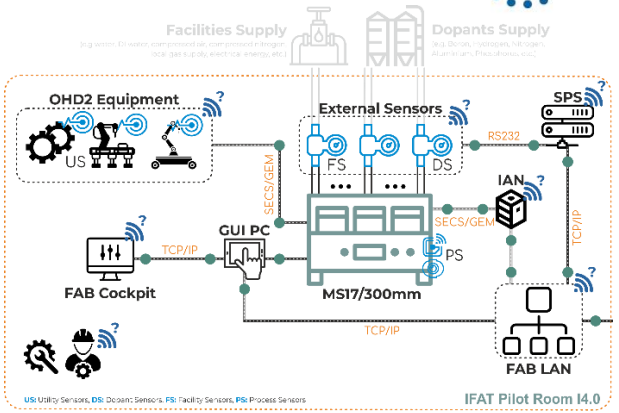
RESILIENCE IN COMPLEX IOT ENVIRONMENTS

IoT4CPS – The Austrian IoT Flagship Project

The IoT4CPS project is partially funded by the “ICT of the Future” Program of the FFG and the BMK

IoT in cyber-physical environments

- Large IIoT systems are **distributed, dynamic and heterogenous**
- CPS rely on **digital units to interact with the physical environment**
  - **Combination of IT and OT** raises new challenges
    → IT focus on Security, Reliability and Privacy
    → OT focus on Safety, Reliability and Resilience

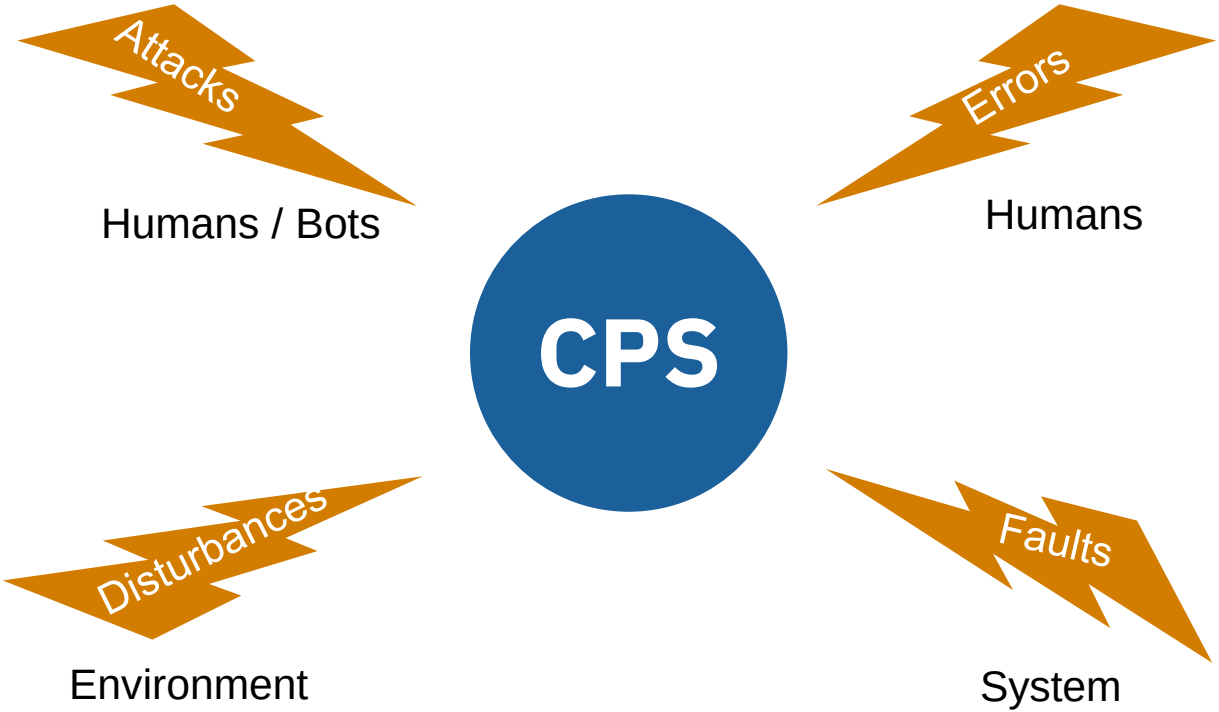


⇒ **Security and dependability** need to be addressed to reduce vulnerability

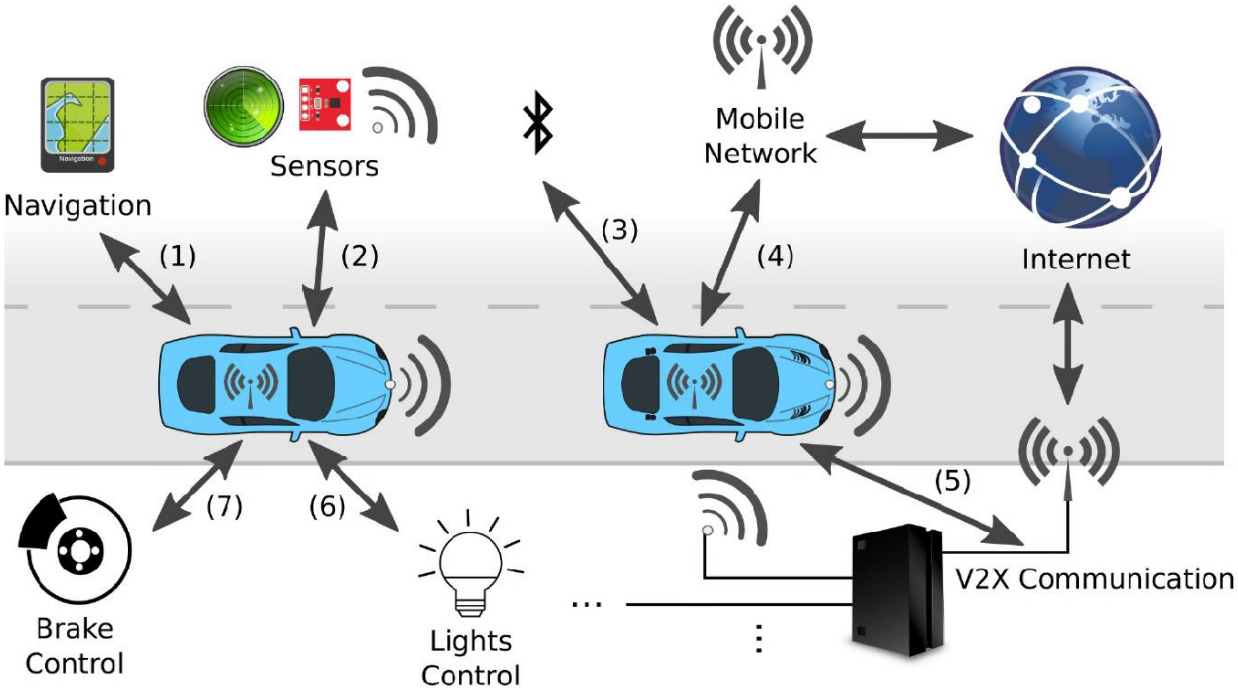
⇒ **Specific tools and methods** to cover all system levels (from sensor to product)

⇒ **Coverage of whole product life-cycle** is necessary to ensure long-term protection

Sources of faults



Faults & Threads in a Connected Vehicle



(1) No signal, GPS traceability

(2) Noise, stuck-to-the-ground, car spying

(3) Bluetooth authentication flaws

(4) Packet injection

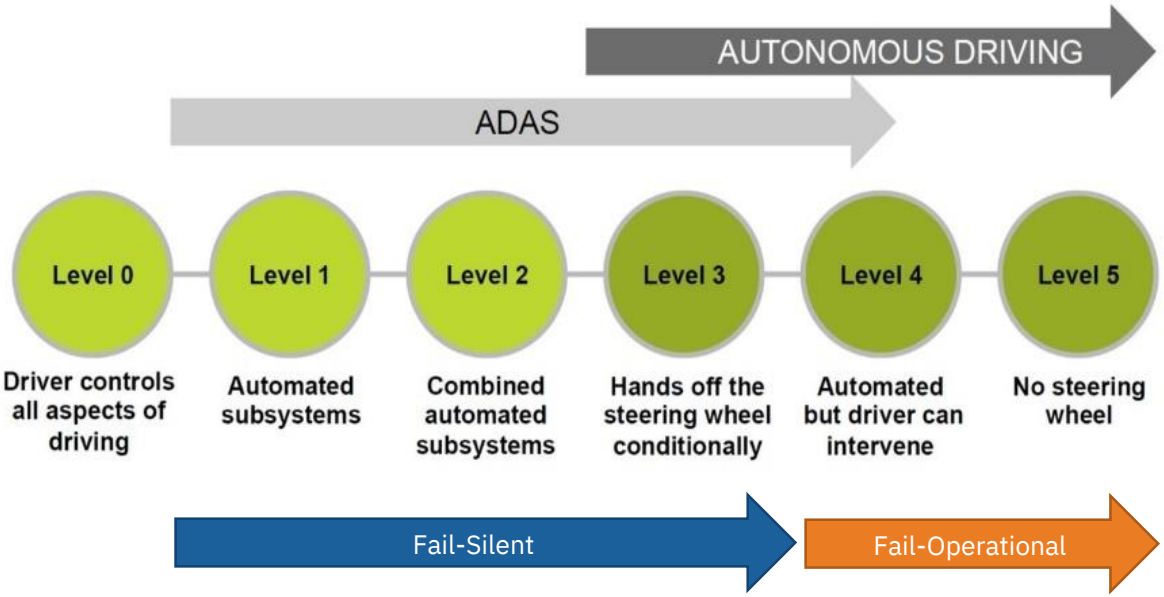
(5) Interference, denial-of-service by flooding

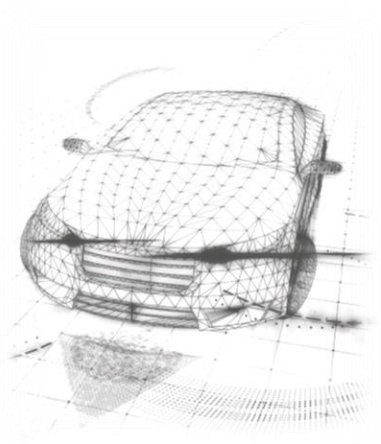
(6) Wrong control due radiation, replay attack

(7) Late message, gain control access

Source: **A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems**, Denise Ratasich, Faiq Khalid, Florian Geißler, Radu Grosu, Muhammad Shafique, Ezio Bartocci, IEEE Access, 2019

Resilience enables higher level of automatization

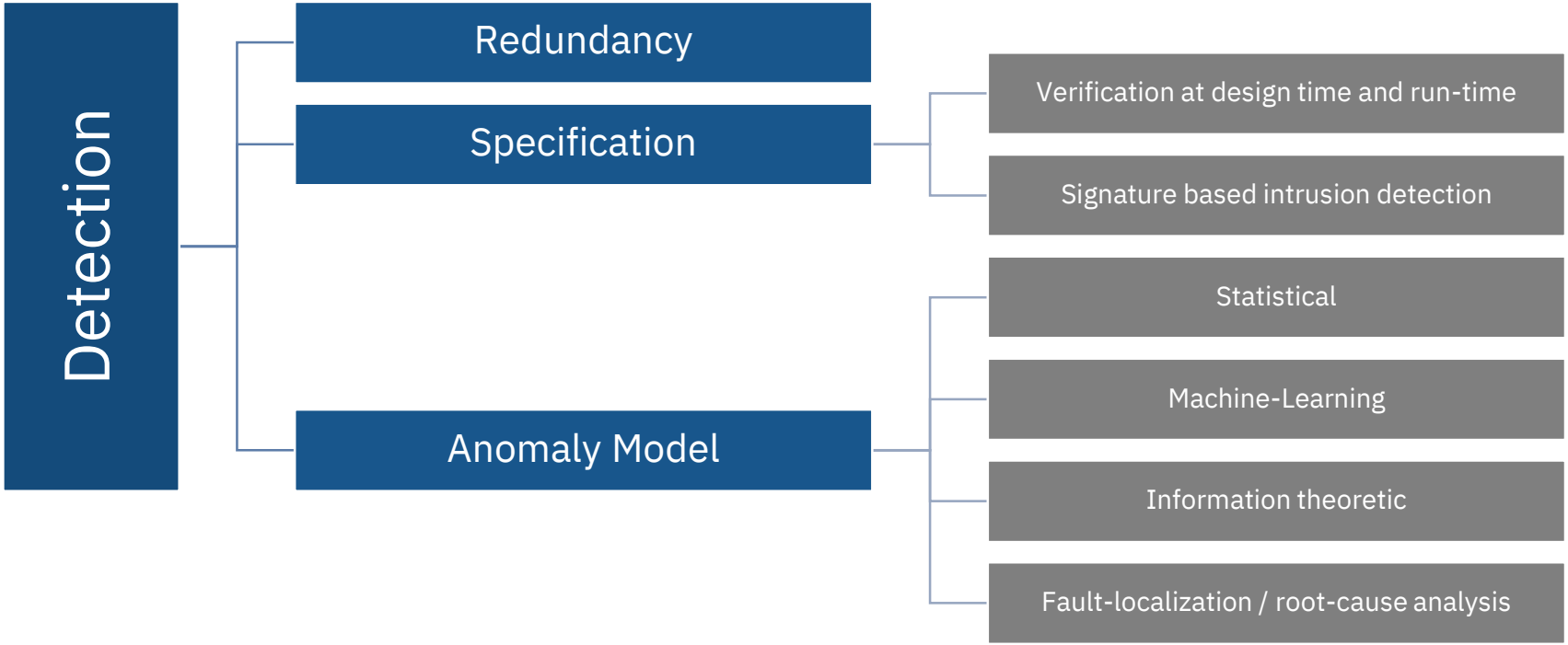




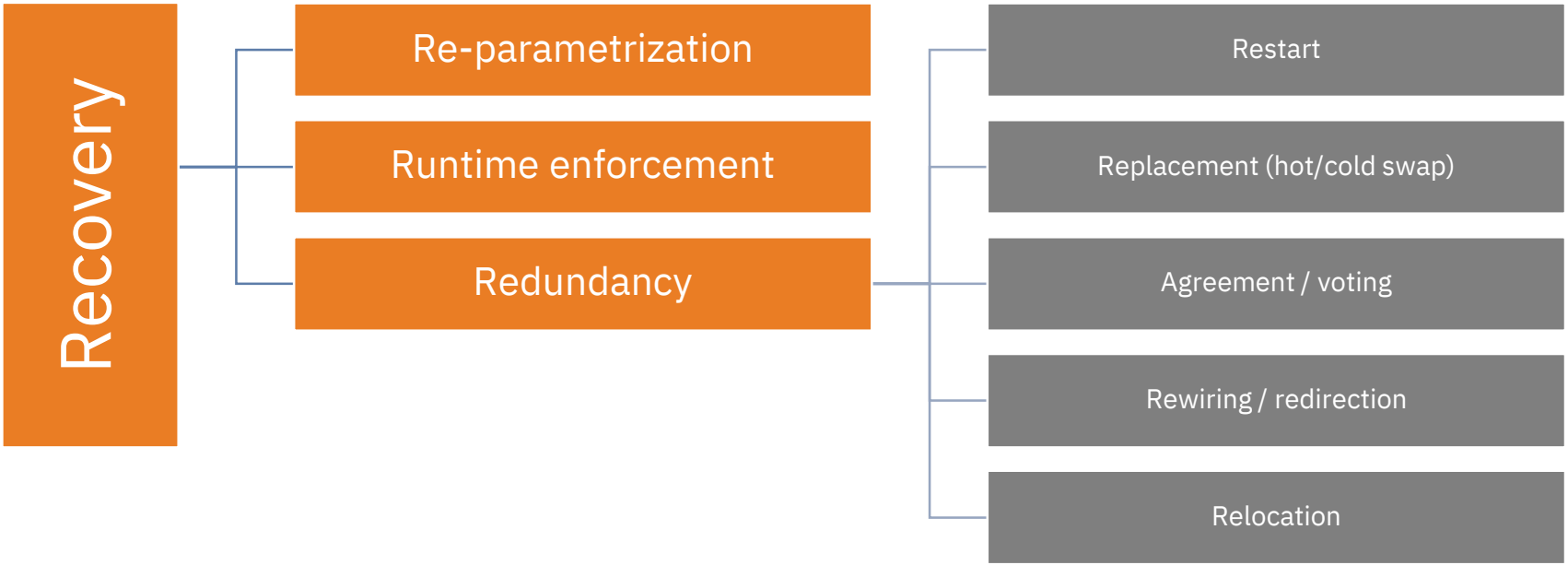
Dependability failures and security threats

	Physical	Network	Control	Information
Depend-ability	• Broken connector • Radiation	• Msg. collision • Desynchronization • Interference	• Input errors • Deadline miss	• Data corruption • Bit flips • Unavailability
Security	• Phys. damage / intervention • Sensor hacking • Crypto attack	• Replay • Spoofing • Jamming • Interruption	• Illegal contr. access • Control signal interception	• Eavesdropping • Data poisoning
Long-term	• Decay • Environm. effects	• Communication overload • Protocol violation	• Aging effects • Upgrades or new requiremt.	• Memory refresh • Capacitor recharging

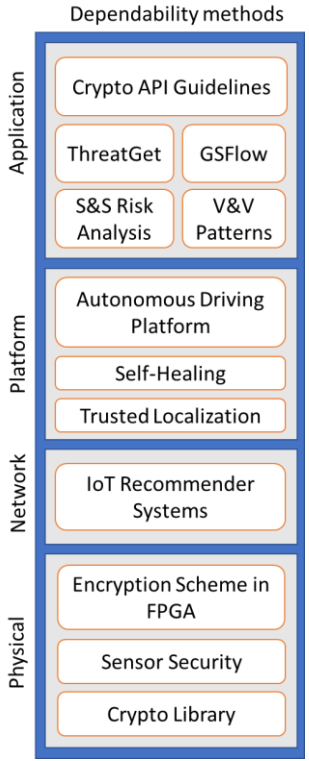
Detection


Detection
Redundancy
Specification
Anomaly Model
Verification at design time and run-time
Signature based intrusion detection
Statistical
Machine-Learning
Information theoretic
Fault-localization / root-cause analysis

Recovery

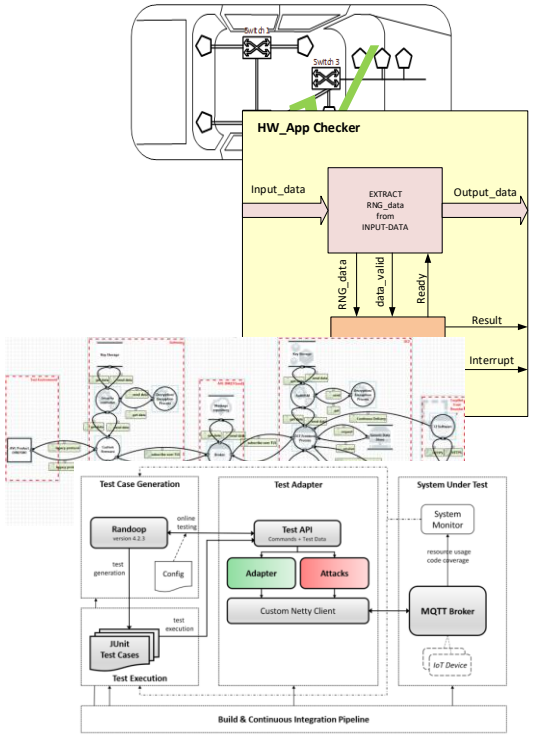

Recovery
Re-parametrization
Runtime enforcement
Redundancy
Restart
Replacement (hot/cold swap)
Agreement / voting
Rewiring / redirection
Relocation

IoT4CPS – Design Methods for Secure CPS



- **Application Level:**
  - Identifies, detects, and understands potential **security threats** in the foundation level of system models.
- **Platform Level:**
  - **Self-Healing by Structural Adaptation** which allows systems to leverage implicit redundancy to achieve resiliency to failures.
- **Network Level:**
  - **Recommender system** for development of dependable IoT systems, to select protocols and system configurations for complex CPS.
- **Physical Level:**
  - **Cryptographic library** for forward-secure key exchange mechanism.
  - Tools and methods such as **sensor security measures** for discovering faulty and hacked sensors.

IoT4CPS – Security Verification & Analysis



- **Human aspects**
  - Human aspects in automated model checking of security protocols, formal verification of human errors
- **Application Level**
  - Threat modelling
  - Automated Security Test Generation
  - Pentest catalogue
- **HW Level**
  - Side-channel protected hardware implementation
  - Dynamically Exchangeable Runtime Checkers in HW
  - Formal hardware property checks
- **Automotive Ethernet protection profile**

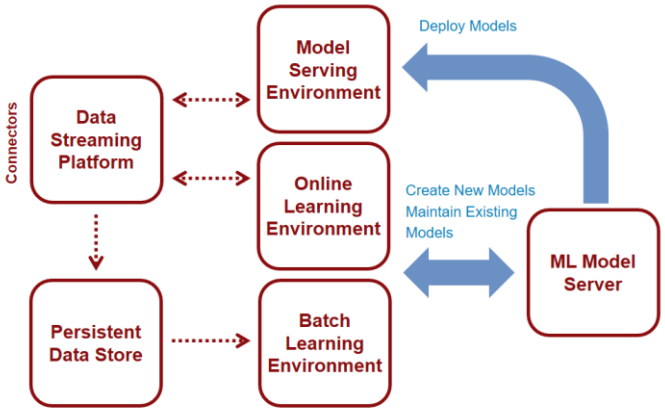
➔ **Analytical Toolbox for Anomaly Detection**

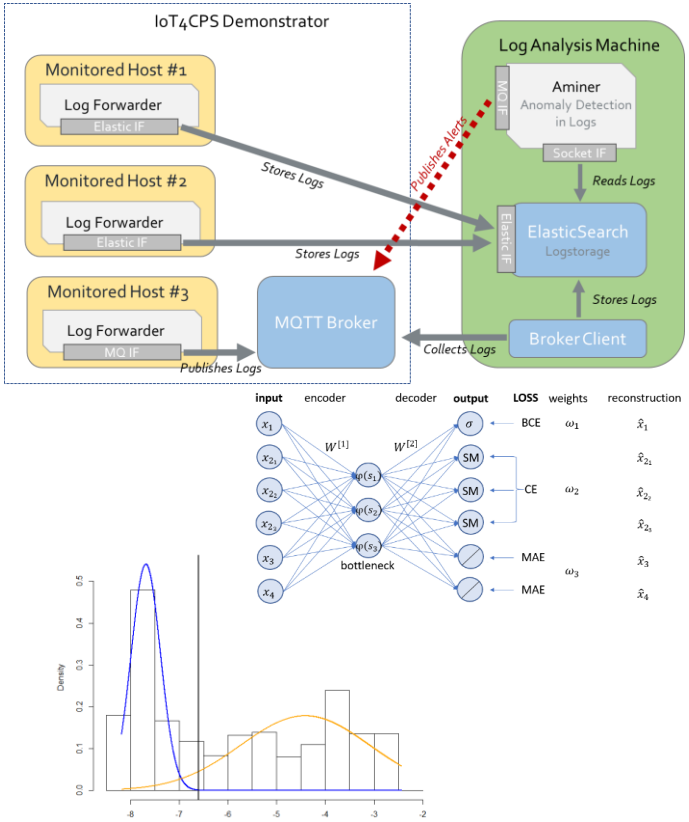
IoT4CPS – Analytical Toolbox

Anomaly detection for IoT at different level

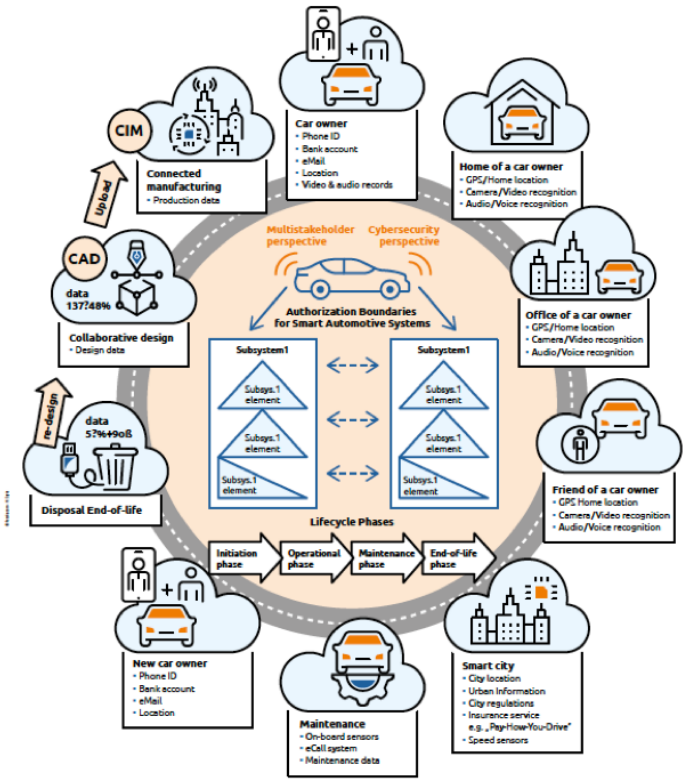
- Hardware level
- System logs analysis
- Network traffic analysis
- Anomaly detection models

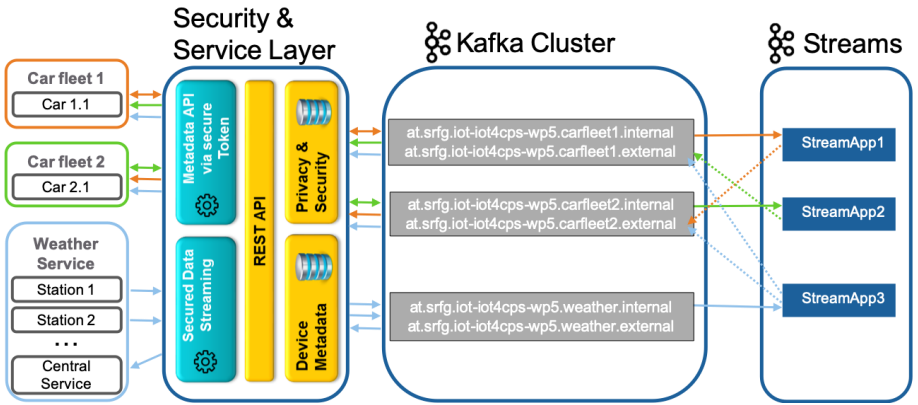
IoT4CPS Analytical Toolbox Architecture





Digital Twin-based traceability



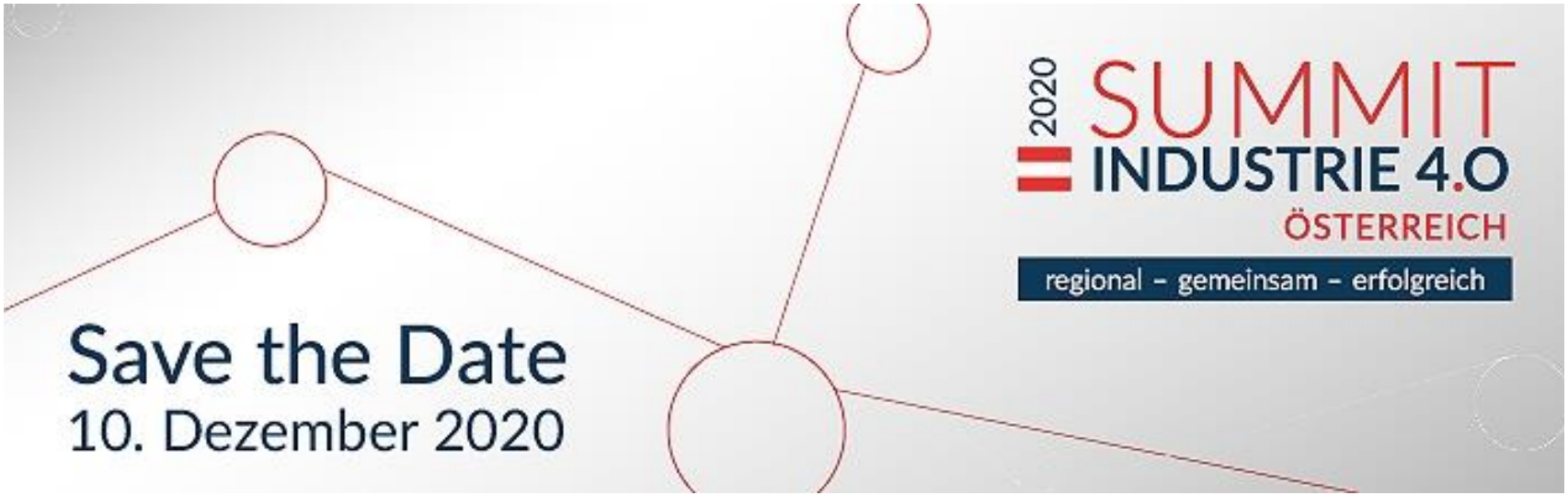


Further Challenges

- Resource limitations
  - How to extract/acquire and analyze a particular characteristics during run-time while considering the design and power constraints?
  - How to reduce the area and energy overhead of the data acquisition, i.e., power-ports, for runtime measurement and modeling?
- Real-time and scalability
  - How can we ensure coverage while maintaining timing behavior of the CPS?
- Interoperability and sharing
  - How can we cover devices which are shared between applications / networks?
- Interoperability and complexity
  - How to identify the reference communication behavior without any reference system?
  - How to model the communication behavior which can be used to identify the anomalous behavior?
  - How to model/identify the reference/golden behavior that covers the key characteristics and can be scalable?

Final Event

IoT4CPS Final Event in cooperation with Plattform Industrie 4.0



Register at: http://www.einladung.cc/industrie40/summit-industrie-40-2020

IoT4CPS
Trustworthy IoT for CPS

Thank you!

Contact:
Mario Drobics
AIT Austrian Institute of Technology
mario.drobics@ait.ac.at
+43 50 550-4810

More Info:
https://iot4cps.at/

FFG Forschung wirkt.

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Projectpartner

The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMK.

AIT Austrian Institute of Technology · TU Wien · Donau Universität Krems · Siemens · Nokia · scch software competence center hagenberg · X-NET · JKU Johannes Kepler Universität Linz · salzburgresearch · infineon · NXP · TTTech Auto · AVL · SBA Research · JOANNEUM RESEARCH · TU Graz