Truck Hacking – Cyber-Security-Risiken und effektive Schutzmaßnahmen für Nutzfahrzeuge

Marko Wolf, Robert Lambert, ESCRYPT GmbH, Automotive – Safety & Security 2017, Stuttgart

- State-of-the-Art **Cyber-Security-Risiken** für Nutzfahrzeuge
  - Real-Life Beispiele von heute
  - Potenzielle Angreifer & Angriffe
  - Potenzielle Geschädigte & Schäden
  - Risiko-Bewertung & Quervergleich mit PKW

- State-of-the-Art **Cyber-Security-Schutz** für Nutzfahrzeuge mittels ganzheitlichen (holistischen) Schutzansatz
  - Schutz für das gesamte NFZ-IT-System
  - Schutz für den gesamten NFZ-Produktlebenszyklus
  - Schutz für die gesamte NFZ-Organisation

Die Digitale Revolution im Nutzfahrzeugbereich

Konnektivität, Elektromobilität und Autonomes Fahren.

escrypt
Embedded Security by ETAS

auto motor sport

BOSCH TRUCK-STUDIE VISIONX

Vollvernetzter Zukunfts-Truck

Lkw nehmen künftig die Überholspur auf dem Datenhighway ein. Wie der Truc das Jahr 2025 aussehen wird, zeit Bosch mit der vollvernetzen Truck-Studie VisionX auf der Nutzfahrzeug-IAA.

Automobilwoche

DIE BRANCHEN- UND WIRTSCHAFTSZEITUNG

Montag, 11. April 2016, 06.07 Uhr

Elektromobilität:

Auch Laster können mit Batterie fahren

E-Autos sind im Straßenverkehr selten, E-Lkw noch eine Kuriosität. Ein Flottenver Daimler zeigt, dass dies nicht so bleiben muss.

Von Michael Gerster

Elektrisch unterwegs: Daimler startet eine mit Batterie-Laster in Stuttgart. (Foto: Da

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV

WIRTSCHAFT

Autonomes Fahren

"In zehn Jahren werden keine Lkw-Fahrer mehr benötigt"

Selbstfahrende Lastwagen dürften bald kommen - alle großen Hersteller arbeiten daran. Technisch sollen sie in wenigen Jahren startklar sein - mit gravierenden Folgen für die 500.000 Brummifahrer in Deutschland.

Von manager-magazin.de-Redakteur Nils-Viktor Sorge

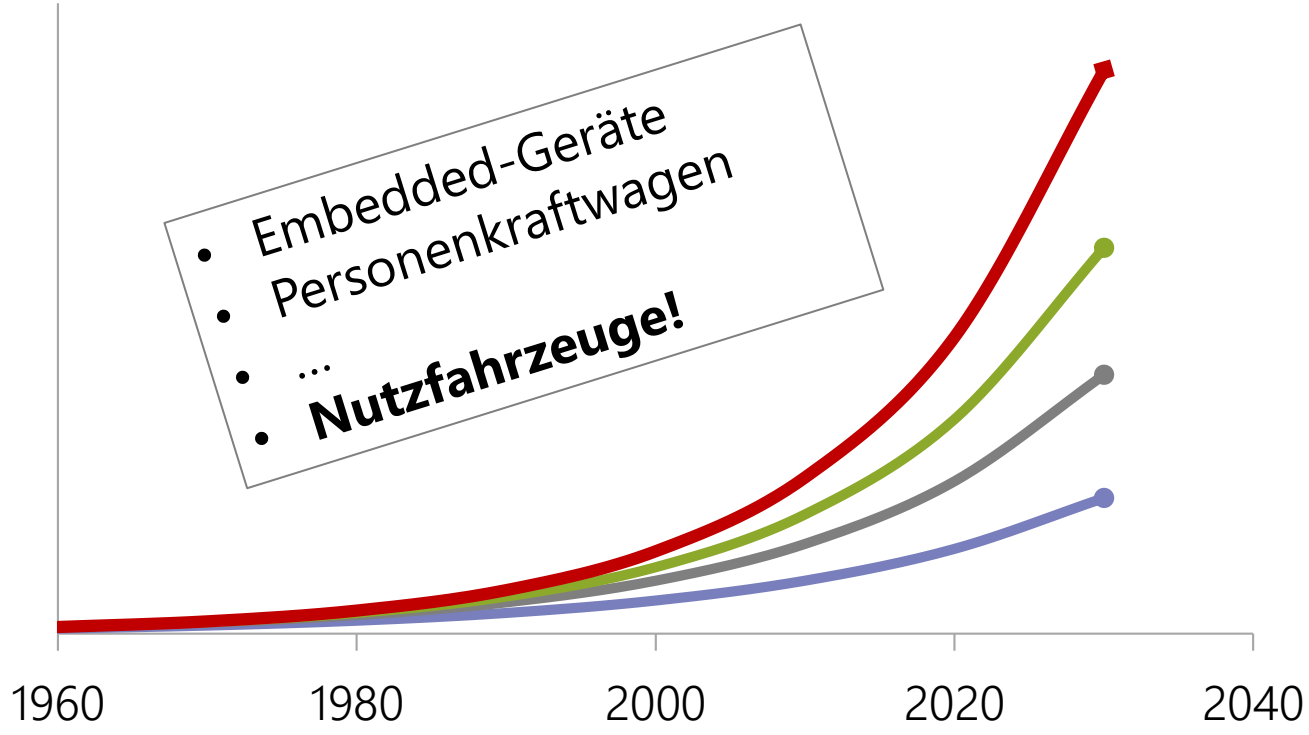
Selbständig fahrender Lastwagen von Daimler

„In den kommenden zehn Jahren werden wir bei Lkw mehr Veränderungen erleben als in den fünf Jahrzehnten davor."

W. Bernhard, Leiter NFZ Daimler, Manager-Magazin, 30.06.16

Quellen: Auto Motor Sport, Automobilwoche, Spiegel Online, Manager Magazin

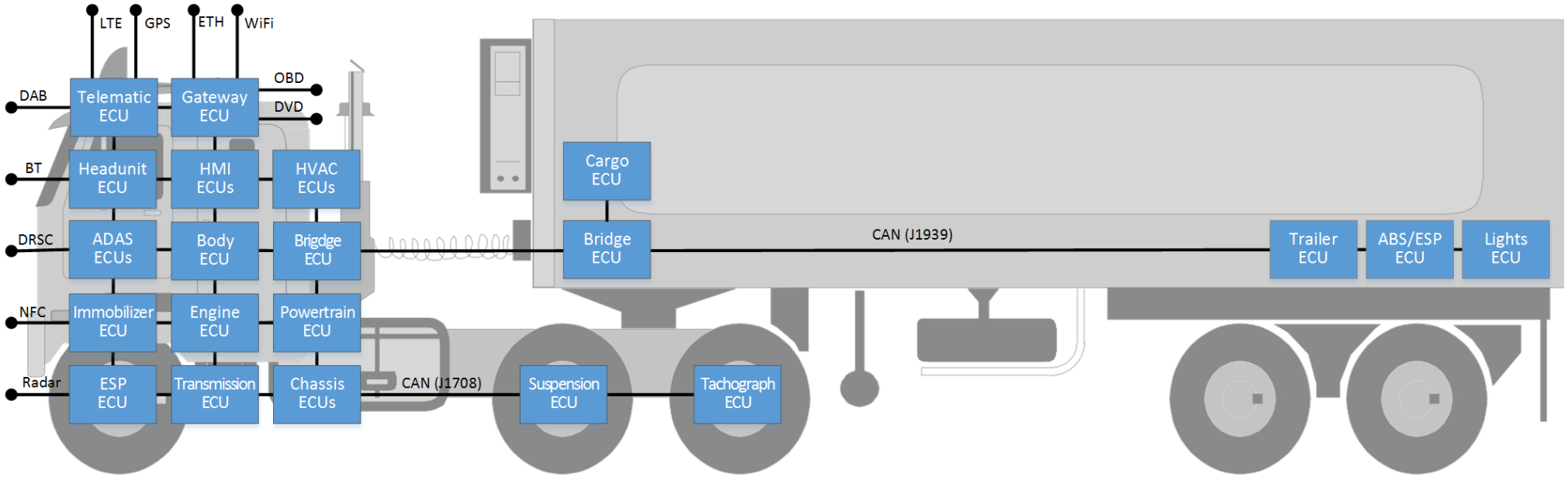
- ⚠ Mehr **Funktionen**, mehr **Software** und mehr **Vernetzung** vergrößern die a) Angriffsfläche und b) die Komplexität.
- ⚠ „**Komplexität** ist der größte Feind von Security.“ (Bruce Schneier)



Referenz: Charette, This Car Runs On Code, IEEE 2009.

Cyber-Security-Angriffspfade im Nutzfahrzeuge

Exemplarische NFZ-EE-Architektur



Wired interfaces	OBD	USB	SD	CD/DVD	Cellular	LIN	Ethernet	J1939	J1708	CAN	Smartcard	HMI	Electric charger	J2400	...
Wireless interfaces	NFC	RKE	Bluetooth	WiFi	DSRC	TMC	GSM/3G	LTE	Digital broadcast	GPS	GLONASS	V2X	Radio	Tyre sensors	...
COM Parties	Driver	Carrier company	Customer	OEM	Supplier	Public authority	Traffic infrastructure	Other Vehicles	Garage	Leasing	Insurance	Toll road operator	After-market	Navigation company	...

EE-Architekturen von NFZ und PKW sind relativ ähnlich i.e.:

- Ca. 50 verteilte Steuergeräte digital vernetzt über CAN und SAE J1039.
- Ca. 20 drahtgebundene (z.B. RMI) und drahtlose (z.B. LTE) digitale Schnittstellen im Nahbereich bis zur globalen Internetanbindung.
- Mehrere 1.000 software-basierte Funktionen und mehrere GB an Software und Daten für Fahrbetrieb, Fahrsicherheit, Ladung, Flottenmanagement …
- Vornehmlich (wie oft) **feature- und safety-getriebene**, das heißt nicht unbedingt security-bewusste Entwicklung, Organisation und Betrieb.

Wireless interfaces	NFC	RKE	Bluetooth	WiFi	DSRC	TMC	GSM/3G	LTE	Digital broadcast	GPS	GLONASS	V2X	Radio	Tyre sensors	…

COM Parties	Driver	Carrier company	Customer	OEM	Supplier	Public authority	Traffic infrastructure	Other Vehicles	Garage	Leasing	Insurance	Toll road operator	After-market	Navigation company	…

⚠ **Folglich sind NFZ auch ähnlichen Angriffspfaden ausgesetzt wie PKK …**

… aber im Vergleich zu PKW:

- ⚠ Benutzen NFZ oft **mehr Software** für komplexere Funktionen (z.B. Platooning).
- ⚠ Erzeugen, verarbeiten, speichern und kommunizieren NFZ oft **mehr Daten** (z.B. weltweites Flottenmanagement).
- ⚠ Besitzen NFZ oft mehr standardisierte, **homogenere EE-Architekturen.**
- ⚠ Besitzen NFZ oft **mehr digitale Schnittstellen** zur Außenwelt.
- ⚠ Transportieren NFZ **teure und/oder gefährliche Güter** (z.B. Chemikalien mit >1 M€ Schadenpotenzial).
- ⚠ Versprechen NFZ **mehr lohnende „Geschäftsmodelle“** für Diebstahl, Erpressung, Betrug usw. (z.B. Maut).
- ⚠ Haben NFZ deutlich mehr Parteien involviert (z.B. Kunde).
- ⚠ Sind NFZ i.d.R. mit **5x Größe und 30x Gewicht** eines PKW **bis 24h/Tag** als potenzielles Angriffsziel unterwegs.

Cyber-Security-Risiken für Nutzfahrzeuge

escrypt
Embedded Security by ETAS

(Technisches) Risiko nach EN50126

Eintrittswahrscheinlichkeit × Schadensschwere

Automotive Cyber-Security-Risiko (nach WoSc12)

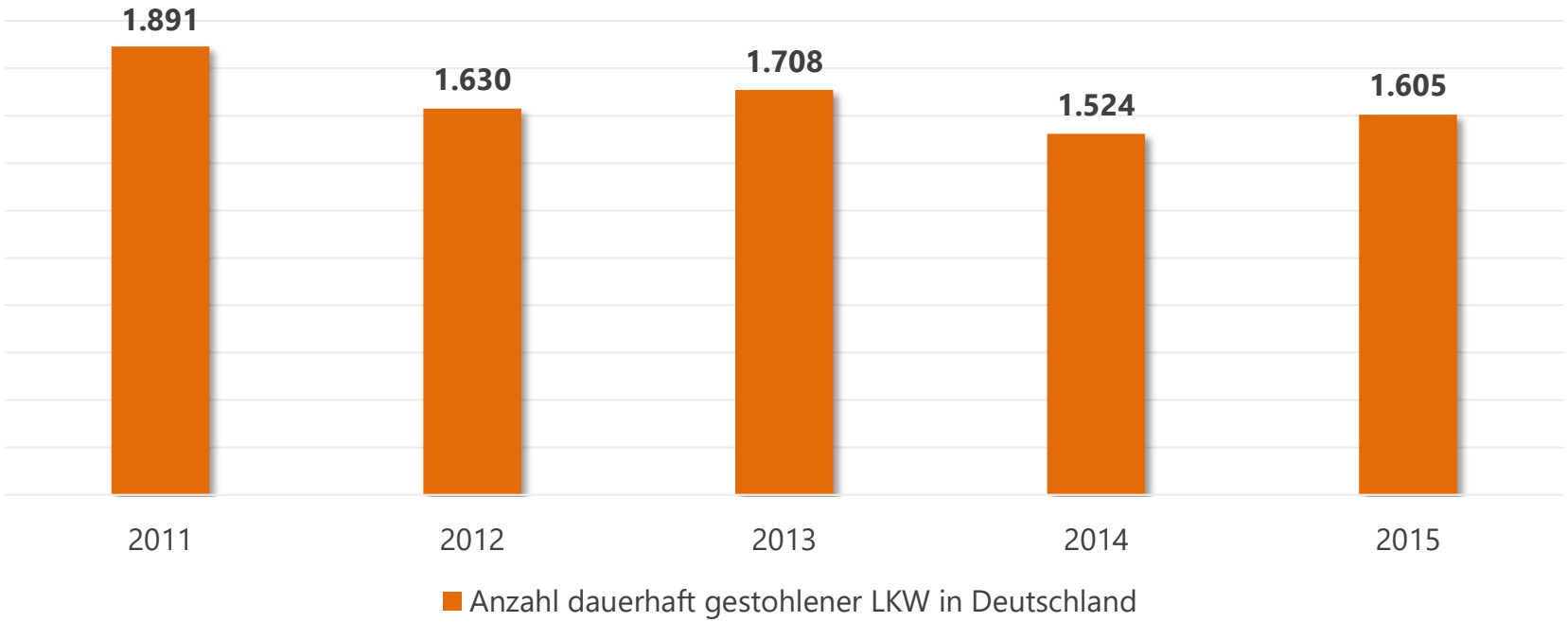
Angriffspotenzial										×	Schadenspotenzial					
Zeit		Expertise		Insiderwissen		Zugriff		Werkzeuge			Funktionalität		Finanziell		Sicherheit	
Stunden	...	Laie	...	Keines (Blackbox)	...	Unbegrenzt	...	Keine	...		Komfort	...	Substanziell	...	Leichte Verletzung	...

Referenz: Wolf, Scheibel. A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems. LNI 2012.

- Vereinfachte 4x4 Automotive **Cyber-Security-Risiko-Matrix**

Schadenpotenzial → **Angriffspotenzial ↓**	**Gering**	**Mittel**	**Erhöht**	**Hoch**
Gering	Gering	Gering	Mittel	Erhöht
Mittel	Gering	Mittel	Erhöht	Hoch
Erhöht	Mittel	Erhöht	Hoch	Hoch
Hoch	Erhöht	Hoch	Hoch	Hoch

⚠ LKW-Diebstahl moderat aber weiter relevant v.a. Ladung aber auch Diesel und Zugmaschine. Schaden lt. BAG ca. **300 m€/Jahr** bei sehr **hoher Dunkelziffer** durch hochprofessionelle **organisierte Banden**.



Quelle: Bundeskriminalamt

Physischer Diebstahl des Fahrzeugs oder Fahrzeugteilen

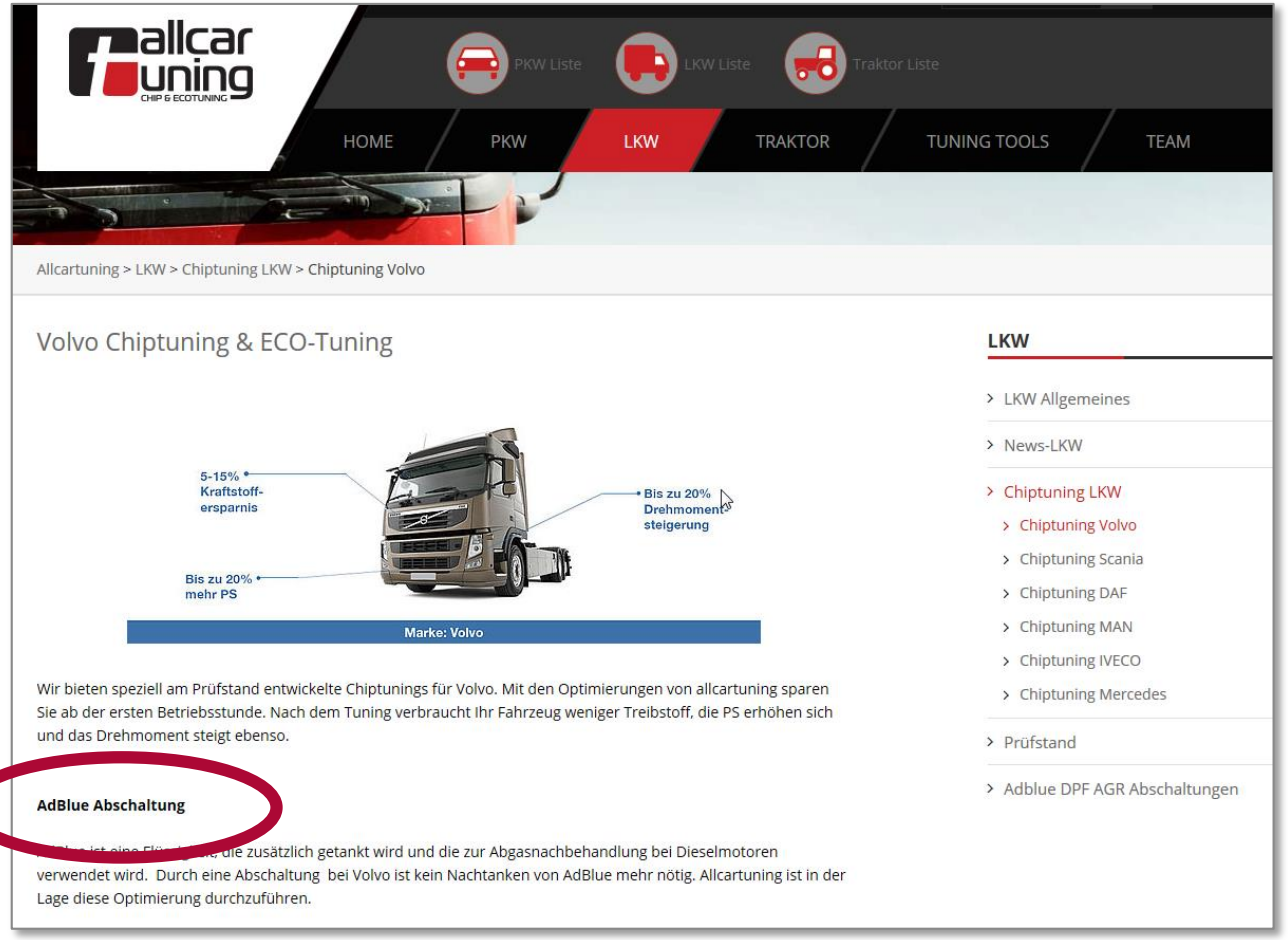
Cyber-Security-Risiko

	PKW	Nutzfahrzeug
Beispiele	Airbag-Diebstahl, Navi-System, Fahrzeugdiebstahl	**Diebstahl** des Navi-Systems, Treibstoff, der Zugmaschine und/oder der Ladung
Typischer Angreifer	Organisierte Kriminalität, Kleinkriminelle	Organisierte Kriminalität
Angriffspotenzial	Erhöht Durchaus Profi-Expertise, aber nicht in der Masse bzw. mehr Diversifizierung	Erhöht: Mehr Expertise, aber auch mehr Schutz möglich bzw. mehr Aufwand notwendig
Geschädigter	Besitzer	Besitzer/Betreiber/Kunde
Schadenspotenzial	Mittel 500 € (Airbag) – 100.000 € (7er BMW)	Erhöht 1.000 € (Ersatzrad) – 300.000 € (Zugmaschine + Ladung)
Cyber-Risiko	Erhöht	Hoch

Manipulation von Fahrzeugfunktionen oder -daten durch Interne

Real-World-Beispiel **Chiptuning**

⚠ **Chiptuning** v.a. zur illegalen Leistungs-steigerung oder Kraftstoffersparnis auf Kosten der **Umwelt** oder **Fahrsicherheit**.



Quelle: ACT Vertriebs GmbH

Manipulation von Fahrzeugfunktionen oder -daten durch Interne

Real-World-Beispiel **Fahrtenschreiber**

escrypt
Embedded Security by ETAS

Manipulationen bei Lkw-Fahrtenschreibern immer ausgeklügelter

vorlesen

heise online 24.09.2016 11:02 Uhr

Lastwagenfahrer müssen regelmäßige Pausen machen, um mehr Sicherheit auf den Straßen zu gewährleisten. Bei Kontrollen fällt aber auf, dass viele Erfassungsgeräte manipuliert sind. Die Logistikbranche gibt sich verwundert.

Manipulation von Fahrzeugfunktionen oder -daten durch Interne

Real-World-Beispiel **Fahrtenschreiber** und **Maut**

escrypt
Embedded Security by ETAS

- ⚠ Manipulation des **Fahrtenschreibers** um Lenkzeit- oder Geschwindigkeitsüber-schreitungen zu verbergen auf Kosten des fairen **Wettbewerbs** und v.a. der **Verkehrssicherheit**.
- ⚠ Manipulation der **elektronischen Mauterfassung** (e.g., FasTrak) auf Kosten des **Maut-Betreibers/Gesellschaft** und des fairen **Wettbewerbs** und der **Umwelt**.

Quelle: Canadian Automotive Instruments Ltd.

Manipulation von Fahrzeugfunktionen oder -daten durch Interne

Cyber-Security-Risiko

	PKW	Nutzfahrzeug
Beispiele	Chiptuning, Tachomanipulation, TV-Sperre ausschalten, EDR manipulieren, Gewährleistungsbetrug, Manipulierte Pay-on-Demand (e.g., Freischaltcodes) oder Pay-as-you-Drive (e.g., Versicherung)	Illegale Leistungssteigerung, **Abgas-reinigung**, Wartungslog oder Ladungs-überwachung manipulieren, technische Beschränkungen abschalten (e.g., $Last_{max}$), Notbremsassistent, Manipulierte **Tacho-graphen**, **Maut**, Pay-as-you-X-Funktionen
Typischer Angreifer	Fahrer/Besitzer	Fahrer/Besitzer und/oder Betreiber
Angriffspotenzial	Mittel: Außer Tacho (noch) nicht in der Masse, vglw. hohes Strafrisiko	Erhöht: Einfach bei hohem Gewinnpotenzial und geringem Risiko
Geschädigter	Hersteller/Drittanbieter/Gesellschaft	Hersteller/Drittanbieter/Gesellschaft
Schadenspotenzial	Mittel: e.g. 3.000 € (Tachomani-pulation im Ø lt. ADAC) – x M€ (Unfall)	Mittel (mindestens): e.g. 1.000€ (Maut) – 100.000€ (Ladung) – x M€(Unfall)
Cyber-Risiko	Mittel	Erhöht

Datendiebstahl und Datenmissbrauch durch Dritte

Real-World-Beispiel **Produktfälschungen**

- ⚠ **Produktfälschungen** verursachen nach Angaben der US-Kartell-behörde einen jährlichen **Umsatzverlust** von **über 12 Mrd. USD***) zusätzlich zu den Schäden durch vorzeitige **Ausfälle** oder **Unfälle** durch geringere Qualität.
- ⚠ Im NFZ-Bereich sind oftmals **Bremsen von Fälschungen betroffen**, die z.B. in Indien geschätzt für ca. 20% und in Saudi-Arabien für bis zu **50% Ursache der tödlichen Verkehrsunfälle** sind.*)

*Erkennen Sie den Unterschied? Das Original (links) und die Fälschung (rechts) eines Bendix MV-3 Bremsdruckluftventils sind äußerlich kaum zu unterscheiden.***)*

Quellen: *) http://www.truckinginfo.com/article/print/story/2014/03/are-your-aftermarket-truck-parts-the-real-deal.aspx
**) http://www.truckinginfo.com/article/story/2012/12/4-ways-to-avoid-selling-counterfeit-or-substandard-parts.aspx

Datendiebstahl und Datenmissbrauch durch Dritte

Real-World-Beispiel **Blackbox Drittanbieter**

escrypt
Embedded Security by ETAS

- ⚠ „**Das Fahrzeug als Zeuge der Anklage** “: Aktuell nur PKW-Beispiele[1)], aber Situation im NFZ ähnlich bzw. oft sogar kritischer (da mehr Datenerfassung, Übertragung, Speicherung, Auswertung möglich).
- ⚠ Laut ADAC[2)] werden **Fahrdaten** von diversen **OEM** z.B. Fehlereinträge, Position, Fahrzeug-Steuerung bis Fernzugriff auf den CAN-Bus **ohne explizites Wissen und ohne Zustimmung** des Kunden zum OEM **übertragen**, **benutzt**, (**verkauft**) und **unbestimmt lang gespeichert**.
- ⚠ Analog[3)] **Drittanbieter-Anwendungen** zur Mauterfassung, Leasing, Versicherung, Logistiksteuerung, Infotainment etc.

Quellen: (1) https://netzpolitik.org/2016/bmw-speichert-keine-standortdaten-gibt-aber-bewegungsprofil-an-gericht/;
(2) https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/
(3) http://www.focus.de/digital/multimedia/tid-7650/big-brother-awards_aid_135688.html; http://www.sueddeutsche.de/wirtschaft/wirtschaftsspionage-innovation-per-spaehangriff-1.789378

Datendiebstahl und Datenmissbrauch durch Dritte

Cyber-Security-Risiko

	PKW	Nutzfahrzeug
Beispiele	Kopieren der Motorkennlinie oder Abgas-reinigungssoftware, gefälschte Ersatzteile (e.g., Airbag), persönliche Daten (e.g., Routen, Kontakte), Fahrverhalten etc.	Motorkennlinie oder Abgasreinigung-SW, **gefälschte Ersatzteile**, Geschäftsgeheimnisse wie Routen, Ladung, Kontakte; Ransomware via E/E-Manipulation, **Daten für Klaggegner**
Typischer Angreifer	Konkurrent, Plagiator, Drittanbieter, Hersteller, Behörden, Dritte, Kriminelle	Konkurrent, Plagiator, Drittanbieter, Hersteller, Behörden, Dritte, Kriminelle
Angriffspotenzial	👽👽👽👽 Erhöht: Für Experten wenig Hindernisse, Datenübertragung noch gering (i.e. proprietär, Konnektivität)	👽👽👽👽 Erhöht: Für Experten wenig Hindernisse, umfangreiche Datenerfassung & Übertragung, wenig effektiver IP-Schutz
Geschädigter	Fahrer/Betreiber/Hersteller/Gesellschaft	Fahrer/Betreiber/Hersteller/Gesellschaft
Schadenspotenzial	☠☠☠☠ Mittel: Verluste durch gestohlenes Knowhow und Plagiate in M€, Daten-Missbrauch noch gering, da rechtlich grenzwertig und noch theoretisch	☠☠☠☠ Erhöht: Verluste durch Plagiate und Knowhow in M€, wertvolle Daten (Kunden, Ware, Routen), teure Ladung, teure Miete (OHW) + enge Termine ↔ Erpressung!
Cyber-Risiko	↯↯↯ Erhöht	↯↯↯↯ Hoch

info@escrypt.com

Angriffe auf die Zuverlässigkeit und Fahrsicherheit (Functional Security)

Real-World-Beispiel **Böswillige Fahreingriffe via SAE J1939**

escrypt
Embedded Security by ETAS

⚠ Alle bekannten **Cyber-Angriffe** auf die **Zuverlässigkeit & Fahrsicherheit** von PKW sind **auch für NFZ** anwendbar – oft sogar einfacher und folgenreicher.

Quellen: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; https://www.usenix.org/conference/woot16/workshop-program/presentation/burakova

Angriffe auf die Zuverlässigkeit und Fahrsicherheit (Functional Security)

Cyber-Security-Risiko

	PKW	Nutzfahrzeug
Beispiele	Löschen von Daten, Sperren von Funktionen, Hijacking von Fahrfunktionen (e.g. Miller & Valasek Jeep Angriff)	Löschen von Daten, Sperren von Funktionen, Gekoppelte Fahrzeuge (e.g., vernetzte Kolonnenfahrt) manipulieren, **Hijacking von Fahrfunktionen** (e.g., UMTRI J1939 Angriff) oder Aggregate
Typischer Angreifer	Terrorist, Erpresser	Terrorist, Erpresser
Angriffspotenzial	Gering Viele proprietäre Systeme, noch vglw. geringe Kommunikationsabdeckung	Mittel Nicht trivial, aber viel Telematik, viele Interfaces und viel mehr Standardisierung
Geschädigter	Fahrer, Gesellschaft	Fahrer, Gesellschaft
Schadenspotenzial	Hoch Unkontrollierter PKW	Hoch Unkontrollierte 40-Tonner
Cyber-Risiko	Erhöht	Hoch

Zusammenfassung: Cyber-Security-Risiken in PKW und NFZ

Cyber-Security-Risiken im NFZ tendenziell höher als im PKW-Bereich

	PKW	NFZ
Physischer Diebstahl des Fahrzeugs/Fahrzeugteilen	Erhöht	Hoch
Manipulation Fahrzeugfunktionen/–daten durch Interne	Mittel	Erhöht
Datendiebstahl und Datenmissbrauch durch Dritte	Erhöht	Hoch
Angriffe auf Zuverlässigkeit und Fahrsicherheit	Erhöht	Hoch
Summe	**Erhöht**	**Hoch**

Müssen wir jetzt in Panik verfallen und zurück zum Pferde-Fuhrwerk? Nein. Moderne LKW/NFZ sind in der Regel sicher und nicht jedes Cyber-Security-Risiko ist sofort ausnutzbar und tödlich, aber…

⚠ **Realistische NFZ-Angriffe**, Angreifer und Angriffsszenarien.

⚠ Cyber-Security-**Risiken für NFZ oft höher** als für PKW.

⚠ **Cyber-Sicherheitsrisiko** ist bereits **real**, Tendenz steigend.

Cyber-Security-Schutz für Nutzfahrzeuge

State-of-the-Art Cyber-Security-Schutz für das vernetzte Nutzfahrzeug

Der ganzheitliche / holistische Schutzansatz

State-of-the-Art Cyber-Security-Schutz für das vernetzte Nutzfahrzeug

Der ganzheitliche / holistische Schutzansatz

Security für den **gesamten Lebenszyklus**

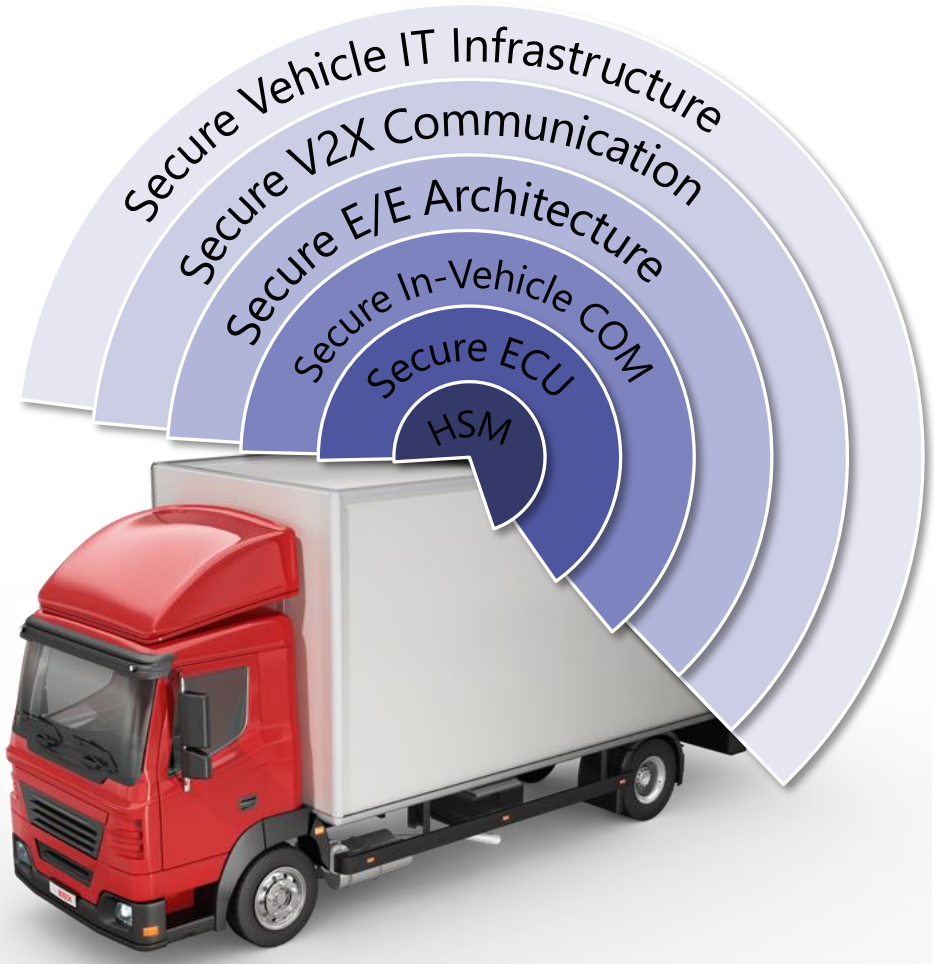
Security für das **gesamte System**

Security für die **gesamte Organisation**

Sicherheit für das ganze NFZ-IT-System inkl. IT-Infrastruktur

Multiple Layers of Defense = Mehrfach gestaffelte Verteidigungslinien über das gesamte System

escrypt
Embedded Security by ETAS



Secure Vehicle Backend & IT Infrastructure
Secure communication channels btw. vehicle & backend.
Secure backend platform and classical network security.

Secure External V2X Communication
Vehicle firewalls and intrusion detection & response systems and security standards for external interfaces.

Secure In-vehicle E/E Architecture
Use separation and securely configured gateways to protect functional domains of E/E architecture.

Secure In-vehicle Communication
Protect integrity of critical in-vehicle signals such as recently standardized in AUTOSAR SecOC.

Secure Electronic Control Unit (ECU)
Protect integrity of software and data using secure/trusted boot, secure software updates, security watchdogs etc.

Secure Trusted Anchor
Hardware Security Module (HSM) combined w/ automotive hypervisor for strong resources separation and control.

Sicherheit für den gesamten NFZ-Produktlebenszyklus

Von der ersten Anforderungsanalyse bis zum Ende der Produktunterstützung

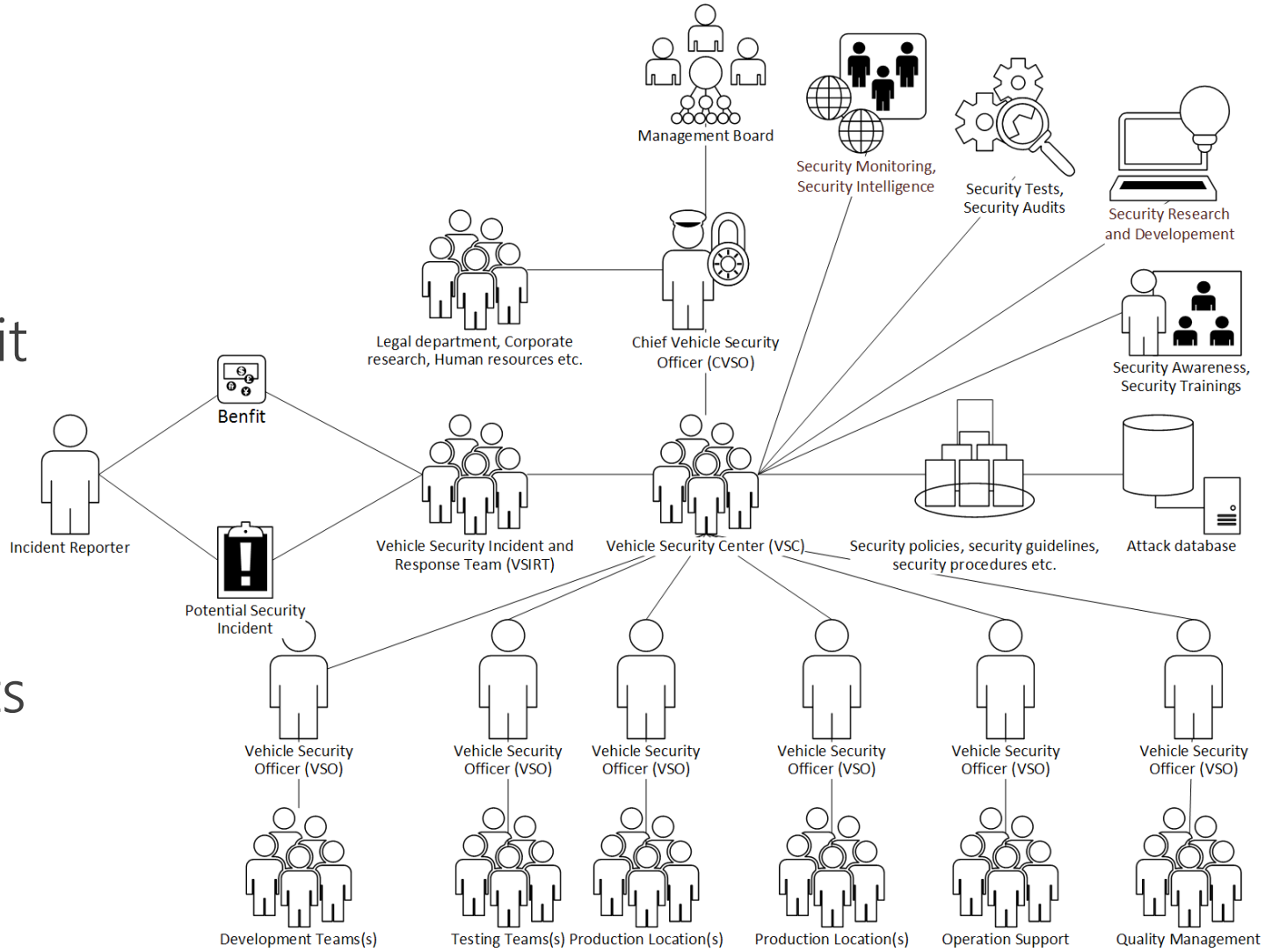
escrypt
Embedded Security by ETAS

- Kreis statt V-Modell denn:
- Security ist **kein Zustand, kein Feature, kein Produkt,** sondern ein **stetiger Prozess**.

Sicherheit über die gesamte Herstellerorganisation

Sichere Prozesse, Berechtigungen, Verantwortlichkeiten und Prüfungen

- ✓ **Bekenntnis!**
- ✓ Security-KPI
- ✓ Regelbudget
- ✓ MA & Zeit
- ✓ XD-Rollen mit Befugnissen
- ✓ Prozesse
- ✓ Richtlinien
- ✓ Trainings
- ✓ Stetige Audits und Weiter-entwicklung
- ✓ …



⚠ **Realistische Angriffe**, Angreifer und Angriffsszenarien.

⚠ Cyber-Security-**Risiken für NFZ oft höher** als für PKW.

⚠ **Sicherheitsrisiko** ist bereits **real**, Tendenz steigend.

- Viele **Schutzmaßnahmen** vom PKW-Bereich **vorhanden** und i.d.R. leicht & mindestens gleichwertig übertragbar.
- Cyber-Security-**Schutz im NFZ** tendenziell **leichter** bzw. **kostengünstiger** umzusetzen als im PKW-Bereich.

ESCRYPT GmbH

Gründung:	2004
Anteilseigner:	100 % ETAS GmbH
Hauptsitz:	Bochum
Mitarbeiter:	100 Sicherheitsexperten in aller Welt
Management:	Martin Ridder, Dr. Thomas Wollinger

Portfolio

ESCRYPT stellt verschiedene Produkte und Services bereit, die Geräte, Anwendungen und Geschäftsmodelle schützen und die Back-End-Infrastruktur sichern. Das Portfolio von ESCRYPT richtet sich an alle Branchen, für die Embedded Security wichtig ist.

- Sicherheits-Consulting und –Services
- Security-Produkte
- Maßgeschneiderte Sicherheitslösungen
- Unterstützende Infrastrukturen

Standorte

Europa

Deutschland:	Berlin, Bochum, München, Stuttgart, Wolfsburg
Großbritannien:	York
Schweden:	Lund

Asien-Pazifik

China:	Shanghai
Japan:	Yokohama
Südkorea:	Seoul

Amerika

USA:	Ann Arbor, MI
Kanada:	Waterloo