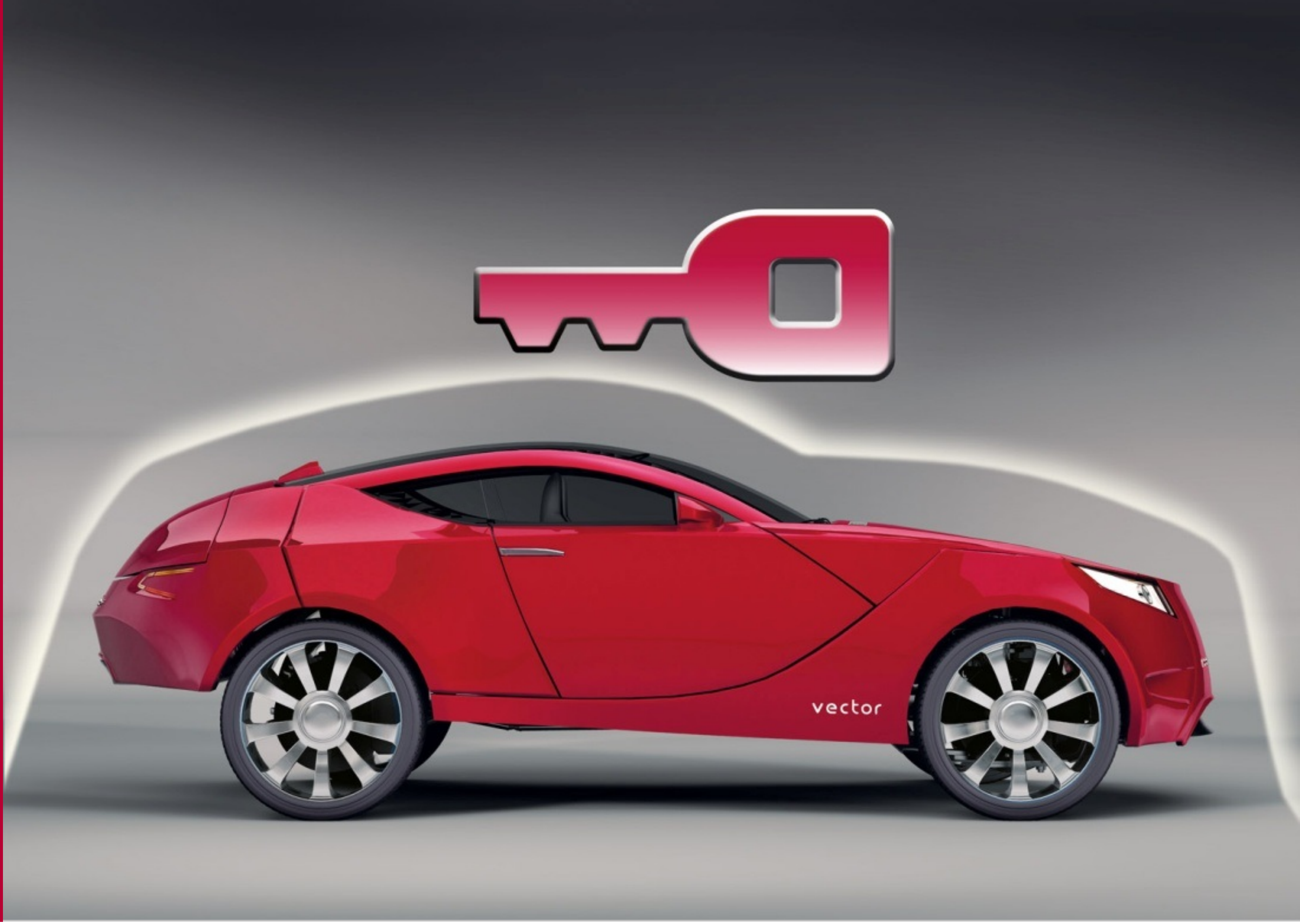


▶▶ Security in Vehicle Networks

Armin Happel, Christof Ebert

Stuttgart, 17. March 2015

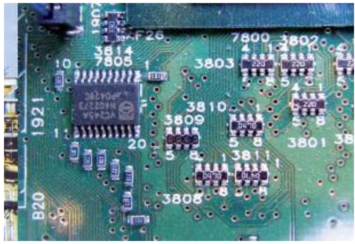
V1.1 | 2015-04-28

Vector Consulting Services

- … supports clients worldwide in improving their product development and IT and with interim management
- … with clients such as Accenture, Audi, BMW, Bosch, Daimler, Huawei, Hyundai, Lufthansa, Munich RE, Porsche, Siemens, Thales, ZF
- … offers with the Vector Group a portfolio of tools, software components and services
- … is globally present as a group with over 1300 employees and well over 250 Mio. €
- **www.vector.com / consulting**
- **www.vector.com / PREEvision**

Automotive

Aviation & Defense



IT

Energy & Environment

Medical & Healthcare

Railway & Transportation

Agenda

1. Introduction

2. Security analysis

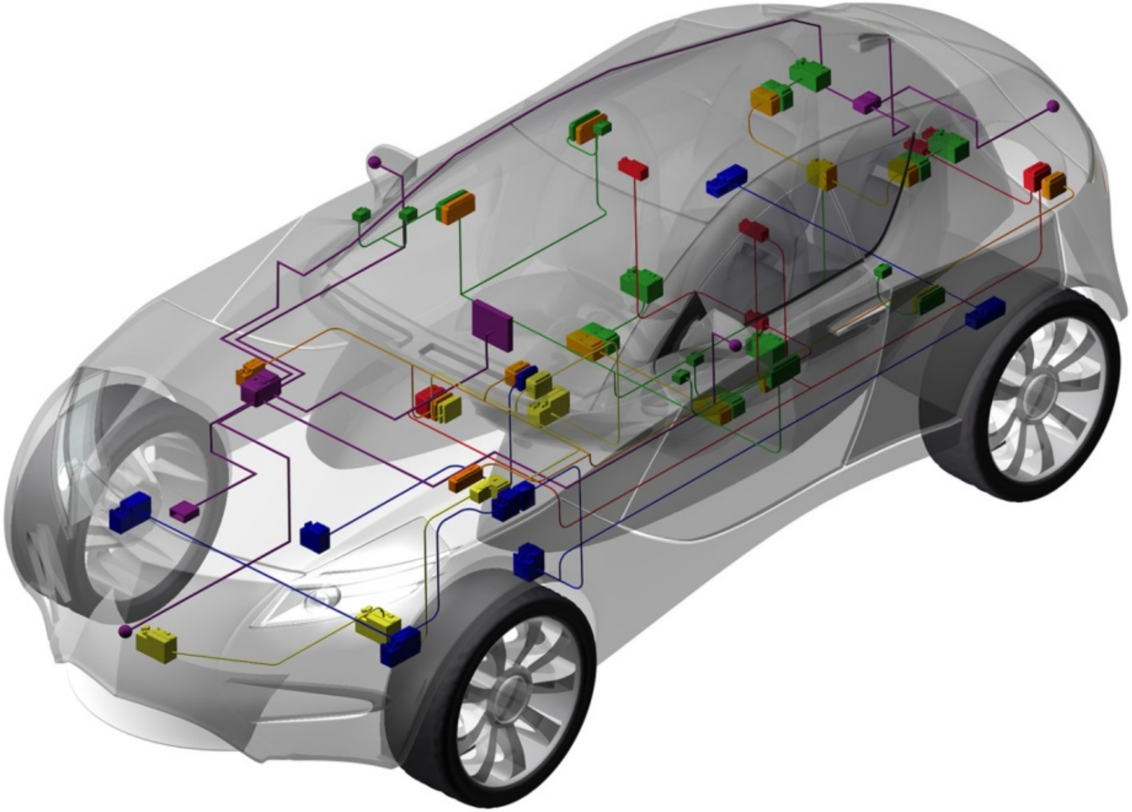
3. Software update and maintenance

4. Security key management

5. Network Strategies

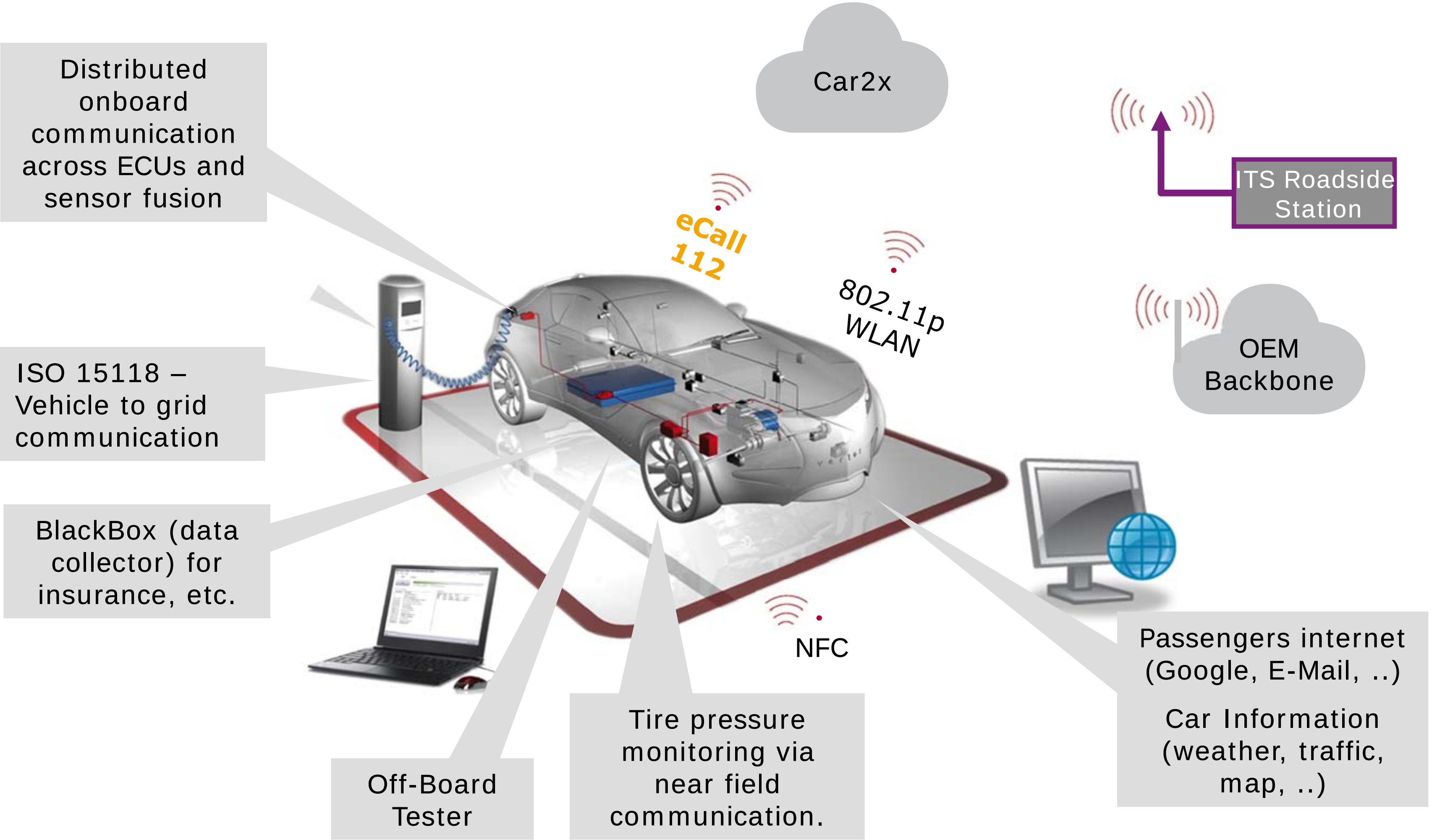
Connected Cars - Today

- Cars contain high data connectivity
- Data access is shielded within the body of the car



Connected Cars - Tomorrow

- Multiple communication paths with access to vital functionality



Distributed onboard communication across ECUs and sensor fusion

ISO 15118 – Vehicle to grid communication

BlackBox (data collector) for insurance, etc.

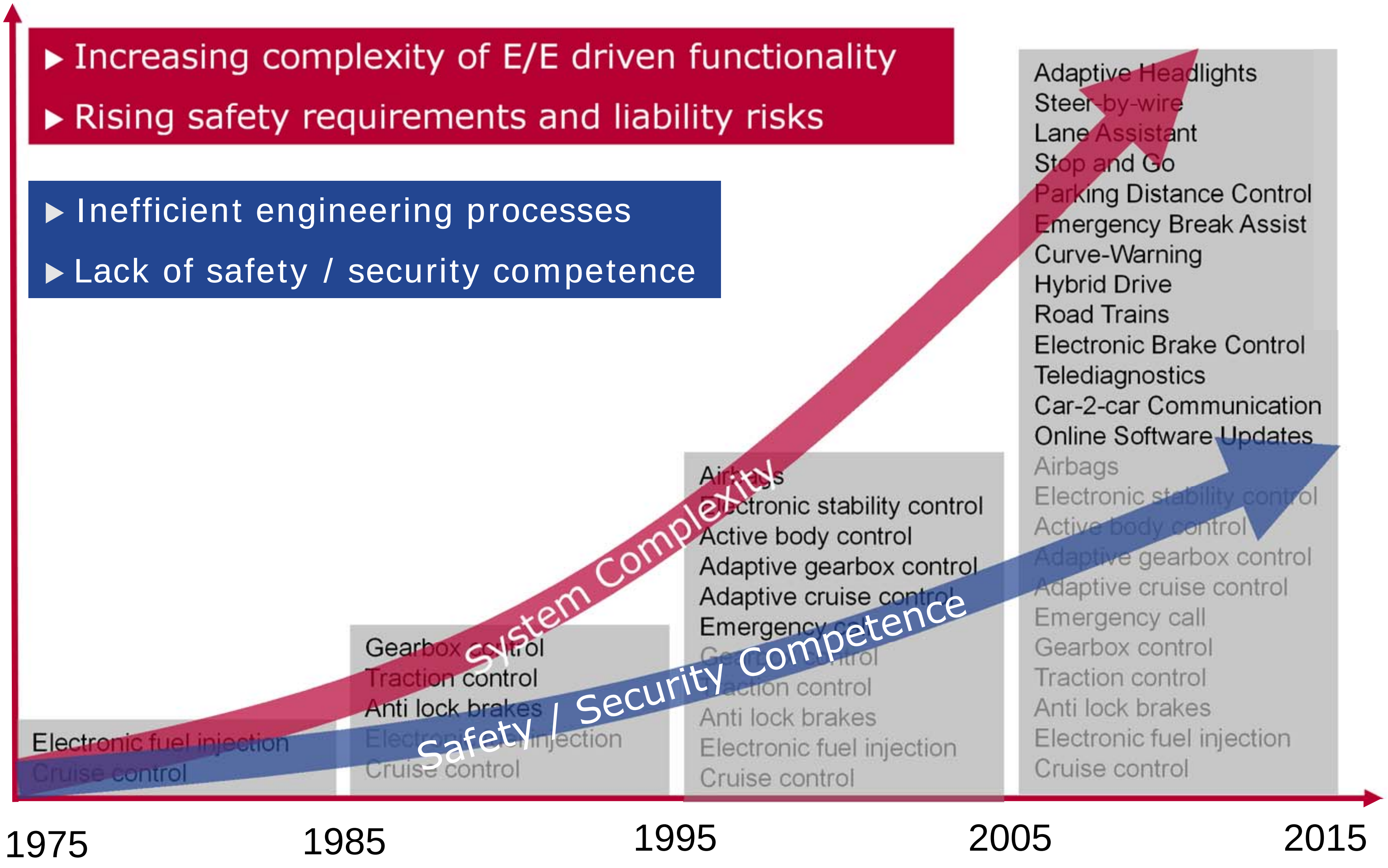
Off-Board Tester

Tire pressure monitoring via near field communication.

Passengers internet (Google, E-Mail, ..)

Car Information (weather, traffic, map, ..)

Complexity and Related Competence Gap Drive Security Risks



- Increasing complexity of E/E driven functionality
- Rising safety requirements and liability risks

- Inefficient engineering processes
- Lack of safety / security competence

Electronic fuel injection
Cruise control

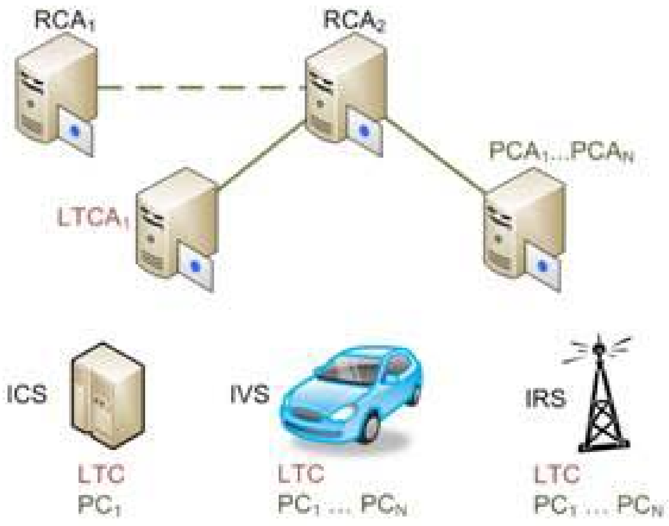
Gearbox control
Traction control
Anti lock brakes
Electronic fuel injection
Cruise control

Airbags
Electronic stability control
Active body control
Adaptive gearbox control
Adaptive cruise control
Emergency call
Gearbox control
Traction control
Anti lock brakes
Electronic fuel injection
Cruise control

Adaptive Headlights
Steer-by-wire
Lane Assistant
Stop and Go
Parking Distance Control
Emergency Break Assist
Curve-Warning
Hybrid Drive
Road Trains
Electronic Brake Control
Telediagnostics
Car-2-car Communication
Online Software Updates
Airbags
Electronic stability control
Active body control
Adaptive gearbox control
Adaptive cruise control
Emergency call
Gearbox control
Traction control
Anti lock brakes
Electronic fuel injection
Cruise control

Security projects for car2x

- Standardization across OEMs and countries needed!
- Projects for Car-2-x
  - SeVeCom (2006-2009, www.sevecom.org)
  - EVITA (2008-2011, www.evita-project.org)
  - SIMTD (2008-2013, www.simtd.de)
  - PRESERVE (2011-2015, www.preserve-project.eu)
  - C2C-CC and ETSI TC ITS WG
- Defined a reference architecture
  - Communication participants
  - Hardware and software requirements
- Determined relevant use cases
  - Scenarios for communication
  - Define involved participants
- Identified threats and risks.
  - Software is never perfect.
  - Remote access provides attack surface.
- Derive hardware and protocol requirements

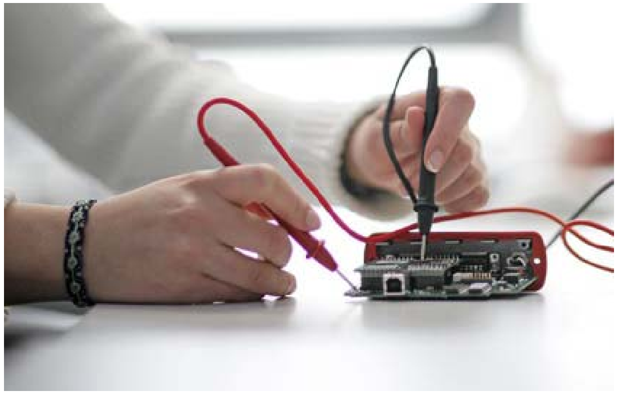


Source: ETSI Security Workshop

Agenda

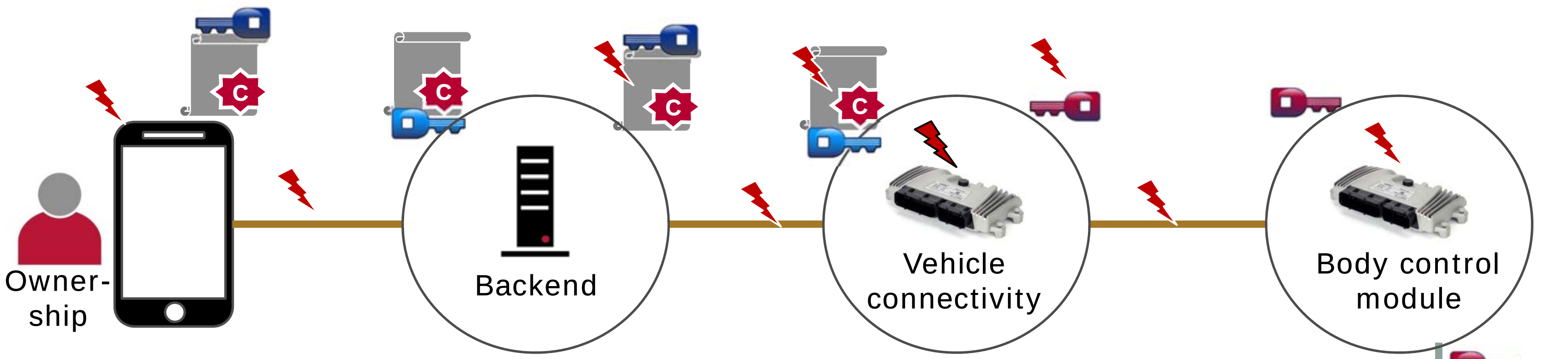
1. Introduction
2. Security analysis
3. Software update and maintenance
4. Security key management
5. Network Strategies

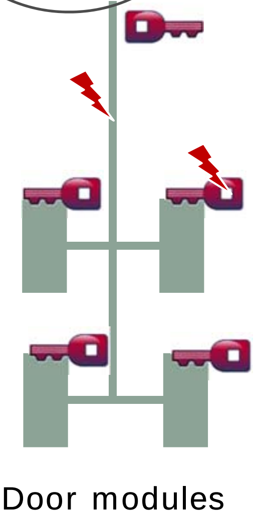
Car hacking analysis



- Physical access to the device
  - Details about the internal hardware
  - Eavesdropping of internal communication
  - Code and data could be extracted.
  - Disassembling the executable code.
- Weakness in the protocols
  - Usage of outdated and insecure crypto algorithm (DES)
  - Replay attacks possible
  - Partly unencrypted communication between ECU and backend.
  - Alert protocol provides failure information (?).
- Weakness in key management and storage.
  - Same key is used for all ECUs!
  - Keys are not stored in a secure memory area.
- No authentication and integrity check for transferred files.
- (No need for advanced hacking line timing analysis or side channel attacks)

Example: Door unlock



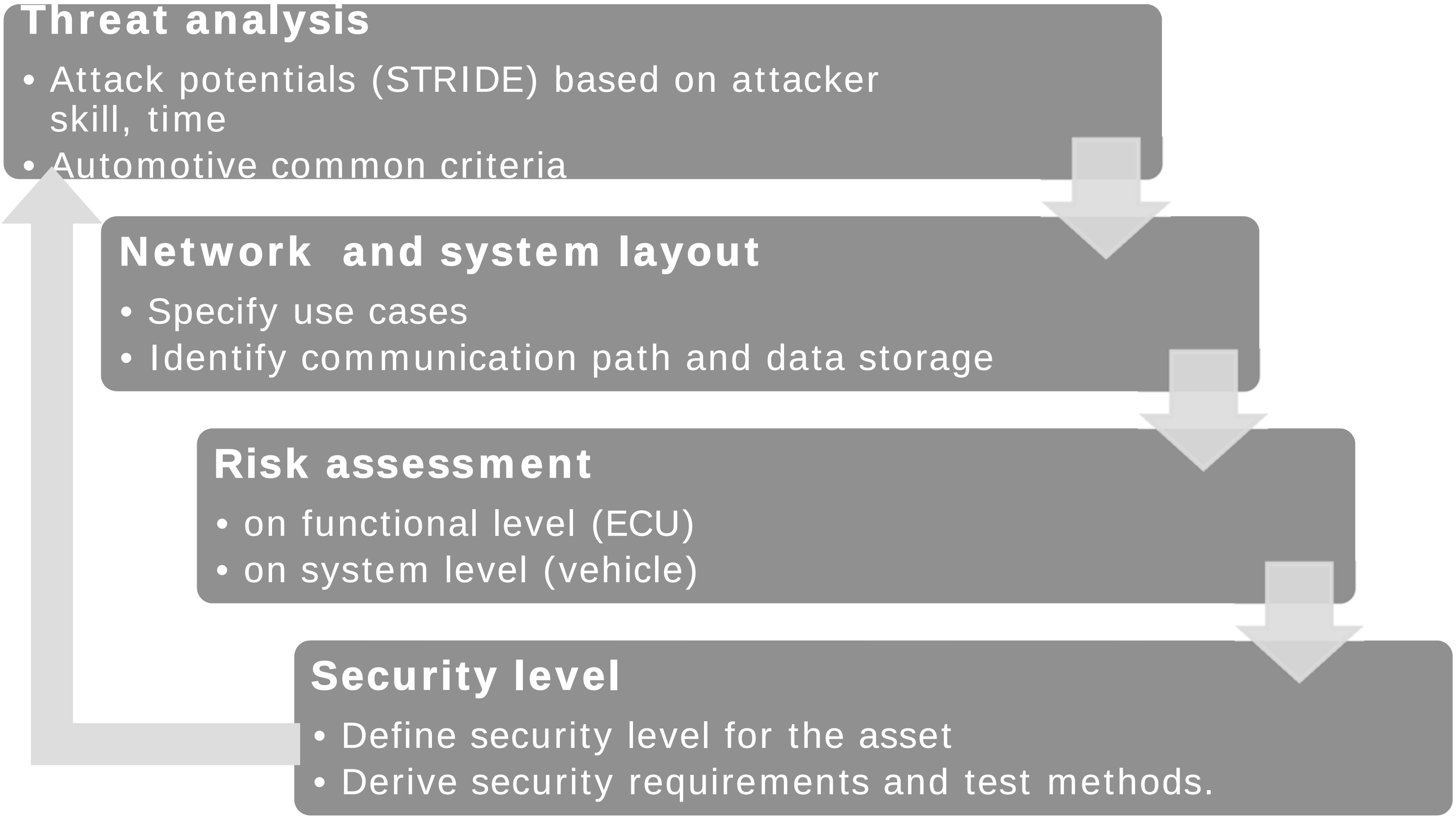


- **Assets**
  - Data along the communication path:
    - Off-board communication between backend and connectivity.
    - On-board communication between connectivity and BCM.
    - Communication between BCM and modules.
  - Security keys of the devices.

- **Threats**:
  - Device manipulation.
  - Compromising keys.
  - Man-in-the-middle.
  - Gaining access control.
  - Denial of services

- **Impacts**:
  - Safety functions.
  - Financial loss.
  - Manufacturer reputation
  - System malfunction
  - Privacy information disclosure

Systematic security analysis approach



Threat analysis

- Attack potentials (STRIDE) based on attacker skill, time
- Automotive common criteria

Network and system layout

- Specify use cases
- Identify communication path and data storage

Risk assessment

- on functional level (ECU)
- on system level (vehicle)

Security level

- Define security level for the asset
- Derive security requirements and test methods.

➔ Vector Security Check relates specific automotive risks

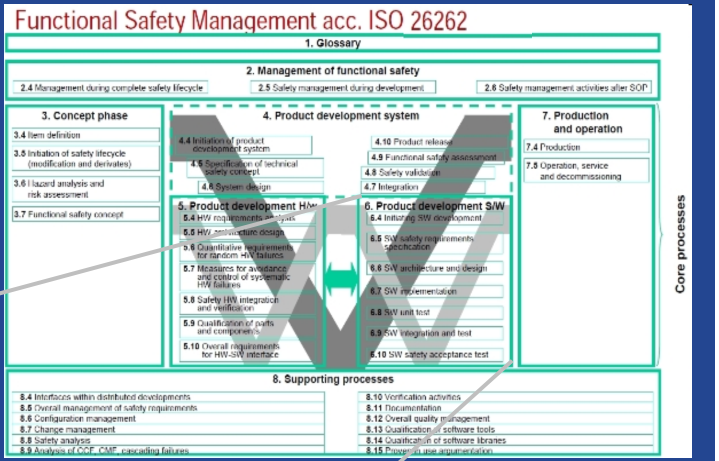
➔ Ensure cost/benefit balance by prioritized security/threat targets

Security Directly Impacts Safety

Functional Safety (ISO 26262)

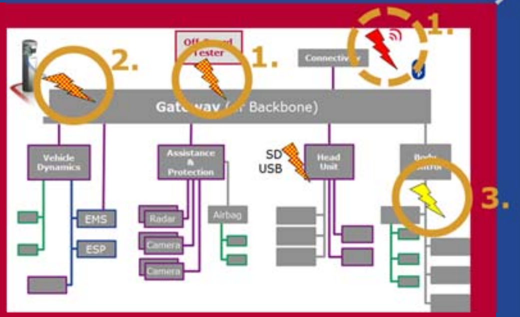
- Hazard and risk analysis
- Functions and risk mitigation
- Safety engineering

Security demands implicitly addressed


Functional Safety Management acc. ISO 26262
1. Glossary
2. Management of functional safety
2.4 Management during complete safety lifecycle
2.5 Safety management during development
2.6 Safety management activities after SOP
3. Concept phase
3.4 Item definition
3.5 Initiation of safety lifecycle (modification and derivates)
3.6 Hazard analysis and risk assessment
3.7 Functional safety concept
4. Product development system
4.4 Initiation of product development system
4.5 Specification of technical safety concept
4.6 System design
4.7 Integration
4.8 Safety validation
4.9 Functional safety assessment
4.10 Product release
5. Product development H/w
5.4 HW requirements analysis
5.5 HW architecture design
5.6 Quantitative requirements for random HW failures
5.7 Measures for avoidance and control of systematic HW failures
5.8 Safety HW integration and verification
5.9 Qualification of parts and components
5.10 Overall requirements for HW-SW interface
6. Product development S/W
6.4 Initiating SW development
6.5 SW safety requirements specification
6.6 SW architecture and design
6.7 SW implementation
6.8 SW unit test
6.9 SW integration and test
6.10 SW safety acceptance test
7. Production and operation
7.4 Production
7.5 Operation, service and decommissioning
Core processes
8. Supporting processes
8.4 Interfaces within distributed developments
8.5 Overall management of safety requirements
8.6 Configuration management
8.7 Change management
8.8 Safety analysis
8.9 Analysis of CCF, CMF, cascading failures
8.10 Verification activities
8.11 Documentation
8.12 Overall quality management
8.13 Qualification of software tools
8.14 Qualification of software libraries
8.15 Proven in use argumentation

+ Security

- Security threats
- Misuse cases and mitigation
- Security engineering



For better efficiency and clear focus security engineering should be embedded to safety framework from hazards to after-sales updates

Towards Automotive Common Criteria

- **Goal**
  Consistent security evaluation and certification of products and protection profiles
- **Applicability**
  Operating systems, key management systems, ICs, smart cards, crypto libraries, …
  Common criteria have been adopted for different critical systems, such as automation, aerospace, defense,
- **Approach**
  ISO 15408: 7 Evaluation Assurance Levels (EAL) for security requirements
  ISO 27001: techniques for security engineering
- **Automotive experiences**
  - Many automotive players so far have unclear security targets and thus no consistent consideration in architecture and life-cycle processes
  - Unnecessary high risk and cost due to overdoing in one area – and failing on others

Tailored protection profile combined with systematic safety/security engineering provide a thorough yet cost-effective solution.

Agenda

1. Introduction

2. Security analysis

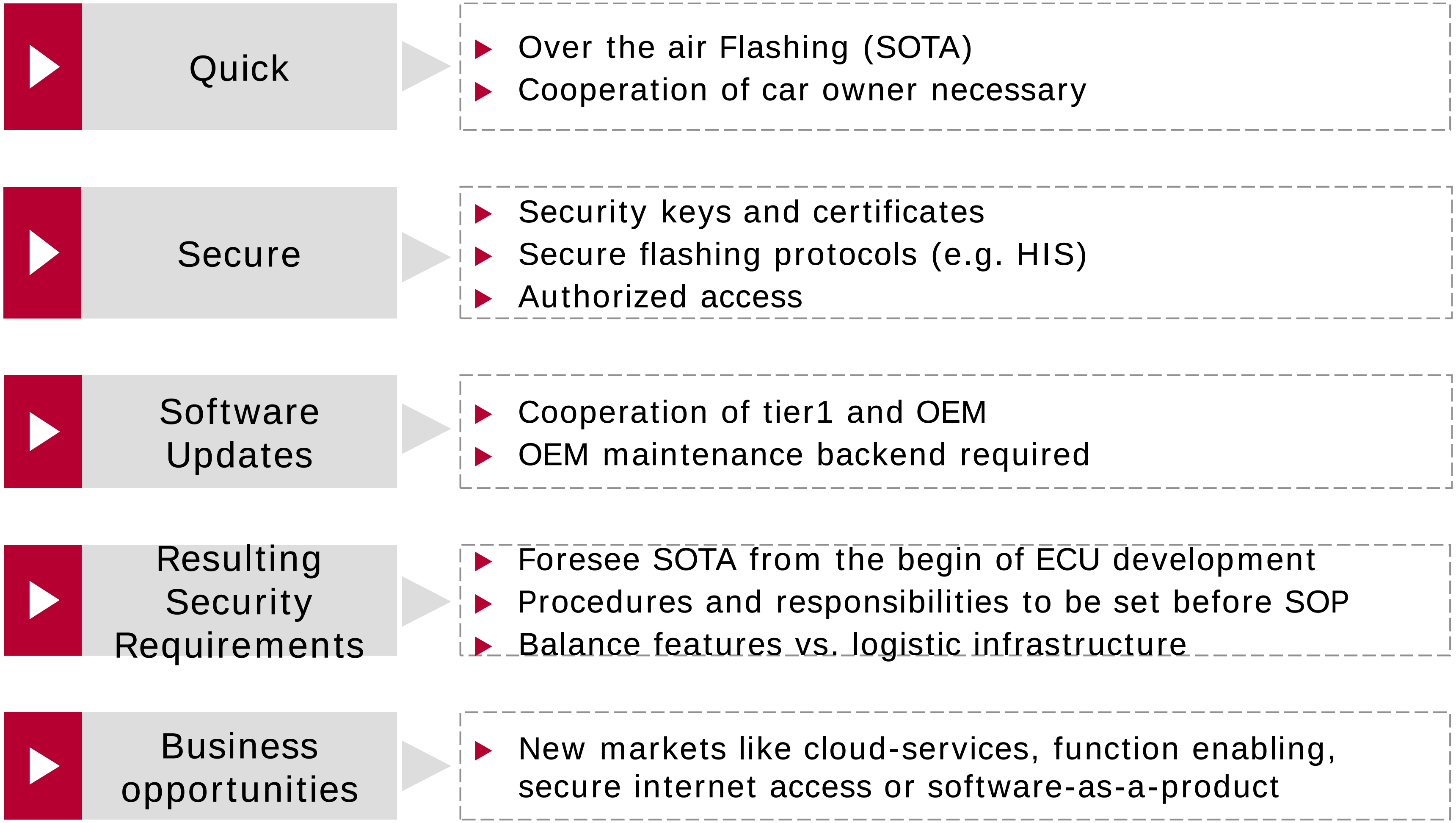
3. **Software update and maintenance**

4. Security key management

5. Network Strategies

Software update and maintenance

New security need: Quick and secure software updates



Quick

- Over the air Flashing (SOTA)
- Cooperation of car owner necessary

Secure

- Security keys and certificates
- Secure flashing protocols (e.g. HIS)
- Authorized access

Software Updates

- Cooperation of tier1 and OEM
- OEM maintenance backend required

Resulting Security Requirements

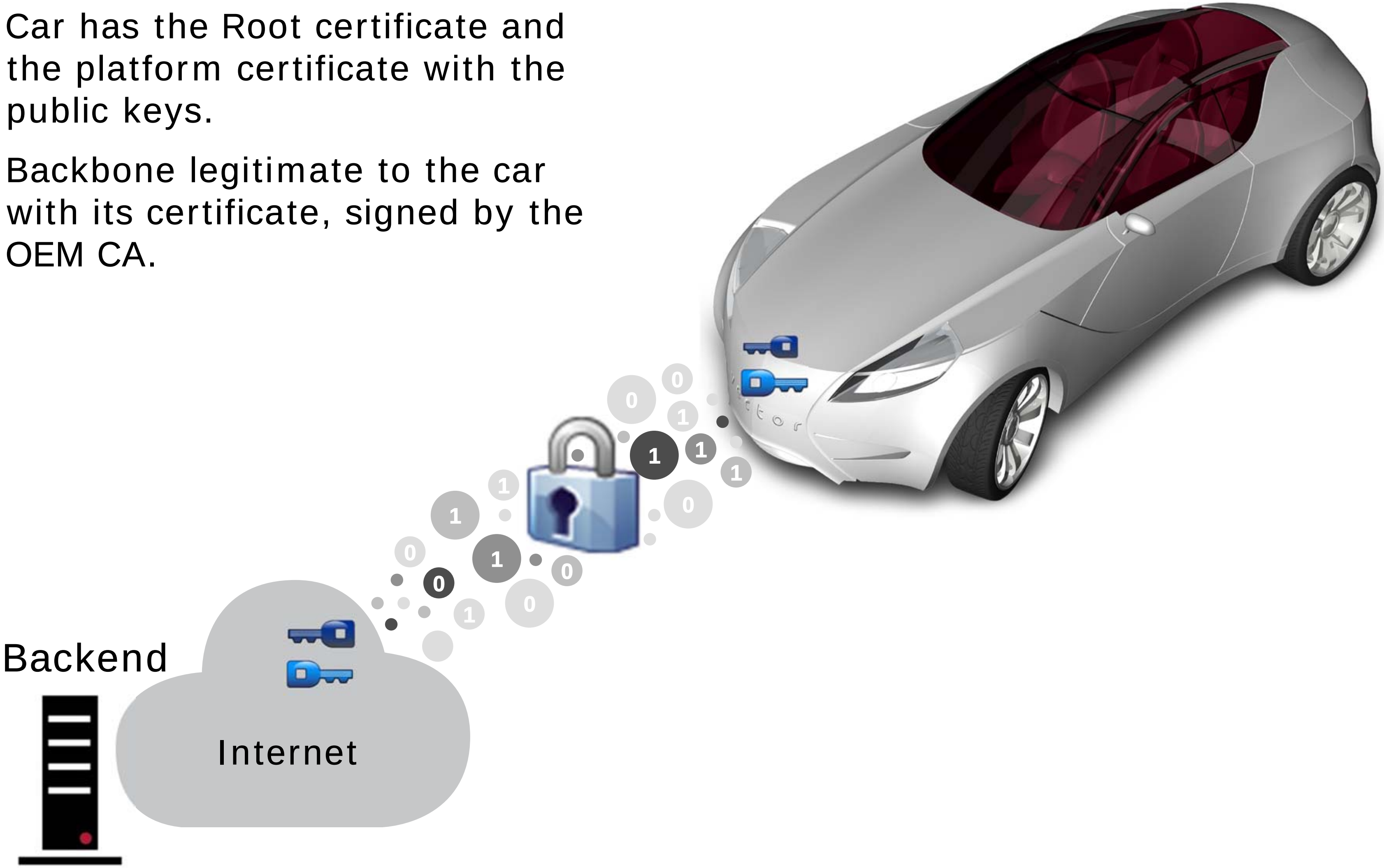
- Foresee SOTA from the begin of ECU development
- Procedures and responsibilities to be set before SOP
- Balance features vs. logistic infrastructure

Business opportunities

- New markets like cloud-services, function enabling, secure internet access or software-as-a-product

Software update over the air (SOTA)

- Car has the Root certificate and the platform certificate with the public keys.
- Backbone legitimate to the car with its certificate, signed by the OEM CA.

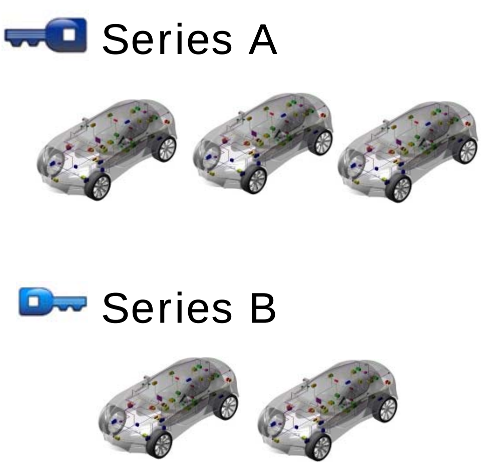


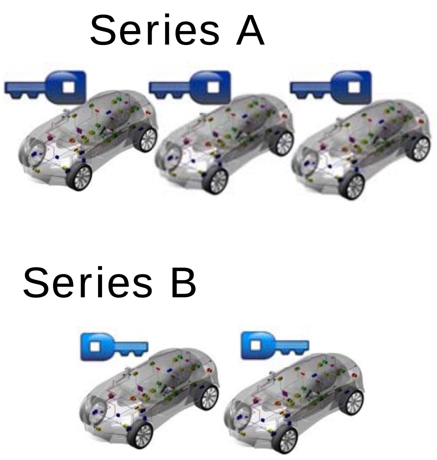
Agenda

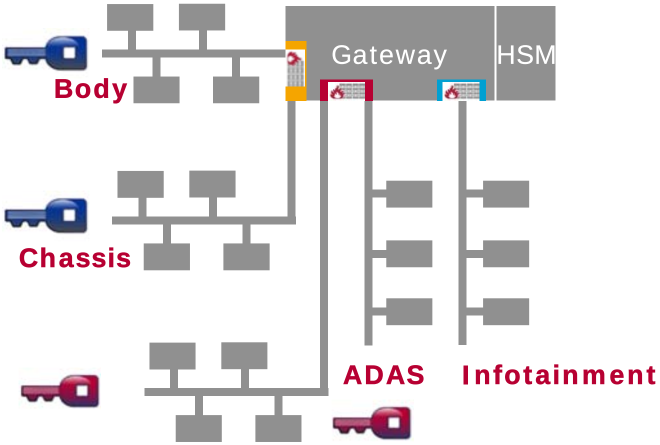
1. Introduction
2. Security analysis
3. Software update and maintenance
4. Security key management
5. Network Strategies

Key management along ECU lifecycle

	few	many
Management	simple	complex
Risk	high	low



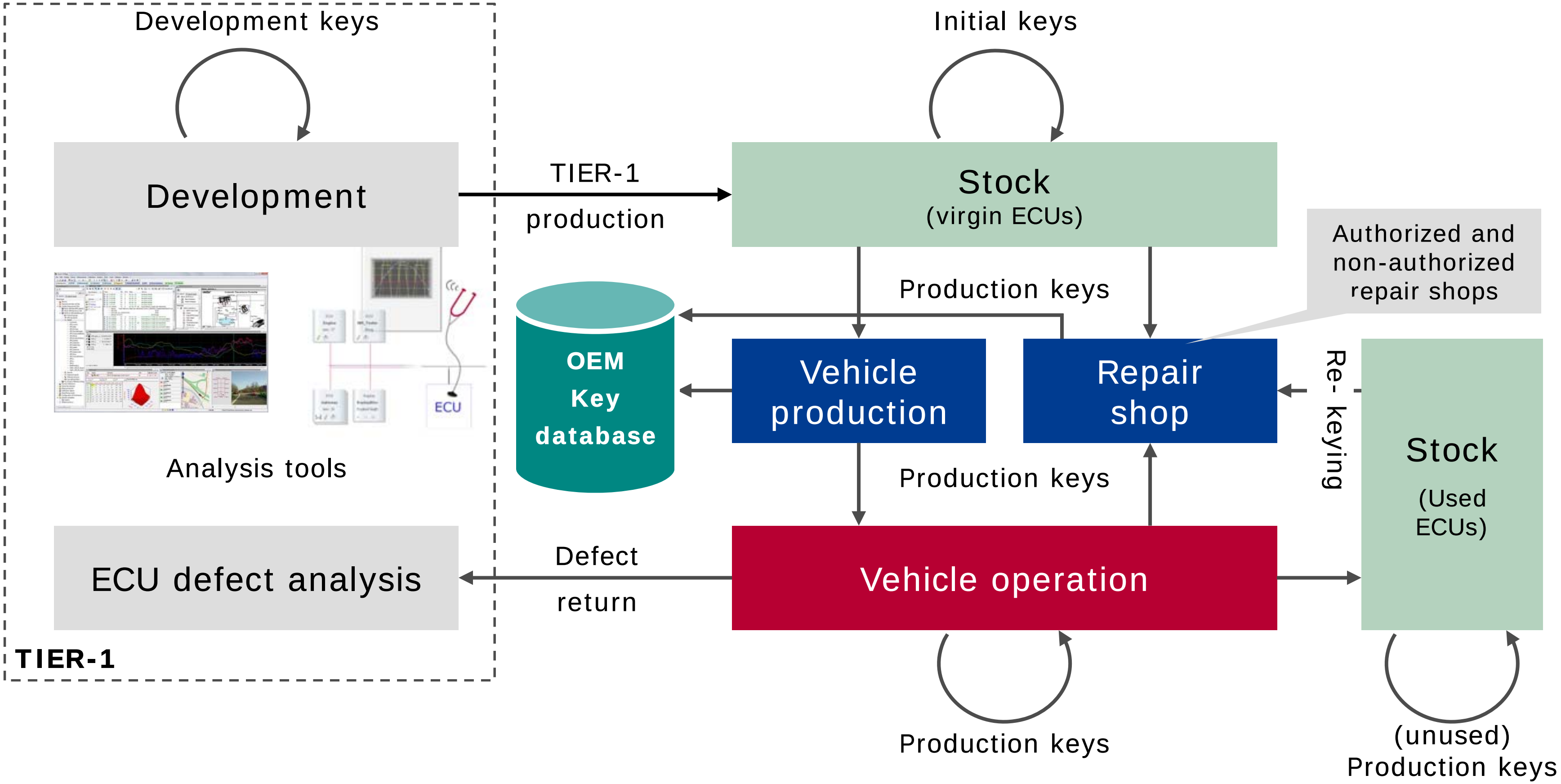




Key management lifecycle

- Development phase
- Failure analysis

- Production phase
- In-field / After-sales



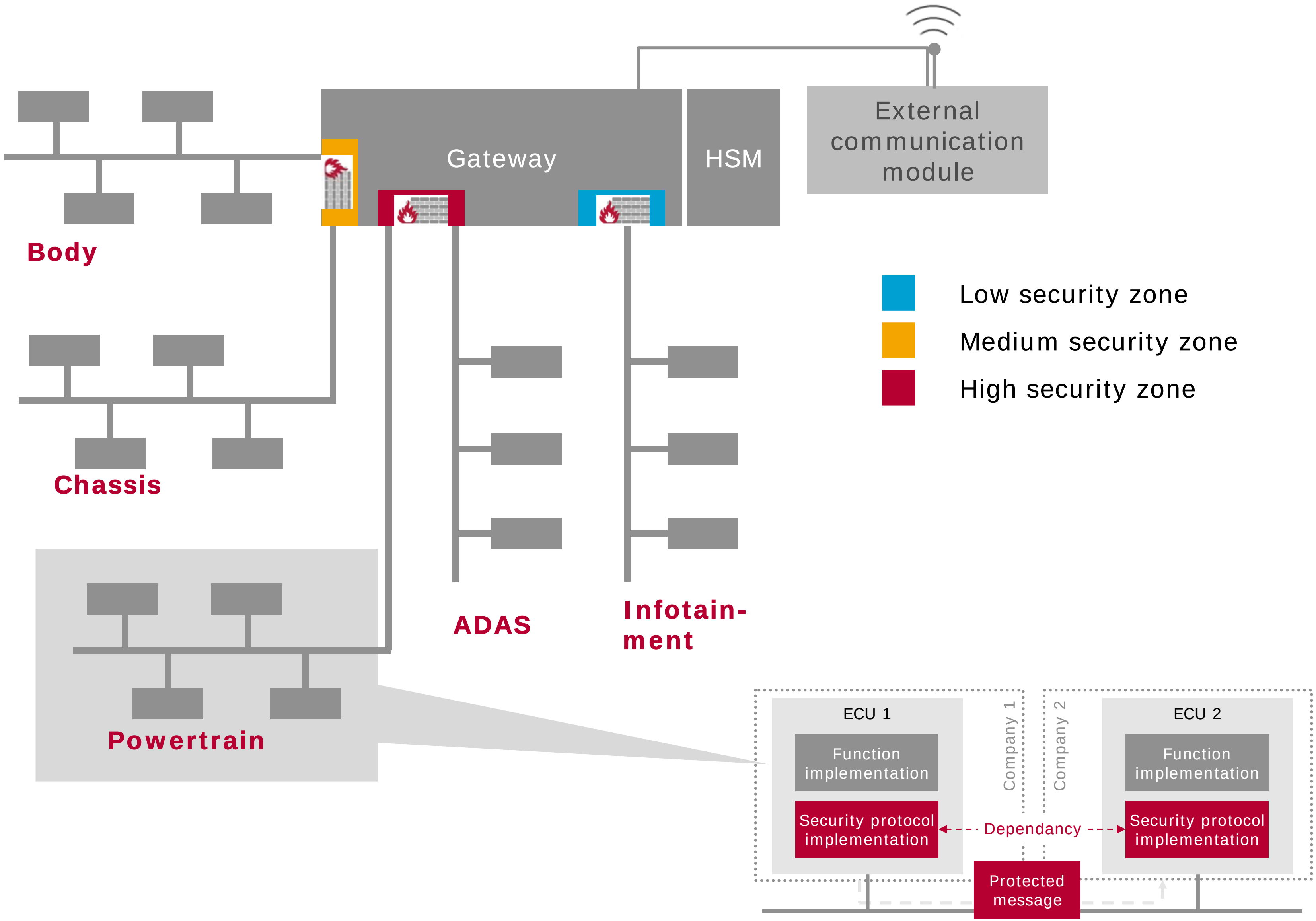
Agenda

1. Introduction
2. Security analysis
3. Software update and maintenance
4. Security key management
5. Network Strategies

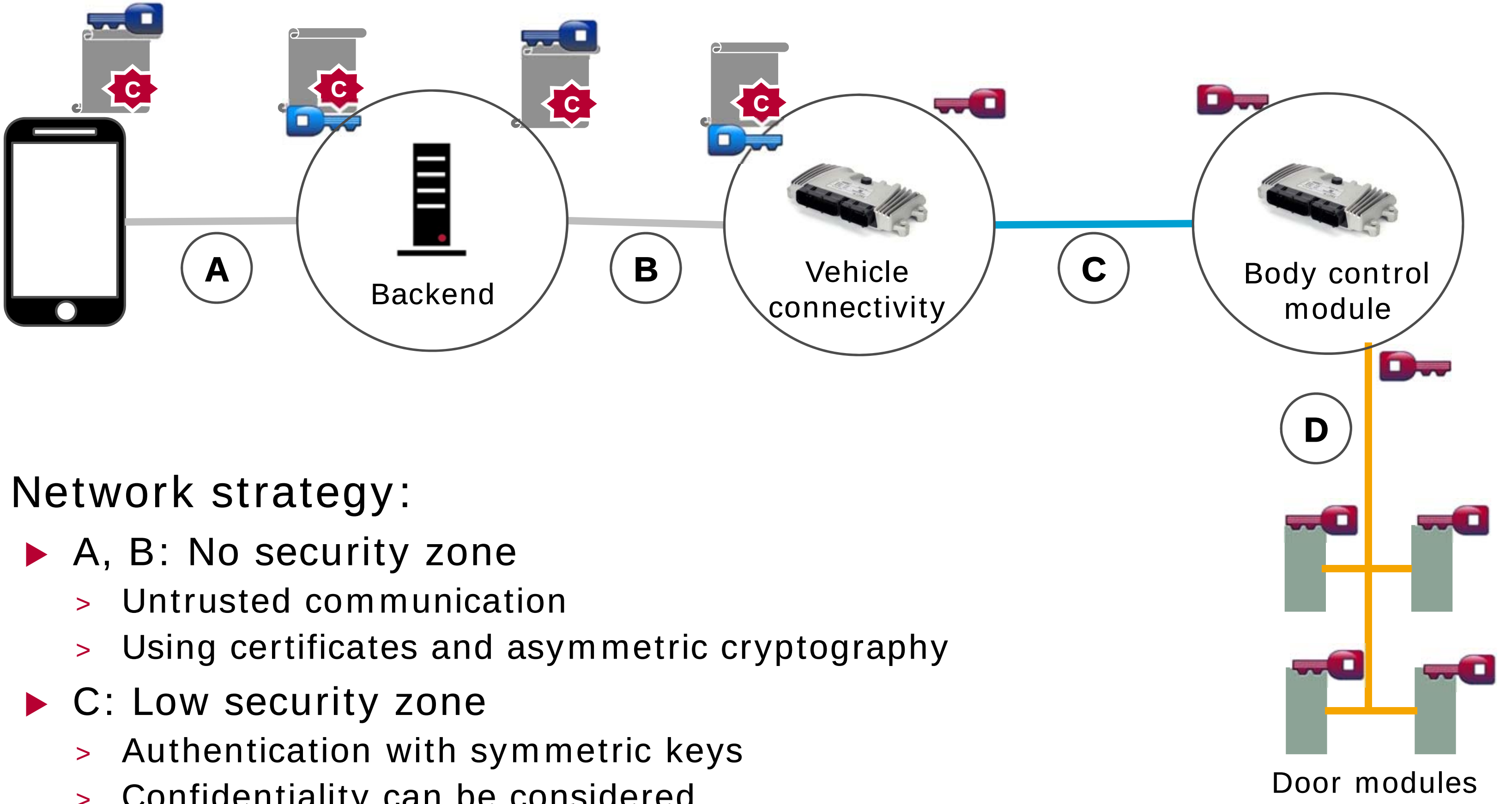
Network Strategies

- Learn from IT Business Know-how
  - Adoption of methods, such as automotive common criteria
  - Governance criteria for security engineering along the life-cycle
- Computers are grouped to separate networks
  - depending on their use case and traffic
  - Depending on the security level of their data assets
  - The access to computers is restricted by the structure of the network.
- Security components like firewall and router to separate networks.
  - A router passes only the relevant and allowed data from one network to the other.
  - A firewall integrated into a router controls the access to the internet.
- Security maintenance can be restricted to updates of the central routers

Network Strategies



Example: Door unlock



- Network strategy:
  - A, B: No security zone
    - Untrusted communication
    - Using certificates and asymmetric cryptography
  - C: Low security zone
    - Authentication with symmetric keys
    - Confidentiality can be considered.
    - Key storage important
  - D: Medium security zone
    - Encapsulated communication area
    - Authentication with symmetric keys

⬜ No security zone
🟦 Low security zone
🟧 Medium security zone
🟥 High security zone

Outlook: Security will ramp up fast

Security Engineering

- Systematic security engineering activities from requirements onwards
- Automotive security common criteria building upon from ISO 15408 etc.
- Security policies and governance
- Thorough training of engineers

Network strategies

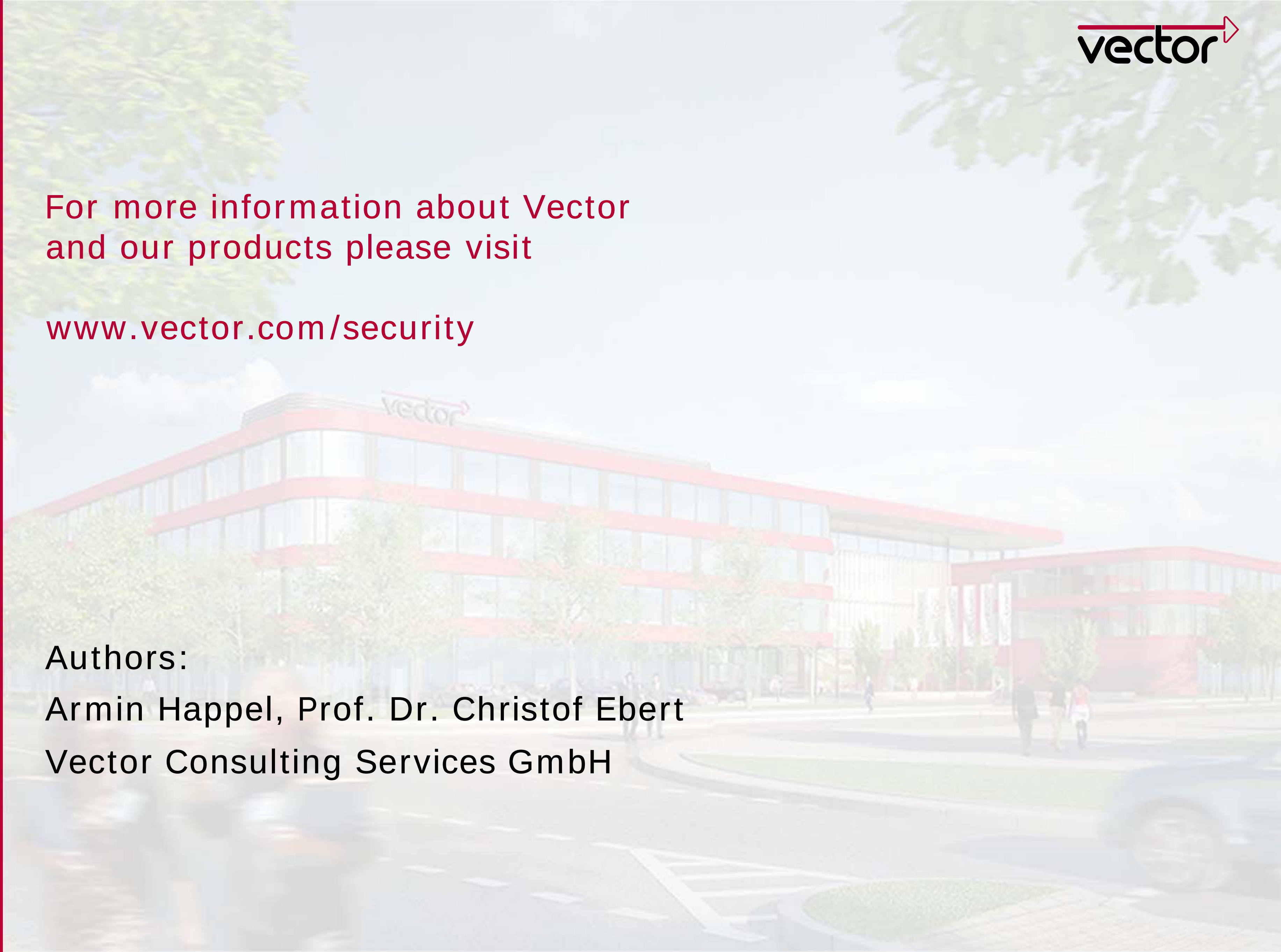
- Automatic data distribution and usage analysis in the network
- Consistent network structure according to security requirements
- Encapsulate nodes and networks with remote access
- Firewalls and secure communication bottom up from ECU and base software

Software update and maintenance

- More thorough and systematic Firewall and protection concepts
- Secure over-the-air (OTA) updates for vulnerabilities with secure cloud services for function upgrades
- Consistent intrusion detection and reporting, with fast counter measures

Security key management

- End-to-end secure key management over the life cycle of the vehicle
- Enhanced encryption schemes
- Long term availability of a secured access and provisioning
- ECU lifecycle protection, e.g., for SW upgrades and HW changes



For more information about Vector
and our products please visit

www.vector.com/security

Authors:

Armin Happel, Prof. Dr. Christof Ebert

Vector Consulting Services GmbH