



Choose cert
Add valu

TÜV SÜD

**Mitigating cybersecurity th
to automotive systems**

Dirk Schlesinger, 09.03.2017

150 YEARS | INS
TRU



1

One-stop technical solution provider

150

years of experience

850

locations worldwide

2,220

million Euro in sales revenue for 2015

24,000

employees worldwide as of February 2016*



Note: Figures have been rounded off.

*As of 29.02.2016: Inclusive of acquisition in January 2016.

MOBILITY



Ensure 100 years in safe mobility:

- Periodical Technical Inspections
- Homologation
- Car business services
- Fleet management

Employees: 5,539
Revenue: € 639 million

INDUSTRY



Maximise reliability, safety & efficiency for:

- Chemical, oil & gas
- Power & energy
- Manufacturing & ind. machinery
- Rail
- Real estate and infrastructure

Employees : 8,164
Revenue: € 945million

CERTIFICATION



Achieve market access for:

- Manufacturing & ind. machinery
- Consumer products & retails
- Healthcare & medical devices
- Telecommunications & IT
- Transportation (Automotive, Aerospace & Marine)

Employees: 6,061
Sales Revenue: € 557 million

The car of tomorrow - a PC on wheels, but much more challenging



Eliminating all comments (which are ignored at compile time)
Windows 10 has 27 - 50 Mio lines of executable code.

+ Motherboard +Graphics Card +Applications
(Office = 40 Mio lines)

→ **Estimate total 100 Mio. lines of code...**
...but no sensors, no actors and in 1 place



- > 50 different sensors in 15 sensor sets
- 28 microprocessors. 6 communication area networks
- 3000 different signals = 300Mbit / s equivalent > 100GB / h

Challenge: getting all the signals to talk to each other while making sure “when one sensor shuts down it doesn’t crash the whole system”.

10 Mio lines of ‘mission critical’ software code...
...3 Mio more than a Boeing 787, 8 Mio more than an F22

→ **Estimate distributed 100 Mio. lines of code...**
...and rebooting in drive is not an option



Always assume you are in a hostile network with a multitude of attack vectors

- *Today*: CDs, Smartphone Apps, Communication Intercepts¹⁾, direct NW access²⁾
- *Tomorrow*: IT-infrastructure of dealer/repair shop, OEM/SP-datacenter, other elements of digital delivery chain

SW protection and quality control become increasingly important

- Existing standards (ISO 26262, OWASP Top 10, CWE/CVSS) not enough
- Ensure quality of commonly used SW-libraries / Open Source without stifling innovation

**Cybersec = necessity
& differentiator for entire
value chain**

Just gateway(s) and anti-virus won't help

- ADAS requires ECUs on both sides of gateways (functions crossing domains)
- Architectures evolving - currently no implemented reference security architecture
- (Managed) Security as a Service?

Holistic view on Cybersecurity needed

- Convergence of IT and OT – in analogy to manufacturing automation
- SAE J3061 – auto specific, but what about datacenter of OEM, qualification of system integrators, security processes