TeleTrusT
Pioneers in IT security.

Informationstag "Das Automobil als IT-Sicherheitsfall"

Berlin, 11.05.2012

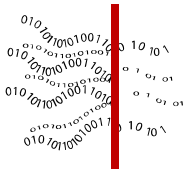
IT-Sicherheitsprüfverfahren im Automotive-Umfeld

Markus Bartsch

TÜViT®

IT Security und IT Safety

Security **SECURITY** Security



TÜViT®

Threats

by man

→ Protection of **IT**

Safety **SAFETY** Safety

TÜV NORD

Hazards

by **IT**

→ Protection of **man**

Hintergrund
2 Studien

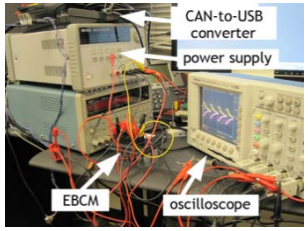
- Experimental Security Analysis of a Modern Automobile - 2010
- Comprehensive Security Analysis of Automotive Attack Surfaces – 2011

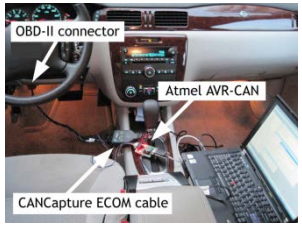
- Embedded Systems
  - ECU (Electronic Control Units) und Interaktionen
  - Telematic
- Bedrohungsmodell
  - Physikalischer Zugang
  - Virtueller Zugang

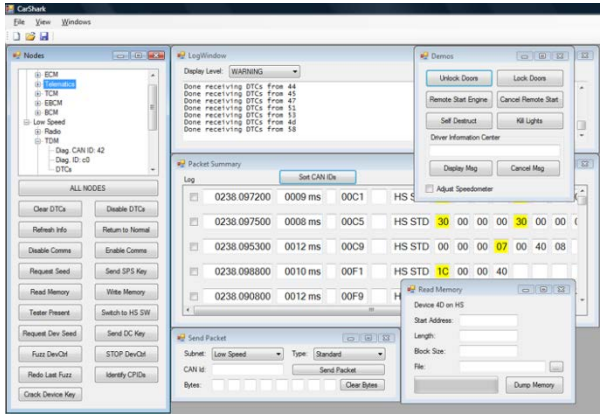
- „Normgerechte“ Prüfmethoden

Experimentelle Security Untersuchungen

- Vorgehen:
  - Test einzelner ausgebauter Komponenten
  - stehendes Fahrzeug (Stationary Testing)
  - Fahrzeug während der Fahrt (Road Testing)
- Monitoring Tool (CarShark)
- Komponenten:
  - ECM
  - EBCM
  - TCM
  - BCM
  - Telematics Module
  - RCDLR
  - HVAC
  - SDM
  - IPC/DIC
  - Radio
  - TDM



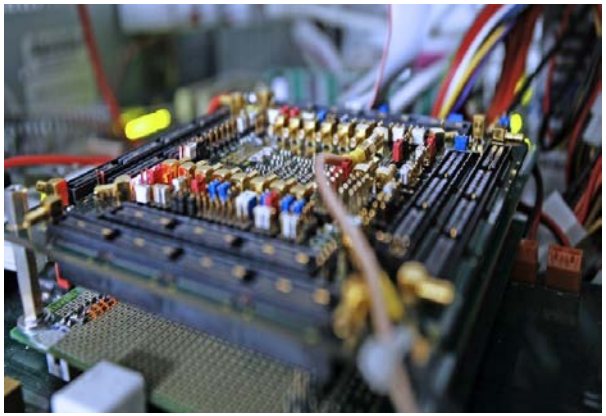




Einfache Angriffszenarien

Intra Vehicle Network Security

- CAN Bus
  - Broadcast Nature
  - DoS – Denial of Service
  - keine Authentisierung
  - Schwache Access Control
  - → Firmware Updates
  - → „offene“ Diagnose
- Abweichung von Standards

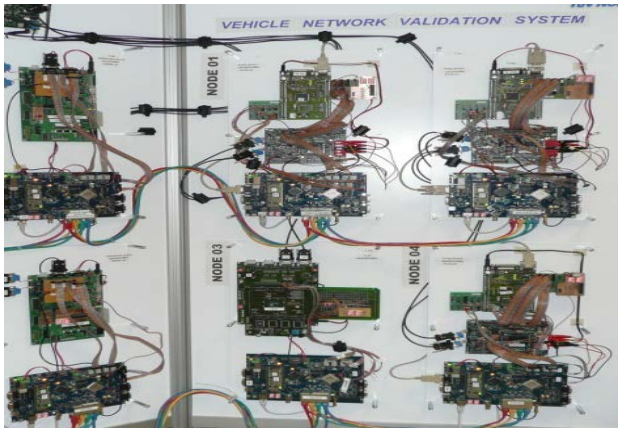


Component Security

- Angriffsmethoden
  - Sniffing / Probing
  - Fuzzing
  - Reverse Engineering
- Testing (Stationary / Road)
  - Radio / Display ✓
  - IPC – Instrument Panel Cluster ✓
  - BCM ✓
  - Engine ✓
  - Brakes ✓
  - HVAC ✓
  - generic DoS ✓

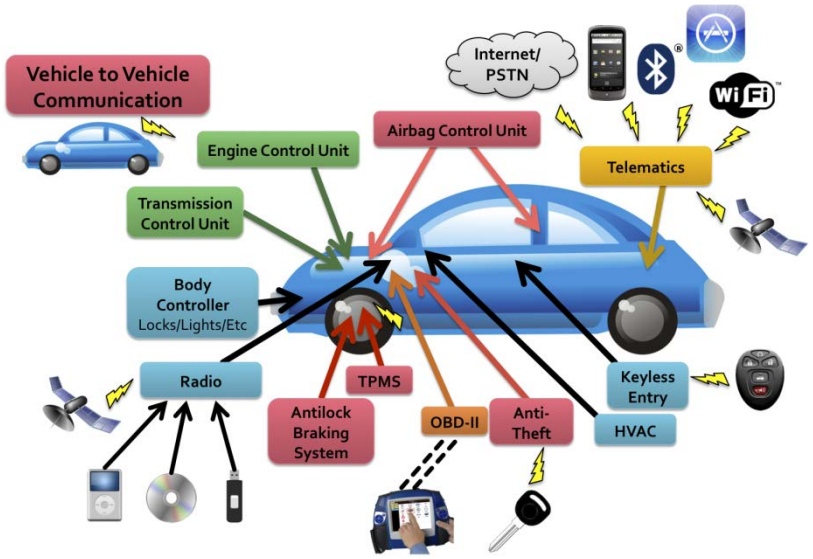
Komplexe Angriffszenarien

- Speedometer
- „Lights Out“
- „Self-Destruct“
- Bridging
- Hosting / Wiping Code



Angriffsvektoren – virtueller Zugang

- **Indirekter physikalischer Zugriff**
  - Media Player
  - OBD
- **Short Range wireless - Bluetooth**
  - Indirect
  - Direct
- **Long Range wireless**



IT Security und IT Safety

Security **SECURITY** Security

Safety **SAFETY** Safety

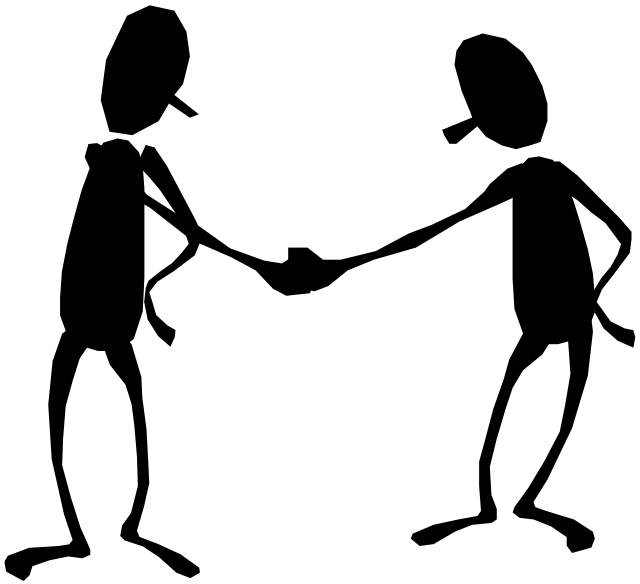
Threats
by man
→ Protection of **IT**

Hazards
by **IT**
→ Protection of **man**

Common Criteria

IEC 61508
ISO 26262

Common Criteria



CONFIDENCE

in implemented

Security Measures

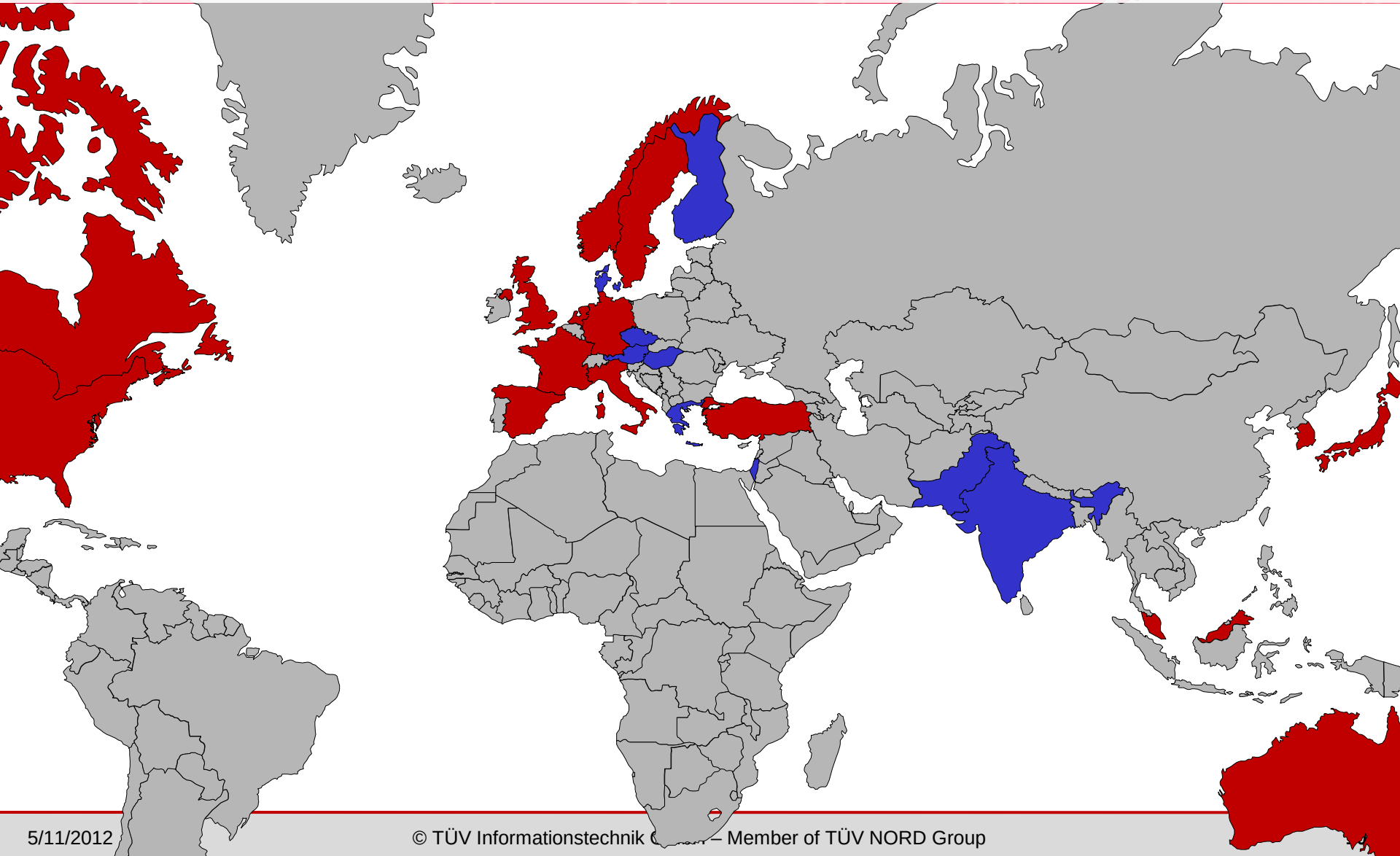
CC Recognizing Countries (CCRA)

Certificate Authorizing

Common Criteria – CCRA

Certificate Issuing and Consuming Nations

Certificate Consuming Nations



Automotive Anwendungen der CC
Beispiele von PP

- Digital Tachograph
  (Vehicle Unit, Tachograph Card)

- Alcohol Interlock

- Boordcomputer Taxi

CC Paradigm - 1

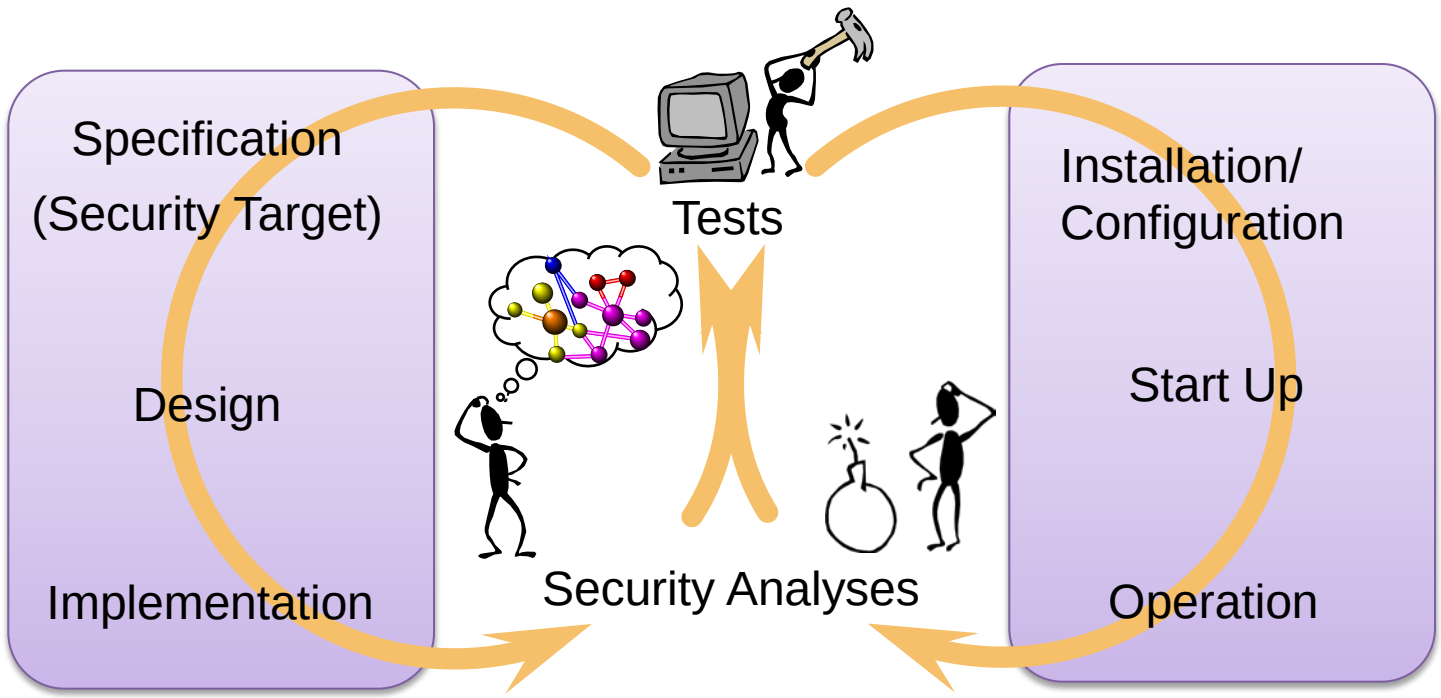
Assets
Usually information/data stored, processed and transmitted by IT products

Threats
Threat agent (e.g. hacker) act adverse (e.g. remotely copying) on an asset (e.g. data on HD)

Countermeasures
Security mechanisms to protect assets

Assurance
Confidence in correct and effective implementation of countermeasures

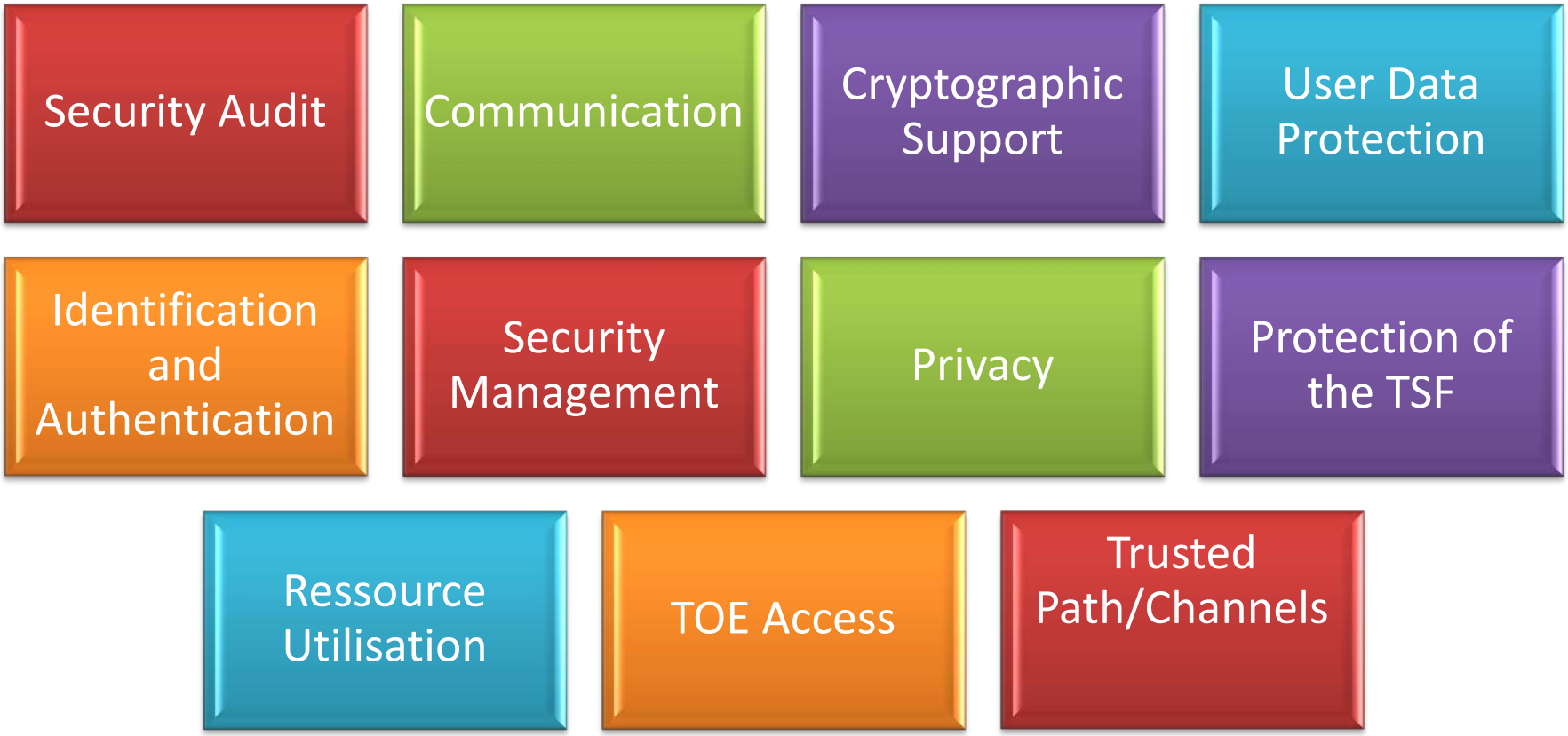
Evaluation Methodology: Life Cycle Review



Development Environment

Operational Environment

Functional Requirements Overview



Evaluation Assurance Levels - EAL

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life-cyle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	1	2	2	3	4	5	5

Fazit
Automobil als „vernetzte Maschine“

- **IT Security** / **Automotive Security** ist essentiell
  - **IT Security** Komponenten müssen verbaut werden
  - **Safety** Anforderungen müssen beibehalten werden

→ **IT Security** in **Real-Time**

- ***Nachvollziehbarkeit*** der **IT Security**
  → Nutzung bestehender Standards (**CC**)
  → Anpassung von Standards
    - **Security** vs **Safety**

Vielen Dank!

TÜV Informationstechnik GmbH
Unternehmensgruppe TÜV NORD

Markus Bartsch
IT Security

Langemarckstr. 20
45141 Essen
Germany

Phone: +49 201 8999 – 616
Fax: +49 201 8999 – 666
E-Mail: m.bartsch@tuvit.de
URL: www.tuvit.de

Referenzen:
www.autosec.org
www.commoncriteriaportal.org
www.bsi.de
http://www.strategiekreis-elektromobilitaet.de/public/projekte/seis