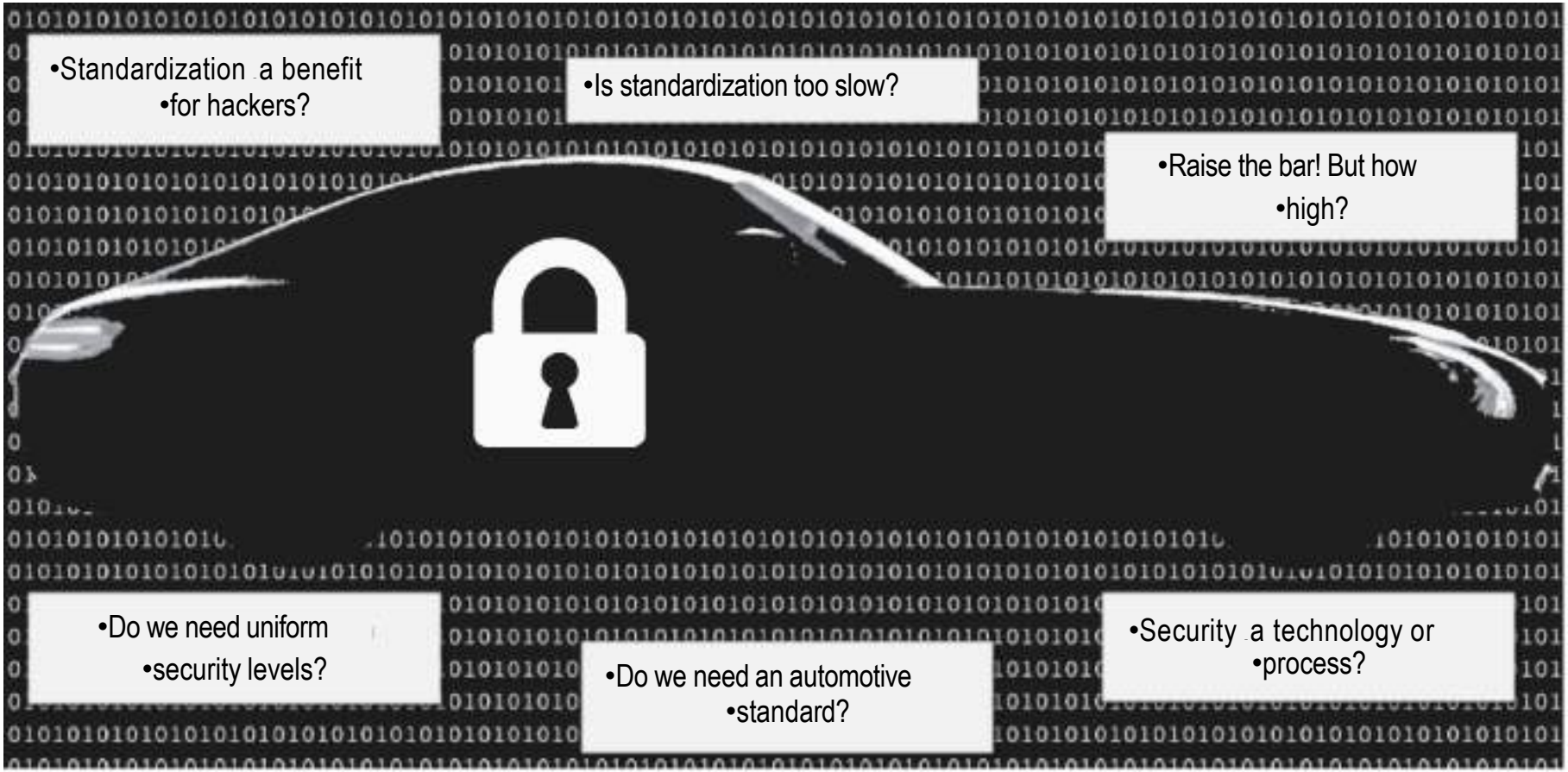
- Lorenz Slansky, 23.06.2016

Mercedes-Benz
Das Beste oder nichts.

•Agenda

1. Motivation
2. Scope of CarIT Security standardization
3. Lessons learned from other businesses
4. Do we need standardized security technologies or processes?
5. Conclusion

•CarIT Security as a standard?



•Scope of CarIT security standardization

•**DIFFERENCES IN...**

cars and architectures complexity of systems ... worldwide markets

•**BUT...**

•...same threats and vulnerabilities

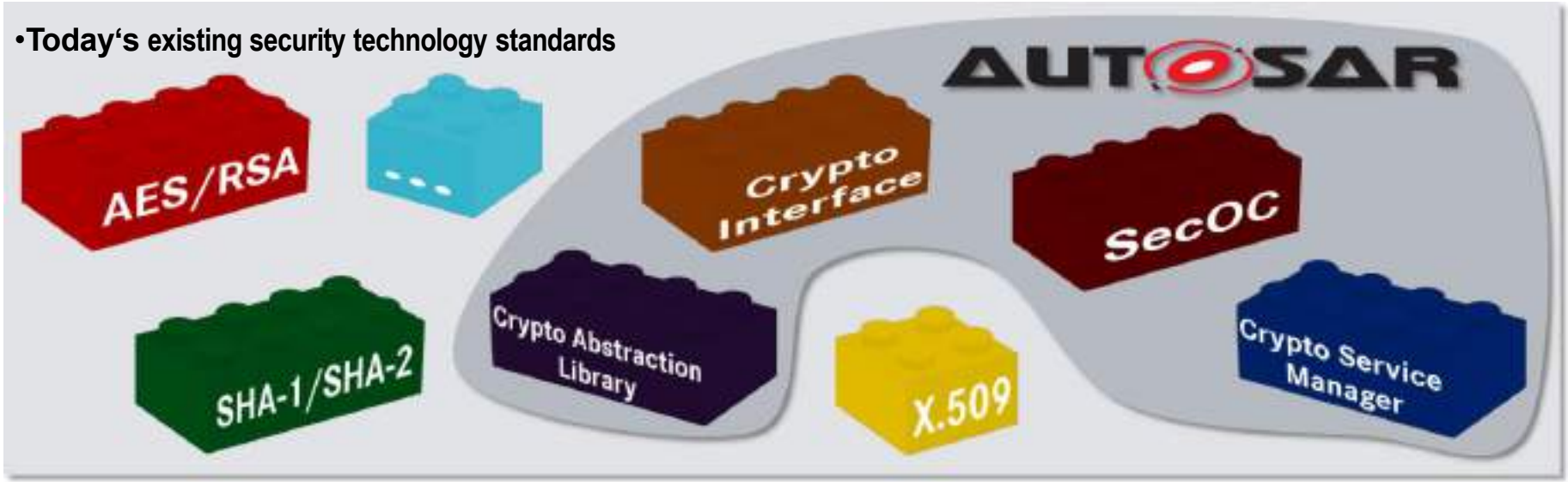
•Do we need standardized security technologies or processes?
•Lessons learned from other businesses

•Security standards

- …are used in many businesses since many years
- …should be chosen carefully
- …must be applied properly
- …make work easier, but don‘t replace a holistic security concept
- …must fulfill different legal regulations (e.g. USA, China, …)

•Security standardization in automotive business is still at the beginning

•Do we need standardized security technologies or processes?



•Do we need standardized security technologies or processes?

•Do we need standardized security technologies or processes?

•**Further need for standardization of technologies?**

•*Examples:*

•Security profiles Key management Rights management

•Do we need standardized security technologies or processes?

•Current activities in process standardization

•SAE J3061 – „Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”

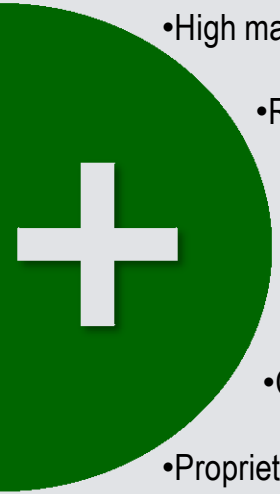
•In set-up phase: two proposals for new work items submitted – consolidation on-going

•Lessons learned from functional safety - standardization brings many benefits:

- Standardized process
- Uniform measures
- Clear criteria
- Unified safety-level
- Manageable complexity
- Homogeneous terminology
- Broad application

- Do we need standardized security technologies or processes?
- Conclusion

- Standardization takes time and by itself doesn't guarantee a higher security level, but…



- High maturity of technologies (four-eyes principle)
- Reduction of efforts and costs
- Better management of complexity
- Consideration of different perspectives gives potential for higher completeness
- Continuous improvement and extension of security measures
- Proprietary solutions might give a false sense of security ("security by obscurity")

- **Standardization is a benefit for security processes as well as technologies!**

- Think! About a standard

I WANT YOU FOR STANDARDIZATION

Mercedes-Benz