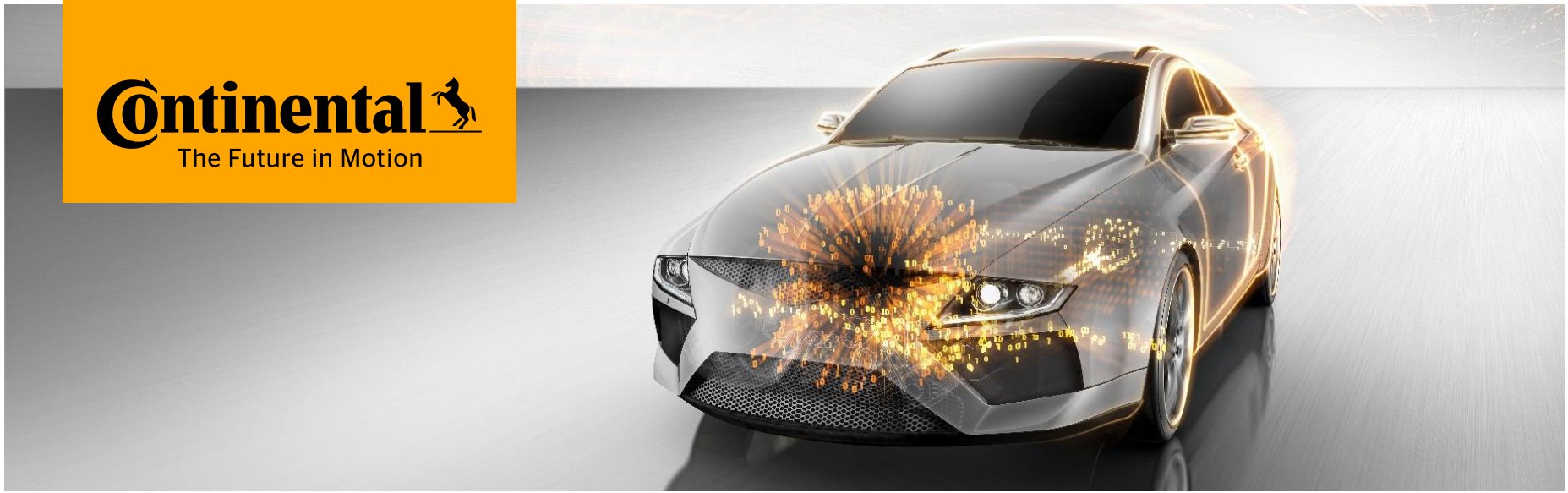
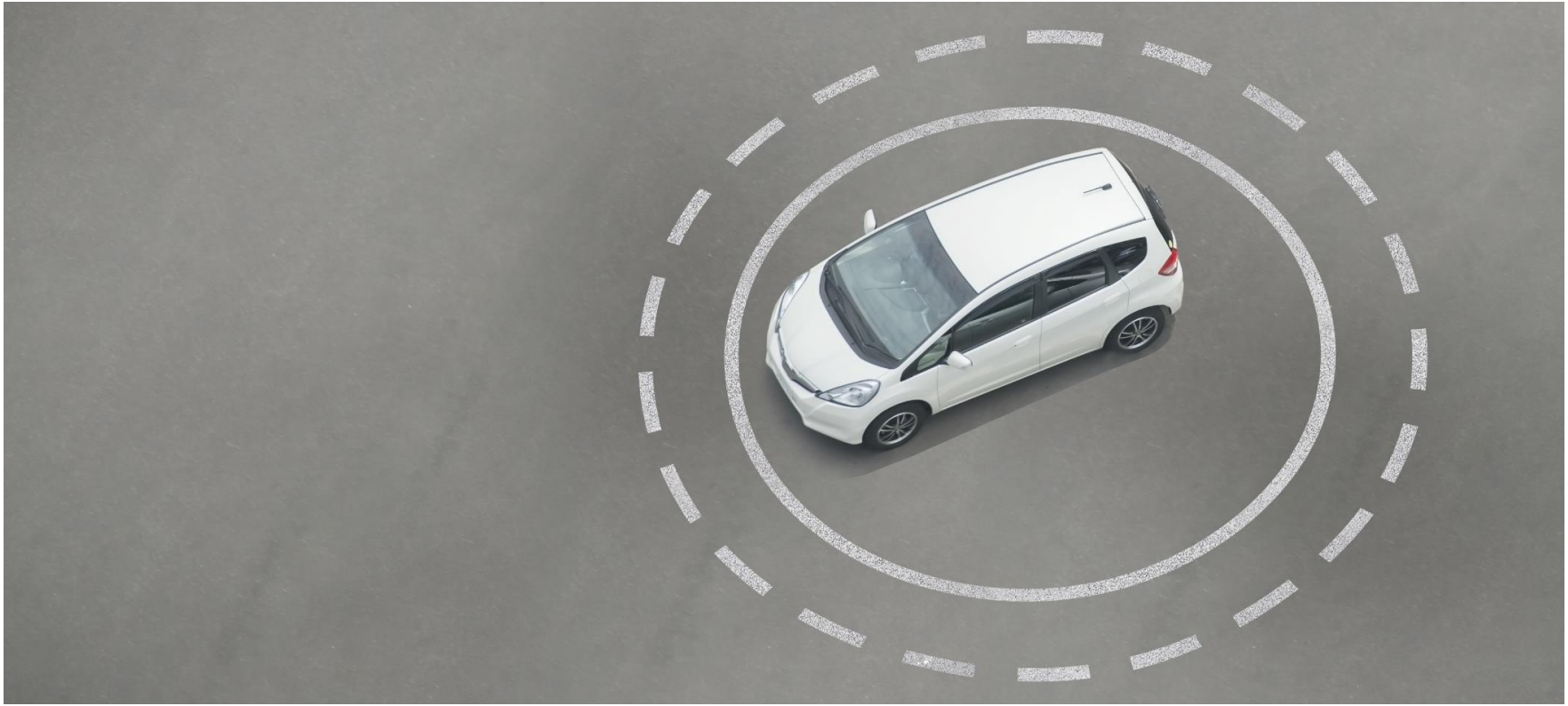


Cybersecurity in the Automotive Domain

PWIN Guest Lecture

Dr. Markus Tschersich | January 23rd, 2018 | Goethe University Frankfurt

https://www.continental-corporation.com/



Cybersecurity in the Automotive Domain
Agenda

1 **Introduction to Continental**

2 Automotive Security

3 New Challenges of Automotive Megatrends

4 Interplay of Safety and Security

5 Developing a Cybersecurity Engineering Standard

6 Entry Possibilities at Continental

„My“ Continental Location

Continental Teves | Frankfurt am Main

4,000

Employees

Chassis & Safety HQ

4 BUs, Corporate

Divisions/ Business Units

EBS, ESC

Main Products

Our Vision

Your Mobility. Your Freedom. Our Signature.

Our world is made up of:

Highly developed, intelligent technologies for mobility, transport and processing

We want to provide:

The best solutions for each of our customers in each of our markets

For our stakeholders:

The most value-creating, highly reliable and respected partner

We Shape the Megatrends in the Automotive Industry:
Safety, Environment, Information, Affordable Cars

Continental Corporation

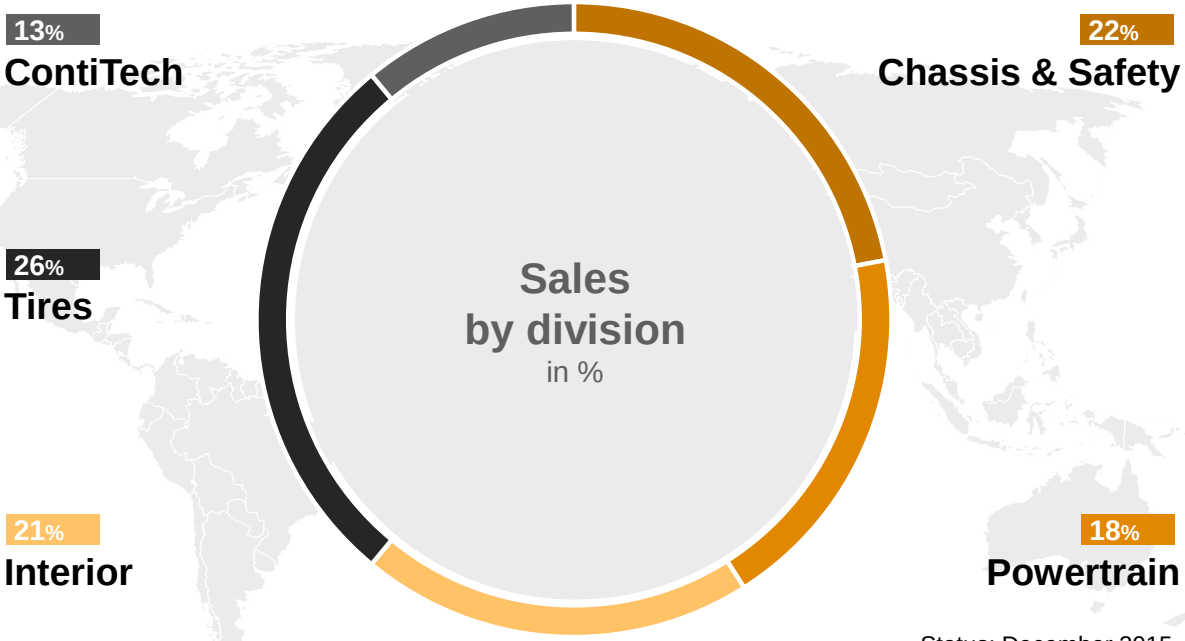
Over 140 Years of Innovation and Progress

Continental Spirit

Continental expanded its business in the 1900s and became a global supplier to the automotive industry. Today, Continental AG is headquartered in Hanover, Germany.

1871 | 1900 | 1930 | 1960 | 1990 | 2017

Continental Corporation
Overview 2016



Status: December 2015

Sales of appr.
€40.5 billion

Cybersecurity in the Automotive Domain
Agenda

1 Introduction to Continental

2 **Automotive Security**

3 New Challenges of Automotive Megatrends

4 Interplay of Safety and Security

5 Developing a Cybersecurity Engineering Standard

6 Entry Possibilities at Continental

Introduction to Automotive Security
Increasing Complexity

Increasing number of ECUs

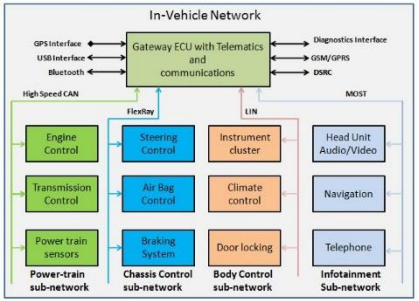
- 1997: 5 ECUs in Audi A6
- 2007: about 50 ECUs in Audi A4
- today: about 80 to 100 ECUs

Change in ECU usage

- Traditionally one task per ECU
- New trend of
  - distributing functions across ECUs
  - Integration multiple functions on one ECU

Variety of Applications

- Lane Assistance
- Collision avoidance
- Accident Reporting (eCall)
- Autonomous and Cooperative Driving



ECU: Electronic Control Unit

Introduction to Automotive Security

Understanding Security

NO

security

security „gate“

OKAY

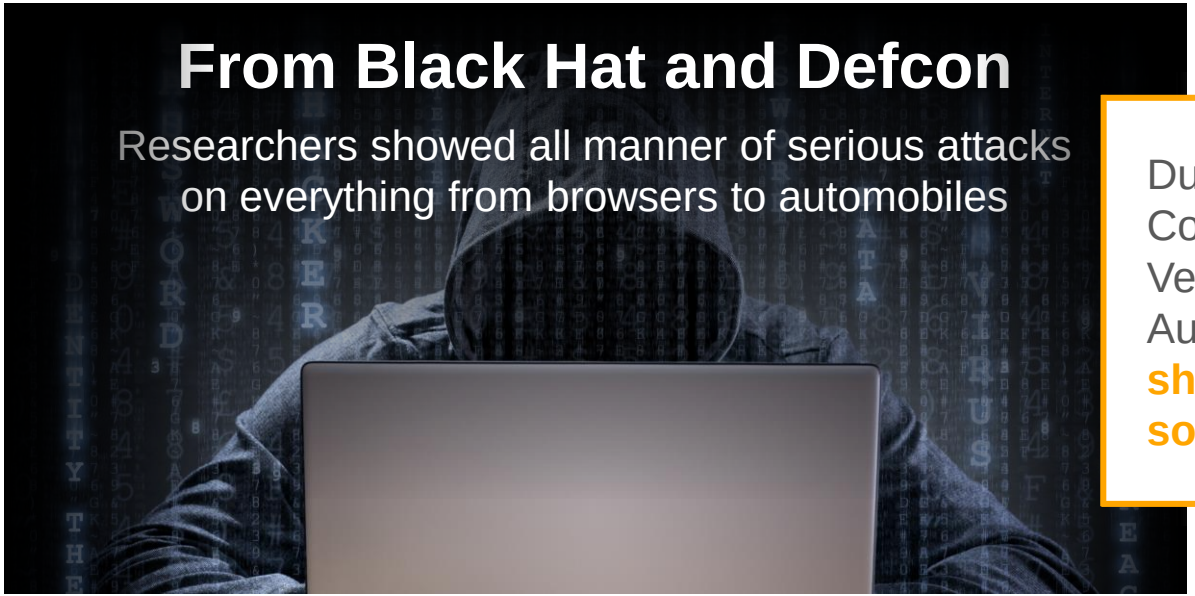
Security

BYPASSED

Unfortunately, implementation attacks are hard to predict.

Introduction to Automotive Security

Consequences from a lack of security



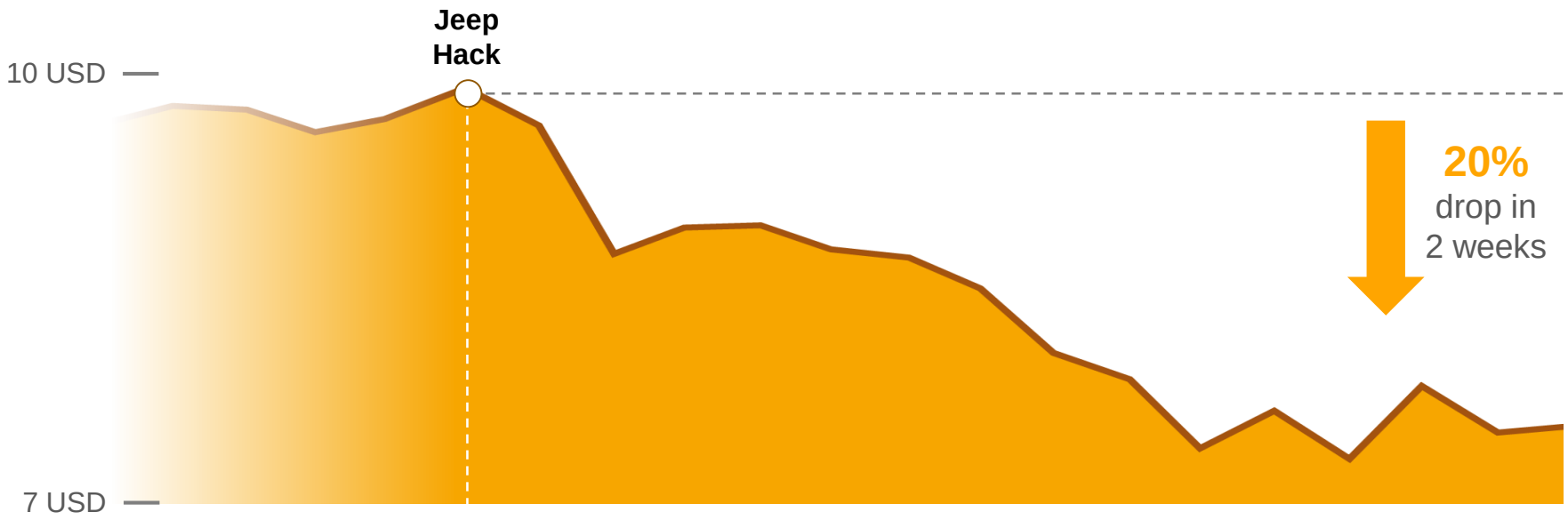
During the Hacking Conferences - “Black Hat Las Vegas & Defcon Las Vegas” Aug 2015 - a **video was shown** and **distributed via social media**.

Introduction to Automotive Security
Consequences

„After this jeep hack, **Chrysler recalled 1.4 Mio. vehicles for a security bug fix**."

Introduction to Automotive Security

Stock Value Fiat Chrysler August 2015



Introduction to Automotive Security

Stock Value Fiat Chrysler August 2015

Lack of Security has a deep impact on a companie's value

Even if the hack is done by only friendly scientists

Introduction to Automotive Security

… and more attacks with increasing press perception

< 2005

2004: DRIVING; Altering Your Engine With New Chip (NY Times)
2003: Gentlemen, Start Hacking Your Engines (NY Times)
2002: How To Hack Your Car (Forbes)

2005-2010

2010: Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study (Rutgers, USC)
2010: Experimental Security Analysis of a Modern Automobile (Center for Automotive Embedded Systems Security)
2007: Hackers can take over car navigation system (The Telegraph)
2005: RFID Chips in Car Keys and Gas Pump Pay Tags Carry Security Risks (John Hopkins University)
2005: Linux Bluetooth hackers hijack car audio (The Register)
2005: Hacking the Hybrid Vehicle (Wired)

> 2010

2016: Nissan Leaf electric cars hack vulnerability disclosed (BBC)
2014: A Survey of Remote Automotive Attack Surfaces (IOActive)
2014: Most Hackable Cars (CNN Money)
2014: How to Hack a Car (Vice)
2014: The Robot Car of Tomorrow May Just Be Programmed to Hit You (Wired)
2013: Digital Carjackers Show Off New Attacks (Forbes)
2013: Jury Finds Toyota Liable in Fatal Wreck in Oklahoma (New York Times)
2013: Adventures in Automotive Networks and Control Units (IOActive)
2013: Car Hacking: Your Computer-Controlled Vehicle Could Be Manipulated Remotely (CBS)
2013: How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles (Defcon 21)
2011: Can Your Car be Hacked? (Car and Driver)
2011: Comprehensive Experimental Analyses of Automotive Attack Surfaces (Center for Automotive Embedded Systems Security)

Introduction to Automotive Security

Odometer Example: Good old times

Expertise	› Automotive mechanist
Tools	› Specific tools or garage
Time	› Hours
Evidence	› Mechanical Traces

Video: https://www.youtube.com/watch?v=vUh-8GEhzJM

Introduction to Automotive Security

Odometer Example: Nowadays

Expertise	› Search on google › Make a call
Tools	› Tester for ODB interface
Time	› Minutes
Evidence	› No digital traces

Video: https://www.youtube.com/watch?v=orMsibfLcFY

Introduction to Automotive Security
Attackers and their Damage Categories

Thieves	› Stealing assets › Stealing vehicles
Owner/Driver	› Manipulating vehicle data › Manipulating vehicle Settings › Spoofing licences
OEM/Tier-1	› Stealing business secrets › Conducting product piracy
Software manufacturer	› Elevating privilidges
Hacker, Virus, Malware	› Stealing of personal data › Manipulating the functional safety

Damage Categories

- Property
- Image
- Business Model
- Legislation
- Know-How
- Reliability
- Functional Safety
- Privacy

Introduction to Automotive Security

Trends on Automotive Products – IT Technology

Inceasing amount of digital electronic and software

Long time ago	Past	Present	Future
			

- Simple mechanical vehicles change to intelligent, connected, and software-based IT-Systems
- Flexibility, compatibility, costs, and weight are driving the change

Introduction to Automotive Security

Trends on Automotive Products – Interconnectivity

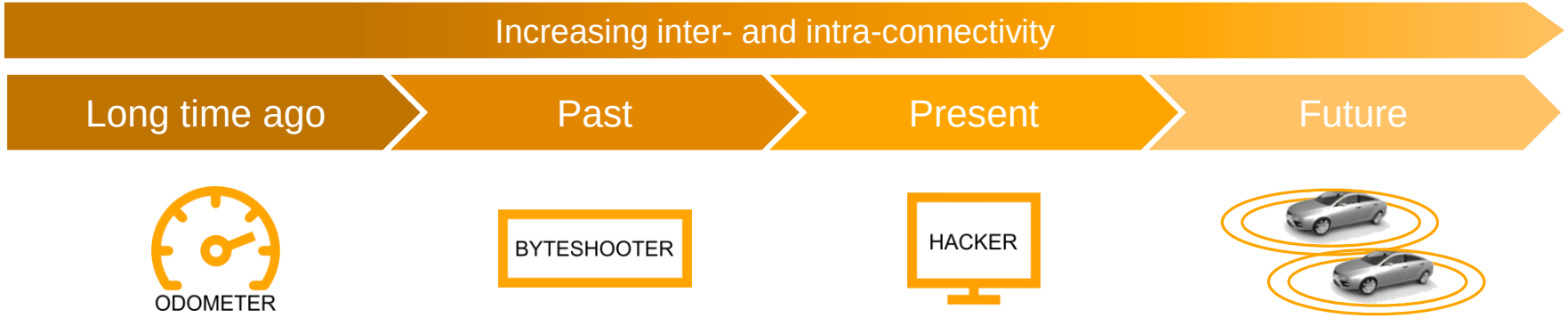
Inceasing inter- and intra-connectivity

Long time ago	Past	Present	Future
			

- Evolutionary step from closed system to a complex interconnected and interactive communication party
- The need for an efficient and safe traffic regulation is one driver next to infotainment and internet connectivity.

Introduction to Automotive Security

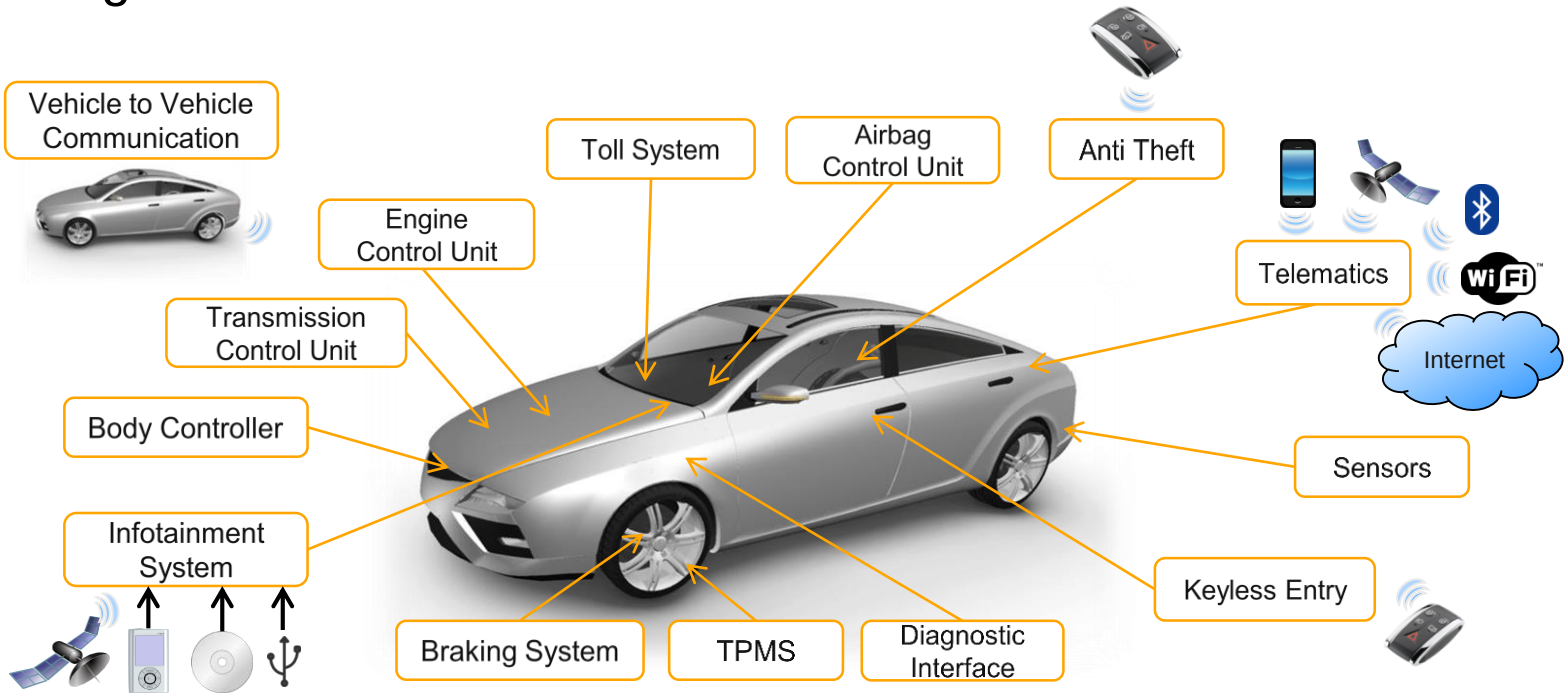
Trends on Automotive Products – Scaleability of Attacks



- Attacks are scaling from single manipulations of ECUs to organized network wide attacks
- Driver for this development on various stakeholder (owner, companies, 3rd parties): fun, fame, sabotage

Automotive Security Threats

Increasing attack surface



Cybersecurity in the Automotive Domain
Agenda

1 Introduction to Continental

2 Automotive Security

3 New Challenges of Automotive Megatrends

4 Interplay of Safety and Security

5 Developing a Cybersecurity Engineering Standard

6 Entry Possibilities at Continental

New Challenges of Automotive Megatrends
Increasing Threats and Attack Potential at the Horizon

Electric Mobility

Autonomous Driving

Information

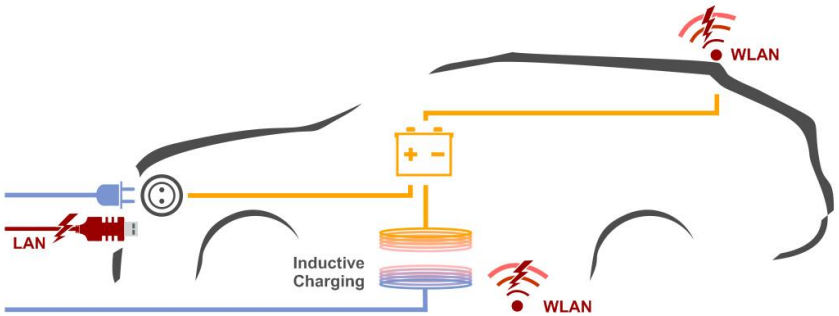
Megatrend: Electric Mobility
Infrastructure Necessary to be Protected

Charging Infrastructure

- Connects Automotive to the critical infrastructure “Electric Power”
- Electromobility is highly depending on the availability of charging infrastructure
- Implications with NIS Directive Regulation on the horizon

Payment

- Needs to be secured to avoid financial harm for supplier and/or customer



Megatrend: Electric Mobility
Attacks Based on Loss of Data Integrity

Attack on EV performance

- Different data sources used to extend range (weather, altitude difference, traffic volume)
- Manipulation can lead to unexpected performance of electronic vehicle

Attack on components

- Overheated battery triggered by manipulation of temperature sensor
- Will cause financial harm

Megatrend: Autonomous Driving

SAE J3016 - Driving Automation Definitions

	SAE Level	Name	Steering, Acceleration, Deceleration	Monitoring of Driving Environment	Fallback Performance	System Capability (Driving Modes)
Human driver monitors the driving environment	0	**No Automation**	Human	Human	Human	n/a
	1	**Driver Assistance**	Human and System	Human	Human	Some driving modes
	2	**Partial Automation**	**System**	Human	Human	Some driving modes
Automated driving system monitors the driving environment	3	**Conditional Automation**	System	**System**	Human	Some driving modes
	4	**High Automation**	System	System	**System**	Some driving modes
	5	**Full Automation**	System	System	System	**All driving modes**

Megatrend: Autonomous Driving

Automated Driving System takes over more responsibility

- Impact of errors/attacks increases due to higher range of functions
- Simple shut-down in case of attacks is not working
- Need for redundancy and fallback systems
- Higher impact on privacy due to increased need of data collection and processing

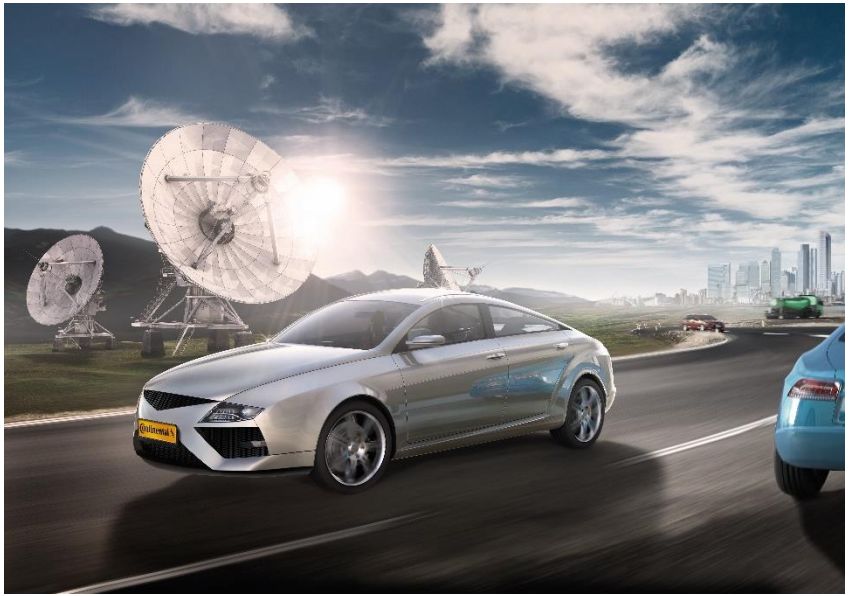
Megatrend: Information
New Opportunities and Risks of Big Data

Collection, processing and connectivity

- Improve driver assistant systems (Safety)
- More attractive/interactive infotainment systems
- Reduction of fuel/energy consumption
- Mobility Services, Smart Cities, Smart Home

Arising Risks of Big Data

- Increasing number of attack vectors
- Compliance with different legal privacy frameworks
- Higher attraction to data theft



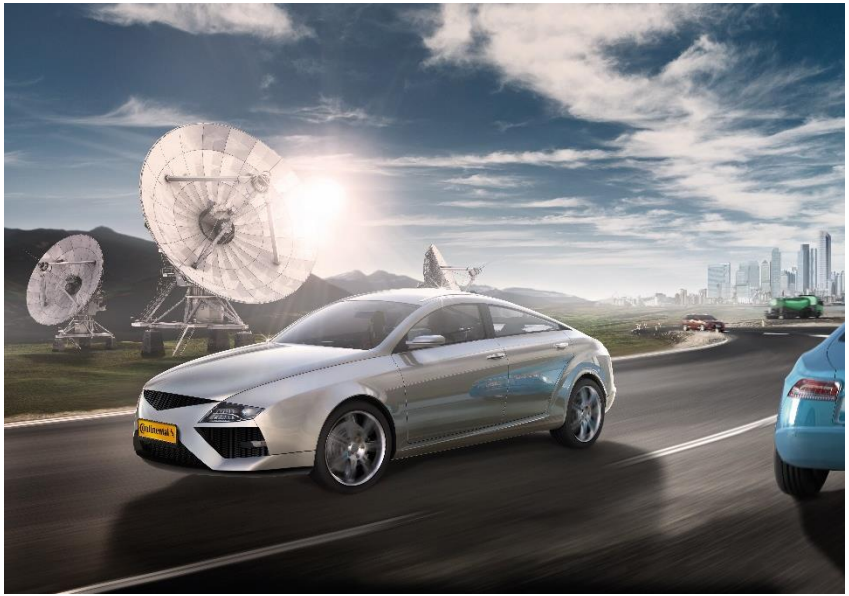
Megatrend: Information
Over the Air is Enabler and Additional Risk

Opportunities

- Smart and fast way for bug fixing and security patches
- Enables automotive app ecosystem
- Provides live information

Attack Vectors

- Connection interface can be attacked
- Risk of infected automotive apps



Cybersecurity in the Automotive Domain
Agenda

1 Introduction to Continental

2 Automotive Security

3 New Challenges of Automotive Megatrends

4 **Interplay of Safety and Security**

5 Developing a Cybersecurity Engineering Standard

6 Entry Possibilities at Continental

Ensuring Device Reliability

Interplay of Functional Safety and Security Required

- Safety a discipline with a long history in automotive
- Functional Safety and Security need to engage with each other to ensure high quality products
- Both disciplines need to be considered by the organization.

Differentiate Safety and Security

Function: Intended functional behavior

Functional Safety

Is there any risk resulting out of a faulty functional behavior?

Covered in Standard: ISO 26262

Safety in use / Safety of the intended functionality

Is there any risk resulting out of the fault free functional behavior?

Actually not standardized, in discussion for ISO 26262 2nd ed./SOTIF

Sensor HW part fault leads to wrong decision

Sensor algorithm takes wrong decision out of environment

Sensor algorithm takes wrong decision due to „jail break“ SW

Cybersecurity

Is there any risk resulting out of a faulty functional behavior?

Annex in ISO 26262:2018
Sep. Standard: ISO-SAE 21434

Differentiate Safety and Security

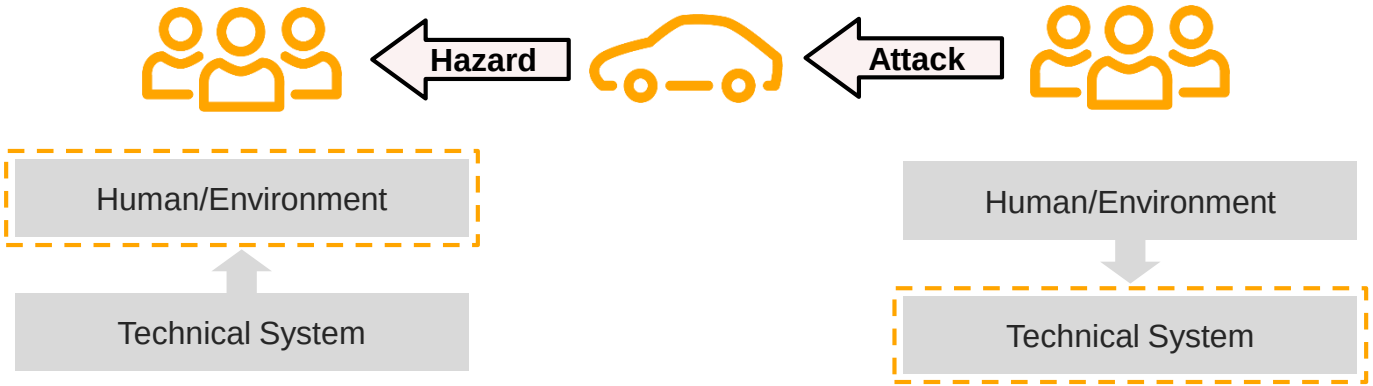
Security vs. Functional Safety

Functional Safety

- Protect human against threats proceeded from (known) technical systems.

Security (IT/Cyber)

- Protect a technical system against attacks (basically unknown) as well as disturbances from the environment or caused by human.



Differentiate Safety and Security
Similarities between Safety and Security

Risk oriented approach
- What can go wrong? How likely is it? What will the consequences be? (note: differences in probability estimations)

Development process
- Safe and secure software is achieved by using a systematic development approach rather than reactive patching

Testing
- Comprehensive testing is essential for confidence in the final product

Redundancy
- Double instances of safety/security mechanisms does not necessarily lead to double safety/security

Ultimate objective
- Achieving a **sufficiently safe/secure product**

Culture and values
- Knowledgeable, motivated and committed management and employees is a success factor for achieving safe and secure products

Differentiate Safety and Security

Differences between Safety and Security

Classification of consequences

- In safety typically divided into several levels (e.g. SIL/ASIL/DAL)
- In security quite binary, system is either compromised or not

Threat analysis, risk assessment

- In safety we have pretty well known, static fault models and fault assumptions
- In security threats changes regarding motivation, knowledge and attack vectors

Non-experts understanding

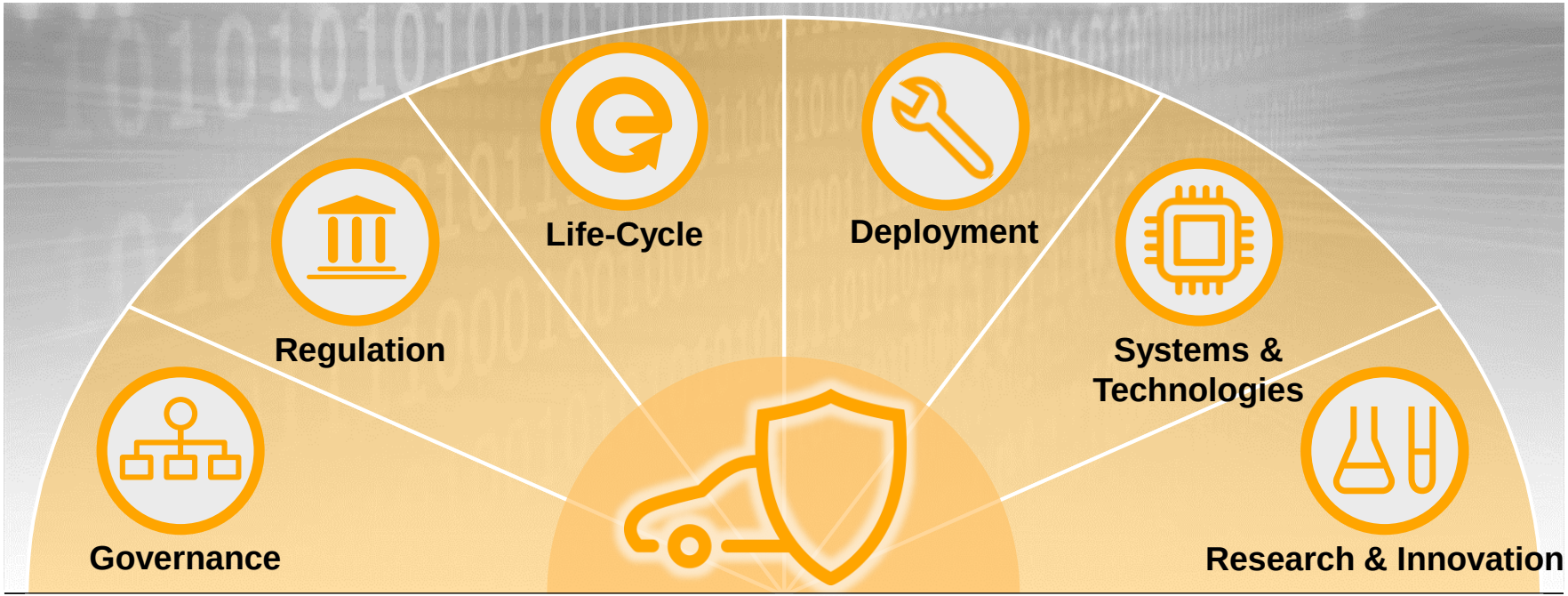
- In safety the consequences are easily understandable
- In security the threat models are often met with scepticism and might be judged as paranoid

Knowledge of experience

- In the safety domain there is a culture of discussion and sharing of experience
- In security, business actors tend to keep their experiences to themselves, thus efficiently slowing down the collective expertise

Address Challenges of Security in Automotive

Parts of the Holistic Approach



Part: Governance
Preparation of the Organisation Necessary

Management

- **Security Strategy**
  Consideration by Management for the overall strategy
- **Processes**
  Revise processes with security respective activities and work products
- **Standardisation**
  Harmonization of internal and external activities
- **Compliance and Audits**
  Ensure correct implementation of security measures over time

Culture

- **Awareness of Management and Engineers**
  Inform about security threats and their impact
- **Trainings, Competence Management**
  Ensure technical skills to address security threats appropriately
- **Security Engineering**
  Consider security in the design
- **Lessons Learned**
  Consider known threats and effective countermeasures

Sustainability

- **Surveillance and Cyber-Defence**
  Awareness about new threats appearing in the field
- **Incident Management**
  Effective and lean processes to mitigate security incident short-term
- **Knowledge Management**
  Documentation of effective solutions

Approach: Regulation
Not Exhaustive List of Regulations | 1

International

- UNECE WP.29 TF Cybersecurity and OTA issues

Europe

- Joint Communication on „Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" (JOIN (2017) 450
- Product-specific Certification, e.g. Tachograph, Event Data Recorder (AD), C-ITS
- General Data Protection Regulation
- NIS Directive (might be relevant in future)

Approach: Regulation
Not Exhaustive List of Regulations | 2

China

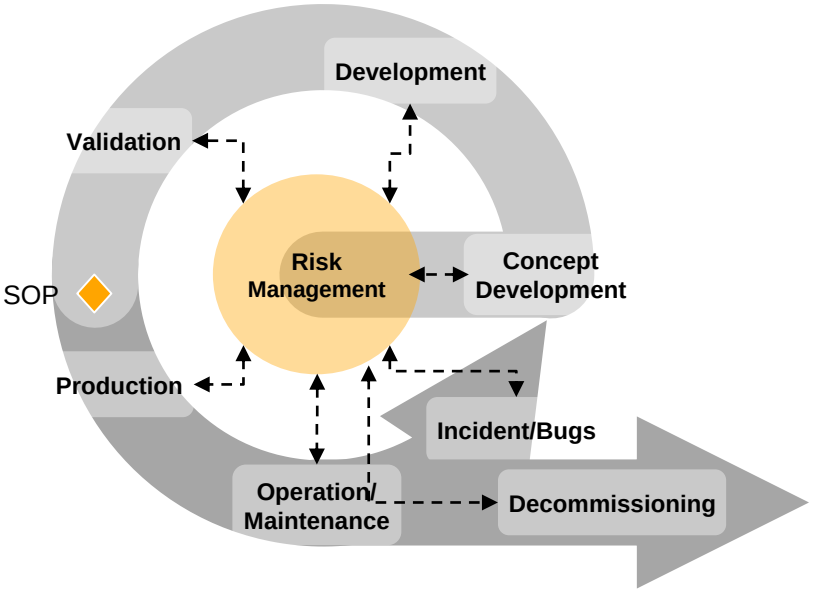
- Cybersecurty Law (中华人民共和国网络安全法)
- Cryptographic Law Draft (中华人民共和国密码法)

USA

- Self-Driving Car Act

Part: Life-Cycle
Consider Cybersecurity from Cradle to Grave

- Low impact by Cybersecurity
- Shall be stable within organisations
- Product independent within organization
- Slight tailoring for specific products
- Clear interfaces due to harmonization in distributed development

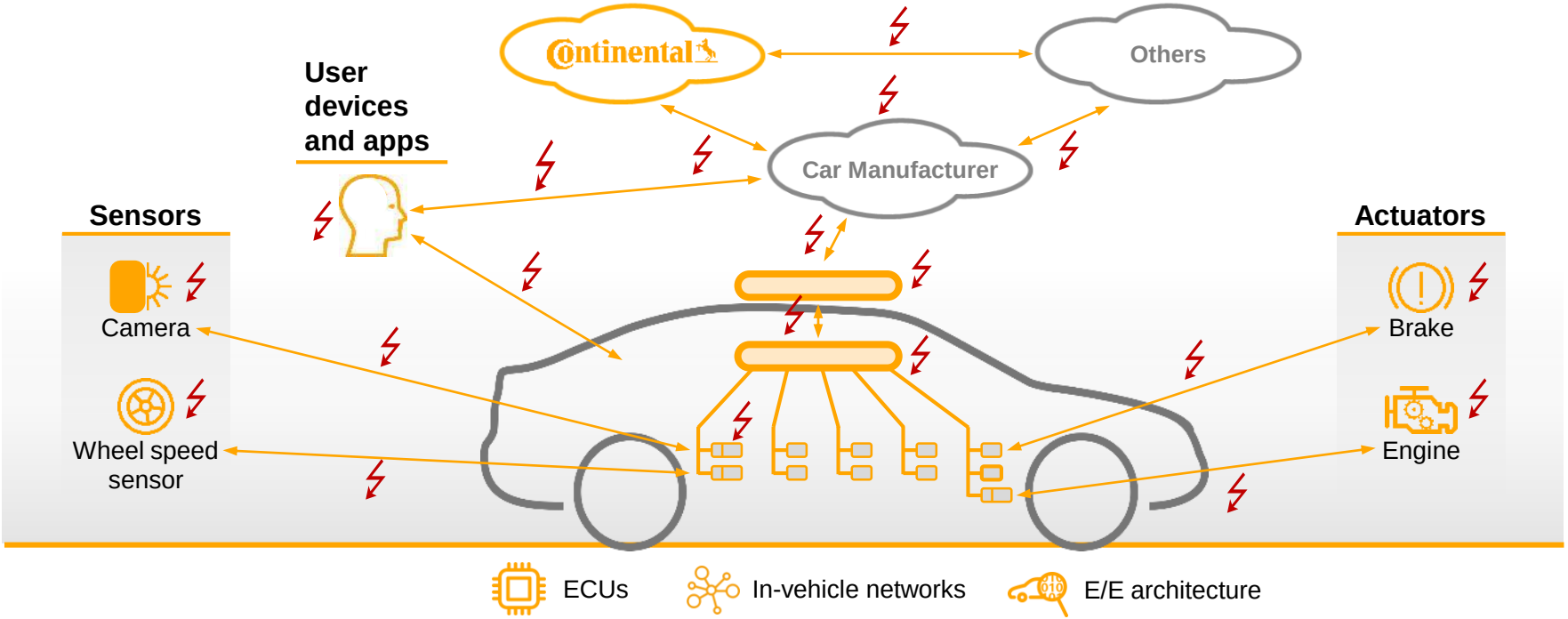


Part: Deployment
Establish Cybersecurity on the Operational Level

- Medium impact by Cybersecurity
- Defined methodologies for transparent and comprehensible decisions, e.g.
  - Risk Management
  - Security Testing
- Supply Chain Management
  - Clear assignment of responsibilities
  - Engineering Interface Agreement
- Dedicated Security Services
  - Online Trust Center
- Configuration & Vulnerability Management

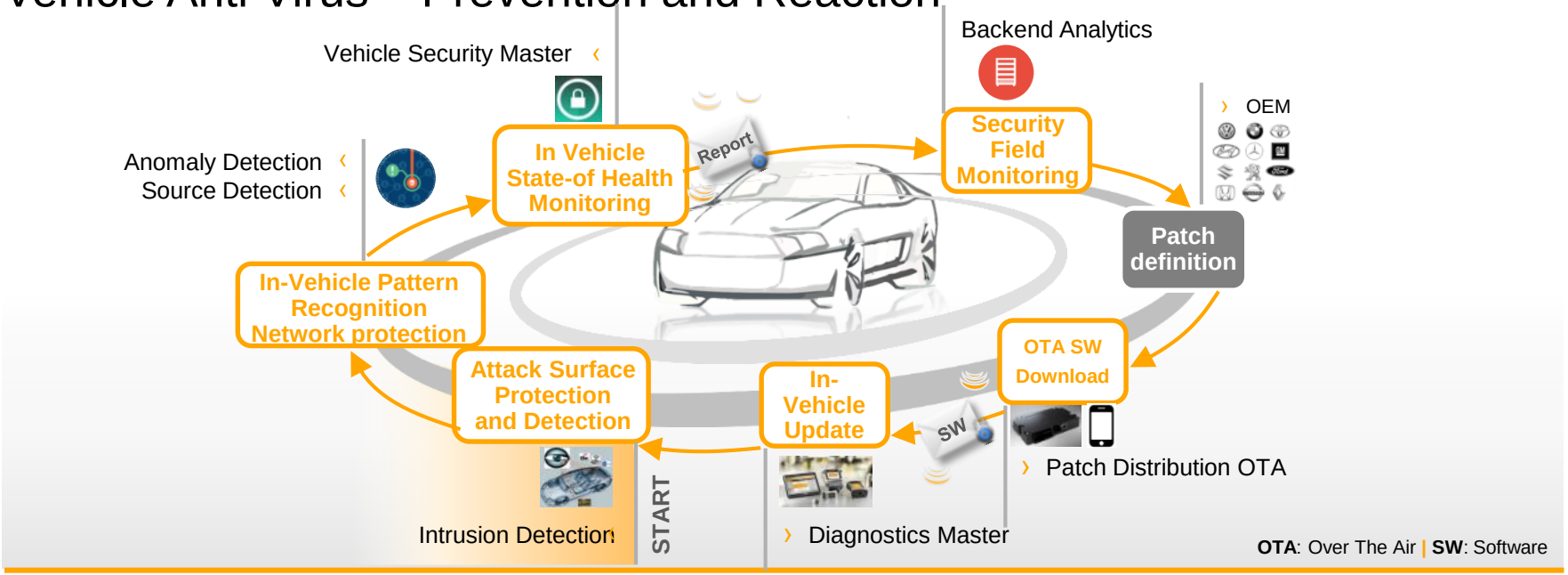
Part: Systems & Technologies

Secure Data, Secure Network, Secure Components



Part: Research & Innovations

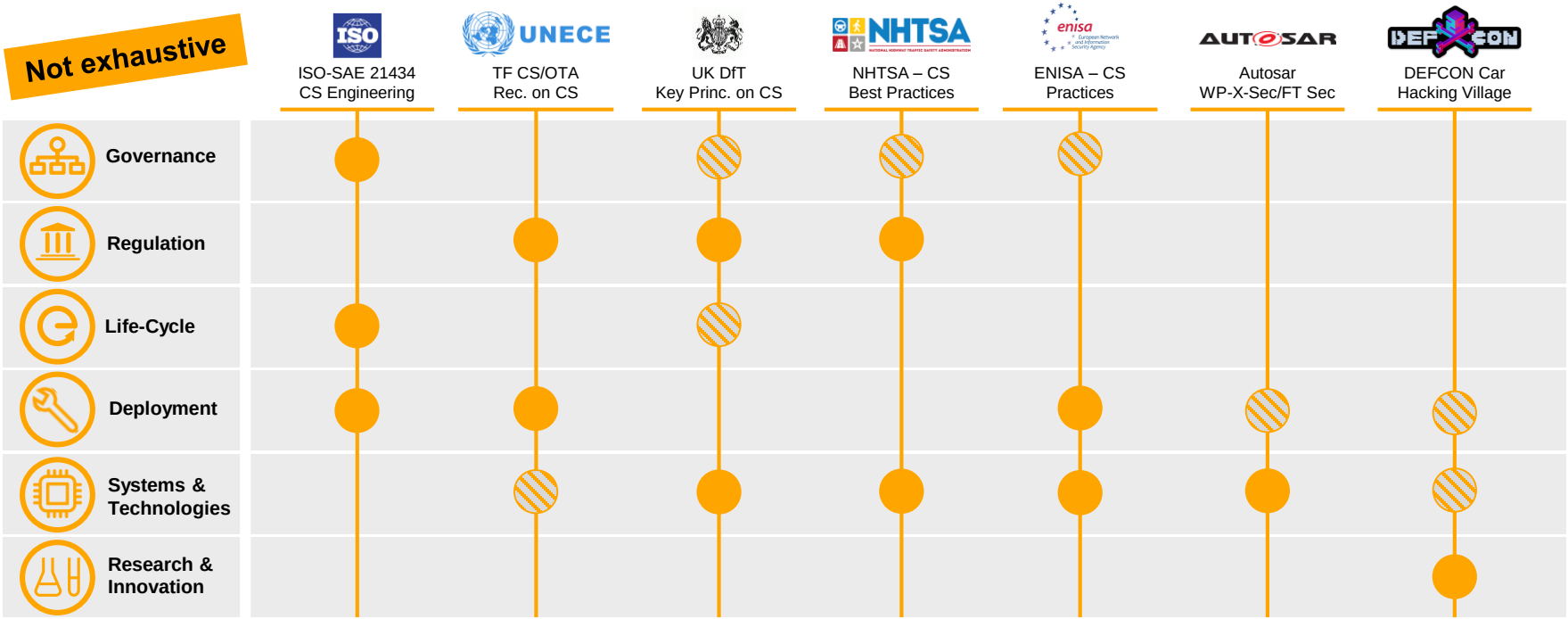
Vehicle Anti Virus – Prevention and Reaction



Cyber Security needs to be continuously observed and if needed be patched

Challenges of Security in Automotive

Different Activities needs to be Considered



Cybersecurity in the Automotive Domain
Agenda

1 Introduction to Continental

2 Automotive Security

3 New Challenges of Automotive Megatrends

4 Interplay of Safety and Security

5 **Developing a Cybersecurity Engineering Standard**

6 Entry Possibilities at Continental

Standardizing Cybersecurity Engineering
Goals of the Initiative

The future standard shall…

1. Give uniform definition of notions relevant to automotive security
2. Specify minimum requirements on security engineering process and activities and define – wherever possible – criteria for assessment
3. Describe the state of the art of security engineering in automotive E/E development

Targeted effects on automotive industry

- Common and internationally agreed understanding of automotive cybersecurity engineering
- Sufficient rigor as reference for legislative institutions; ensure legal certainty

Road Vehicles – Cybersecurity Engineering

Towards a joint ISO/SAE Standardization Project

2014/2015	Preparatory work independently within VDA, SAE: research and drafting
01/2016	Publication of SAE J3061 “Guidebook for Cyber-Physical Vehicle Systems
01/2016	Submission of ISO NWIP3556 “Automotive Security Engineering” (Germany)
04/2016	Submission of ISO NWIP3586 based on SAE J3061 (USA)
05/2016	ISO/TC22 approves NWIP3556 and NWIP3586
06/2016	Start of negotiations at ISO/TC22 and SAE level about joint project
09/2016	PSDO* Agreement signed by ISO and SAE; Agreement to start joint project as PSDO
10/2016	ISO TC22/SC32 starts Project AWI 21434
10/2016	Kick-Off Meeting of ISO/SAE Joint Working Group in Munich

*Partnership Standards Development Organizations

Standardizing Cybersecurity Engineering
ISO/SAE 21434 – Overview

Joint Working Group

Working Groups within ISO
- ISO/TC22/SC32/WG11 - Cybersecurity
- JWG for ISO/SAE Cybersecurity Engineering

Co-Convenors
- SAE: Lisa Boran (Ford, US)
- ISO: Gido Scharfenberger-Fabian (carmeq/VW, DE)

Expert Groups
- 12 national delegations are involved

Document

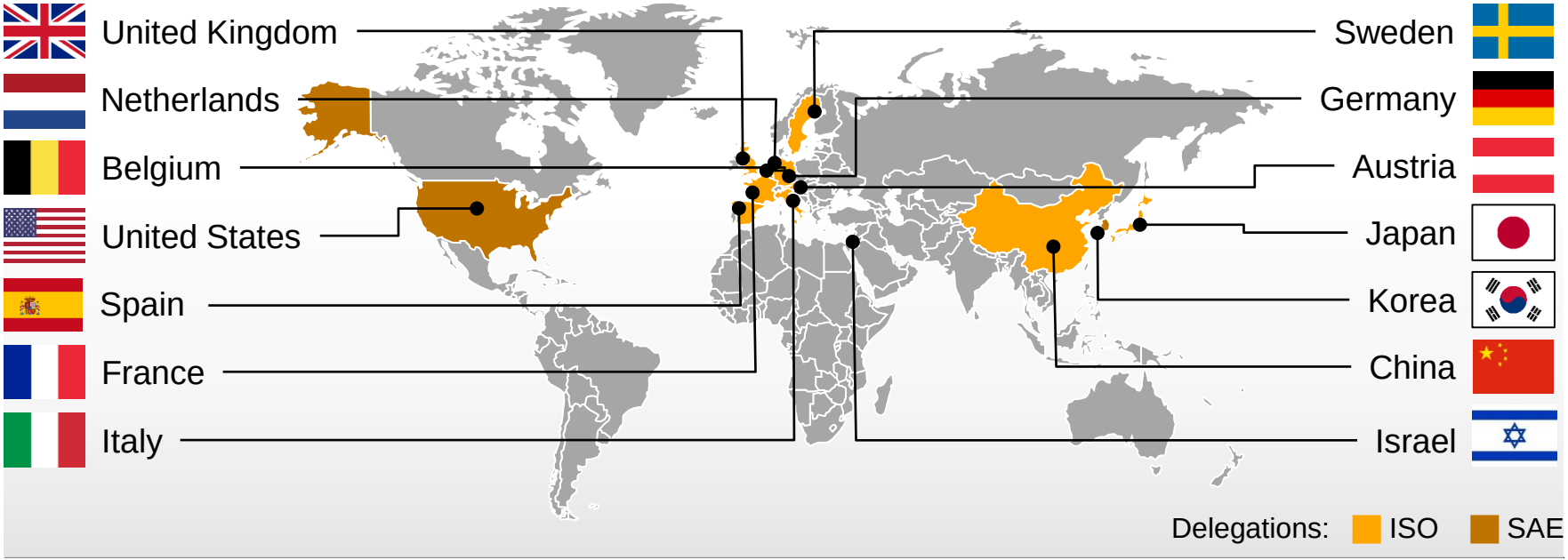
Standard
- ID: ISO/SAE 21434
- Title: Road vehicles – Cybersecurity Engineering

Scope
- Requirements for cybersecurity risk management
- process framework
- Common language
- Road vehicles (pre-defined by TC22)

Expected Publication Date
- Begin of 2020

Road Vehicles – Cybersecurity Engineering

National Delegations



Road Vehicles – Cybersecurity Engineering

Involved Organizations

OEM

BMW, VW, Opel, DAIMLER, Ford, FCA (FIAT CHRYSLER AUTOMOBILES), HONDA, GM, JAGUAR, LAND ROVER, VOLVO, TOYOTA, NISSAN MOTOR COMPANY, RENAULT

Tier-1

Continental, BOSCH, DELPHI, Honeywell, MAGNA, MAGNETI MARELLI, JTEKT 株式会社ジェイテクト, DENSO, HELLA, HITACHI, Valeo, ZF

Supplier

SYNOPSYS, VECTOR, RENESAS, infineon, ON, QUALCOMM, Melexis, LEAR CORPORATION, Panasonic, Karamba Security, TOWERSEC, kapsch

Cert. Body

BUREAU VERITAS, SGS, TÜV SAAR, UL, TÜV NORD, TÜV SÜD, CERAM GROUPE UTAC CERAM

Regul. Body

CATARC, RDW, NIST

Consulting

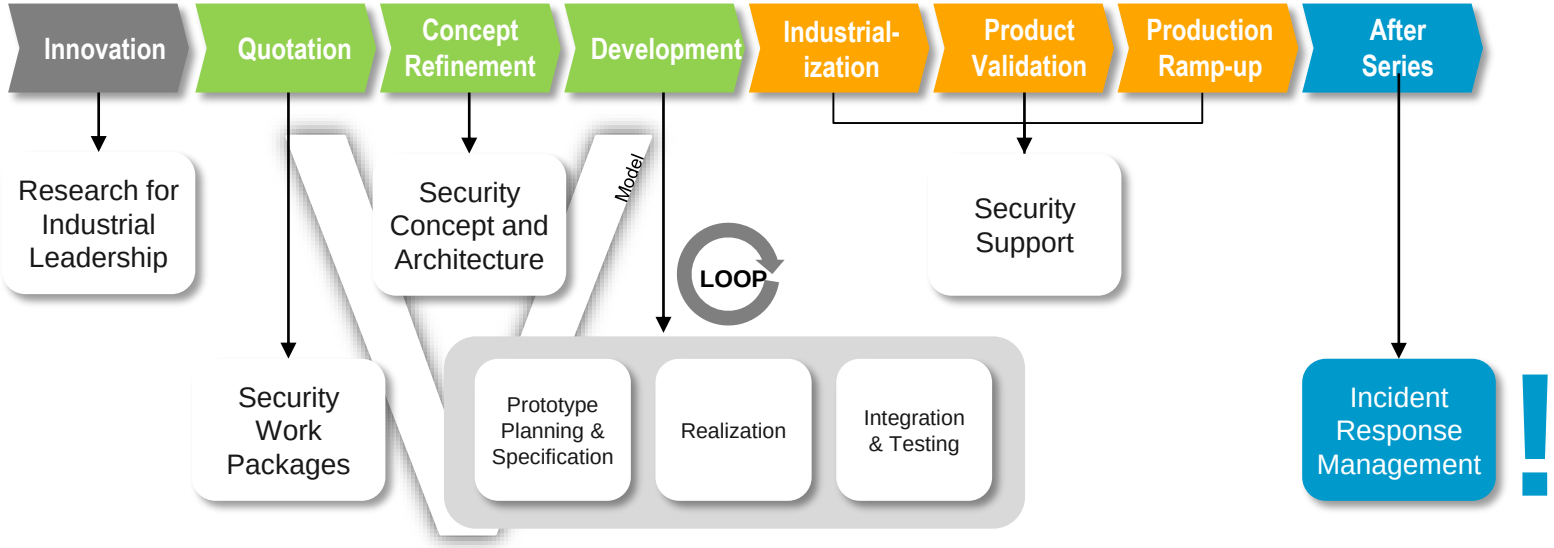
methodpark, secunet, THALES

Academia

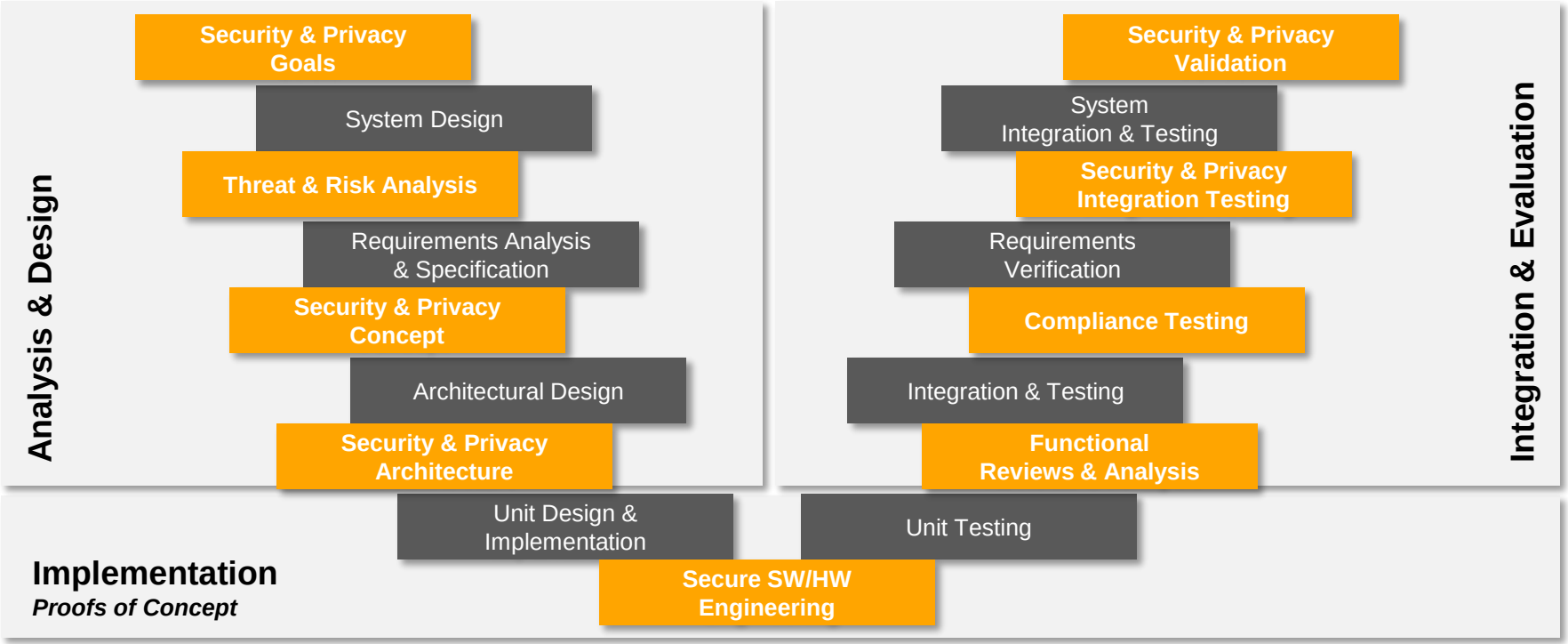
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY, SwRI, WMG THE UNIVERSITY OF WARWICK

Standardizing Cybersecurity Engineering

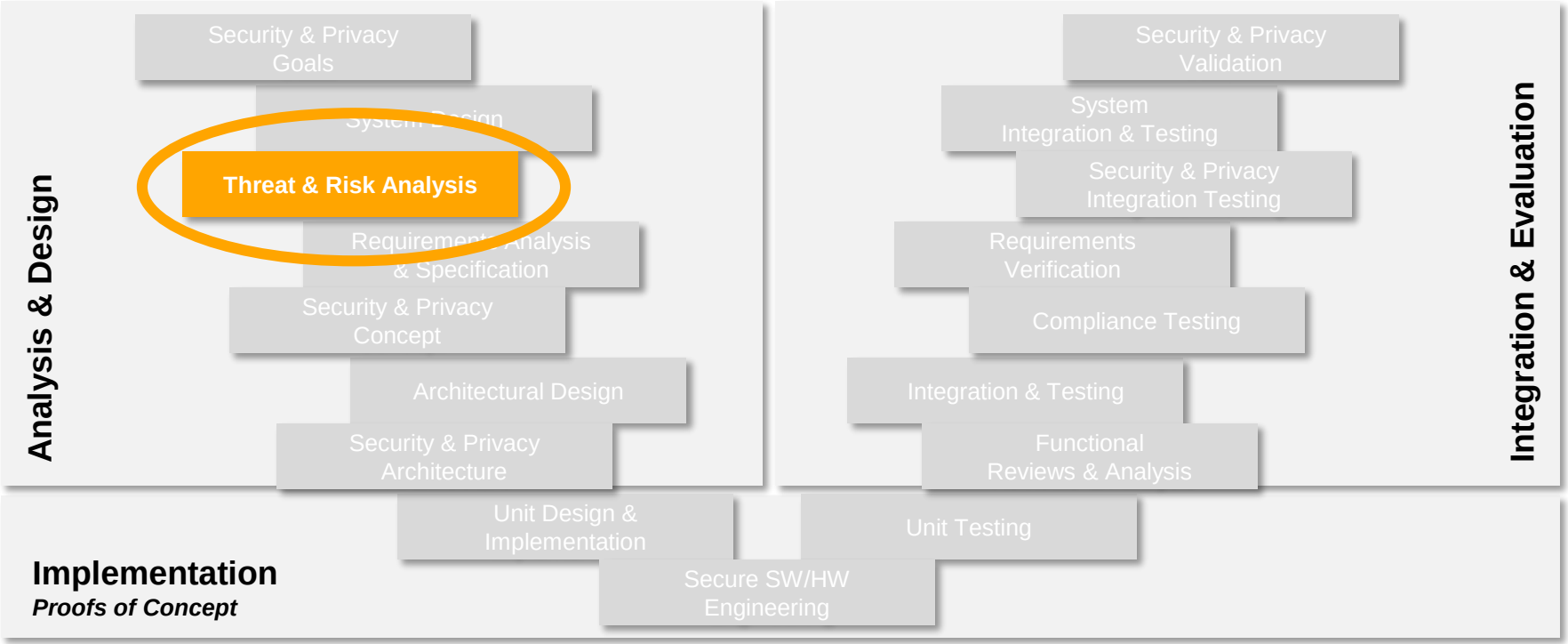
Security in the whole Product Life Cycle



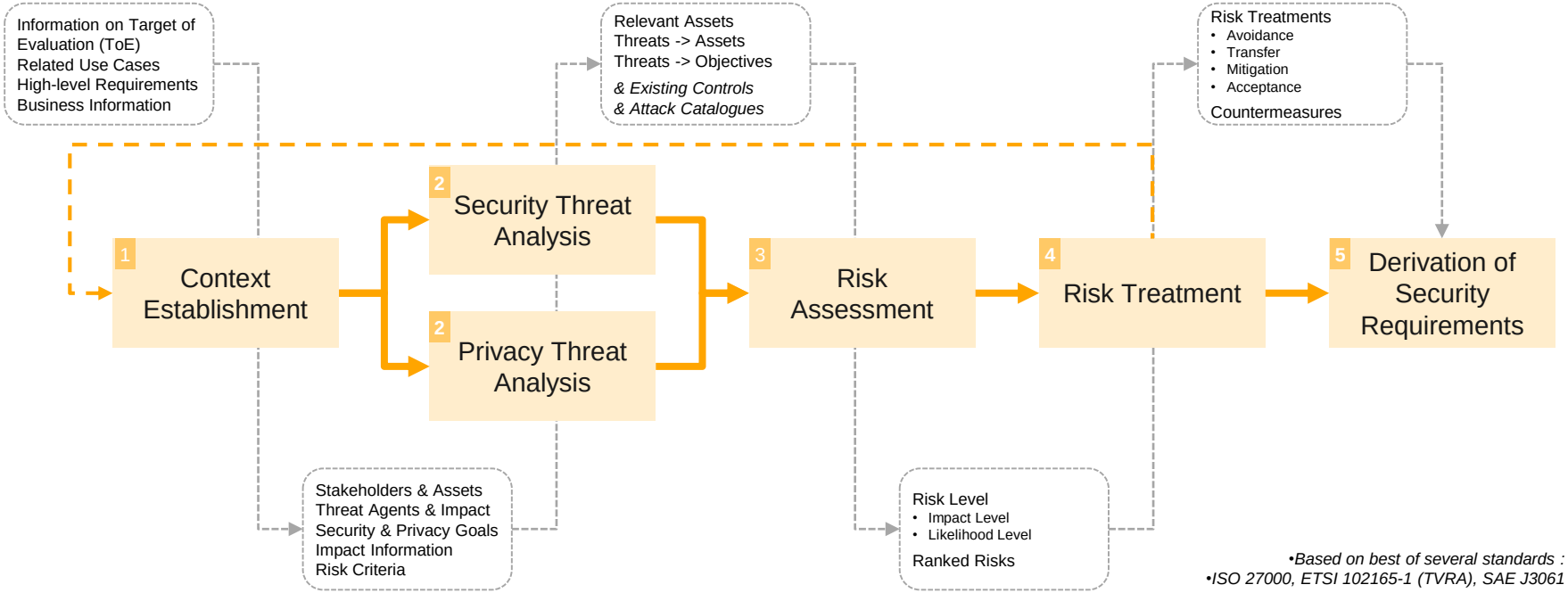
V-Model: Security & Privacy



V-Model: Security & Privacy



Threat Analysis and Risk Assessment (TARA*)



•Based on best of several standards :
•ISO 27000, ETSI 102165-1 (TVRA), SAE J3061

Cybersecurity in the Automotive Domain
Agenda

1 Introduction to Continental

2 Automotive Security

3 New Challenges of Automotive Megatrends

4 Interplay of Safety and Security

5 Developing a Cybersecurity Engineering Standard

6 **Entry Possibilities at Continental**

Entry Possibilities at Continental

This is Continental

- Truly international team around the globe
- Performance-oriented working atmosphere
- Early responsibility and exciting job challenges
- Achieving exceptional results through passion
- Open & informal culture: open doors & open minds
- Innovative Technology
- Significant contribution to sustainable mobility

Entry Possibilities at Continental

From Internship to Permanent Position

Possible entries at **Continental AG**

Students

- **Student** @Continental
- **Intern-ship**
- **Working Students**
- **Thesis**

Graduates

- **Continental Trainee & Graduates Programs**
- **Direct Entry**

Professionals

- **Direct Entry**

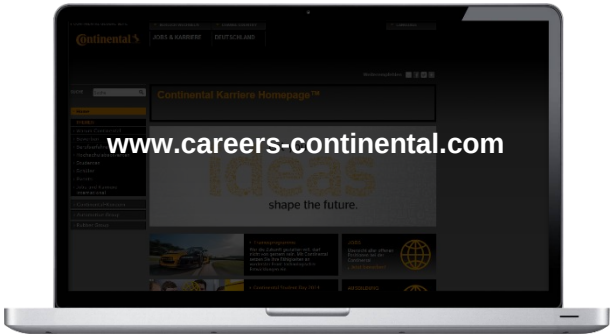
Entry Possibilities at Continental
Internship and Thesis

Requirements:

- **Apply 2 to 3 months before** your preferred internship start date
- Duration: **3-6 months**
- Current certificate of matriculation
- Very good language skills in **English**
- Proficient experience in working with **MS Office** (esp. Word, Excel, Power Point)

Take your chance!

Apply online:



Have we sparked your interest?
Then spark ours!

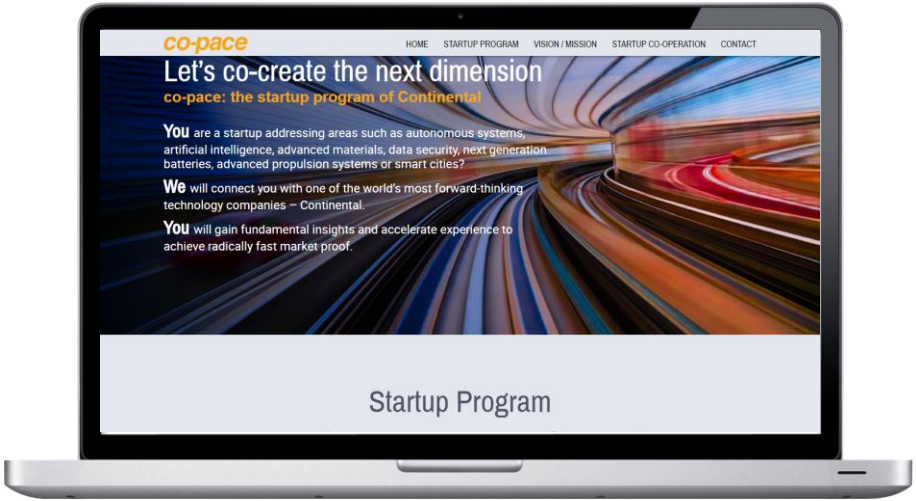
www.careers-continental.com

www.facebook.com/ ContinentalCareer

www.continental-people.com

Have we sparked your interest?
Then spark ours!

www.co-pace.com



Corporate Systems & Technology
Contact Details

Specialist Security & Privacy

Dr. Markus Tschersich

Continental Teves AG & Co. oHG
Cross Divisional Systems
Security & Privacy Competence Center
Guerickestraße 7
60488 Frankfurt am Main, Germany

Phone: **+49 69 7603-1832**

eMail: **markus.tschersich@continental-corporation.com**