VECTOR

Risk Based Security

Automotive Safety & Security, 30. Mai 2017

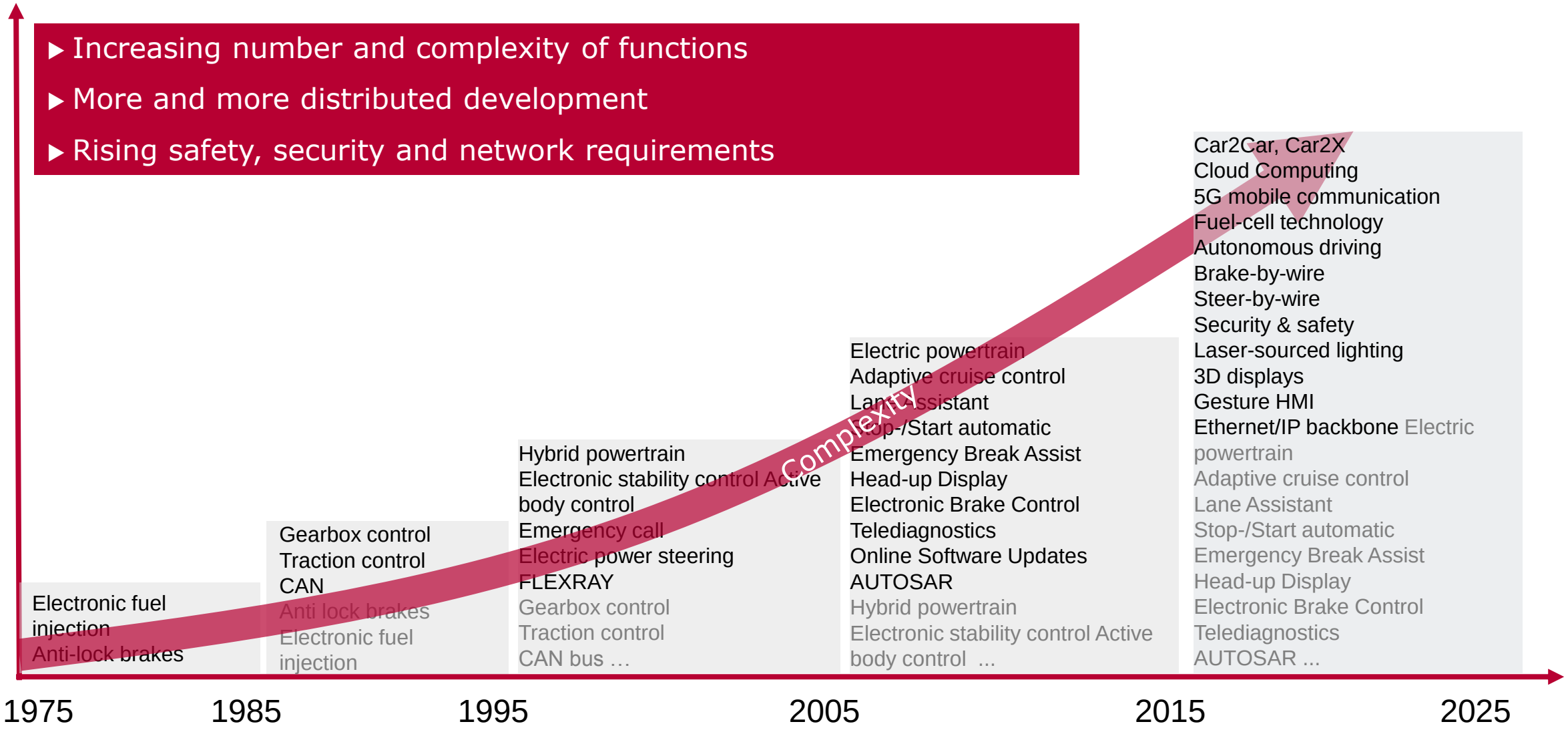
Christof Ebert and Dominik Lieckfeldt, Vector Consulting Services

Agenda

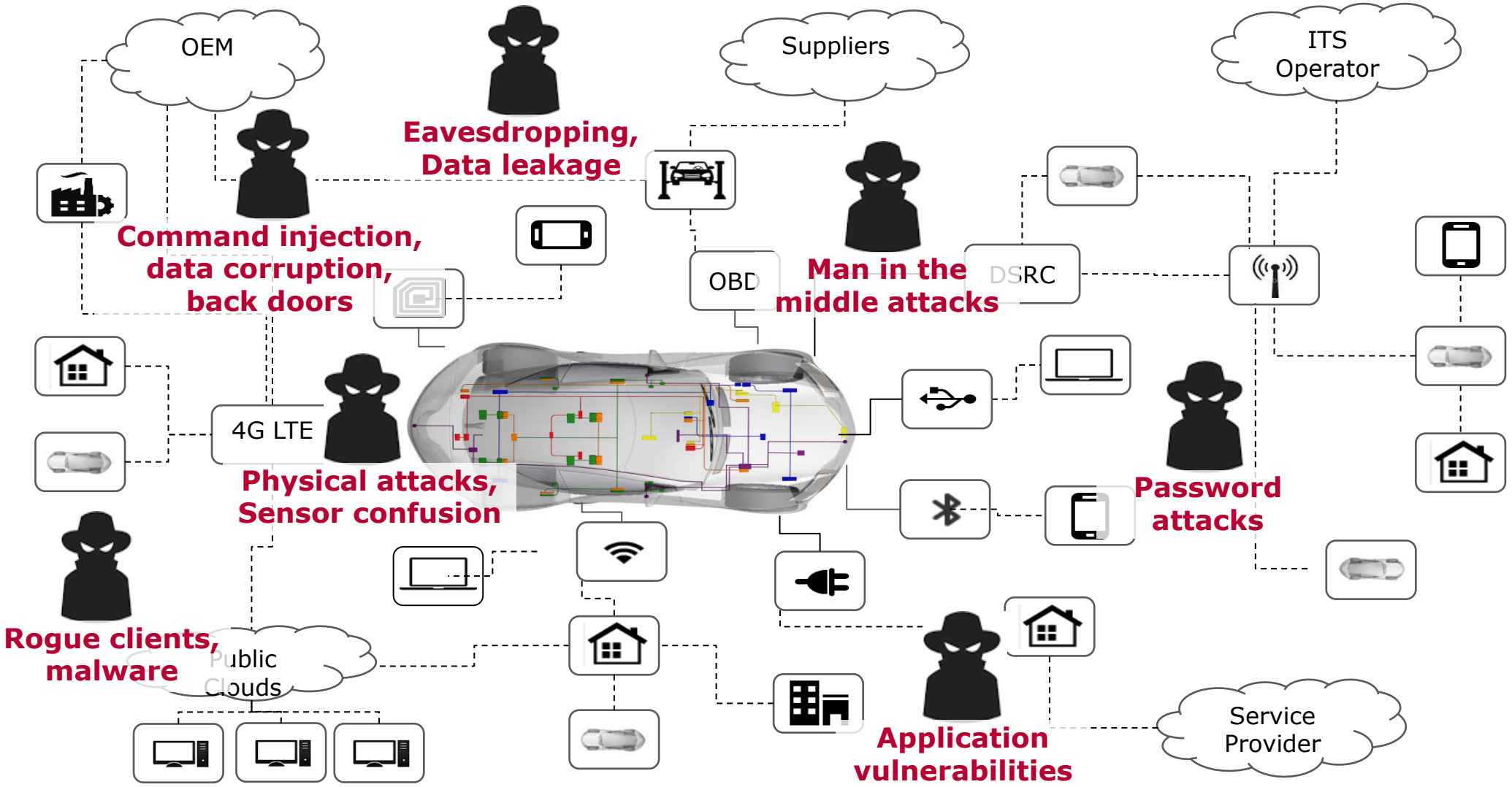
- **Motivation**
- Risk-based approach to Cybersecurity
- Conslusion

The Challenge of Increasing Functionality

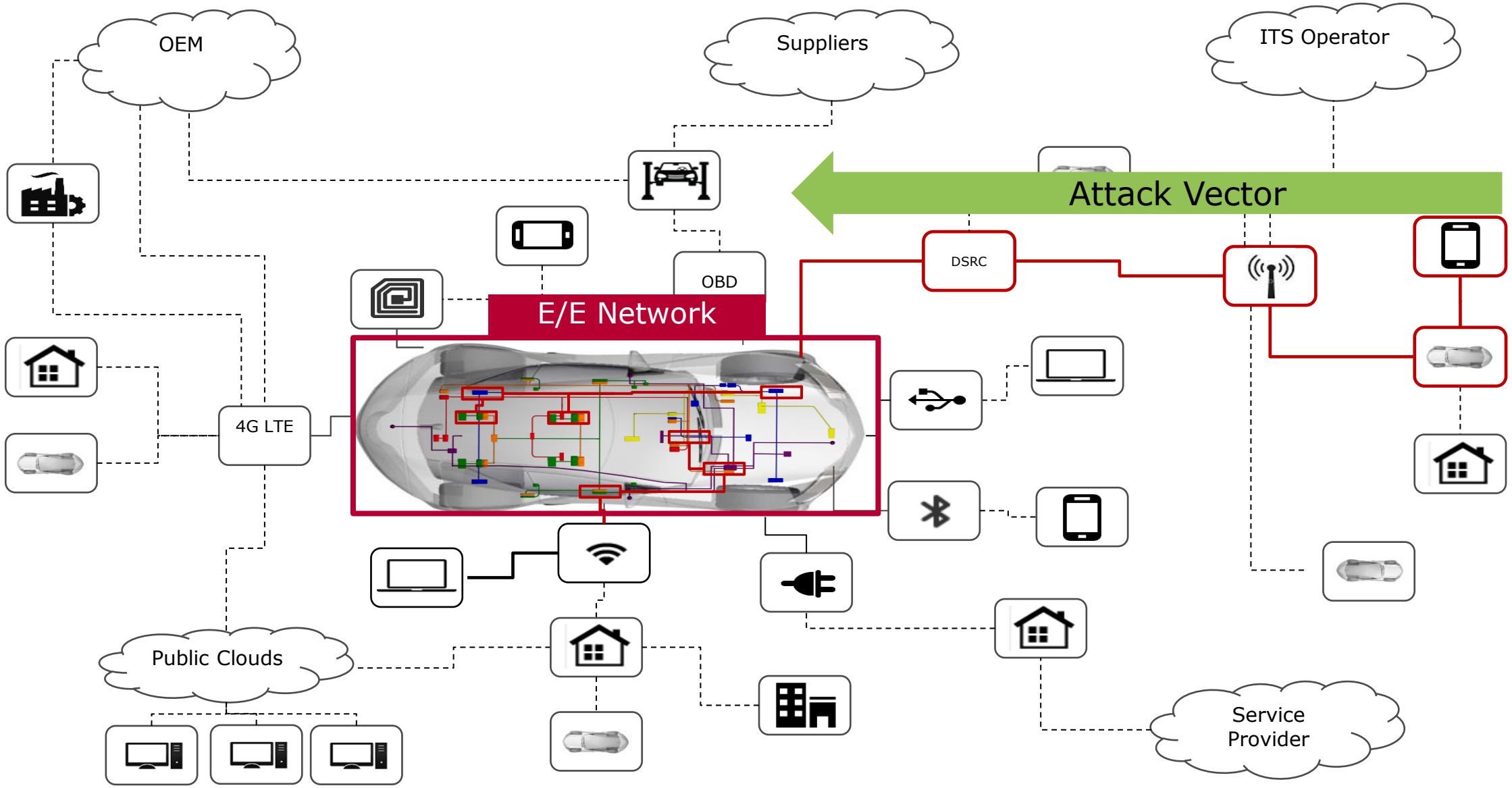
- Increasing number and complexity of functions
- More and more distributed development
- Rising safety, security and network requirements



Connectivity + Complexity = Cyber Attacks



Many different *attack vectors* to be regarded



Why do we need to care about Cybersecurity

Functional Safety

- Goal: Protect health
- Risk: Accident
- Governance: ISO 26262
- Methods:
  - HARA, FTA, FMEA, …
  - Fail operational, …
  - Redundancy, …

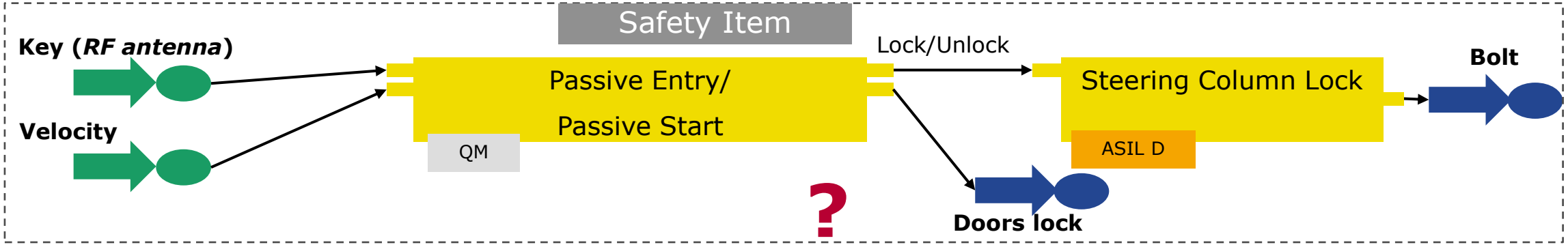
Cyber Security

- Goal: Protect assets
- Risk: Attack, exploits
- Governance: ISO 27001 etc.
- Methods:
  - TARA, …
  - Cryptography, IDIP, …
  - Key management, …

Privacy

- Goal: Protect personal data
- Risk: Data breach
- Governance: Privacy laws
- Methods:
  - TARA,…
  - Cryptography,…
  - Explicit consent, …

Feature Example: Experiences from developer's daily life …



Function	Hazard	S/E/C	ASIL
Passive Entry	After starting from standstill a **nearby second key opens the car from remote** by accident. Doors are unlocked and opened unintentionally. Car could open and hit pedestrian on low speed.	S2/E3/C1	QM
Steering Column Lock	During driving on high speed (Highway) **steering column is locked** and vehicle crashes in safety fence	S3/E4/C3	D
Steering Column Lock	… **Person nearby is locking steering column from remote whereby the vehicle is on medium speed.**	S3/**??**/C3	**??**

Functional safety methods do not cover security issues. An automotive standard is missing.

Different Threats Demand Holistic Systems Engineering

Functional Safety

- Goal: Protect health
- Risk: Accident
- Governance: ISO 26262
- Methods:
  - HARA, FTA, FMEA, …
  - Fail operational, …
  - Redundancy, …

Cyber Security

- Goal: Protect assets
- Risk: Attack, exploits
- Governance: ISO 27001 etc.
- Methods:
  - TARA, …
  - Cryptography, IDIP, …
  - Key management, …

Privacy

- Goal: Protect personal data
- Risk: Data breach
- Governance: Privacy laws
- Methods:
  - TARA,…
  - Cryptography,…
  - Explicit consent, …

Liability ➔ Risk management ➔ Holistic systems engineering

Agenda

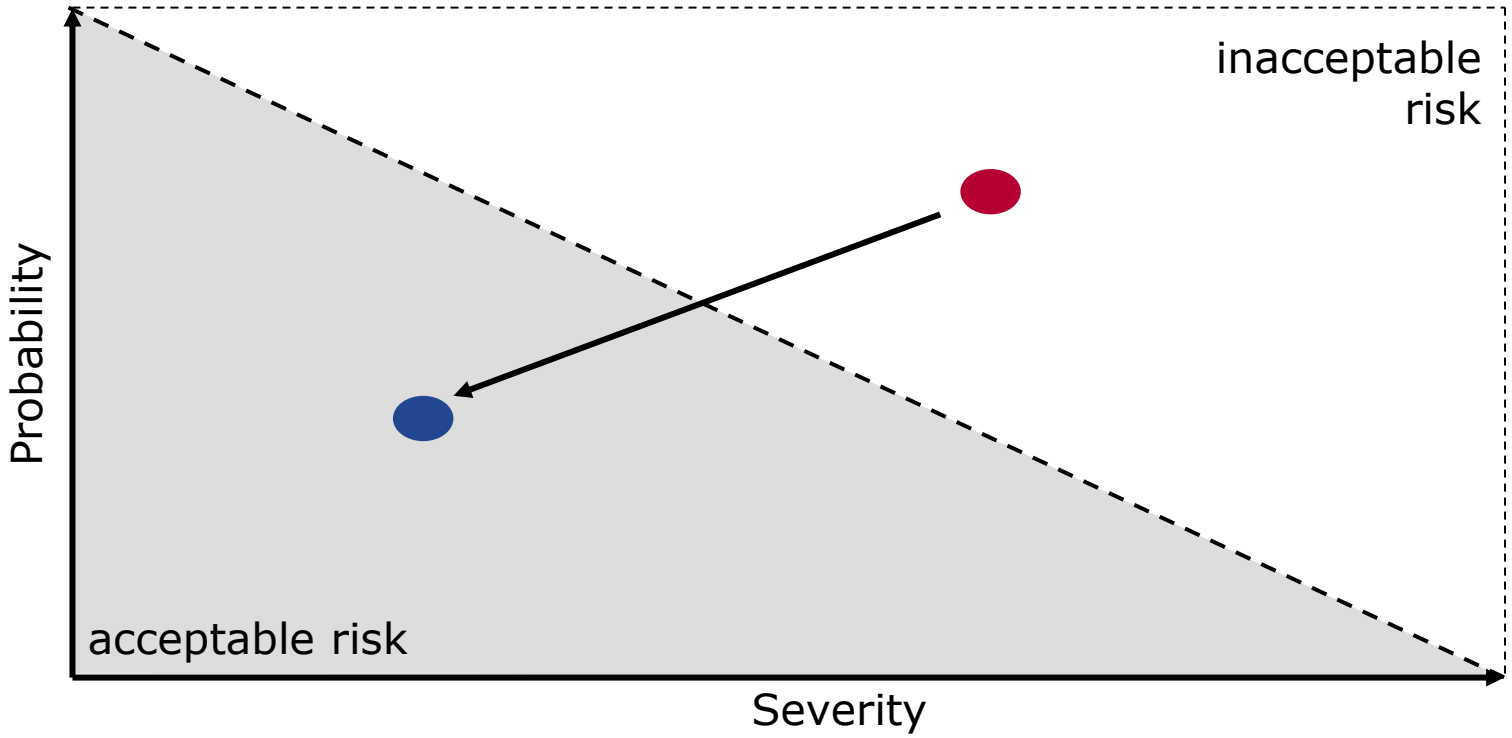
Motivation

- **Risk-based approach to Cybersecurity**

Conslusion

Functional safety & Cyber security – Risk based approach

Risk = Severity of harmful event × Probability of occurrence

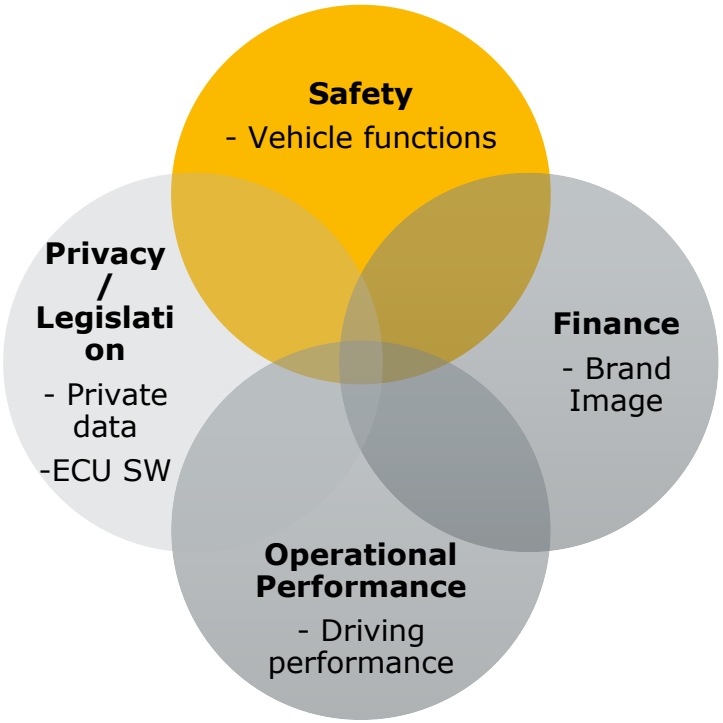


The purpose of development measures is to **reduce the residual risk** (caused by new features) to an acceptable level.

Concept of *Threat Analysis and Risk Assessment* (TARA)

Assets → Threat-Model & Risks → Measures → Concept for Solution → Verification

General automotive asset categories



Example: Identified threats

- **Safety**
  - 1 Injuries because of malfunctioning Passive Entry
- **Financial**
  - 2 Loss of annual sales due to damage to brand image
- **Operational Performance**
  - Doors locked
- **Privacy/Legislation**
  - 3 Theft of private data

Security considers a larger scope of threats compared with **Safety**.

Detailed Steps for TARA

Asset/Function	Security Attack	Threat	Risk
Asset 1	Attack-type 1	Threat 1	EAL (Evaluation Assurance Levels)
Function 1	Attack-type 2	Threat 2	ASIL
…	…	…	…

Asset/ Function	Attack	Threat	Threat-Level (*e.g. Expertise, Equipment*)	Impact-Level (*e.g. Financial, Privacy, Safety*)	Risk level
Passive entry	Authenticity: Attacker unlocks the vehicle doors.	Vehicle doors are unlocked and vehicle is stolen.	High	High 3	Medium
	Authenticity: Attacker unlocks the vehicle doors.	Vehicle doors are opened at high speed. Vehicle crashes into opposing traffic.	Very High	Very High 1	Very High
	Authenticity: Attacker unlocks the doors of many vehicles.	Vehicle doors are unlocked and many vehicles are stolen.	Medium	Very High 2 3	High

TARA Tool from *Real World*

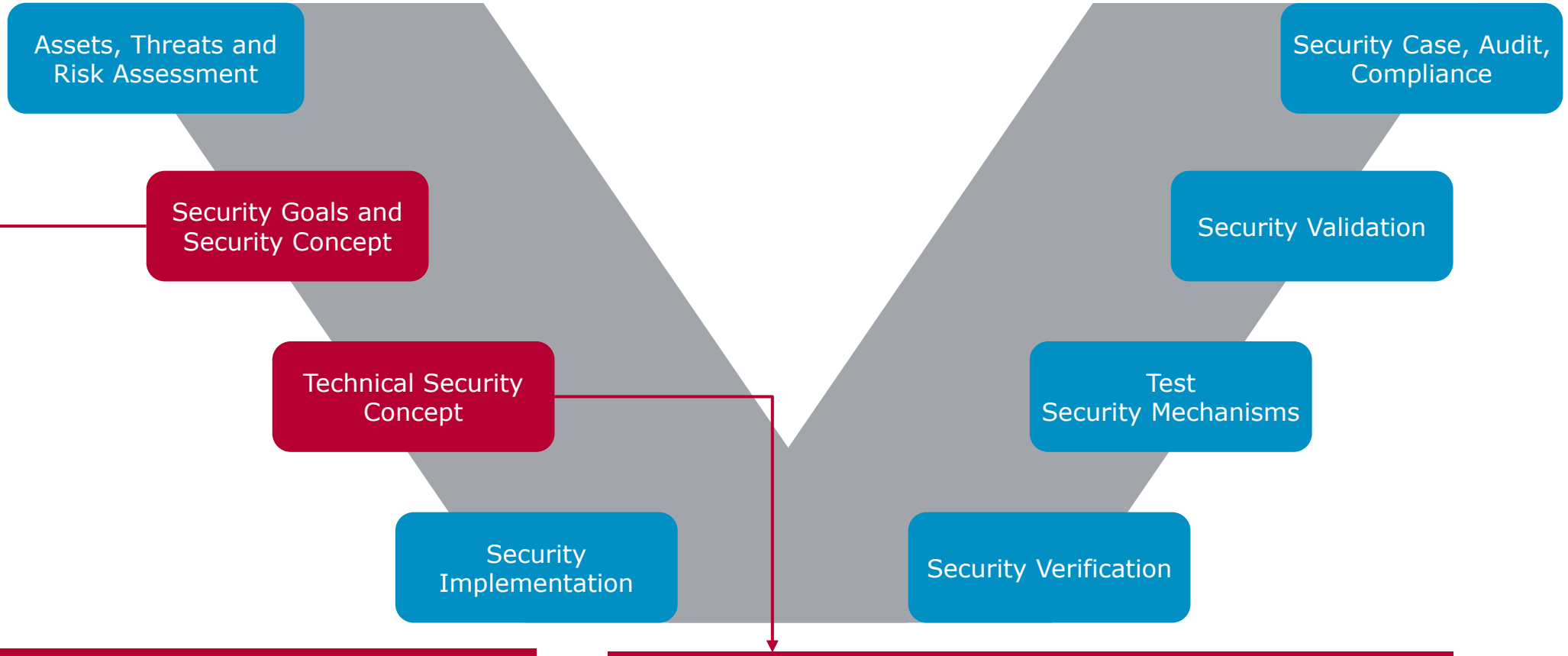
CIAAG
Confidentiality, **I**ntegrity, **A**vailability, **A**uthenticity, **G**overnance

Resulting Security Goals

Maximum
(Safety, Financial)

No.	Variant	Asset ID	Asset / Vehicle Function	CIA	Threat ID	Hazard / Threat	Expertise	Window of Opportunity	Knowledge	Equipment	Threat level	Safety	Financial	Operational	Privacy	Impact Level	Security level	SG ID	Security Goal
1	Platform (TBC)	Ast 2	Braking to prevent collision	A	Tht-1	Driver crashes into preceding car. Passengers in both cars are severly wounded or killed.	Expert	Medium	Sensitive	Bespokes	Low	Life-threatening or fatal injuries	Low	High	No impact	Critical	Medium	**SG1**	If requested the brakes shall be activated
2	Platform (TBC)	Ast 2	Braking to prevent collision	I	Tht-2	Braking although not authorized, e.g. > 10 km/h	Expert	Medium	Sensitive	Bespokes	Low	Severe and life threatening injuries	High	High	No impact	Critical	High	**SG2**	Unauthorized braking shall be avoided.
3	Platform (TBC)	Ast 1	IPR of functions	C	Tht-3	RCTA function becomes public knowledge	Expert	High	Public	Bespokes	Medium	No injuries	High	No impact	No impact	Critical	High	**SG3**	RCTA function shall remain secret.

Security Architecture Design



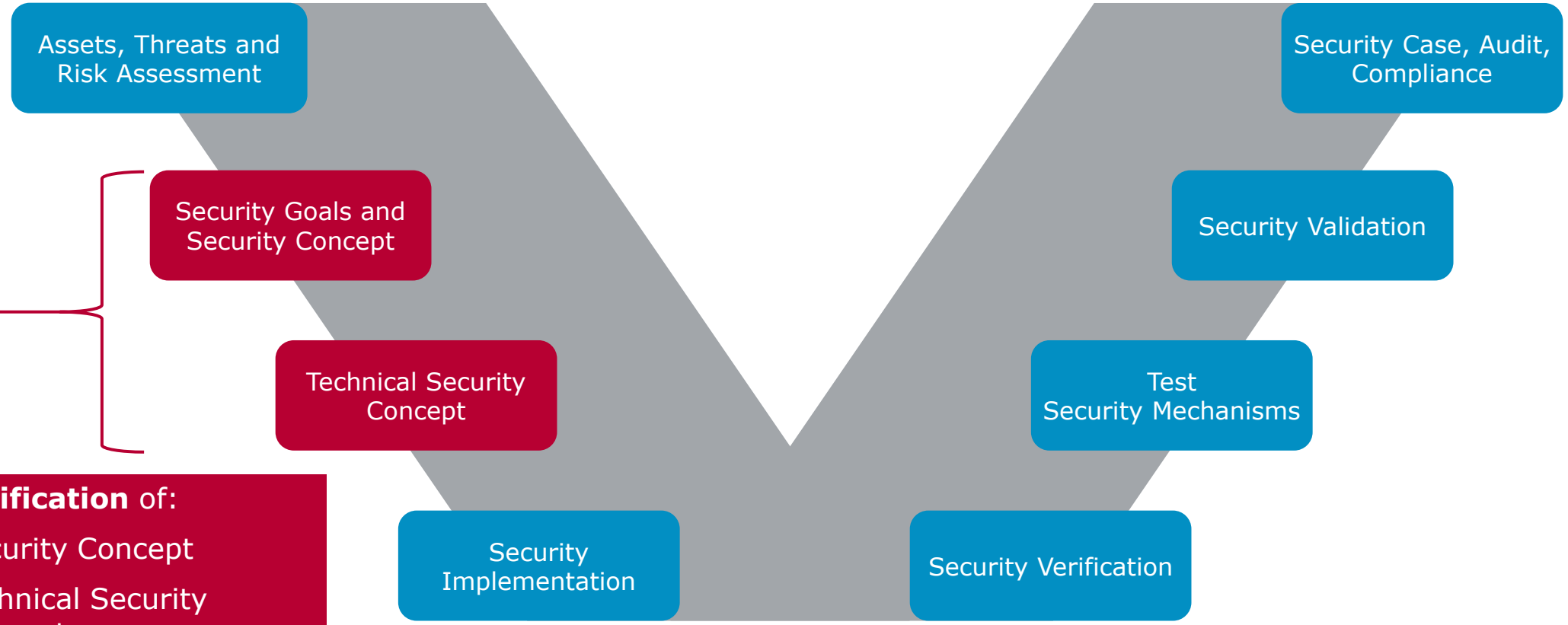
Security Concept:

1. Refinement of Security Goals to **Functional Security Requirements (FSeR)**
2. Allocation of *FSeR* to the first level of system architecture

Technical Security Concept:

1. Refinement of system architecture to technical component level (SW/HW components)
2. **Technical Security Requirements (TSeR)** are refined out of the Security Concept

Security Architecture Design



Verification of:

- Security Concept
- Technical Security Concept

- Peer Reviews
- **Attack Trees** as System Vulnerability Analysis

Derive Appropriate Security Mechanisms

	Prevent	Detect	Forensic
Critical	++	++	++
High	+	++	++
Medium	+	+	++
Low	(+)	+	+
QM	O	O	+

O: No recommendation for or against approach

+: Approach is recommended for security level

++: Approach is highly recommended for security level

Examples

- Network/process/ information separation
- Encryption, digital signatures
- Key management
- Access control
- Firewall
- Intrusion prevention systems

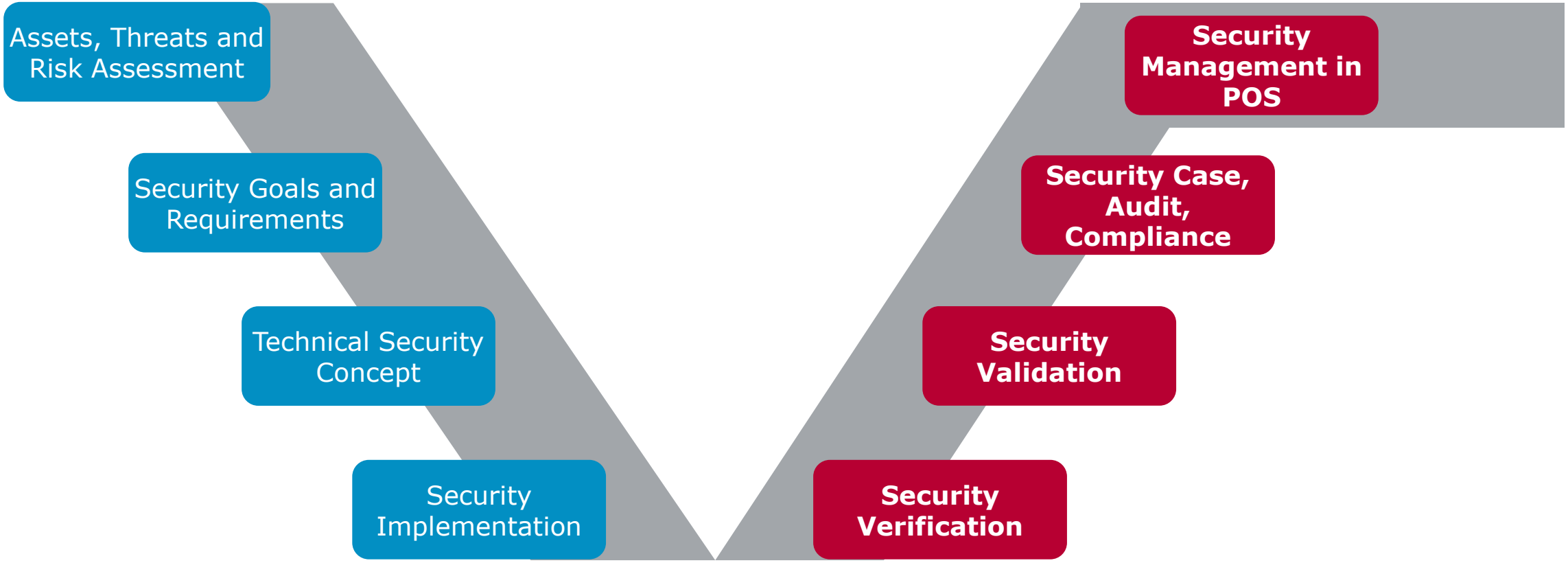
Examples

- Intrusion detection systems (IDS)
- Monitoring

Examples

- Logging
- Security issue knowledge base
- Analysis and investigation of digital evidence

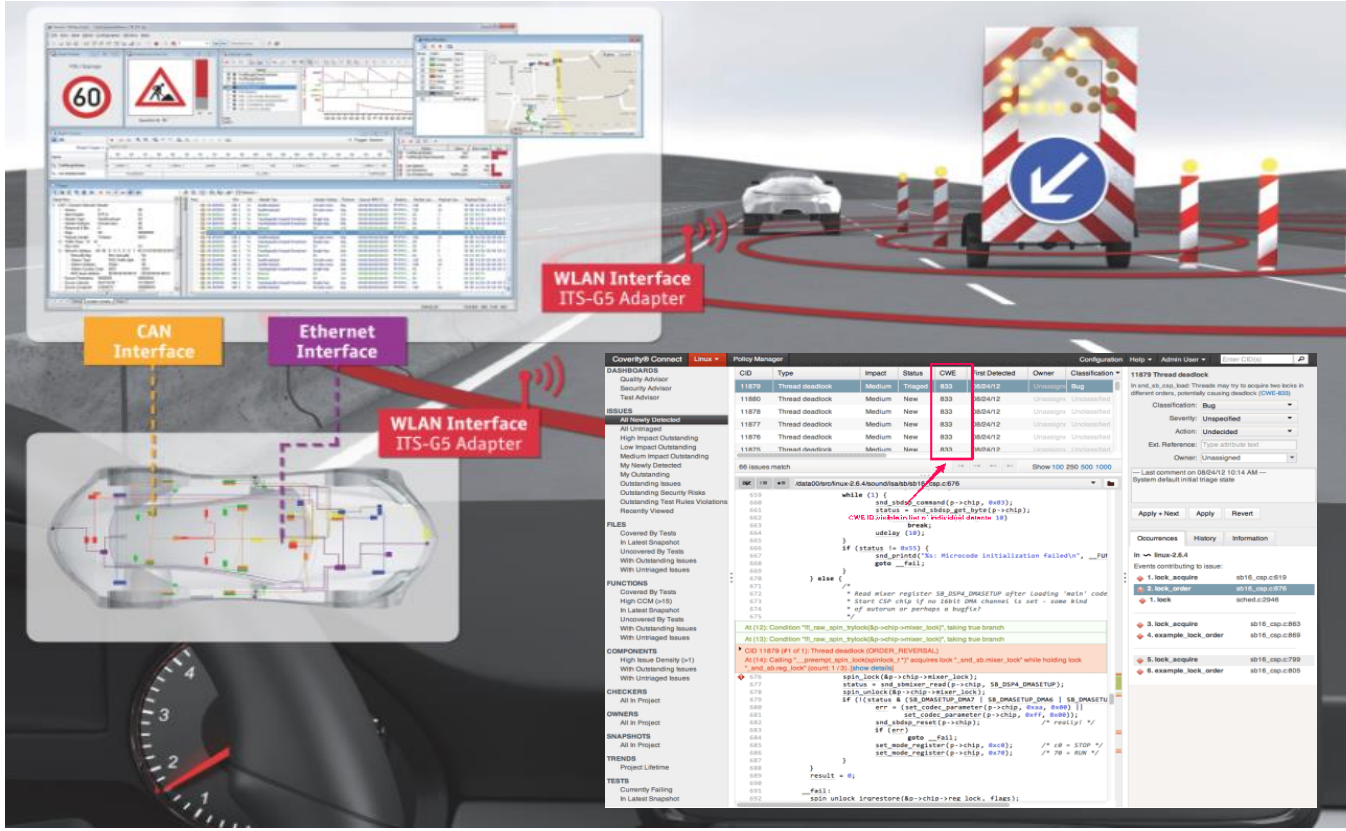
Security Engineering



Implement Security by Design: Verification and Validation

- **Tools**
  - Static / dynamic code analyzer
  - Encryption cracker
  - Vulnerability scanner
  - Network traffic analyzer / stress tester
  - Hardware debugger
  - Interface scanner
  - Exploit tester
  - Layered fuzzing tester

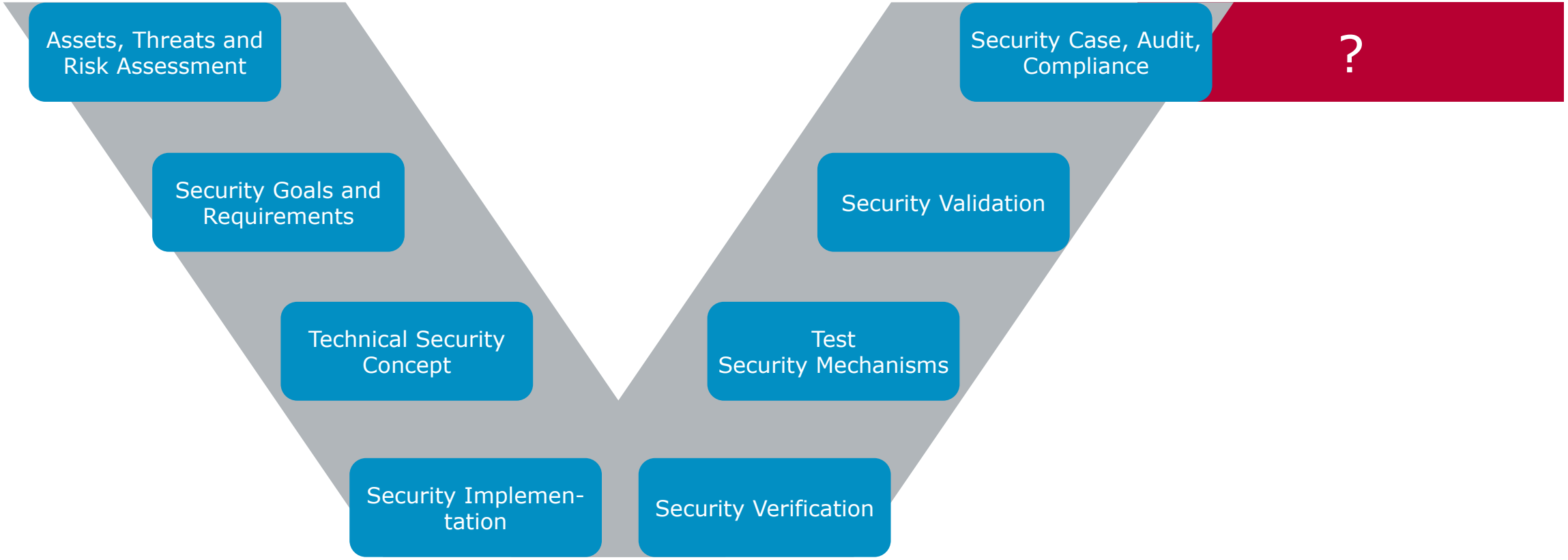
- **Life Hacking**
  - Penetration testing
  - Attack schemes
  - Governance and social engineering attacks



Test for the known – and for the unknown.
Ensure automatic regression tests are running with each delivery.

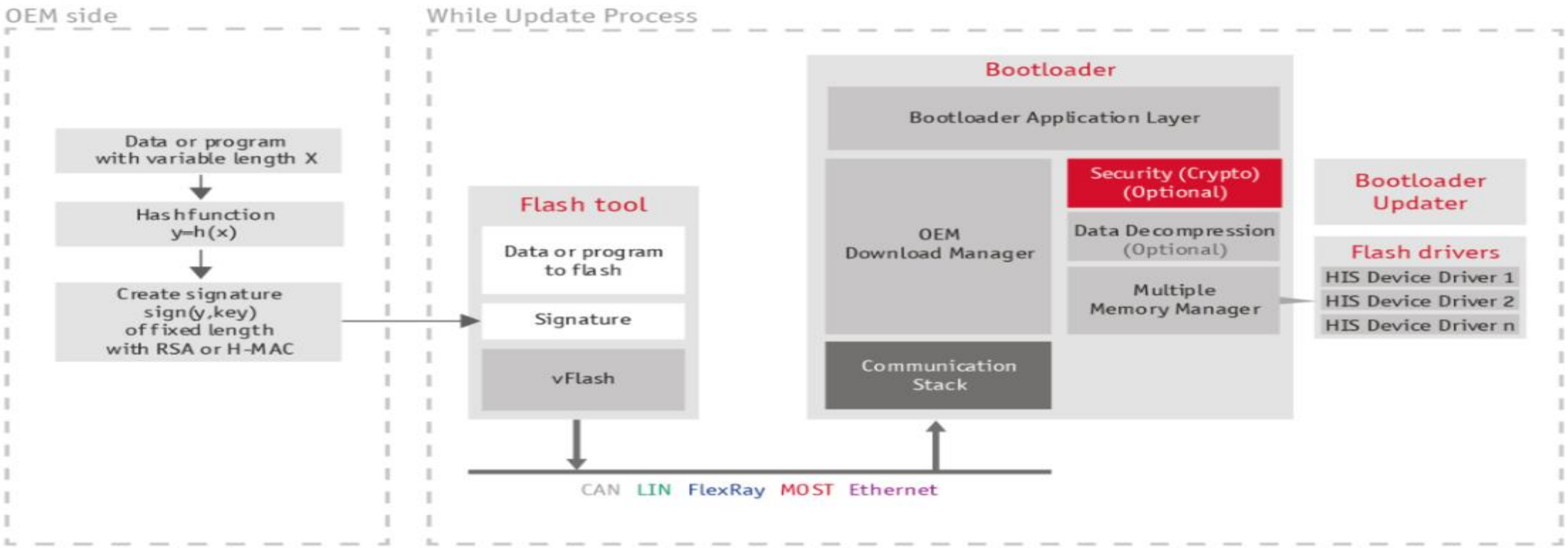
VECTOR

Security By Design: What will happen to *After Sales Services*?



Major difference between security & safety: Risk-management during vehicle lifetime.

Game Changer: Deploy Security for Service & Operations: OTA



Over the Air (OTA) Update: This feature opens the gate for a big number of threats and is a solution at same time.

Agenda

Motivation

Risk-based approach to Cybersecurity

- **Conslusion**

VECTOR

Automotive Cyber Security

- **Security demands a thorough culture change**
  - Advance a cyber security culture across functions
  - Enforce strong governance end-to-end, not just encryption and key management

- **Risk based security is the order of the day**
  - Apply systems engineering for safety and cyber security
  - Systematically use professional tools such as Threat Analysis and Risk Assessment (TARA), vulnerability analysis, secure by design methods, hacking invitations, and various penetration testing
  - Close known vulnerabilities as soon as possible (➔ OTA)
  - Audit your suppliers and achieve a holistic perspective on risks and solutions

It needs the ability to think like a **Criminal**
and preemptively act as an **Engineer**

Vector Cyber Security is Defined by Three Levers

Digitization

Automotive and IT industries increasingly converge. Software and IT are the major market driver in automotive. IT departments and automotive E/E must collaborate.

Vector proposition:

- Bridging best practices from IT and engineering
- Holistic systems Engineering for Security and Safety

Attacks

Critical systems are by definition insecure. A 100% security solution is not possible. Advanced risk assessment and mitigation is the order of the day.

Vector proposition:

- Risk based security assessment and engineering
- AUTOSAR software, HW based security, engineering services

Governance

Abuse, misuse and confuse cases will make it to the headlines. Especially if safety and privacy are impacted. Systematic security engineering needs a thorough culture change.

Vector proposition:

- Security culture: Competences, organization, process
- Secure by design: Infrastructures, methods, tools

Vector Cyber Security Portfolio

Security Solutions

- **Consulting**
  Vector Security Check, Security Engineering, …
- **Software**
  AUTOSAR, Re-programming ECUs, OTA, Smart Charging…
- **Tools**
  Test, Diagnosis, …
- www.vector.com/security

Trainings and media

- Training "Automotive Cyber Security"
  Stuttgart, Tue. 5. Jul. 2016
  www.vector.com/training-security
- In-house trainings tailored to
  your needs available worldwide
- Free white papers…
  www.vector.com/media-security

Questions?

Thank you for your attention.
For more information please contact us.

Vector Consulting Services

Your Partner in Achieving Engineering Excellence

Phone +49 711 80670-0 www.vector.com/consulting
Fax +49 711 80670-444 consulting-info@vector.com