QUALITY ENGINEERING FOR AUTOMOTIVE SOFTWARE OF CONNECTED VEHICLES

HOW TO SECURE A VEHICLE THAT IS “TALKING” TO EVERYTHING?

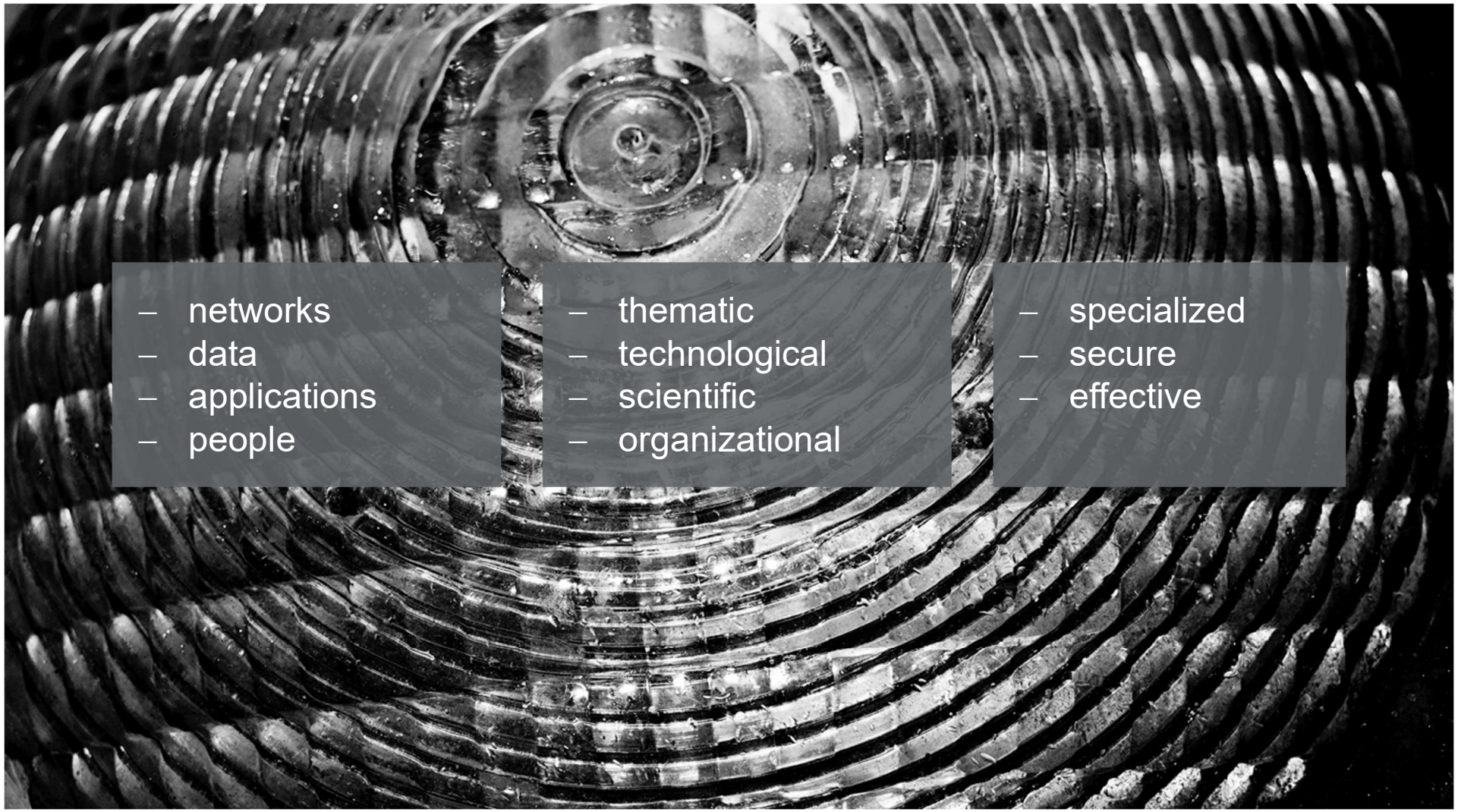
Ina Schieferdecker, Jürgen Großmann, June 29th, 2016

9. Fachkonferenz: Qualität 4.0 im Automobil, Stuttgart

Engineering a Connected World

Fraunhofer FOKUS

FOKUS = THE NETWORKING INSTITUTE OF FRAUNHOFER



Fraunhofer FOKUS

FRAUNHOFER FOKUS: EXPERTISE IN V2X COMMUNICATION

Research

PRE-DRIVE C2X

DRIVE C2X

simTD

FOT-NeT

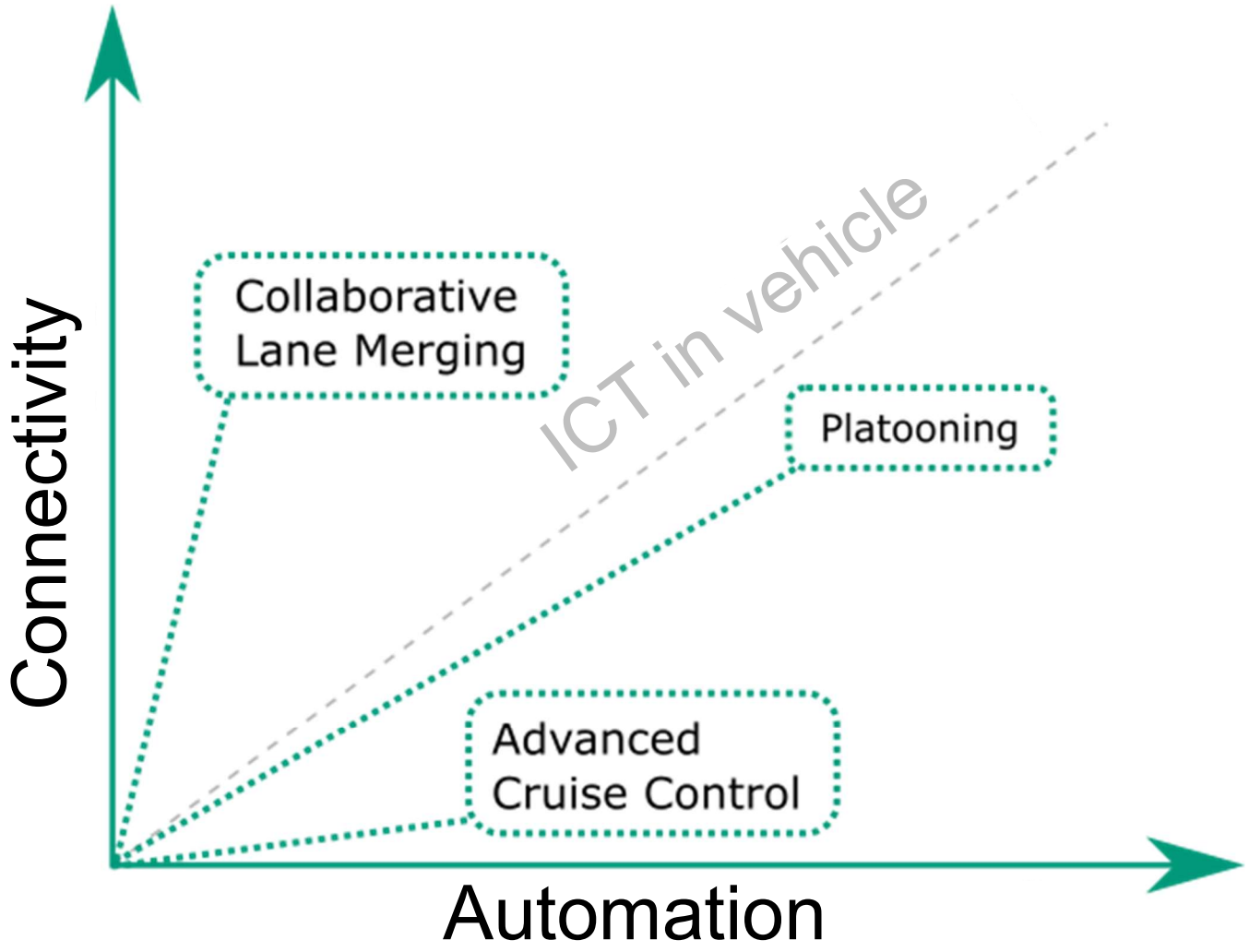
- V2X Application
- V2X Security
- V2X Validation
- V2X Management & Simulation

Standardization & Deployment

CAR 2 CAR COMMUNICATION CONSORTIUM

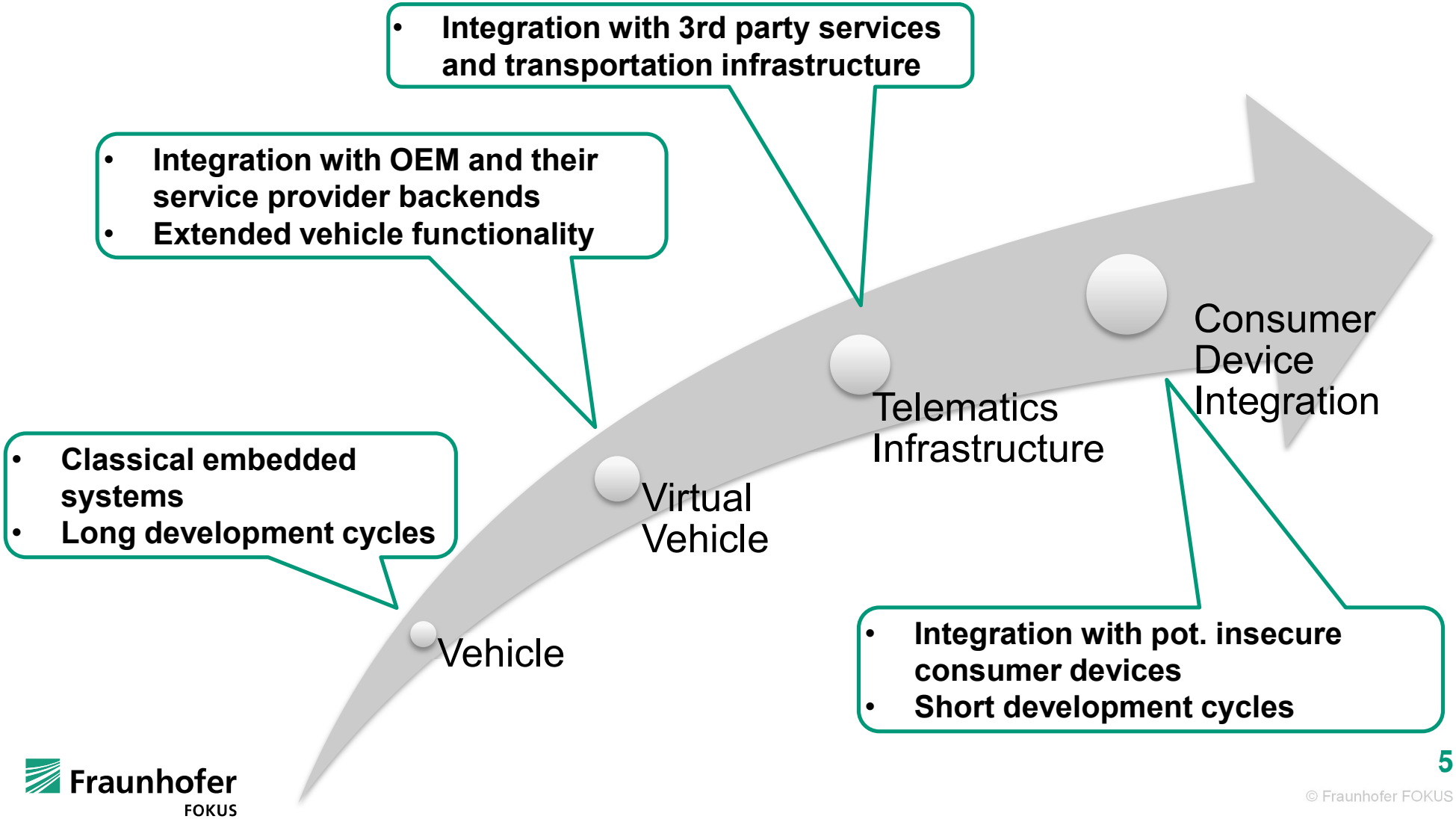
ETSI World Class Standards

CONNECTIVITY AND AUTOMATION



THE NETWORK GROWS

Larger perimeter opens new attack vectors

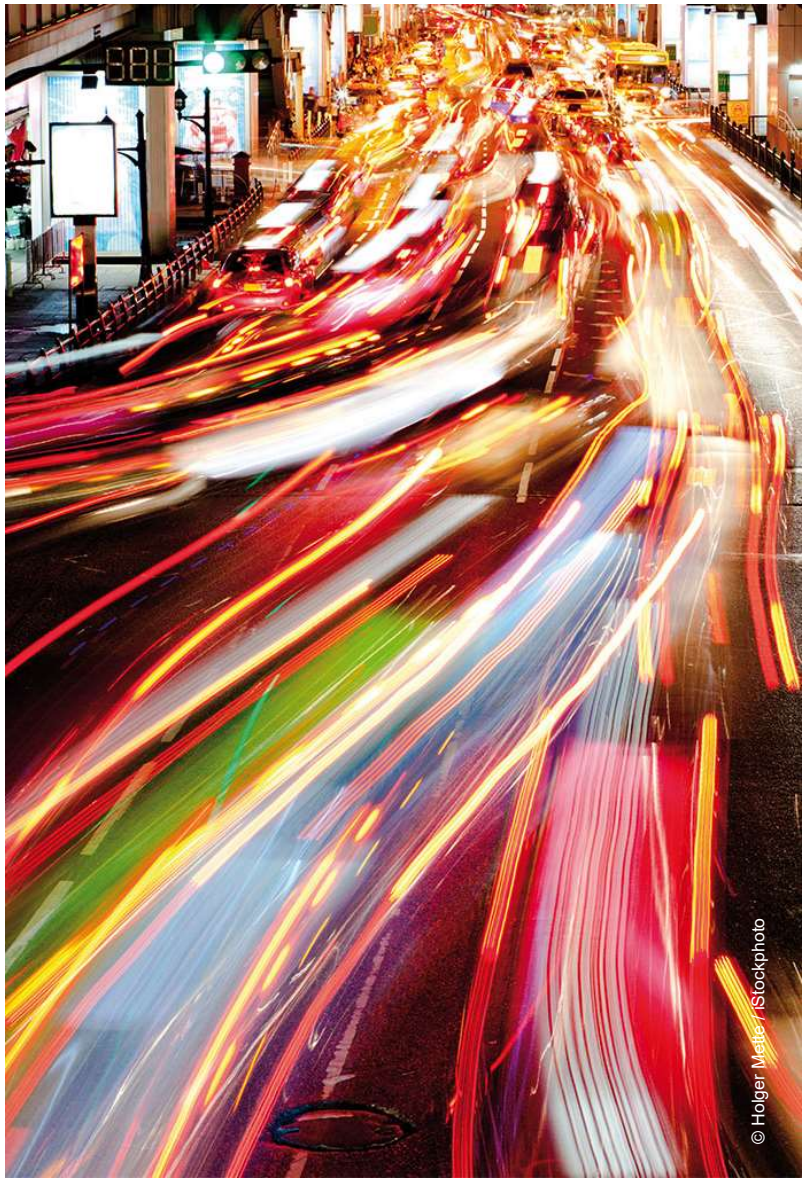


EMERGING NEW APPLICATIONS AND TECHNOLOGIES

The vehicle is only one thing

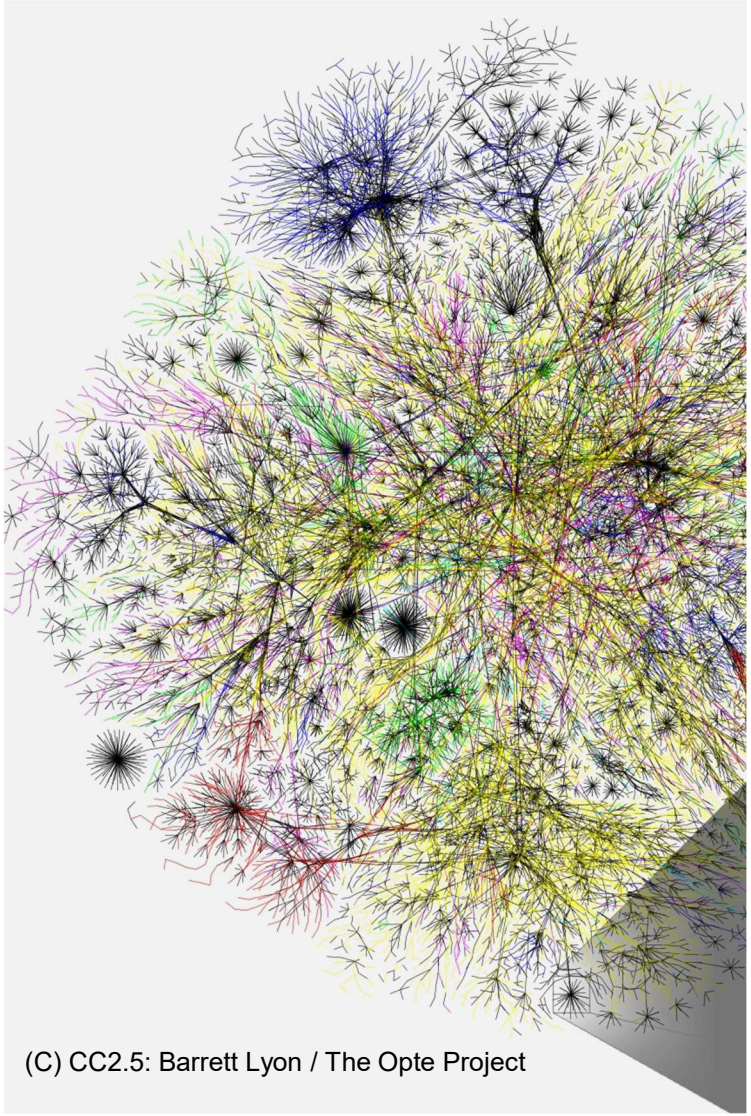
- **New applications and services**
  - Smart navigation, smart sharing
  - Highly automated driving
- **New architectures**
  - Service-oriented
  - Cloud-based
  - Communication-based
- **New protocols and technologies**
  - IPv6, 802.11p, 5G

- **New Challenges**
  - Providing interoperability and security (by maintaining dependability)



SECURITY IMPEDES SAFETY, QUALITY IMPEDES SECURITY

- Devices can be poorly designed and implemented
- Heterogeneous protocols and technologies create complex configurations
- Lack of security standards and limited guidance for
  - secure development of devices
  - lifecycle maintenance and management of devices
- Missing methods for achieving situational awareness and no best practices for incident response activities
- Privacy concerns are complex and not always readily evident.

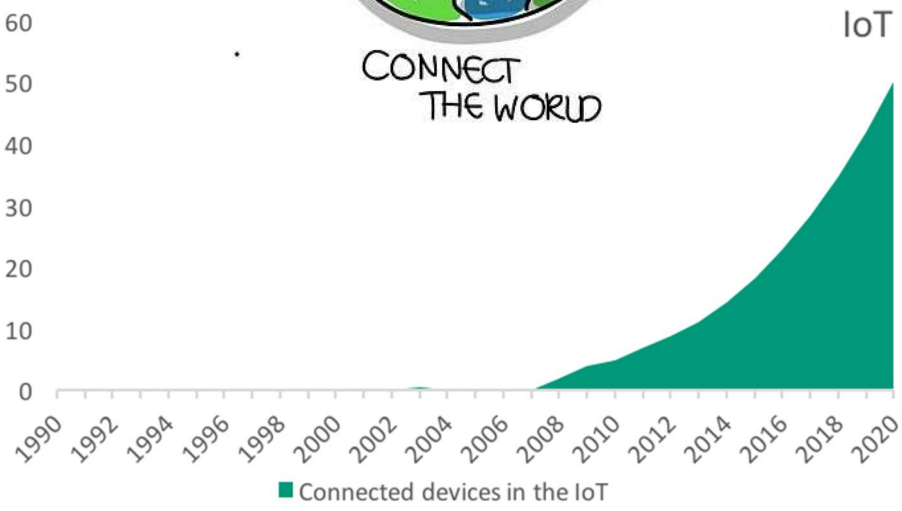


(C) CC2.5: Barrett Lyon / The Opte Project

YOU ARE NOT ALONE !

- By 2020, the number of active wireless connected devices
  - will exceed 40 billion.
  - will more and more integrate critical systems and infrastructures
  - increasingly become attractive target for cybercriminals

- More connected devices mean more attack vectors and more possibilities for hackers and cyber criminals

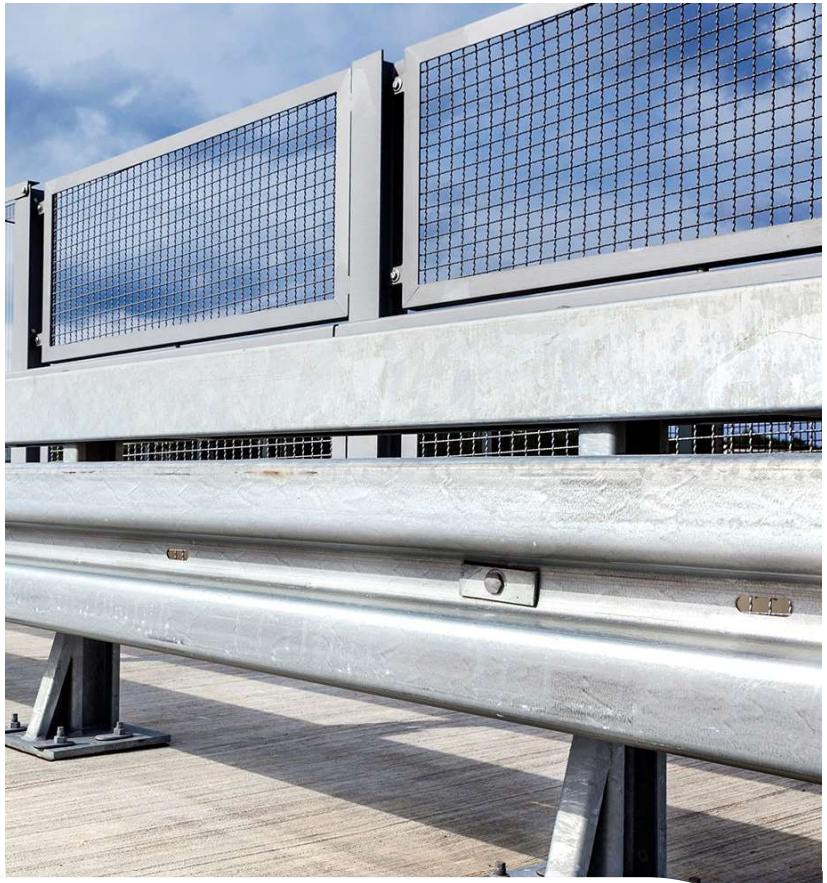


Source: https://www.flickr.com/photos/maerskline/8432240103/in/photostream/
License: https://creativecommons.org/licenses/by-sa/2.0/

KNOW YOUR RISKS

Prevent that security hurts!

1. **Reputation:** uncertainty and costs through security incidents (damages, loss of reputation)
2. **Cost:** high development costs (required conversion of established platforms, high effort to realize and check security)
3. **Complexity:** heterogeneous security solutions globally different regulations
4. **Restriction:** planned business models can not be realized (e.g. data protection) due to regulation



Changing your habits in …

1 Assessment | 2 Technology | 3 Processes | 4 Organization | 5 Regulation

1 ASSESSMENT: TEST AUTOMATION

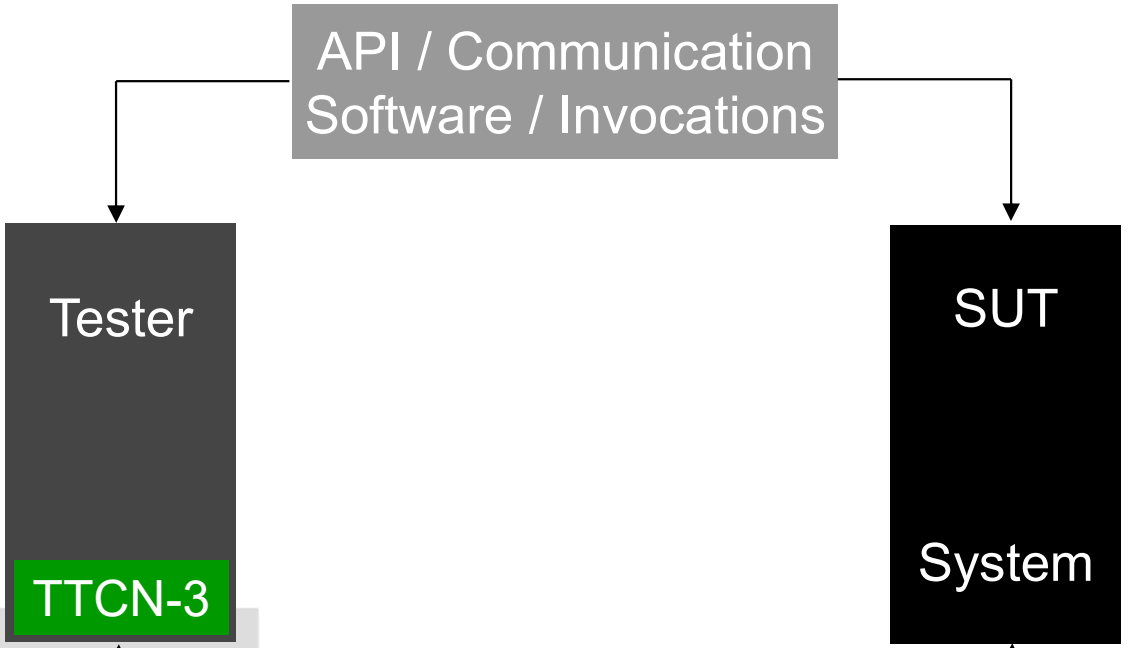
- TTCN-3 is the Testing and Test Control Notation
- Internationally standardized testing language for formally defining test scenarios. Designed purely for testing

```
testcase Hello_Bob () {
        p.send("How do you do?");
        alt {
        []p.receive("Fine!");
                {setverdict( pass )};
        [else]
                {setverdict( inconc )}  //Bob asleep!
        }
}
```

TTCN-3 DESIGN

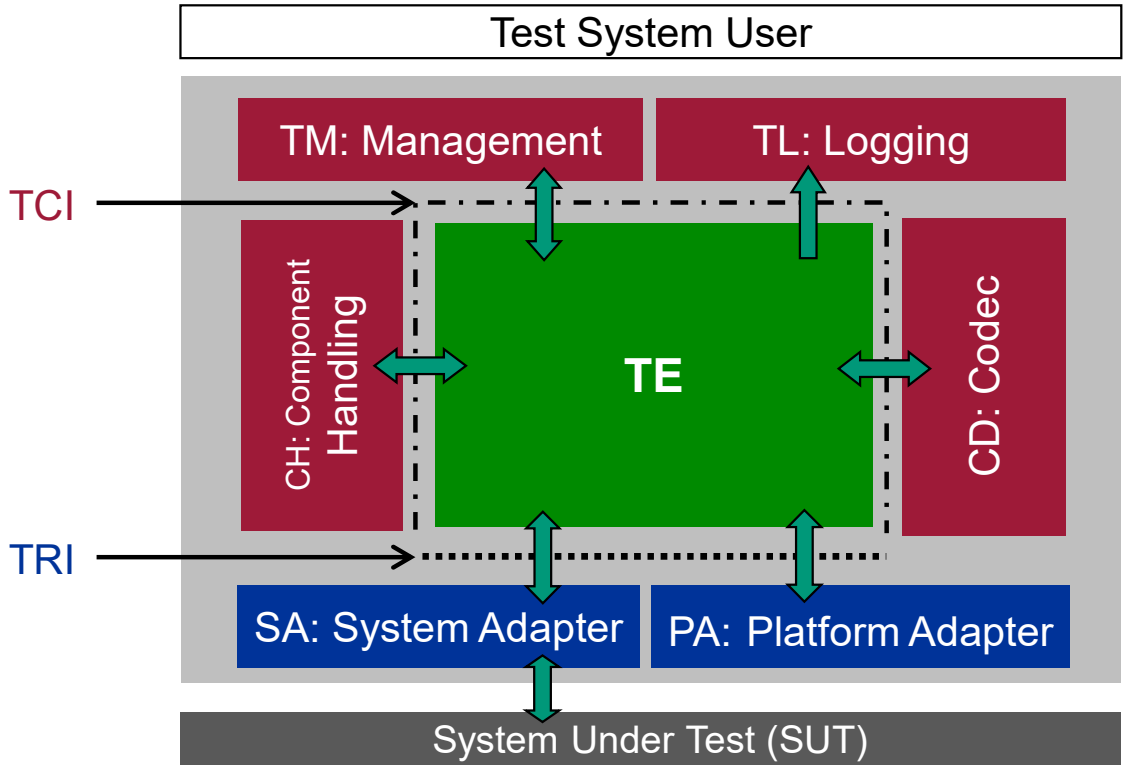
- One test technology for different tests
  - Distributed, platform-independent testing
  - Integrated graphical test development, documentation and analysis
  - Adaptable, open test environment

- Areas of Testing
  - Regression
  - Conformance/functionality
  - Interoperability/integration
  - Real-time, performance, load, stress
  - Security




```
testcase Hello_Bob () {
        p.send("How do you do?");
        alt {
        []p.receive("Fine!");
                {setverdict( pass )};
        [else]
                {setverdict( inconc )}  //Bob asleep!
        }
}
```

TTCN-3 TEST SYSTEM ARCHITECTURE

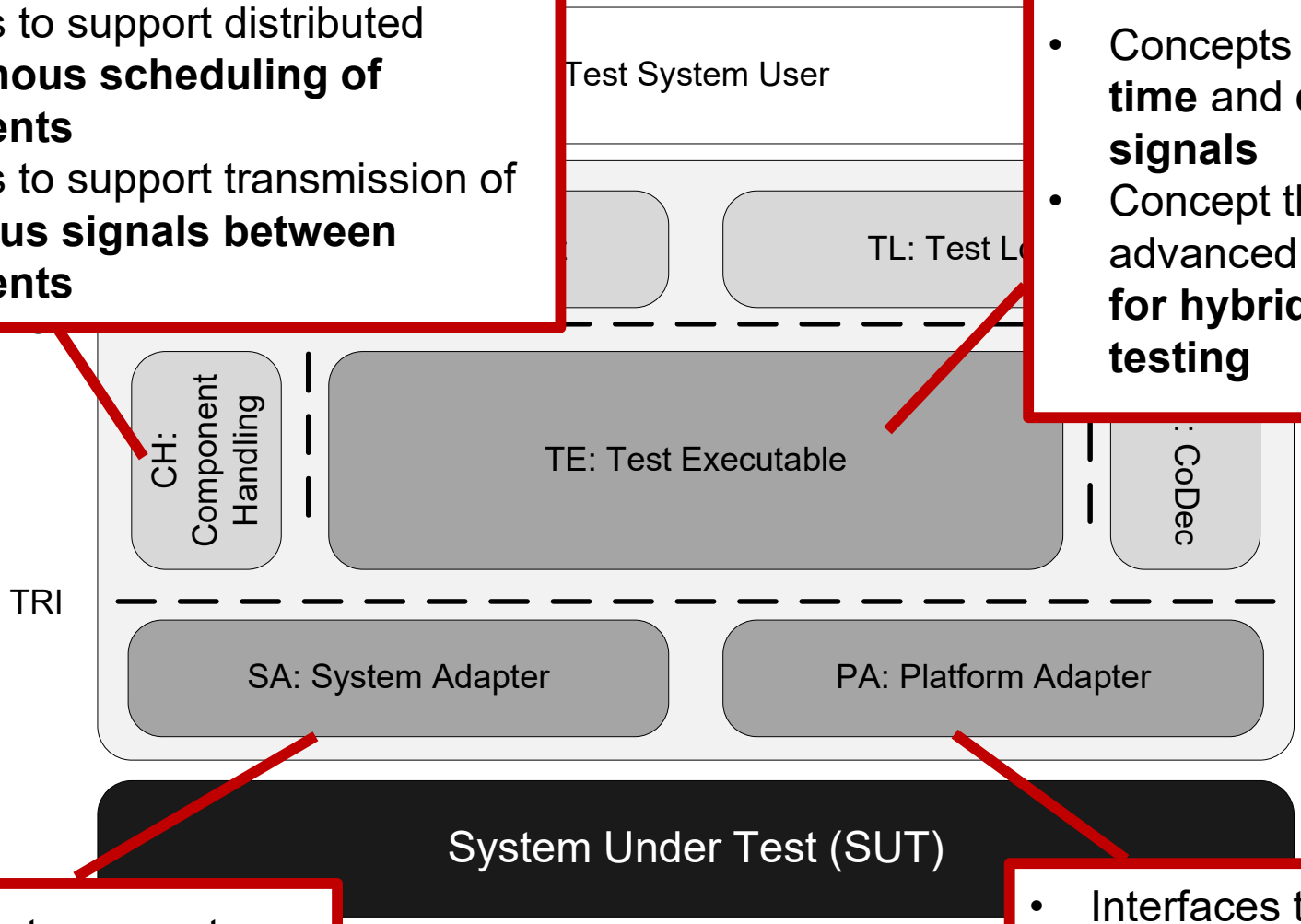


TE – TTCN-3 Executable
TM – Test Management
TL – Test Logging
CD – Codec
CH – Component Handling
SA – System Adapter
PA – Platform Adapter
SUT – System Under Test

ETSI ES 201 873-1 TTCN-3 Core Language (CL)
ETSI ES 201 873-5 TTCN-3 Runtime Interface (TRI)
ETSI ES 201 873-6 TTCN-3 Control Interfaces (TCI)

TESTING EMBEDDED SYSTEMS

- Interfaces to support distributed **synchronous scheduling of components**
- Interfaces to support transmission of **continuous signals between components**

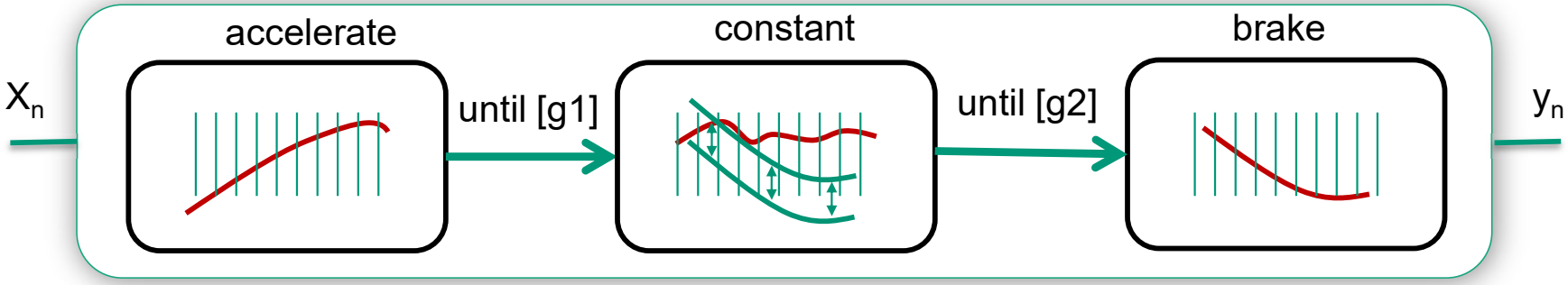


- Concepts to deal with **time** and **continuous signals**
- Concept that allow advanced **control flow for hybrid system testing**

- Interfaces to support **stimulation** with and **evaluation** of **continuous signals**

- Interfaces to support **access to time** and **sampling**

TTCN-3 EMBEDDED MODES



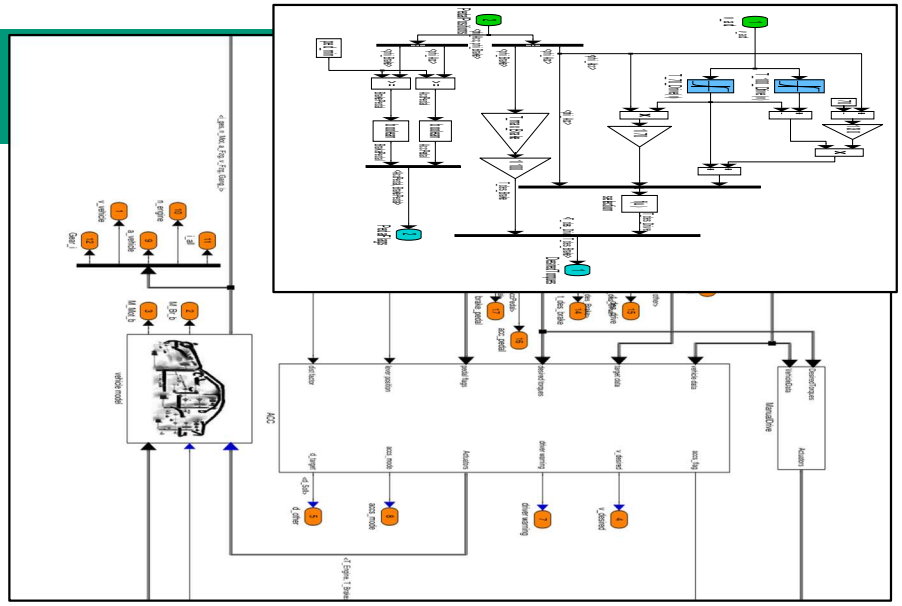
SIGNAL GENERATION BUILDING BLOCKS

```
testcase signal_generation() runs on mtcType{
 seq{
  apply_noise(Throttle, 5.0, 5.0);
  apply_noise(Throttle, 10.0, 5.0);
  apply_ramp(Throttle, 10.0, 10.0, 2.0, 3);
  …}
```

INTEGRATION IN ML/SL

```
// accelerate vehicle until 35
//  ms and activate ACCS

cont{
  onentry{v_other.value:= 25.0}
  phi_acc.value:=80.0;
}
until{
 [v_ego.value > 35.0] {
   phi_acc.value:=0.0;
   lever_pos.value:= MIDDLE;
 }
}
// wait for several seconds
wait(now+10.0);
// evaluate
cont{
  assert(v_ego.value <= 38.0); }
until{
 [d_other.value < sd] { ...
```

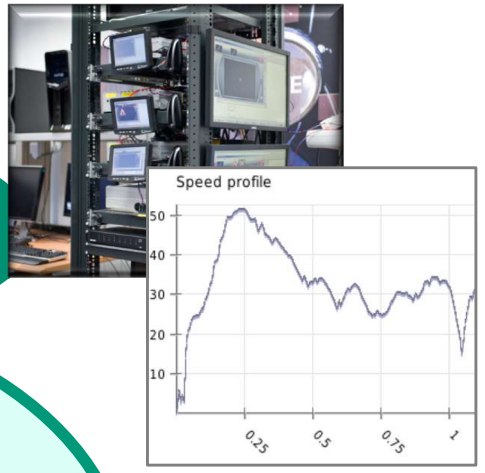


1. Introduce a vehicle ahead
2. Accelerate the ego vehicle until its velocity rises to more than 35 m/s.
3. Activate the cruise control.

AUTOMA[illegible]T BED

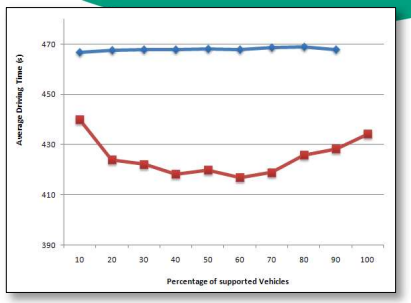
Tool suite for test automation and interoperability testing

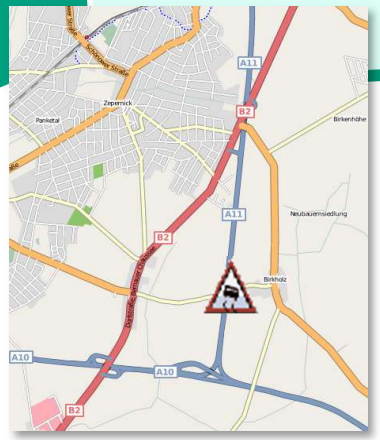
Test Execution



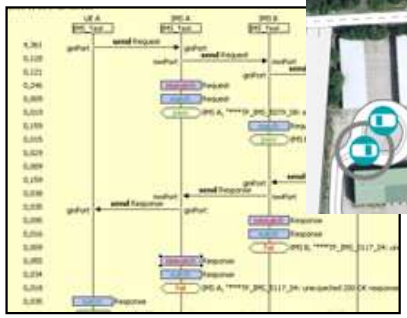
V2X Test Bed and Tool Suite

Test Data Generation (e.g. Traffic Simulation Data)

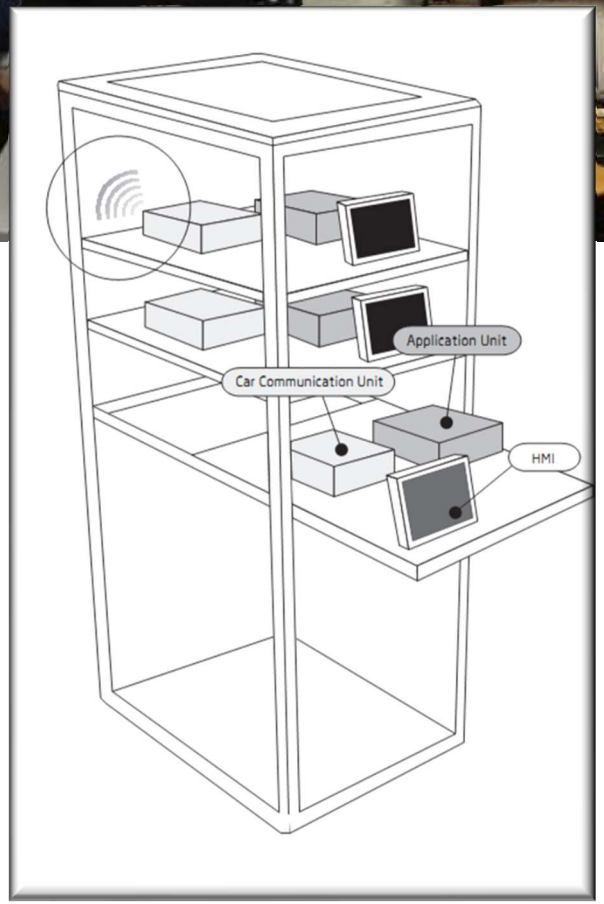




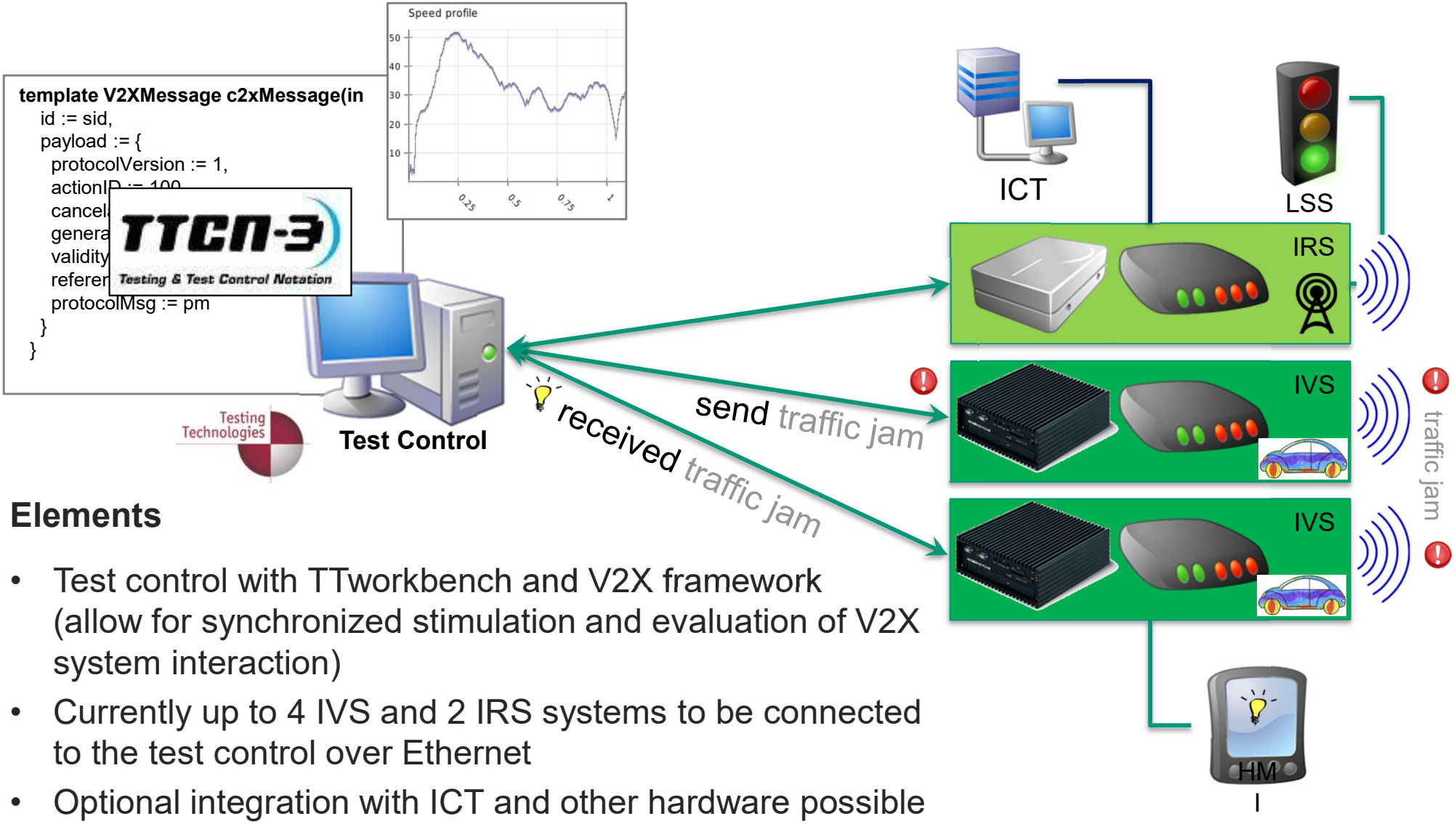
Log File Analysis and Visualization



THE SIM^{TD} SET UP IN THE LAB



V2X TEST BED ARCHITECTURE

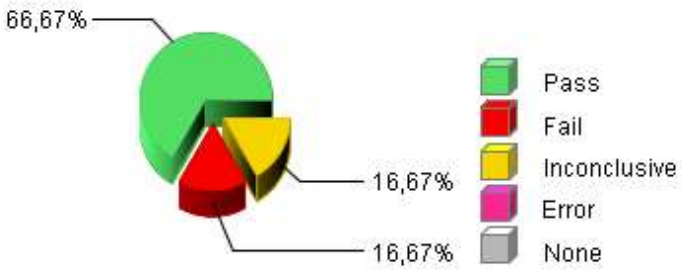


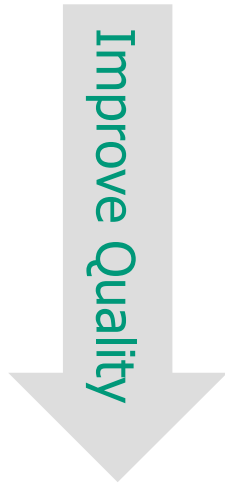
Elements

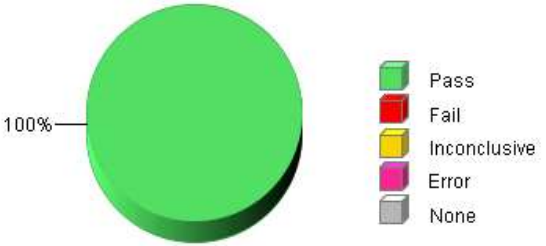
- Test control with TTworkbench and V2X framework (allow for synchronized stimulation and evaluation of V2X system interaction)
- Currently up to 4 IVS and 2 IRS systems to be connected to the test control over Ethernet
- Optional integration with ICT and other hardware possible

SIM^{TD} REFERENCE TESTS

- **40 Communication tests and test variants**
  - CAM variants
  - CAM frequencies, message life time handling etc.
  - DENM variants
- **20 Application tests**
  - testing event detection, propagation, handling and user notification for several V2X applications
- **Reference circuit**
  - event handling and user notification for several V2X applications
- **Reference circuit with load**
  - event handling and user notification for several V2X applications by applying networked and CPU load
- **Goals: <u>Integration</u>, <u>regression</u> and acceptance testing**

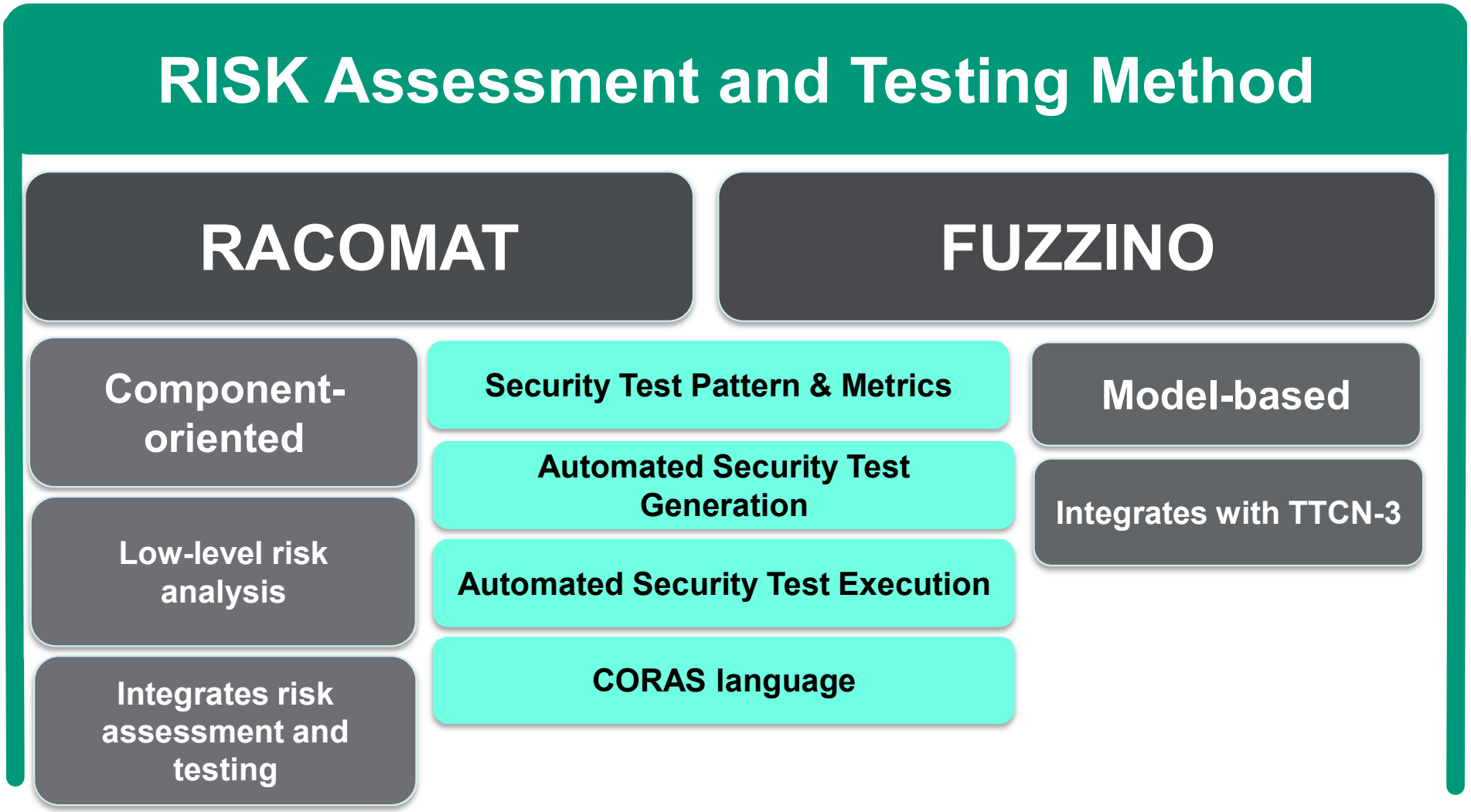




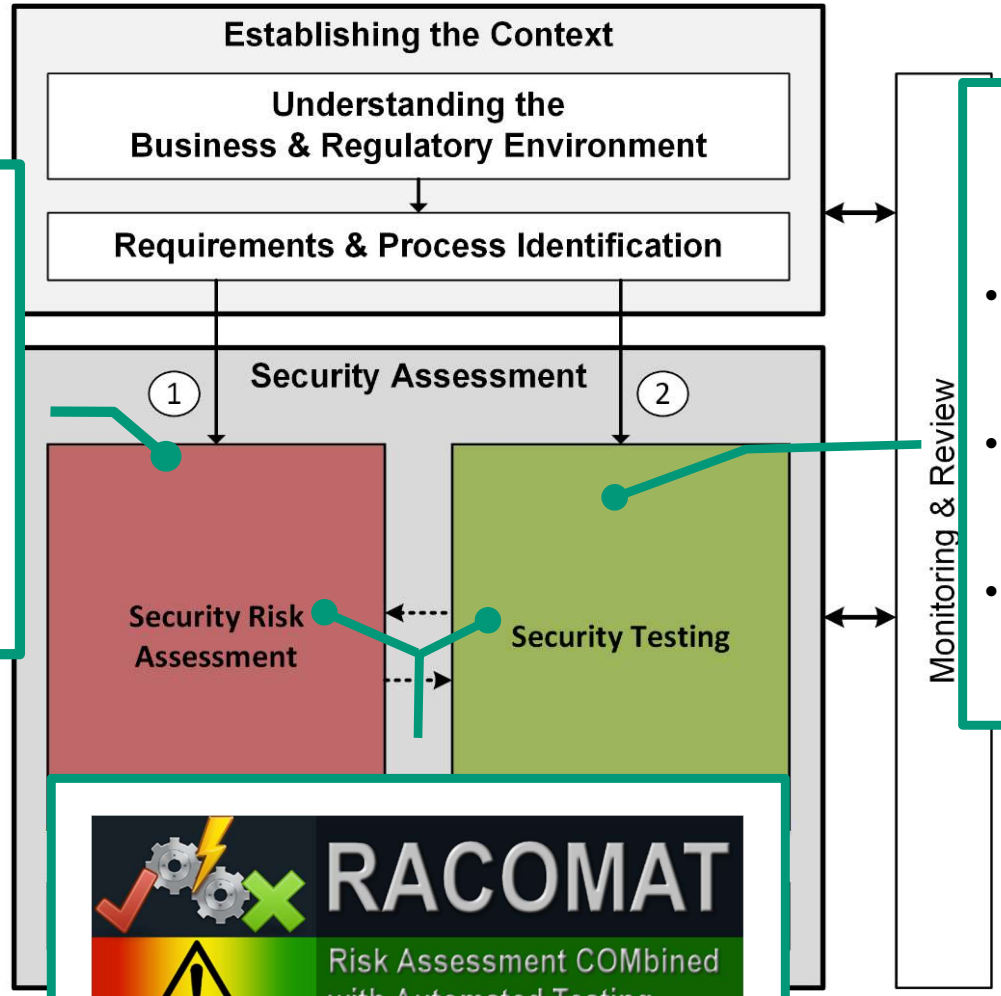


Project with Audi, Bosch, BMW, Continental, Daimler, Opel, Telekom, VW

RISK ASSESSMENT AND SECURITY TESTING



ADVANCED TOOL SUPPORT



CORAS

- A language for threat and risk modelling
- A tool designed to support documenting, maintaining and reporting analysis results

FUZZINO

- A library that provides generation of test data for fuzz testing
- injecting invalid or unexpected input data to the SUT.
- Support to find security-related weaknesses in your code.

RACOMAT

Risk Assessment COMbined with Automated Testing

- A language and tool to support risk-based security testing

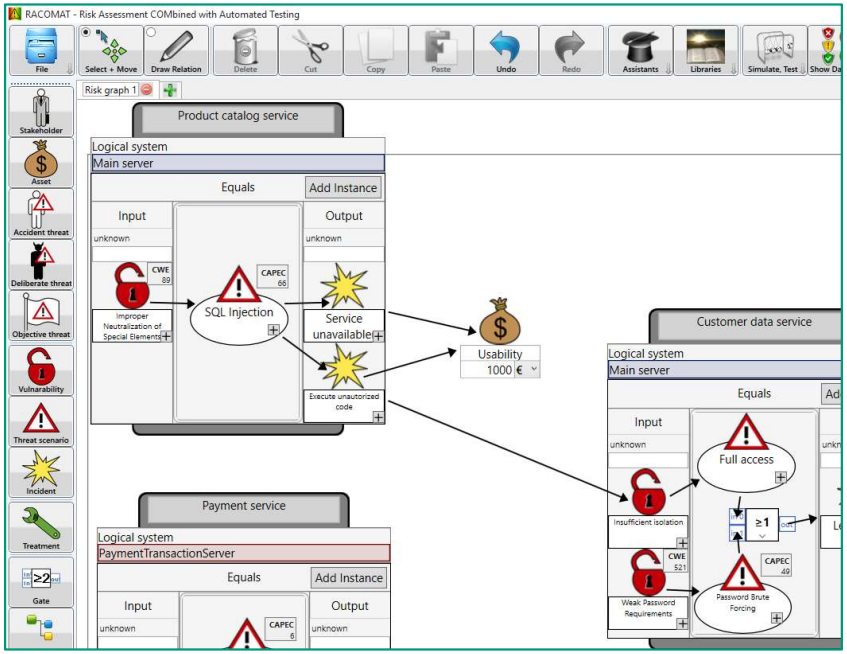
FRAUNHOFER RACOMAT

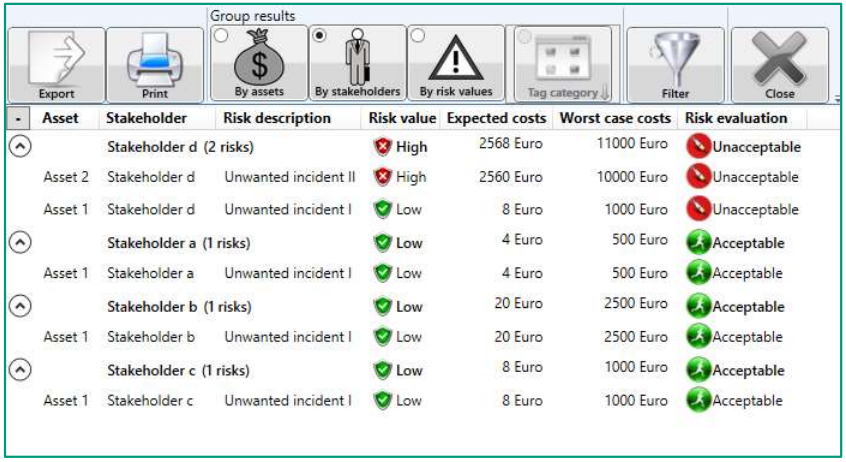
A toolset for Risk Assessment and Automated Testing

- Tool developed by Fraunhofer FOKUS within the RASEN project

- Assisted, literature based risk assessment
- Compositional risk assessment with incident simulation
- Risk based security testing
- Test based risk assessment
- Dashboard risk evaluation results to support the management

- Stand alone tool and Visual Studio plug-in
- Integration platform for other tools

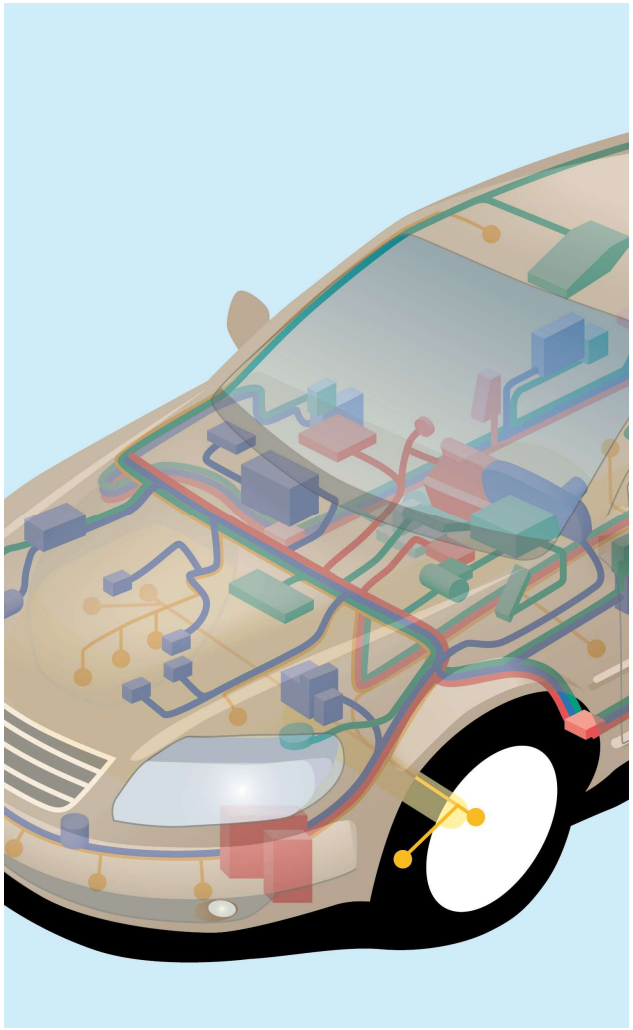




Asset	Stakeholder	Risk description	Risk value	Expected costs	Worst case costs	Risk evaluation
	Stakeholder d (2 risks)		High	2568 Euro	11000 Euro	Unacceptable
Asset 2	Stakeholder d	Unwanted incident II	High	2560 Euro	10000 Euro	Unacceptable
Asset 1	Stakeholder d	Unwanted incident I	Low	8 Euro	1000 Euro	Unacceptable
	Stakeholder a (1 risks)		Low	4 Euro	500 Euro	Acceptable
Asset 1	Stakeholder a	Unwanted incident I	Low	4 Euro	500 Euro	Acceptable
	Stakeholder b (1 risks)		Low	20 Euro	2500 Euro	Acceptable
Asset 1	Stakeholder b	Unwanted incident I	Low	20 Euro	2500 Euro	Acceptable
	Stakeholder c (1 risks)		Low	8 Euro	1000 Euro	Acceptable
Asset 1	Stakeholder c	Unwanted incident I	Low	8 Euro	1000 Euro	Acceptable

Modules for a secure vehicle

- Use basic security best practices
  - risk assessment incl. analysis of side-channel attacks
  - make use of established and secure protocols
- Introduce secure architectures
  - Authentication and encryption
  - Functional decoupling and partitioning
  - Securely consolidate ECUs diversity
- Use security software and trusted hardware
  - Firewall, intrusion detection, incident management
  - Secure software updates, secure storage and secure key management
  - Secure runtime environment (secure boot, virtualization, partitioning)



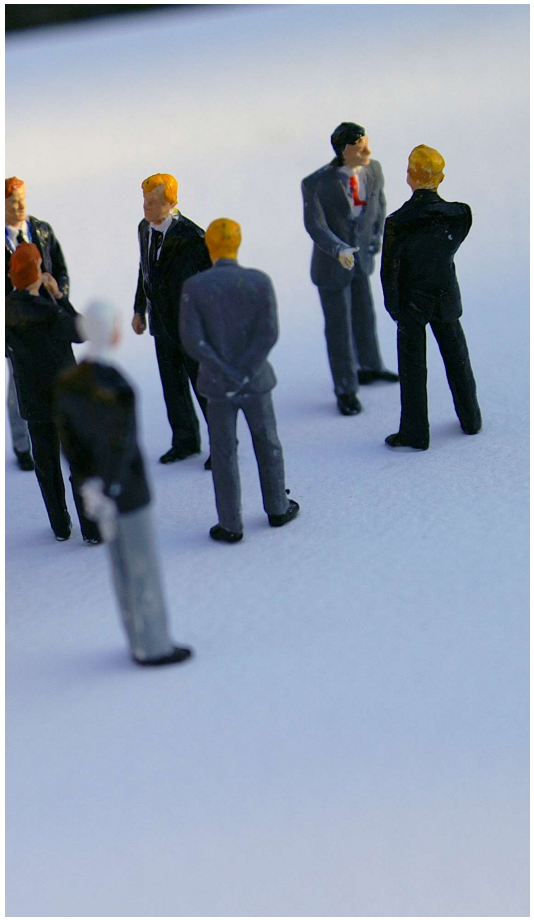
3 PROCESSES

Activities to develop and maintain secure systems

- Introduce a Security Development Lifecycle (risk modeling, security requirements, architecture, validation & maintenance)
- Integrate the processes for security & safety over the whole supply chain
- Synchronize with the current work on security in the automotive industry (AUTOSAR, C2C-CC, ETSI)
- Adopt best practices from other industries and from security standards (ISO 27K, 31K etc.)
- Coordinate with regulatory and certification bodies

4 ORGANIZATION

Support people to do the right thing!



- Internal organizational structures to actively approach security
- Central departments for Product Security that cover the Information Security Process (prevention, detection, response)
- Education and training program for employees
- Inter-organizational structures for networking and cooperation between OEMs, suppliers and infrastructure partners:
  - Reference architectures, protection profiles, standardization
  - Vulnerability databases, attack databases etc.
  - Dealing with acute crisis and attacks: crisis management, reporting of security incidents
- Cooperation with government bodies (BSI, BASt)

5 REGULATION

Trust is good, but control is better!

- Mandatory IT security requirements for the automotive industry
  - USA: IT Security Act on the way
  - DT: Contribution of IT security requirements on the Road Traffic Licensing Regulation conceivable
- Vision: certification and acceptance concept for vehicles
  - With ISO26262 coordinated security standard
  - Inclusion of security aspects in type approval
    - Challenge: However, once approval, security mechanisms need regular re-evaluation (development of methods of attack, etc.)
  - Minimum standards for the vehicle and for the whole supply chain incl. appropriate security assurance program
  - Selective CC and TR certification for critical components
  - Starting an Automotive Initiative with the BSI (similar as in Cloud Computing, Critical Infrastructure Protection and e-Health)

SUMMARY

- "Software is eating the world", online pioneer and entrepreneur Marc Andreessen, 2011 - **security, safety, privacy and trustworthiness** are key
- We do not only have to quality assure **software**, but also **protocols**, **services**, **data** and **systems of systems**
  - Apply a **secure systems engineering** approach to architecting and deploying new vehicle systems (Security-by-Design), implement layered security protections to defend your assets
  - Define and implement a **logging/audit framework** for the vehicle's ecosystem
  - Define **lifecycle controls and maintenance** for vehicle systems and the related infrastructures.
  - Implement **data protection** best-practices to protect sensitive information
  - Analyze privacy impacts to stakeholders and adopt a **privacy-by-design** approach to development and deployment
  - Don't fear **certification** and use advanced **risk analysis and testing** methods

CONTACT

Fraunhofer FOKUS
Kaiserin-Augusta-Allee 31
10589 Berlin, Germany
www.fokus.fraunhofer.de

Ina Schieferdecker

ina.schieferdecker@fokus.fraunhofer.de
Tel. +49 (0)30 3463-7201