

How connectivity influences security in Mobility. Challenges for the Automotive Industry

Rob Short
Technology Manager Automotive
Rohde & Schwarz International GmbH
Munich

rob.short@rohde-schwarz.com

Rohde and Schwarz group at a glance

■ History

Established 1933 in Munich, Germany

■ Type of enterprise

Independent family-owned company

■ Global presence

In over 70 countries, approx. 60 subsidiaries

■ Net revenue

EUR 1.92 billion (FY 15/16, July through June)

■ Export share

85 percent

■ Employees

10,000 worldwide, with approx. 6000 in Germany

■ Success

A leading international supplier in all of its fields of business



R&S Business fields and Expertise– 4 technical pillars

1 Test & Measurement



Broadcasting/Video **2**



3 Secure
Communications and
IT Security



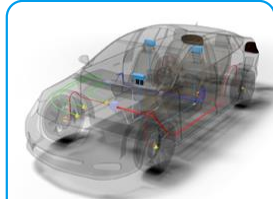
4 SIGINT, Signal
Monitoring and Signal
Location



The internet of things challenges



Mobile devices



Connected Cars



Healthcare



Smart Homes



Smart Factories



Smart Cities



The mobile industry and the "Internet of things" comprises many different areas...
... and many different devices...



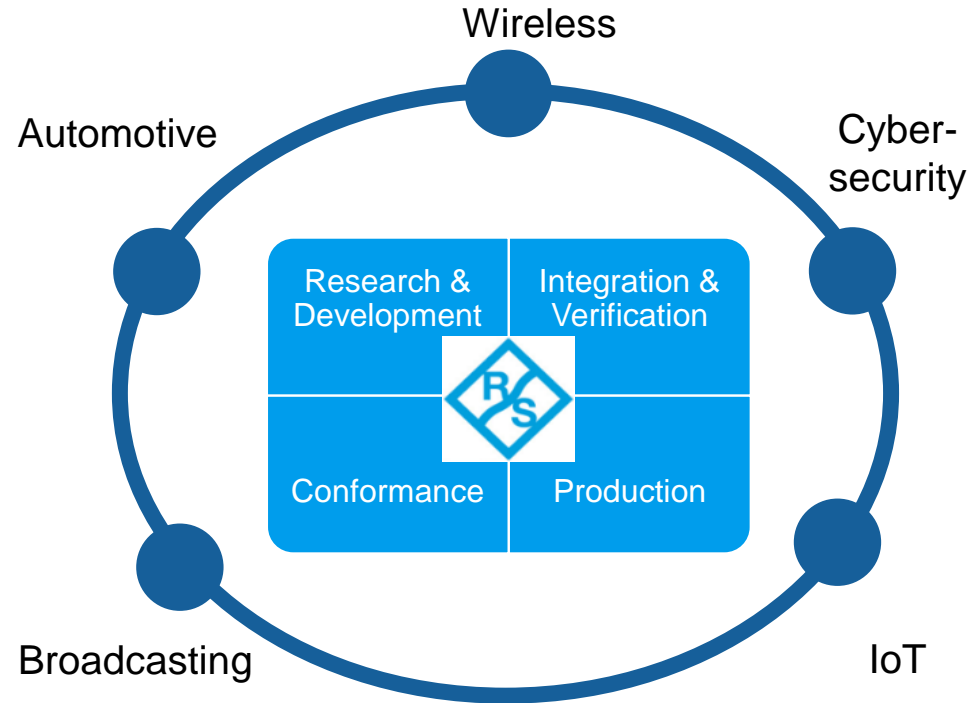
Especially IoT platforms are most likely proprietary, as standardization is still in progress and technical specifications are not yet ready for implementation.

Outlook:

Certification provides the framework for regulatory and operator specific requirements ensuring economy of scale

Automotive will require complete real-world test scenarios and are in the need for security solutions

Rohde & Schwarz is committed to support the industry with the solutions needed to investigate, standardize, develop and implement autonomous driving.



How to connect Automotive and Wireless!

EMC Standards for Vehicles and ESA (Electronic Sub Assemblies)

ISO / CISPR

USA	Europe	China	Japan
SAE	2004 / 104 / EEC	GB...	JASO
Car Manufacturers			
GM 3097	VW TL	PSA B21	BMW GS95002



Committees and Standards for Mobile Communication and Connectivity

3GPP
A GLOBAL INITIATIVE

IEEE

oma
Open Mobile Alliance

GCF
Global Certification Forum

ngmn
Next Generation Mobile Network

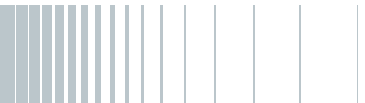
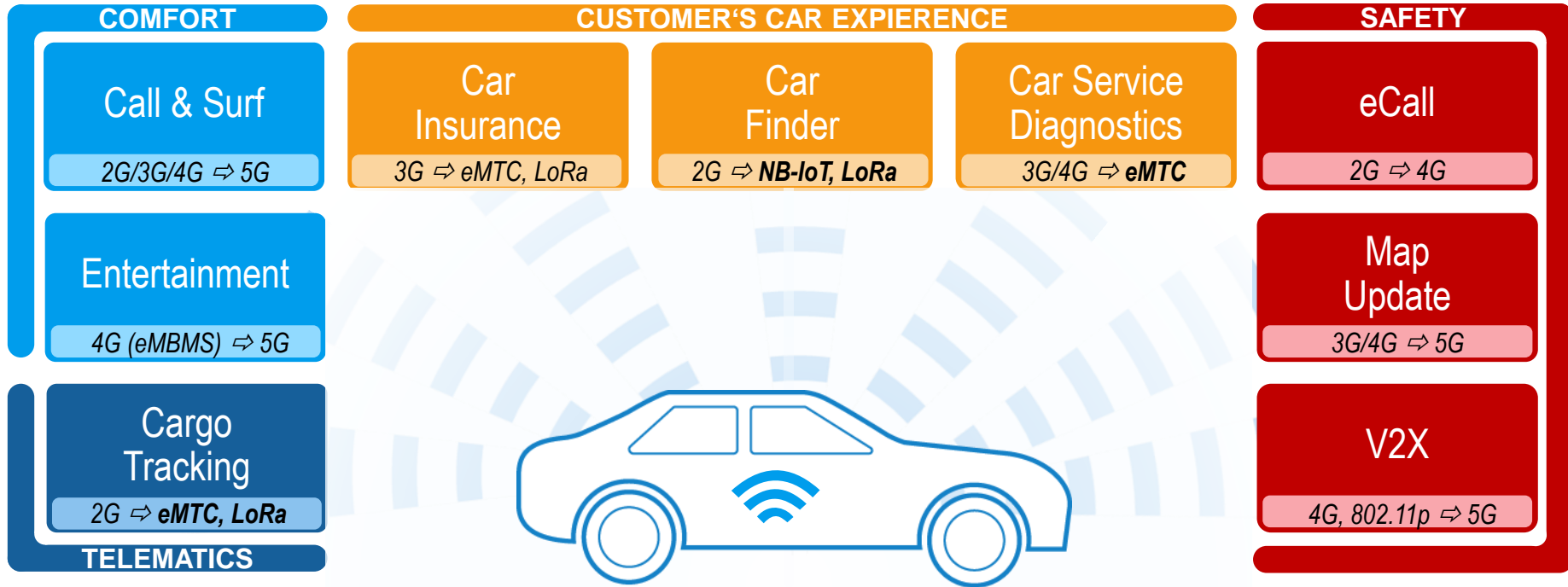
ETSI

CAR 2 CAR
COMMUNICATION CONSORTIUM

5GAA
Automotive Association

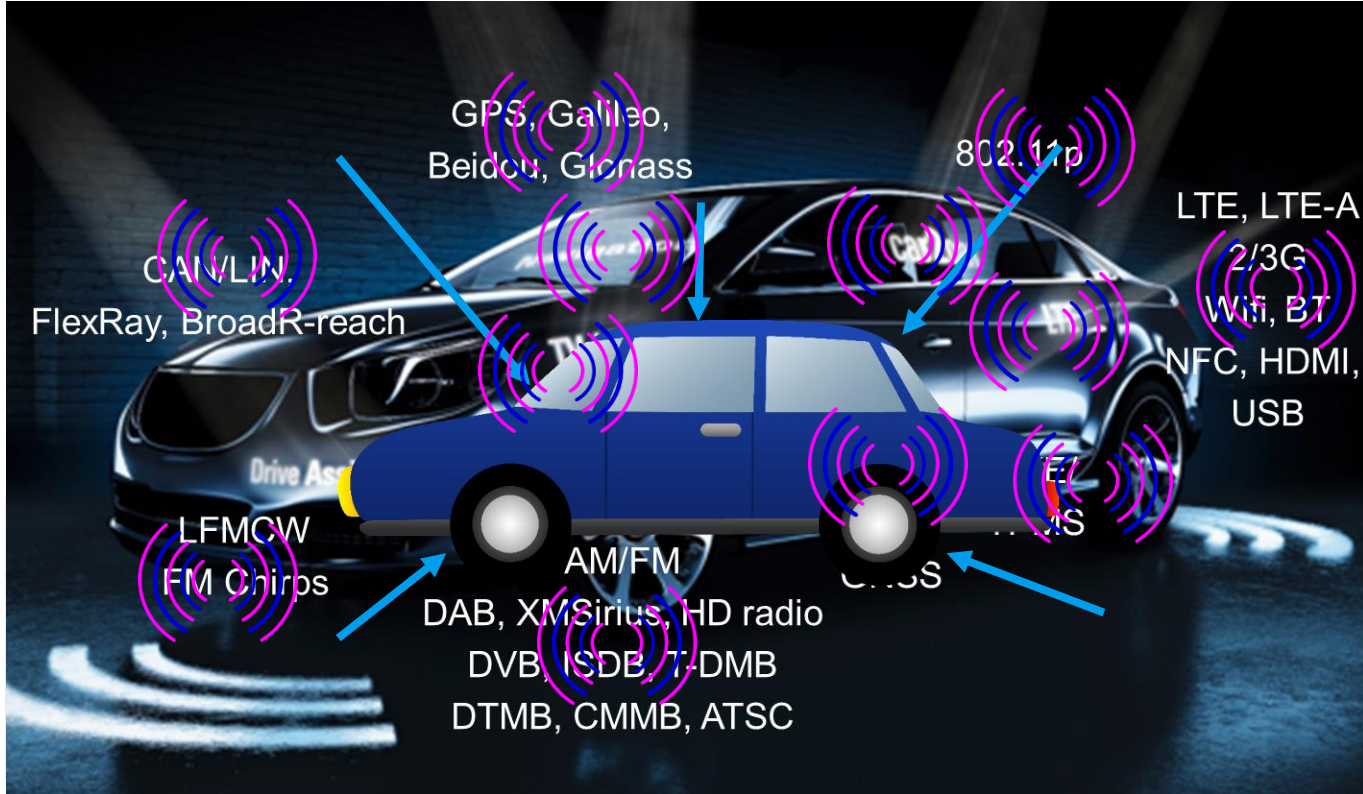


The Internet of Cars or the value of hyper-connected vehicles: Use of several flavors of cellular IoT



Secure Coexistence in a system:

Many Tx & Rx!



R&S test solutions for Automotive

GNSS / eCall

R&S[®]SMBV R&S[®]CMW

GNSS Simulation Solutions

EMC

R&S[®]TS9982 R&S[®]SMB100A R&S[®]FSW R&S[®]NRP

R&S[®]ESRP R&S[®]ESW R&S[®]RTO

R&S[®]BBA

Complete EMC measurement solutions.

Audio / Video / Infotainment

R&S[®]BTC R&S[®]SFE100 R&S[®]CMW

R&S[®]UPV R&S[®]VTC R&S[®]SMBV

R&S[®]UPP R&S[®]RTO

Evaluate the quality of infotainment systems

Automotive Radar Solutions

R&S[®]FSW R&S[®]ARTS R&S[®]SMW

R&S[®]SMF R&S[®]ZNB R&S[®]SMZ

Verification of Driver Assistance Systems

Car2Car / Car2X

R&S[®]SMW R&S[®]FSW

R&S[®]ITS100 R&S[®]CMW R&S[®]FSWP

Communication and Interference

Automotive Bus Systems

R&S[®]RTM R&S[®]RTO R&S[®]RTH

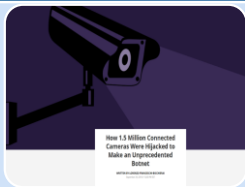
Bus analysis with dedicated options for CAN, BroadR-Reach,...

IT Risks - Cyberspace attacks

Examples

+++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS

DDOS attack by hijacked IP cameras and baby phones...



Service Disruption

Mobile phone steals personal information...



Steal Information

Hackers take control of an connected car...



Take Control

+++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS +++ NEWS

Story 1: <http://motherboard.vice.com/read/15-million-connected-cameras-ddos-botnet-brian-krebs/>
 Story 2: https://www.kryptowire.com/adups_security_analysis.html
 Story 3: <https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/>

The connected car and who receives the Data

IOT delivers fast data streams from sensors and equipment

Driver assistance system

e.g. autonomous parking, driving

Garage/Manufacturer

e.g. remote maintenance, warning



Insurance company

e.g. Pay as you drive, Police



Garage/Manufacturer

e.g. remote maintenance, warning



V2V

e.g. distance control, Collision warning,.....



Taxi, Car rental, Car sharing

e.g. invoicing



Passenger

e.g. Entertainment, WLAN, Navigation



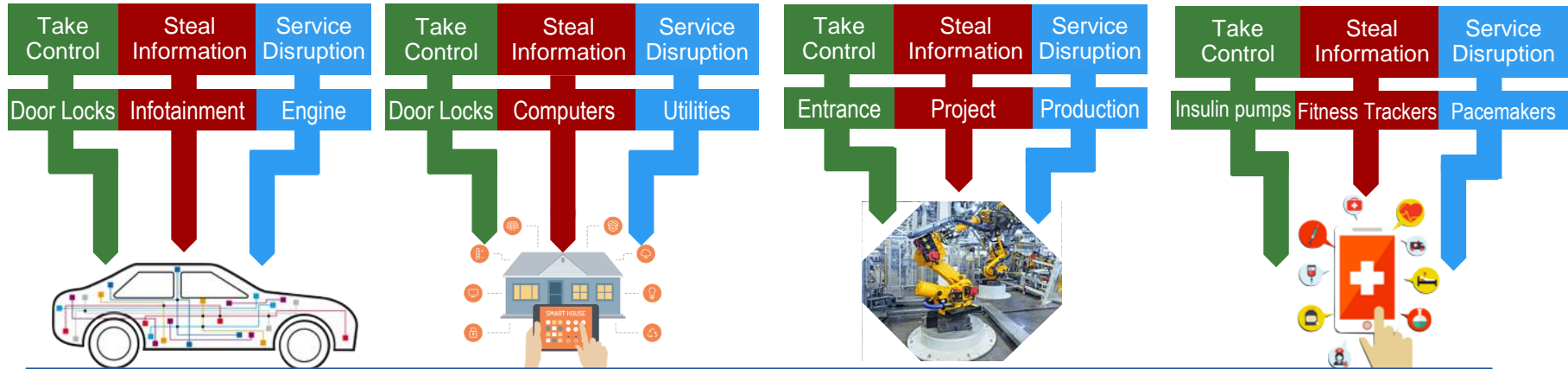
Infrastructure, Traffic control

e.g. Messages, Toll, eCall, Map



Security Challenges

Automotive and New Verticals: How to Solve the Security Issues?



Security Solutions at R&S



IP Traffic Monitoring



End to End Encryption



Next Generation Firewalls

The Security Challenge:

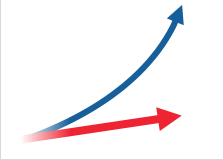


The market moves forward, but security is not keeping pace

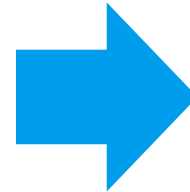
- Generally „Always-On“ – in Automotive or the (I)IoT in general – holds significant security challenges
 - **Traditional manufacturers may become subject to cyberattacks**
 - **Legacy systems / networks (e.g. CAN)**
 - **No standardized solutions available (e.g. OneM2M platform not mature yet)**
 - **Update Cycles**



The IoT Security Challenge:

There is a demand for innovative approaches

	Strong evolution of the networks (bandwidth, latency, # devices ...) But what about Security?
	Adding more security to legacy systems and protocols might be difficult
	Limitations of implementing security on often unmanaged, resource limited devices

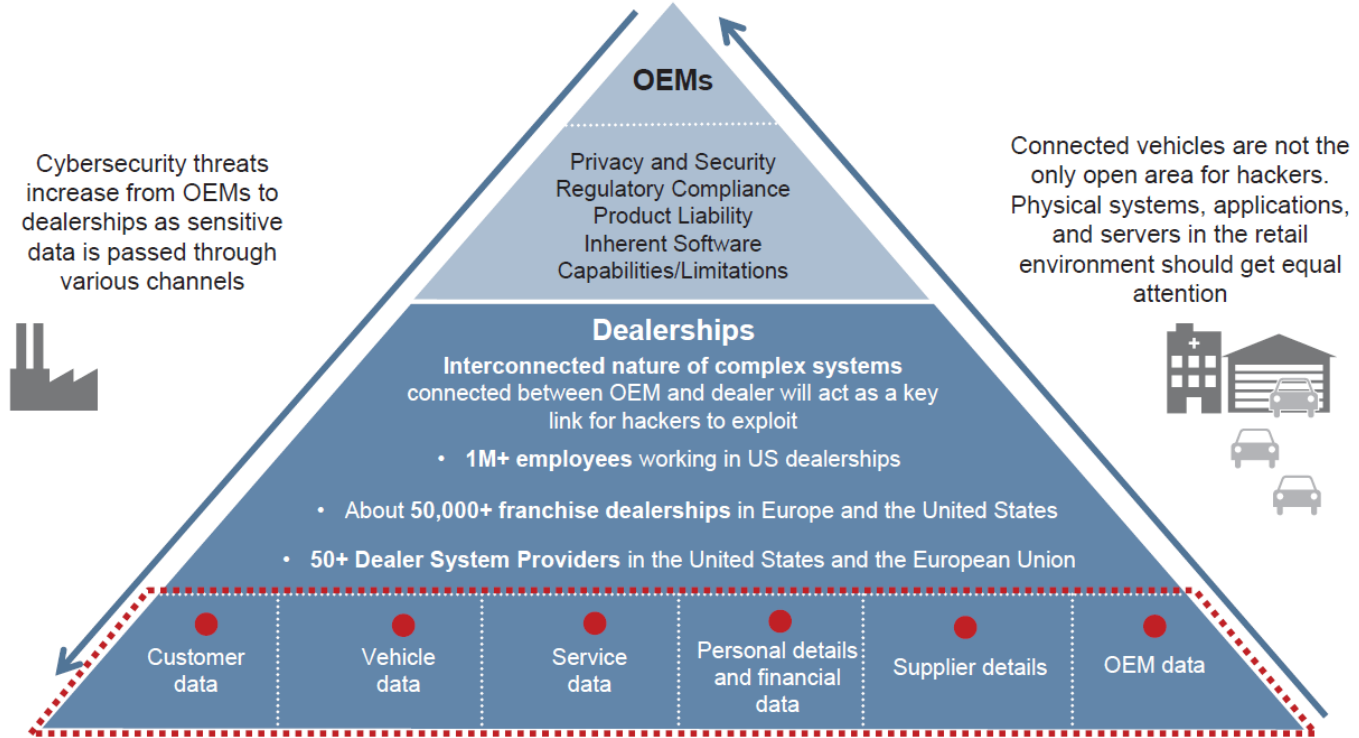


 Take over control	 Steal information
 Disrupt Service	 Infect devices



Cybersecurity Trends

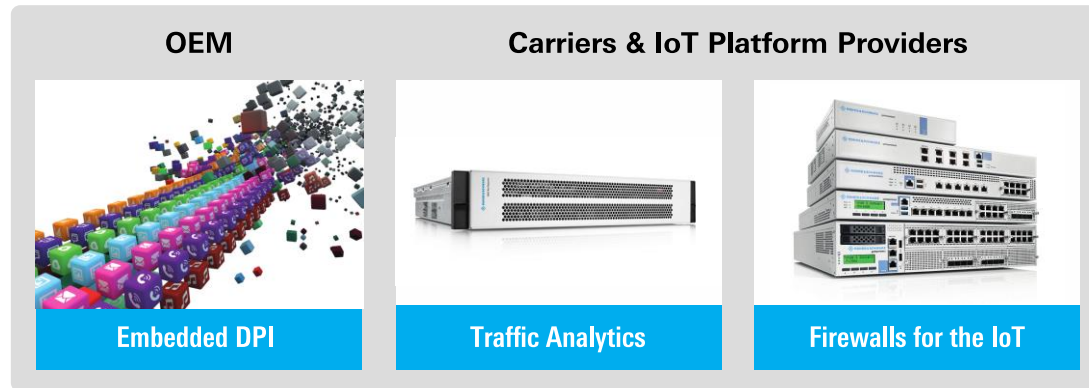
Automotive Cybersecurity Market: Automotive Retail Cybersecurity Threats, North America and Europe, 2015



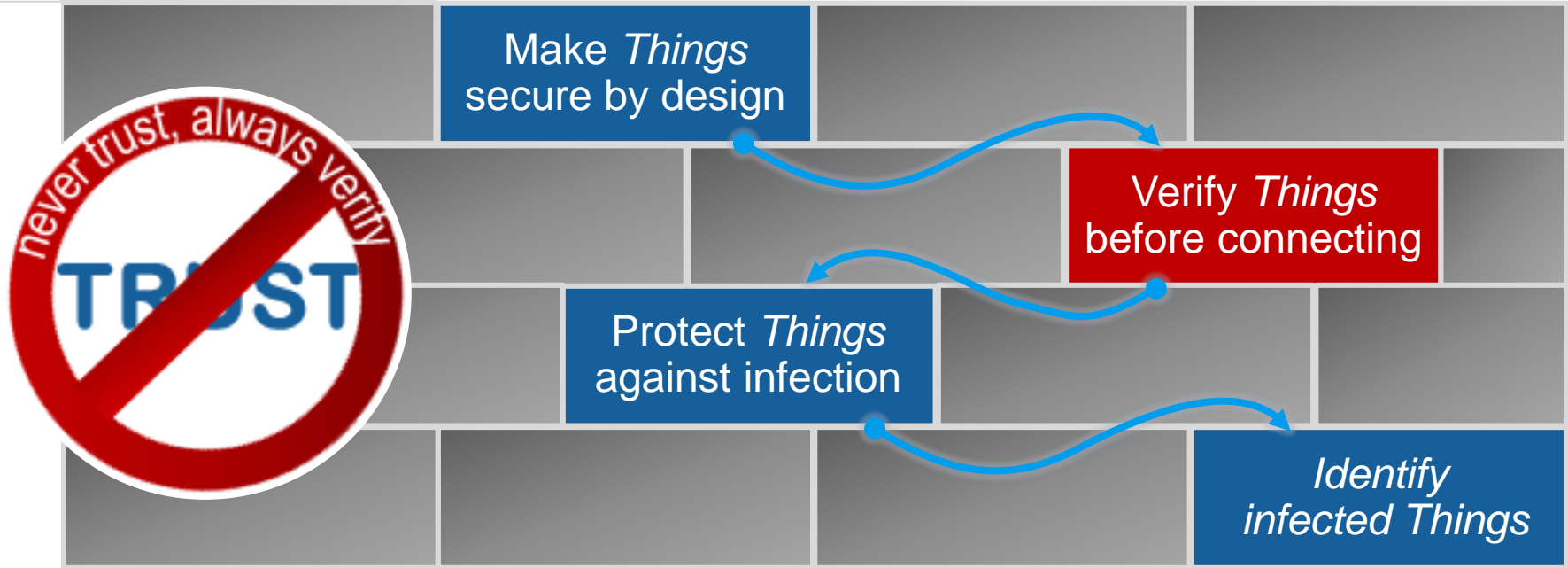
Source: Frost & Sullivan

What we see:

- **The OTA connection is one of the most-used entry points** → It needs isolated security that works even when cars & platforms are compromised
- **Networks within cars are often „Full-Trust“-Domains** and therefore lacking functionalities to guarantee confidentiality, integrity & authenticity
- **Network analytics & protection helps** to reach this security goals



The consequent implementation of the Zero-Trust model requires verification of Things



OTA Test solution: Verify *and* test before connecting: Identification of potential IP connection vulnerabilities



Application & IP Connection details
incl. end point geolocation



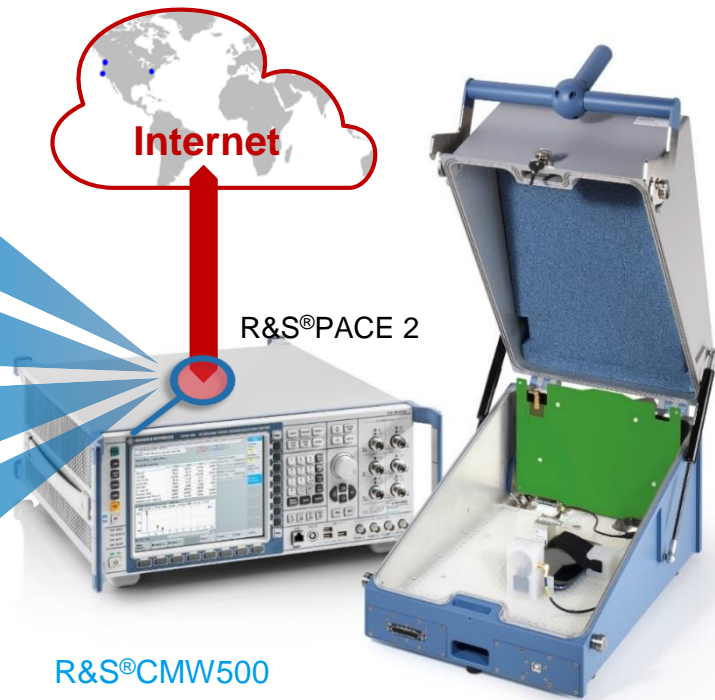
Analysis of encrypted/unencrypted traffic
(strength, certification details)



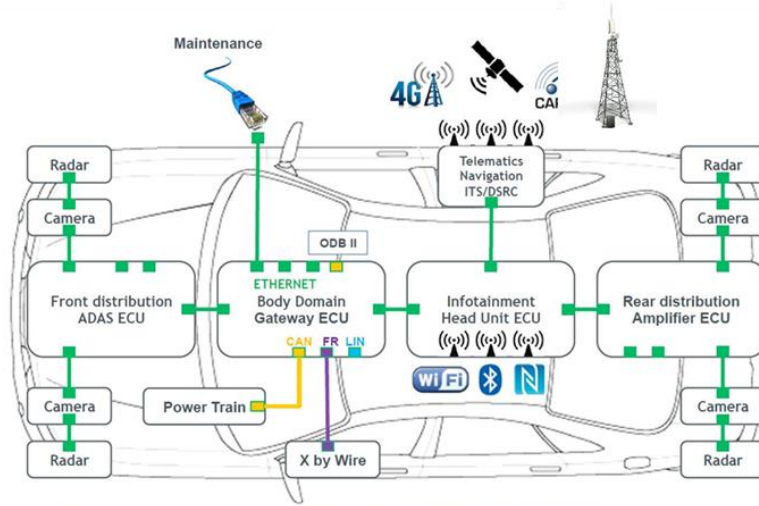
Clear text keyword matching
analysis in IP stream



IP port analysis of device under test
(TCP/UDP open port scan)



Secured Communication - Solutions



External Surfaces

(LTE, WLAN, BT, Radar, DSRC)

- NR / NS
- IPOQUE Probes
- Secure Connection
- DenyAll – Web apps
- Browser in the Box

Internal buses

(CAN, LIN, Ethernet, OBD)

- NR/NS
- Secure Connection
- Secure Boot
- Virtualisation)
- Encryption
- Trusted disk

Factory

- Netreporter / Sensor
- DPI
- DenyAll
- Specialised Firewall
- T.O.M.
- Trusted Desktop

R&D

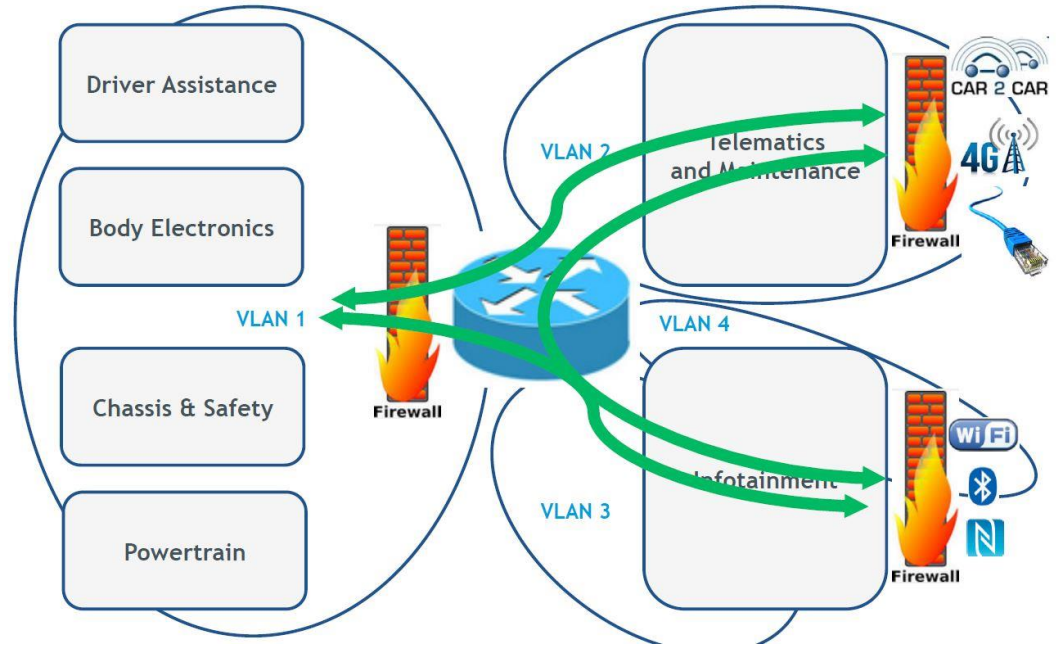
- DPI: NR/NS
- L2 Encyptors
- Trusted Desktop
- DenyAll
- Firewalls

Securing the in-car communication

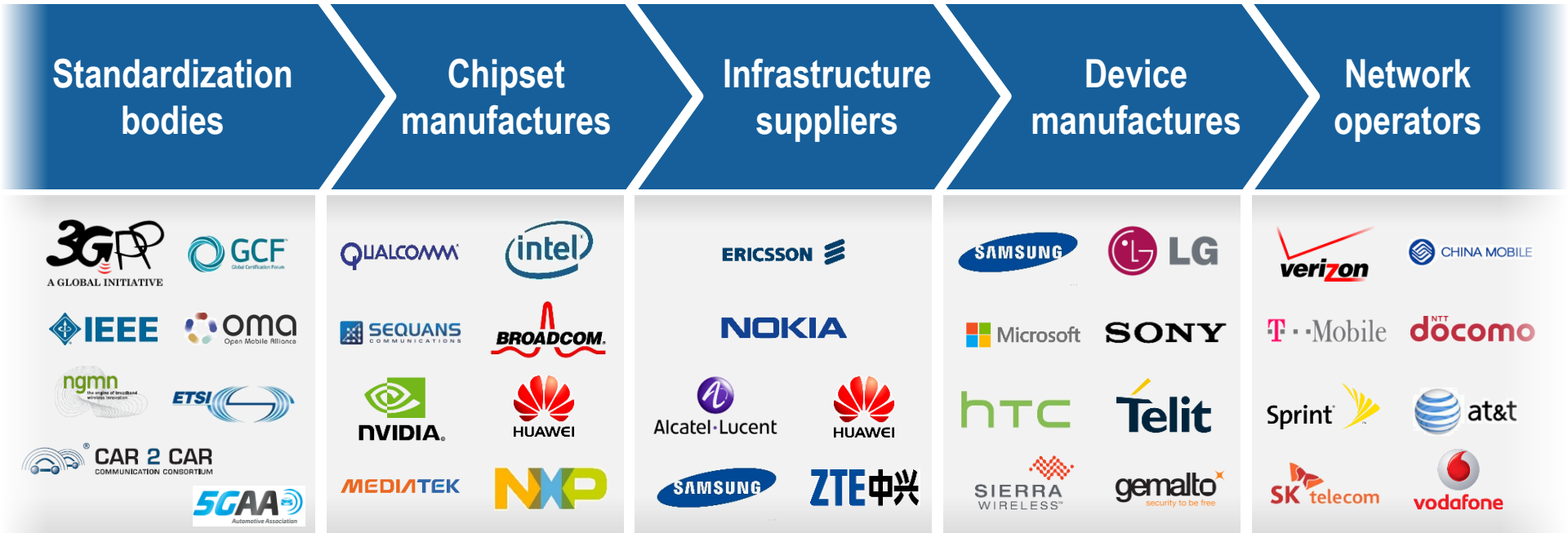


Solution Summary

- Use virtual LAN's to segment the Network according to security levels
- Central in-car firewall inspects ALL communication between those segments
- Firewall increases security through:
 1. **Blocking of unwanted connections & messages**
 2. **Enforce & validate encryption, authentication**



We are an experienced partner in all parts of the process chain of the wireless communications industry..



Thank You for Your Attention