AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles

1st International workshop on the Integration of Safety and Security Engineering (ISSE'14)

Christoph Schmittner, Zhendong Ma, Paul Smith

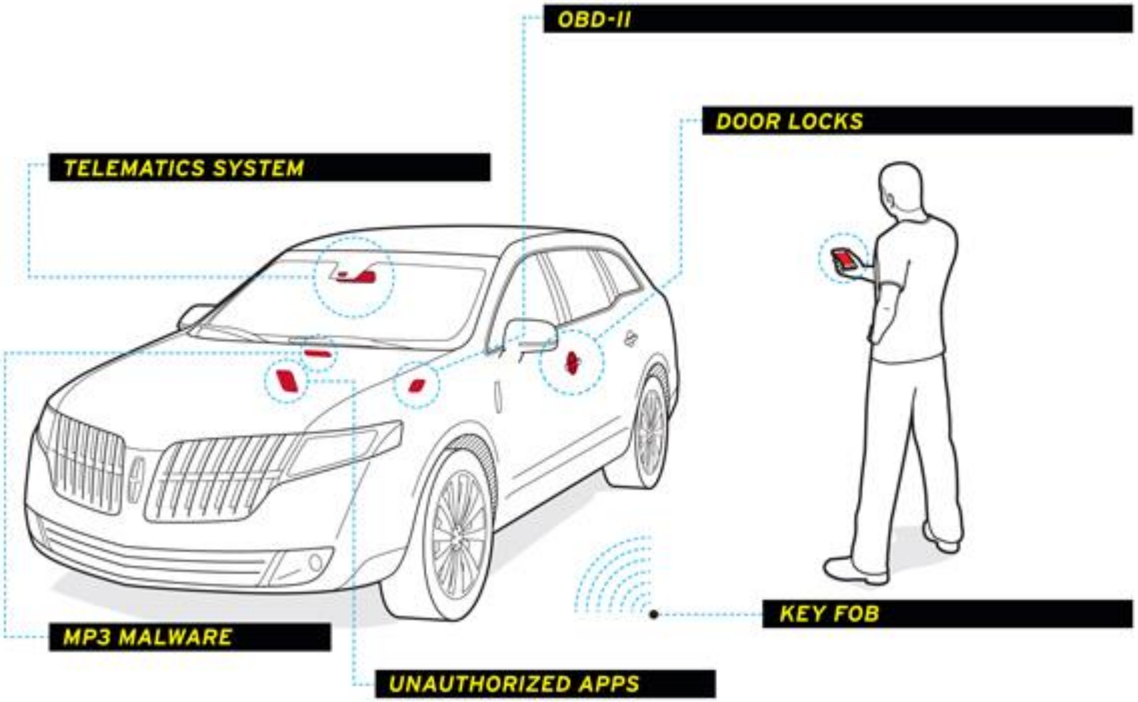
Agenda

- Background & Motivation
- Analysis Method and Results
- Outlook

Background & Motivation

Security is a rising concern for vehicles

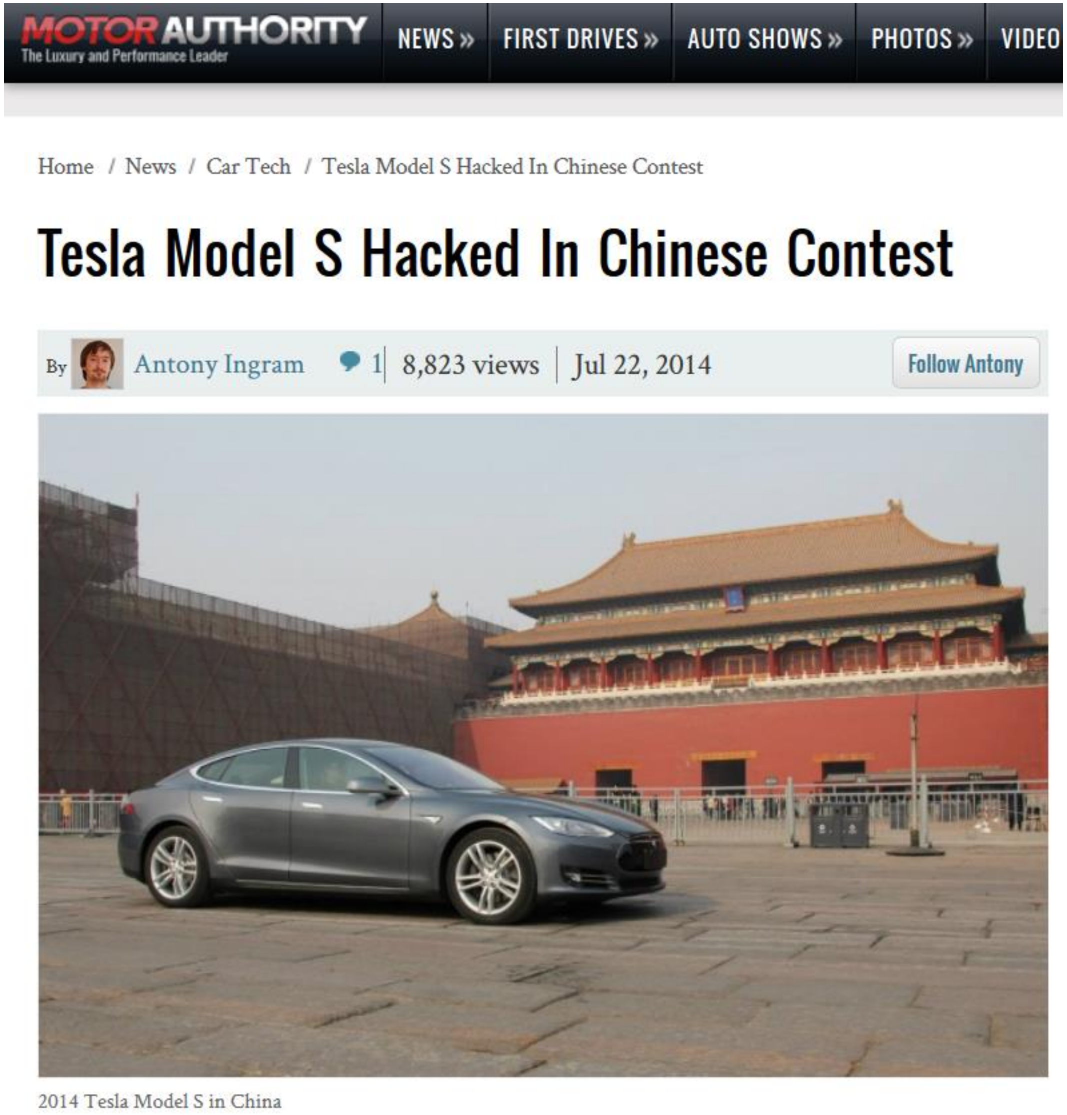
- Increased connectivity



Security is a rising concern for vehicles

- Hacking contest for a Telsa as part of a competition at the annual SyScan conference in Beijing

- “A Survey of Remote Automotive Attack Surfaces” C. Miller, C. Valasek



Home / News / Car Tech / Tesla Model S Hacked In Chinese Contest

Tesla Model S Hacked In Chinese Contest

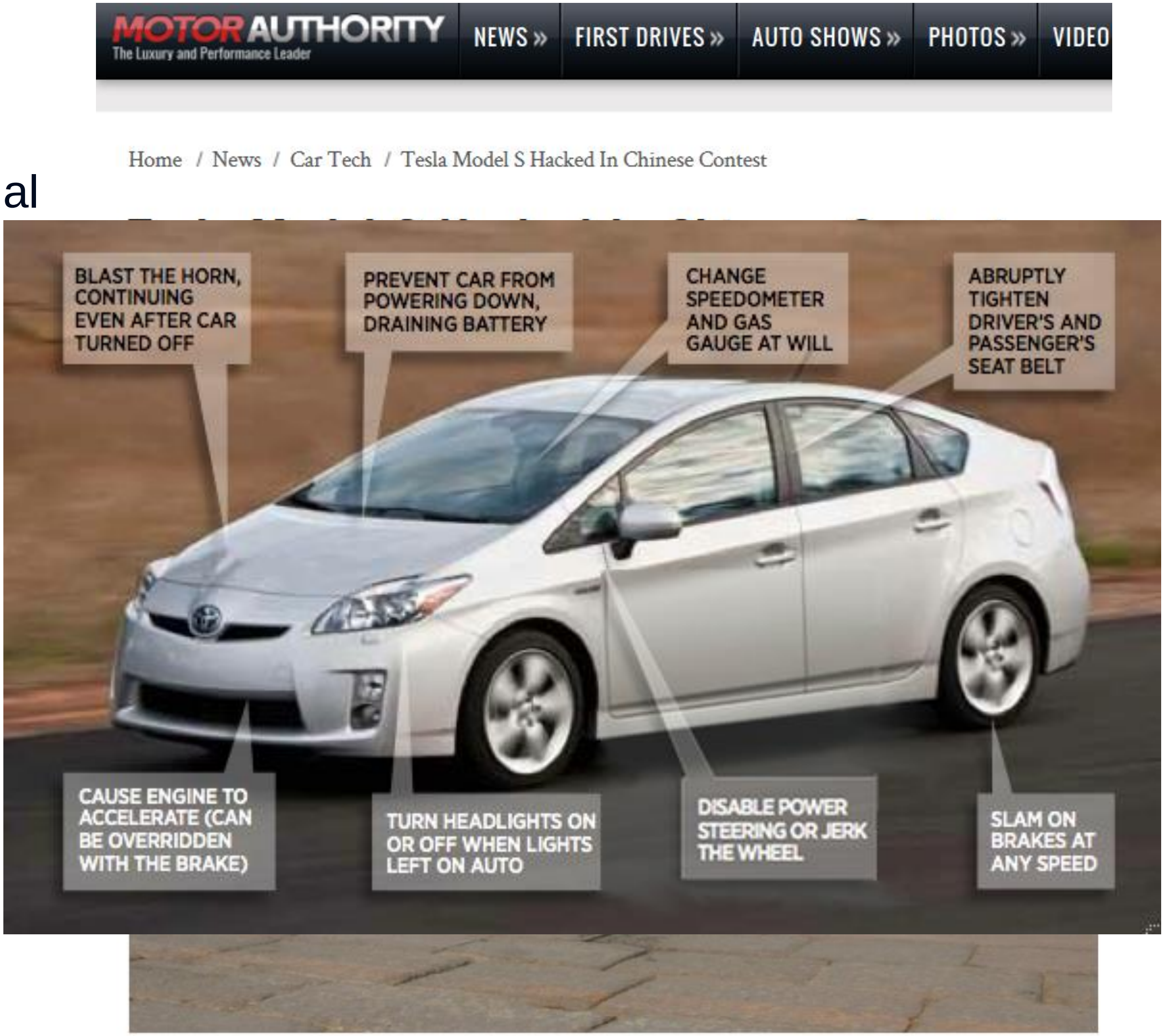
By Antony Ingram 1 | 8,823 views | Jul 22, 2014

2014 Tesla Model S in China

http://www.motorauthority.com/news/1093422_tesla-model-s-hacked-in-chinese-contest

Security is a rising concern for vehicles

- Hacking contest for a Telsa as part of a competition at the annual SyScan conference in Beijing
- “A Survey of Remote Automotive Attack Surfaces” C. Miller, C. Valasek



MOTOR AUTHORITY The Luxury and Performance Leader

NEWS » FIRST DRIVES » AUTO SHOWS » PHOTOS » VIDEO

Home / News / Car Tech / Tesla Model S Hacked In Chinese Contest

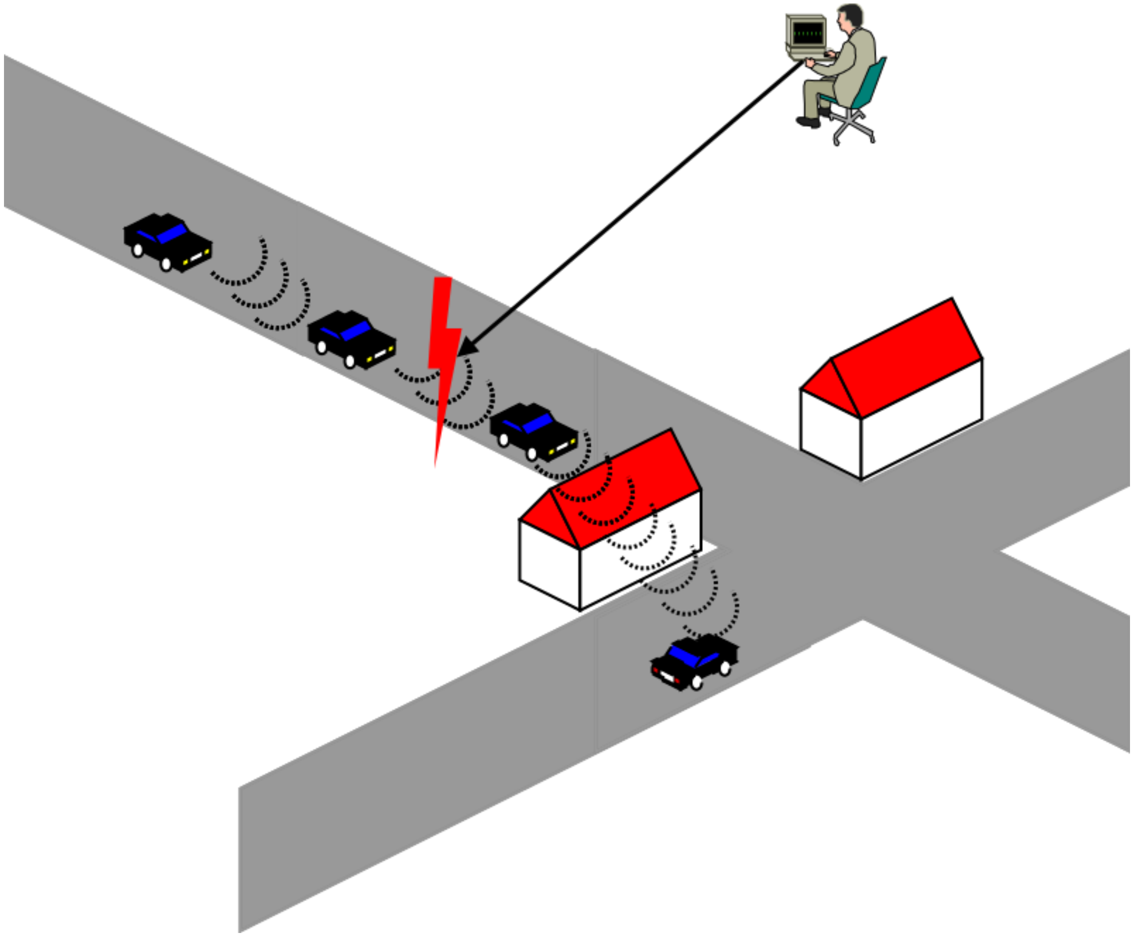
BLAST THE HORN, CONTINUING EVEN AFTER CAR TURNED OFF
PREVENT CAR FROM POWERING DOWN, DRAINING BATTERY
CHANGE SPEEDOMETER AND GAS GAUGE AT WILL
ABRUPTLY TIGHTEN DRIVER'S AND PASSENGER'S SEAT BELT
CAUSE ENGINE TO ACCELERATE (CAN BE OVERRIDDEN WITH THE BRAKE)
TURN HEADLIGHTS ON OR OFF WHEN LIGHTS LEFT ON AUTO
DISABLE POWER STEERING OR JERK THE WHEEL
SLAM ON BRAKES AT ANY SPEED

2014 Tesla Model S in China

http://www.motorauthority.com/news/1093422_tesla-model-s-hacked-in-chinese-contest

With cooperative driving security will be a major risk factor

- Vehicle control depends on information from other vehicles or infrastructure

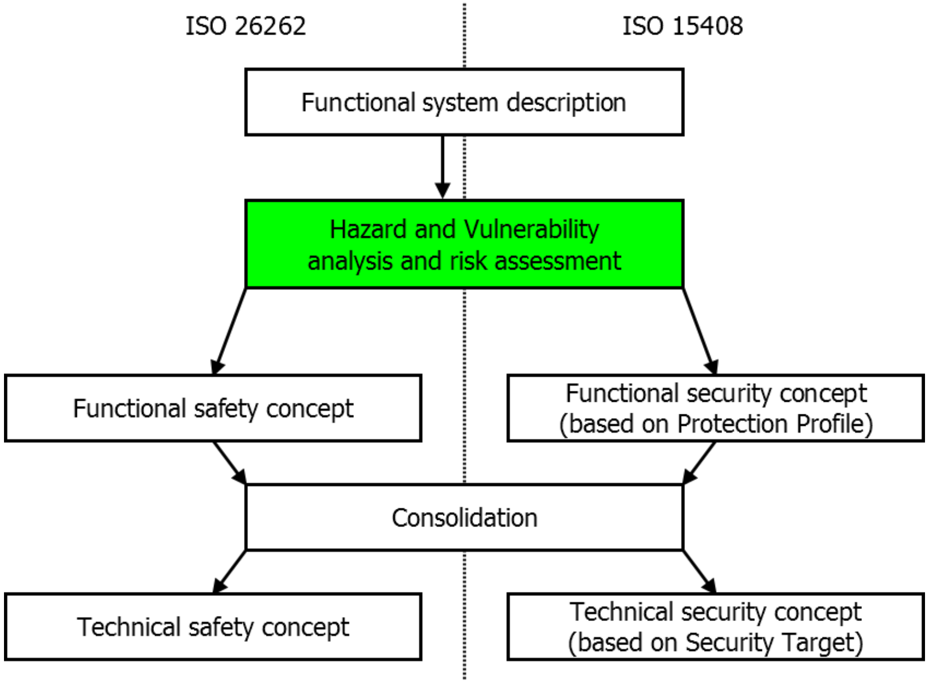


Safety engineering for vehicles and systems of vehicles needs to include security

- A holistic approach is necessary
- ISO 26262 does not mention security
- We try to integrate ISO/IEC 15408 (Common Criteria) with ISO 26262

Vision

- True holistic approach


ISO 26262
ISO 15408
Functional system description
Hazard and Vulnerability analysis and risk assessment
Functional safety concept
Functional security concept (based on Protection Profile)
Consolidation
Technical safety concept
Technical security concept (based on Security Target)

Analysis Method and Results

Hazard and Vulnerability analysis and risk assessment

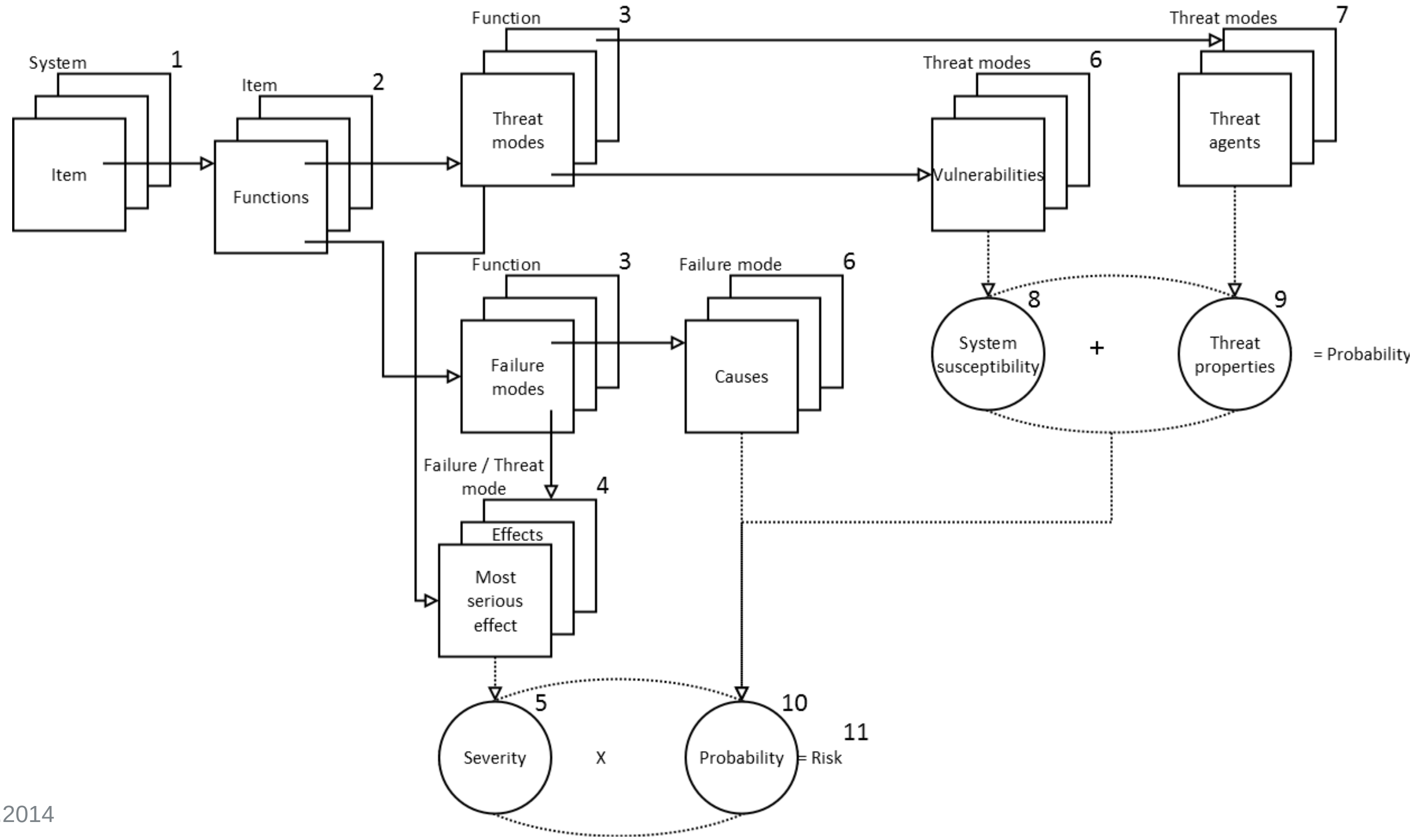
- Threat and failures analysis for a generic vehicle system

- The aim is to identify potential Threat Modes and Failures early in the design process

- We analyzed a generic vehicle system architecture and verified the results based on available penetration test data

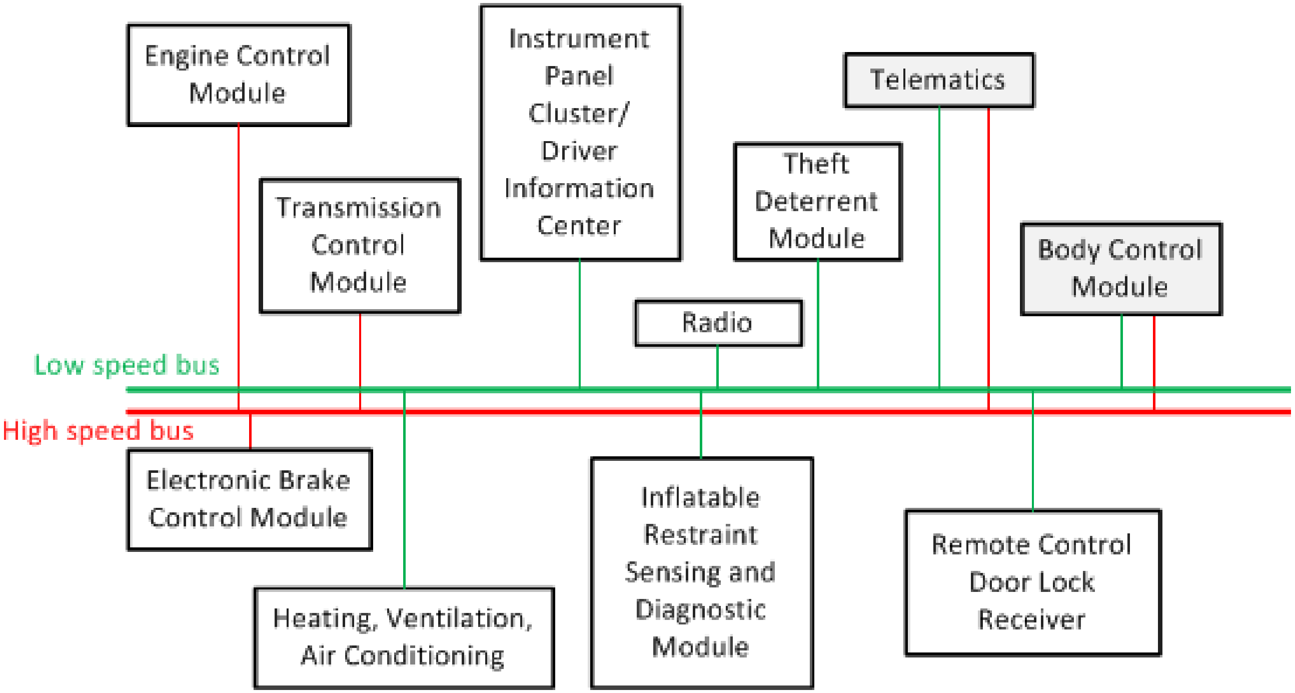
Failure Modes, Vulnerabilities and Effects Analysis (FMVEA)

- A combined safety and security analysis method
- Vulnerabilities causes Threat modes



Abstract vehicle system architecture

- Simplified vehicle architecture, LIN/MOST is excluded


Engine Control Module
Instrument Panel Cluster/ Driver Information Center
Telematics
Transmission Control Module
Theft Deterrent Module
Body Control Module
Radio
Low speed bus
High speed bus
Electronic Brake Control Module
Inflatable Restraint Sensing and Diagnostic Module
Remote Control Door Lock Receiver
Heating, Ventilation, Air Conditioning

Analysis focuses on the Telematics Unit

- Bridges High and Low Speed Can
- Has the largest attack surface

Safety and Security Services	Information and Navigation	Entertainment	Diagnostics
Send crash data	Call technical support	Receive voice communication	Transmit diagnostic data
Send vehicle position	Connect Wi-Fi / Bluetooth devices	Connect to external media sources	Receive over the air (OTA) firmware updates
Receive door look signal			

Analysis Results

- Excerpt from the FMVEA table

Function	Vulnerability / Failure Cause	Threat Mode / Failure Mode	Threat Effect / Failure Effect	System Status	System Effect	Severity	System Susceptibility	Threat Properties	Attack / Failure Probability	Risk
Over the Air Update	insufficient authentication of Telematics Network Operations System	Attacker masquerades itself as TNOS and sends own firmware Update (Spoofing)	Attacker deploys own firmware	-	safety-critical, Attacker has control over the vehicle	6	4	4	8	Very high

Analysis Results

- Excerpt from the FMVEA table

Function	Vulnerability / Failure Cause	Threat Mode / Failure Mode	Threat Effect / Failure Effect	System Status	System Effect	Severity	System Susceptibility	Threat Properties	Attack / Failure Probability	Risk
Over the Air Update	connection is lost	Data missing from update	Update is interrupted	Updating	none	1	…	…	6	Very low

Outlook

Next steps

- Compare results to other combined Safety&Security analysis methods
  - CHASSIS, STPA-SEC

- Extend analysis to include systems of cooperative vehicles

- Derive security requirements from the analysis results

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

AIT Austrian Institute of Technology

your ingenious partner

Christoph Schmittner
Christoph.schmittner.fl@ait.ac.at
Ma Zhendong
Zhendong.ma@ait.ac.at
Paul Smith
Paul.smith@ait.ac.at