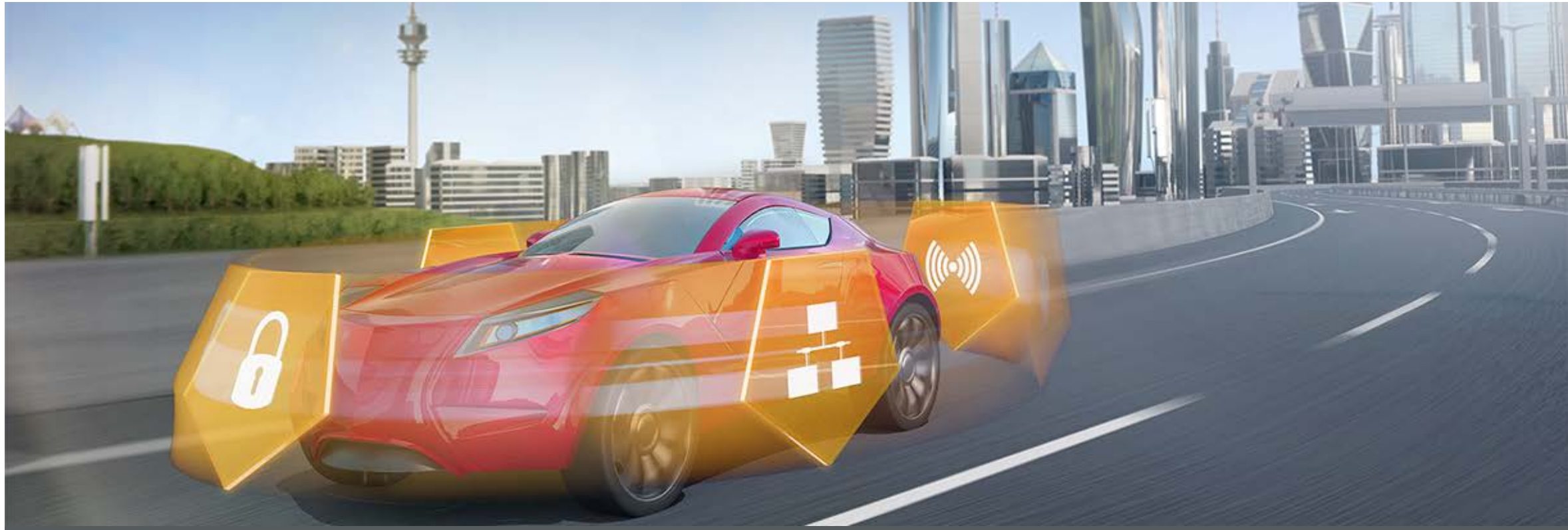
VECTOR



Automotive Cyber Security Mechanisms

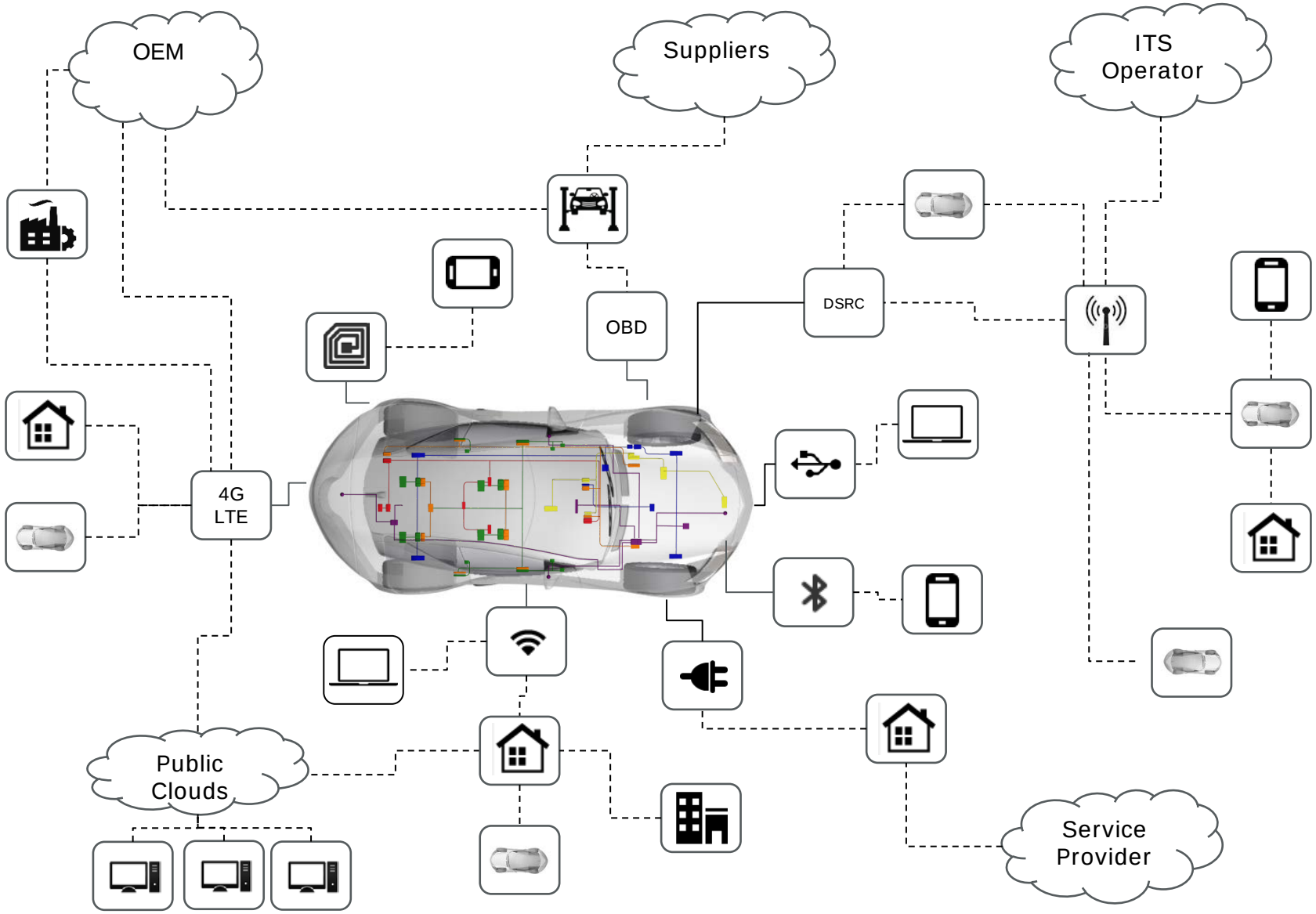
Status of Standardization and Next Steps

V2.01.00 | 2016-05-09

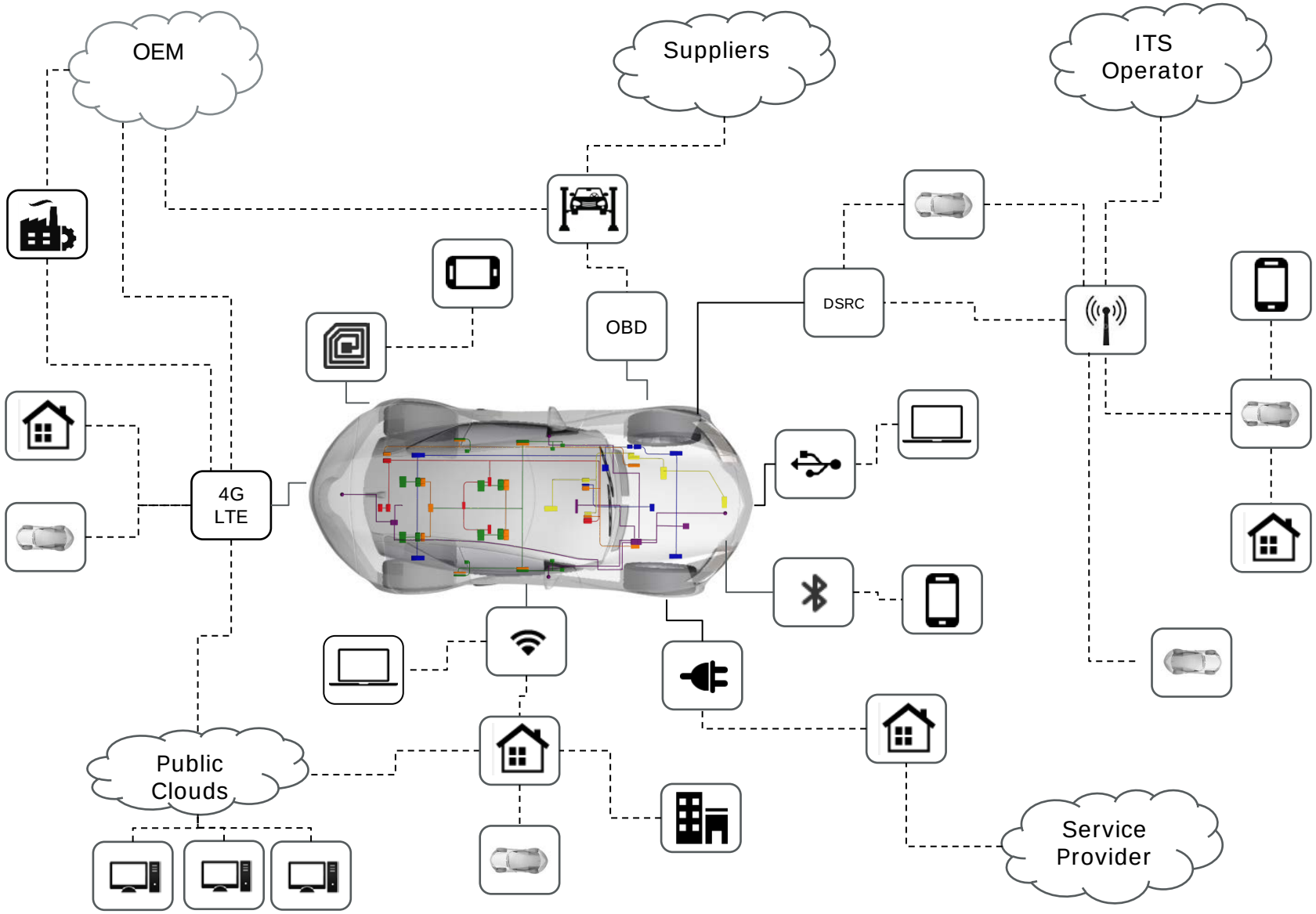
Agenda

- **Introduction**
- Security Engineering
- Security Mechanisms for Embedded Automotive Systems
- Security Mechanisms in AUTOSAR 4.3
- Advanced Security Mechanisms
- Summary

Vehicle is a Part of the Internet of Things

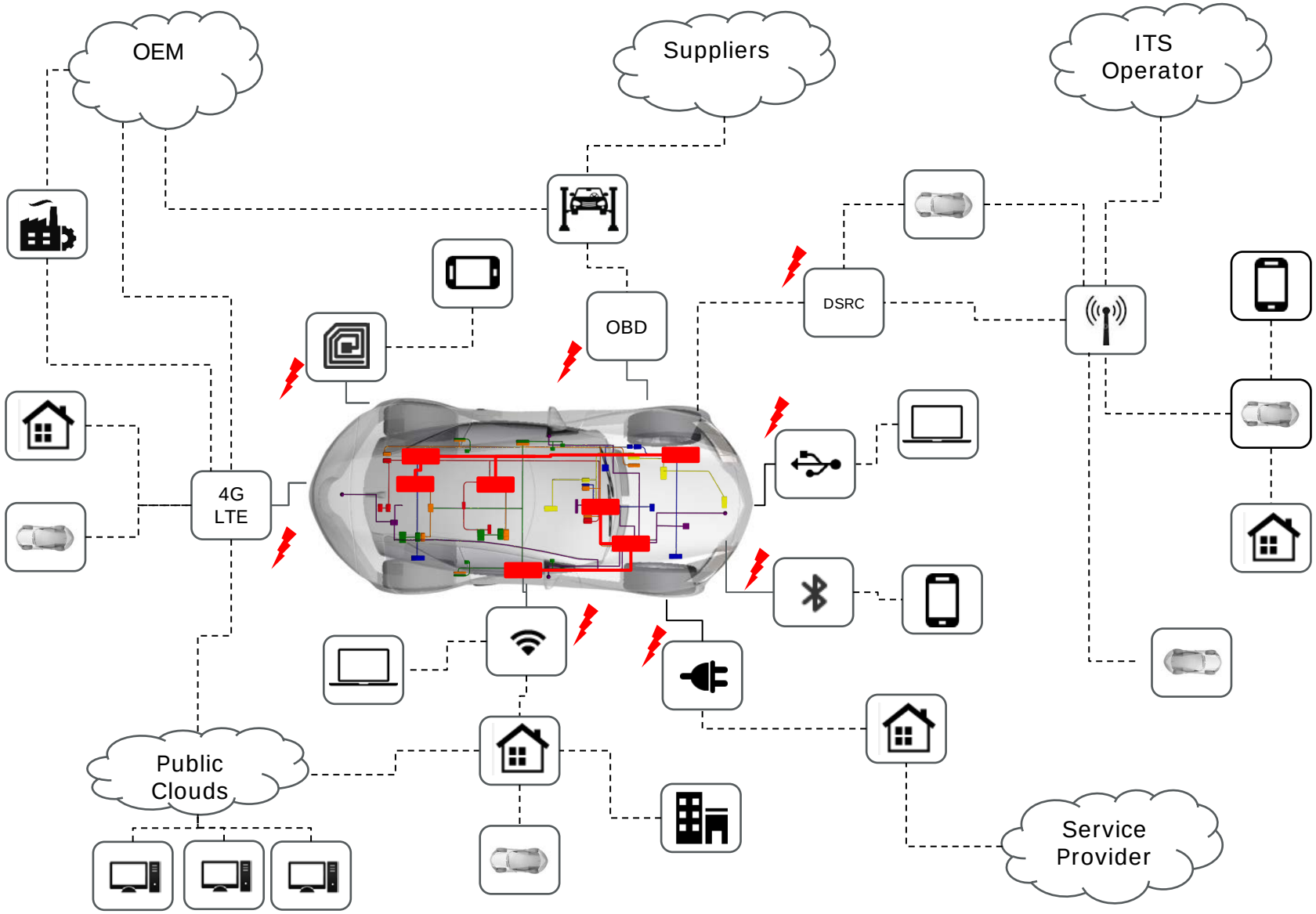


New Features and Business Models



- Flashing over the air
- Software as an aftersales product
- Remote feature activation
- Data mining campaigns
- Autonomous driving
- Electronic license plate
- Traffic management
- Toll collection
- ...

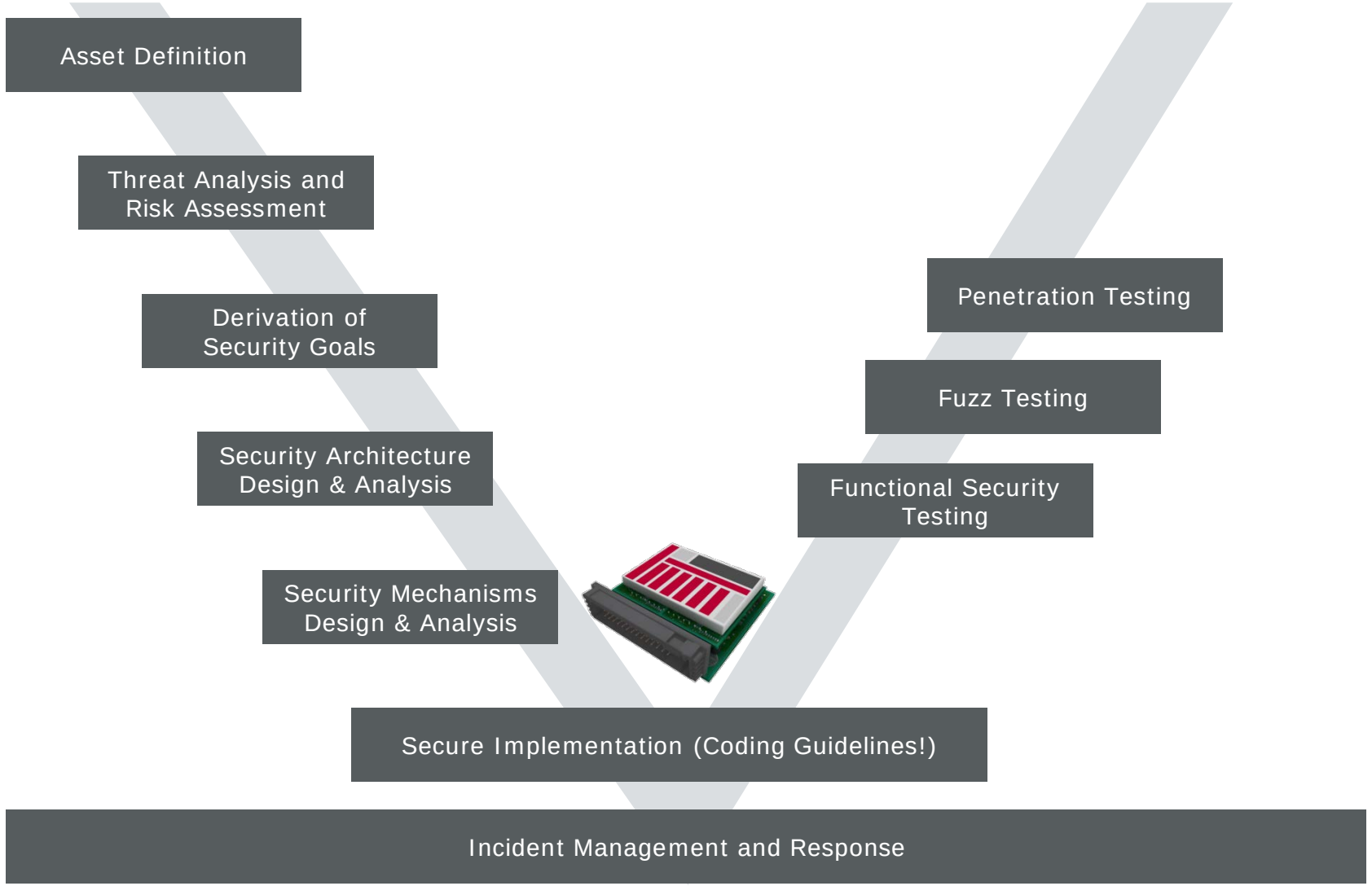
Many different Attack Vectors and Threats



- Chip tuning
- Privacy abuse
- Remote controlled vehicles
- Unlocking of feature sets
- ...

Agenda

Security Engineering Lifecycle

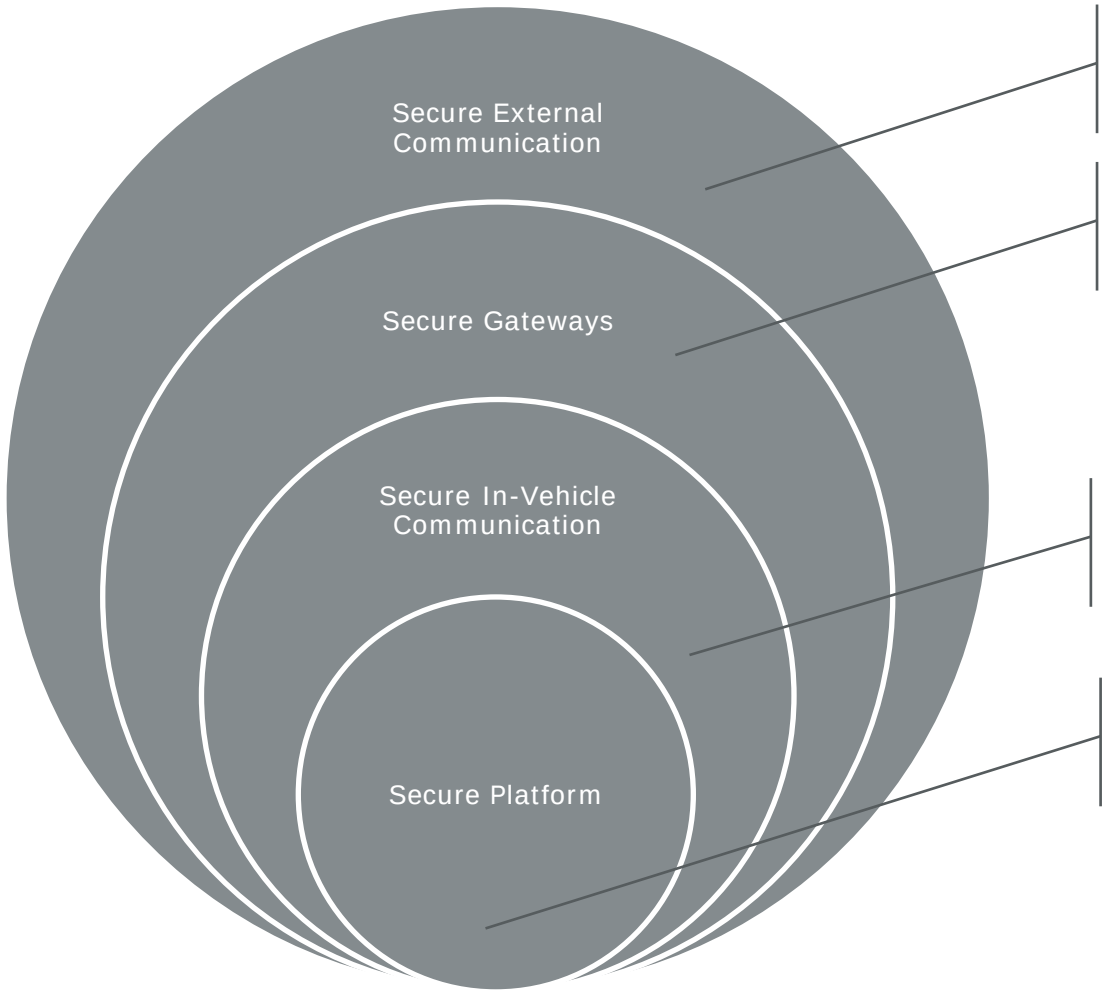


- Cyber Security does not start or end with cryptography
- Similar to functional safety, security needs to be considered throughout the development process
- Automotive specific initiatives for security engineering have been started
  - SAE J3061
  - Joint ISO/SAE standardization group “Automotive Security Engineering” started

Agenda

- Introduction
- Security Engineering
- ▶ **Security Mechanisms for Embedded Automotive Systems**
- Security Mechanisms in AUTOSAR 4.3
- Advanced Security Mechanisms
- Summary

Layered Security Concept (Logical View)



Associated Security Concepts

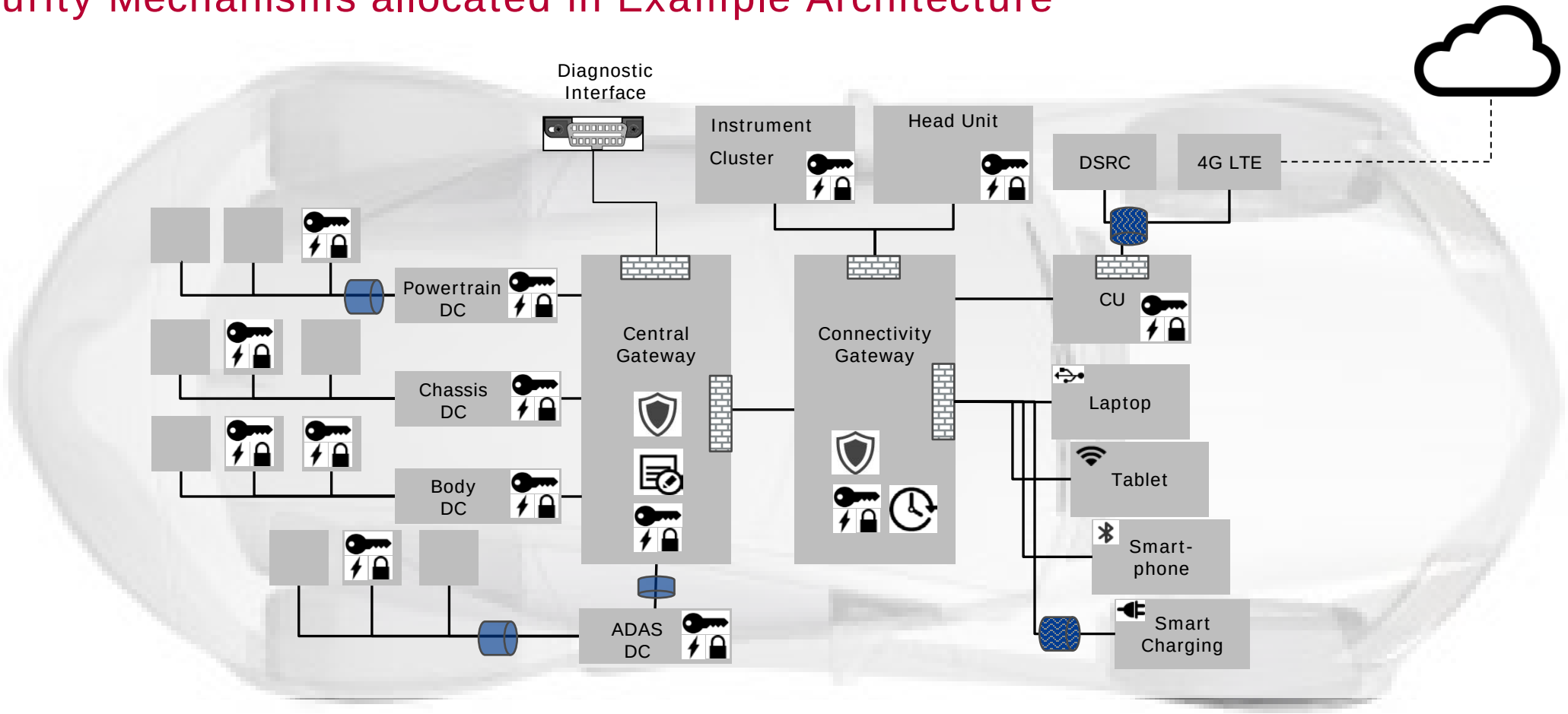
- Secure communication to services outside the vehicle

- Intrusion detection mechanisms
- Access control
- Firewalls
- Key management (update, distribution)
- Synchronized secure time

- Authenticity of communication
- Integrity and freshness of communication
- Confidentiality of communication

- Key storage
- Secure boot and secure flash
- Crypto algorithms
- HW trust anchor (HTA)

Security Mechanisms allocated in Example Architecture



Secure Update & Boot

Key Infrastructure

Crypto Algorithms

Security Event Log

Secure Synchronized Time Manager

Intrusion Detection / Prevention

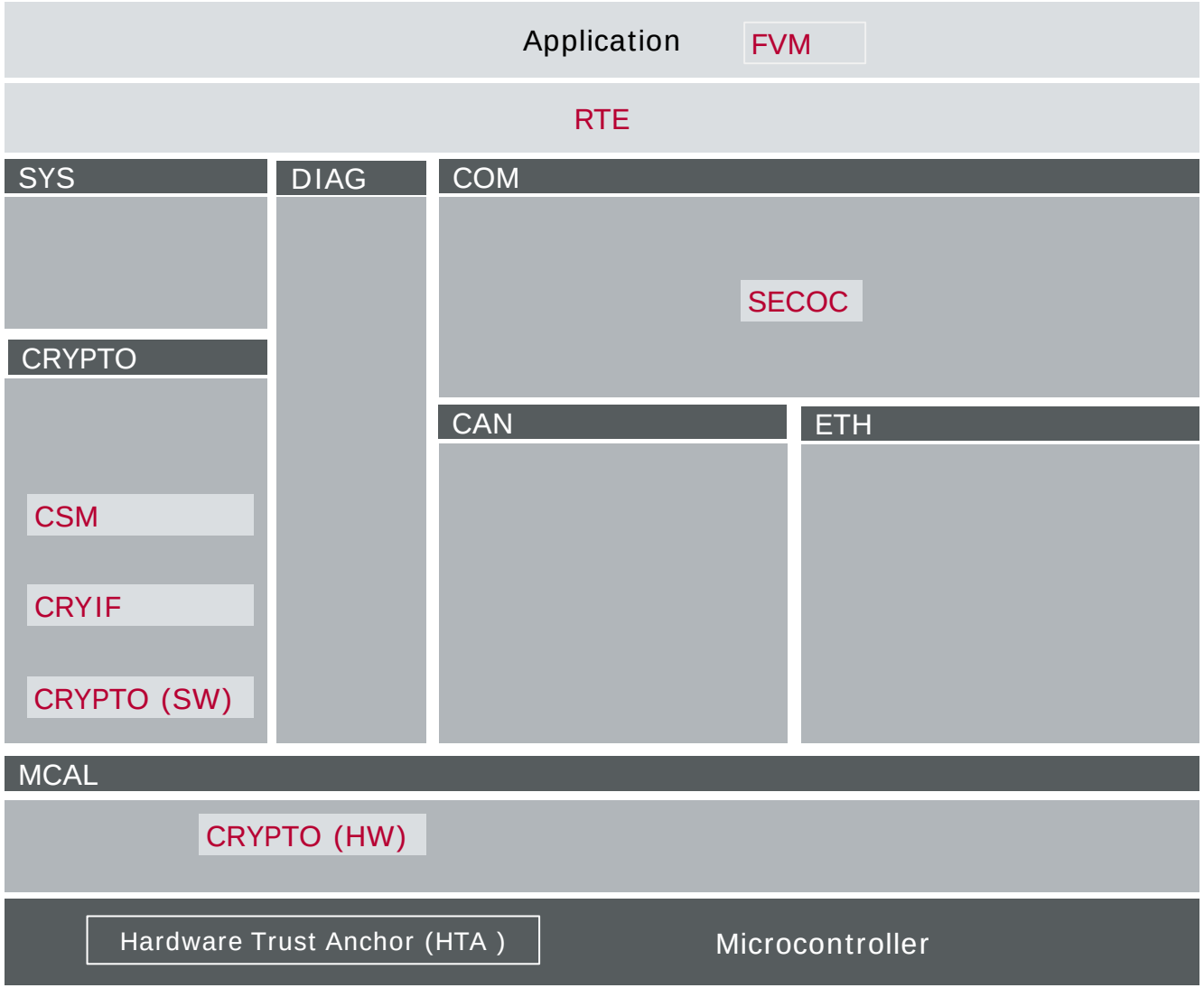
Secure On Board Com.

Secure Off Board Com.

Firewall

Agenda

MICROSAR 4.3 Security Modules



Cryptographic Functions

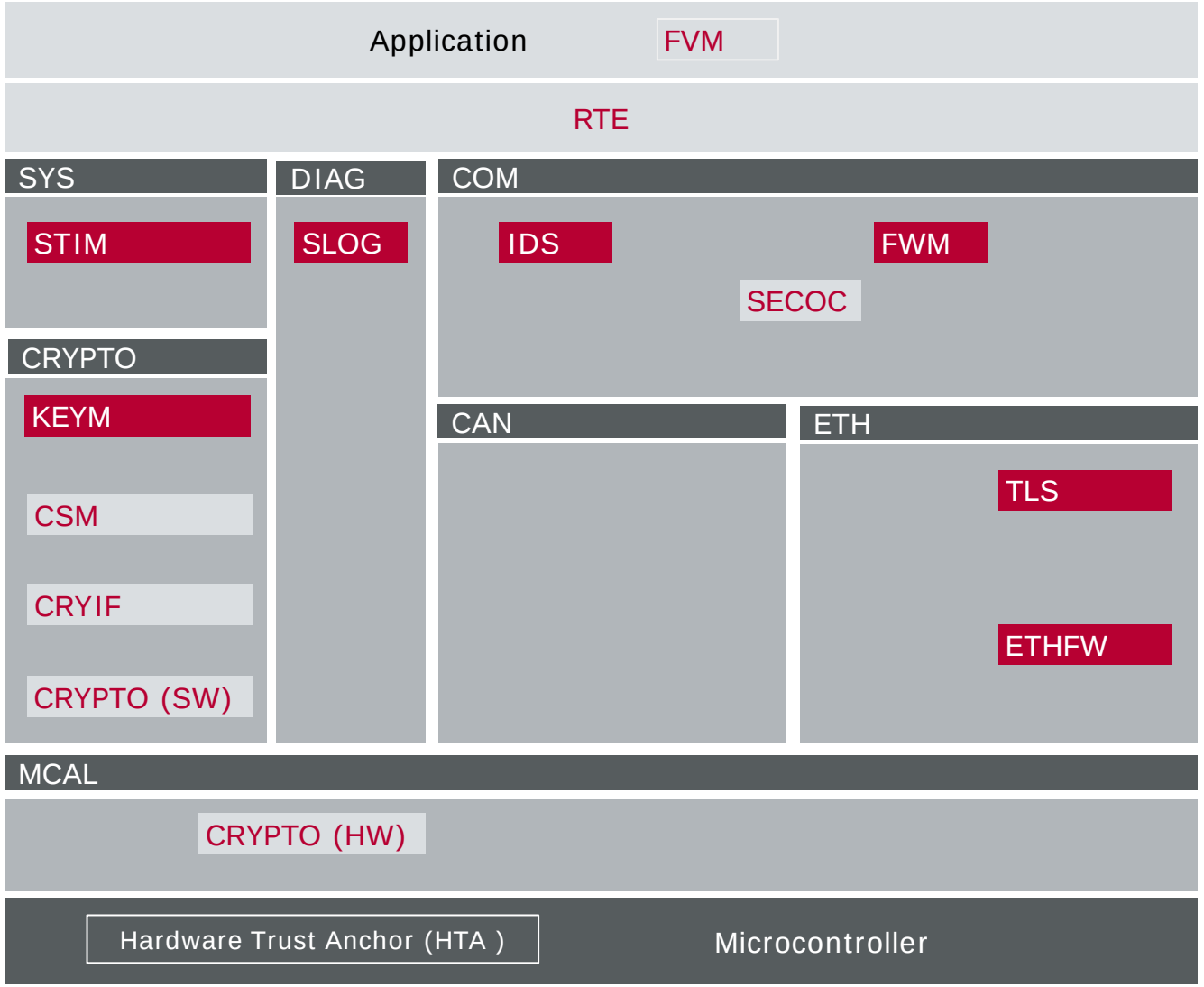
- Crypto Service Manager (CSM)
- Crypto Interface (CRYIF)
- Crypto (SW) / Crypto (HW)

Protection of Onboard Communication

- Secure onboard Communication (SECOC)
- Freshness Value Manager (FVM)

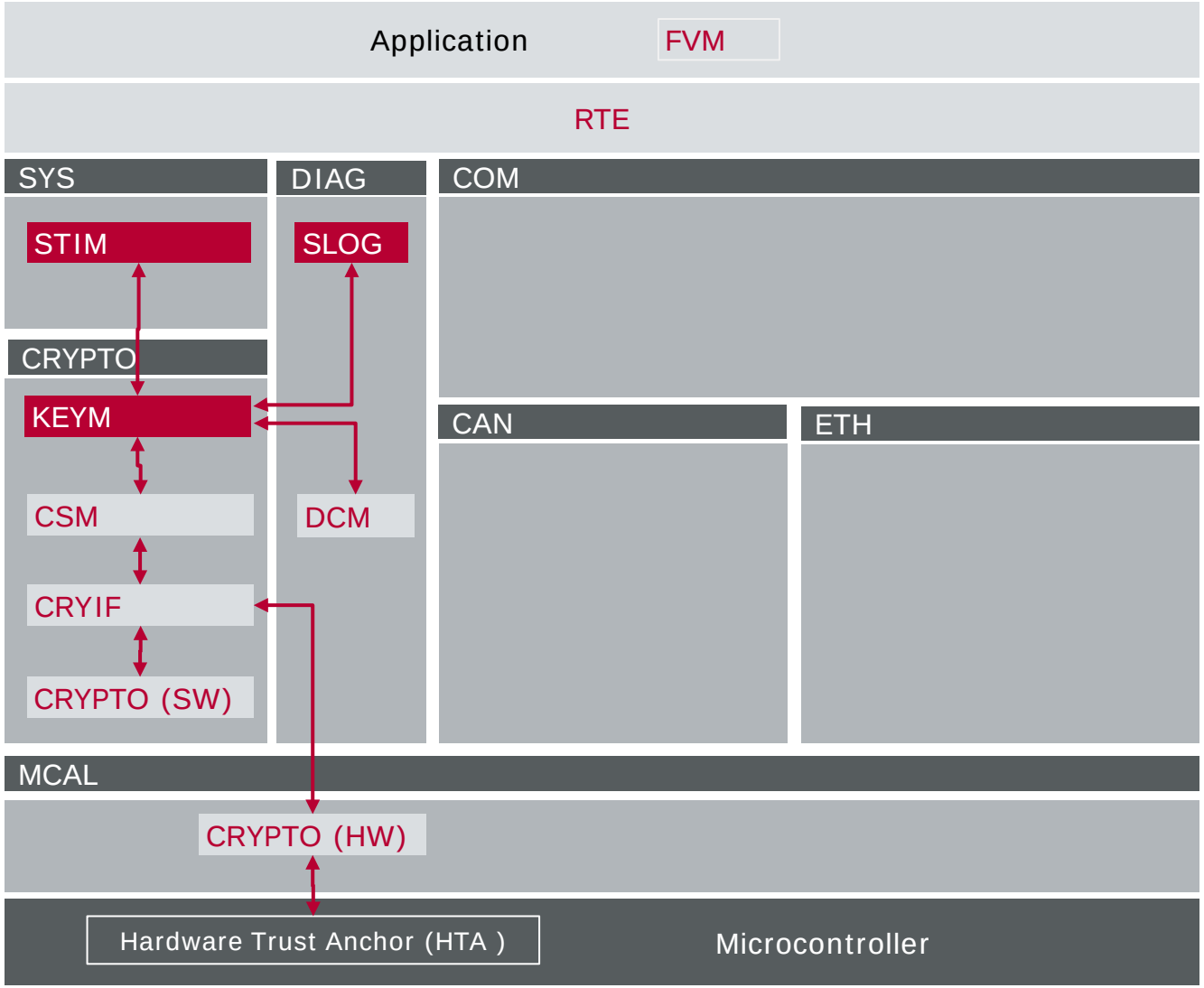
Agenda

Security Mechanisms currently not specified by AUTOSAR



- Key Manager (KEYM)
- Secure Time Manager (STIM)
- Security Event Log (SLOG)
- Firewall Manager (FWM)
- Ethernet Firewall (ETHFW)
- Intrusion Detection System (IDS)
- Transport Layer Security (TLS)

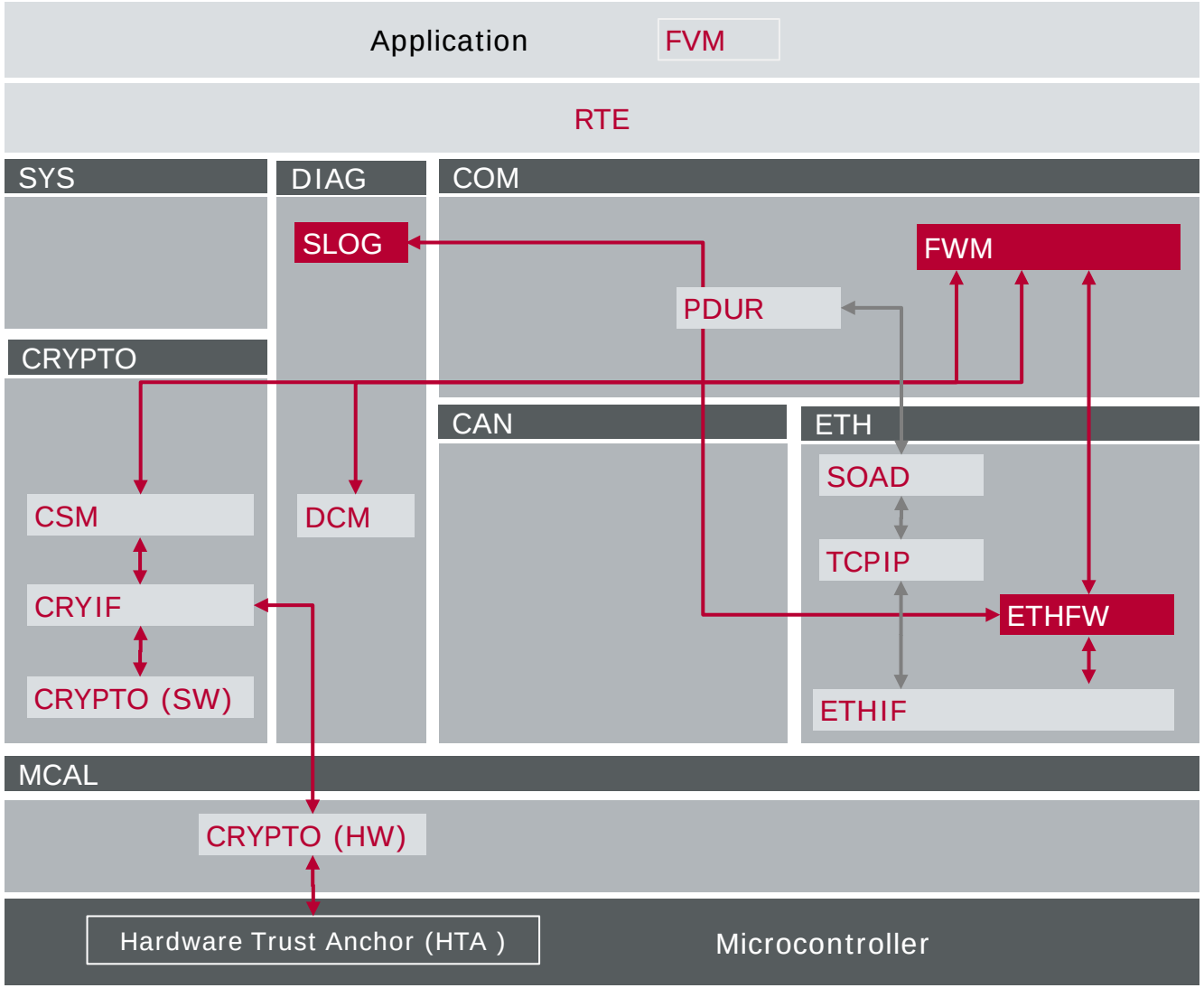
Management of Cryptographic Material (Keys, Certificates)



Key Manager (KEYM):

- Receives new **cryptographic material** (keys, certificates) via diagnostic routines
- Verifies authenticity, integrity and freshness of cryptographic material
- Implements business logic for **key lifecycle phases** (production, initialization, update, repair, replacement)
- Supports **derivation** of new keys
- Supports secure **distribution** of shared secret keys
- Logs security events to SLOG

Ethernet Firewall



Ethernet Firewall (ETHFW):

- DENY-ALL Firewall (Whitelist)
- Post-build loadable support
- Evaluates filter rules (policy) based on
  - Ethernet information (VLAN, frame priority, Ether Type, MAC addresses, next layer protocol)
  - AVB information (Stream ID)
  - IP information (IP addresses, next layer protocol)
  - IP protocol (UDP, TCP, RAW)
  - UDP/TCP protocol (ports)
- Logging of non-policy-conform packets in tamper proof SLOG

Firewall Manager (FWM):

- Manages state of individual firewalls
- Securely stores and updates firewall filter rules (policies)

Key Points

- New features and business models require cyber security as an enabler
- Security does not start or end with cryptography → Security Engineering
- Layered security concept supports defense in depth
- AUTOSAR provides improved security stack with AUTOSAR 4.3, but…
- Further security extensions are required (e.g. Key Management, Firewalls)

- **Remember to visit the Vector Automotive Cyber Security Symposium 2017/10/12**

For more information about Vector and our products please visit

www.vector.com

Author:

Dr. Eduard Metzker

Vector Informatik GmbH