CyReV

Cyber Resilience for Vehicles

Cybersecurity for automotive systems in a changing environment

Behrooz Sangchoolie, RISE

Autosec FFI Conference, Stockholm

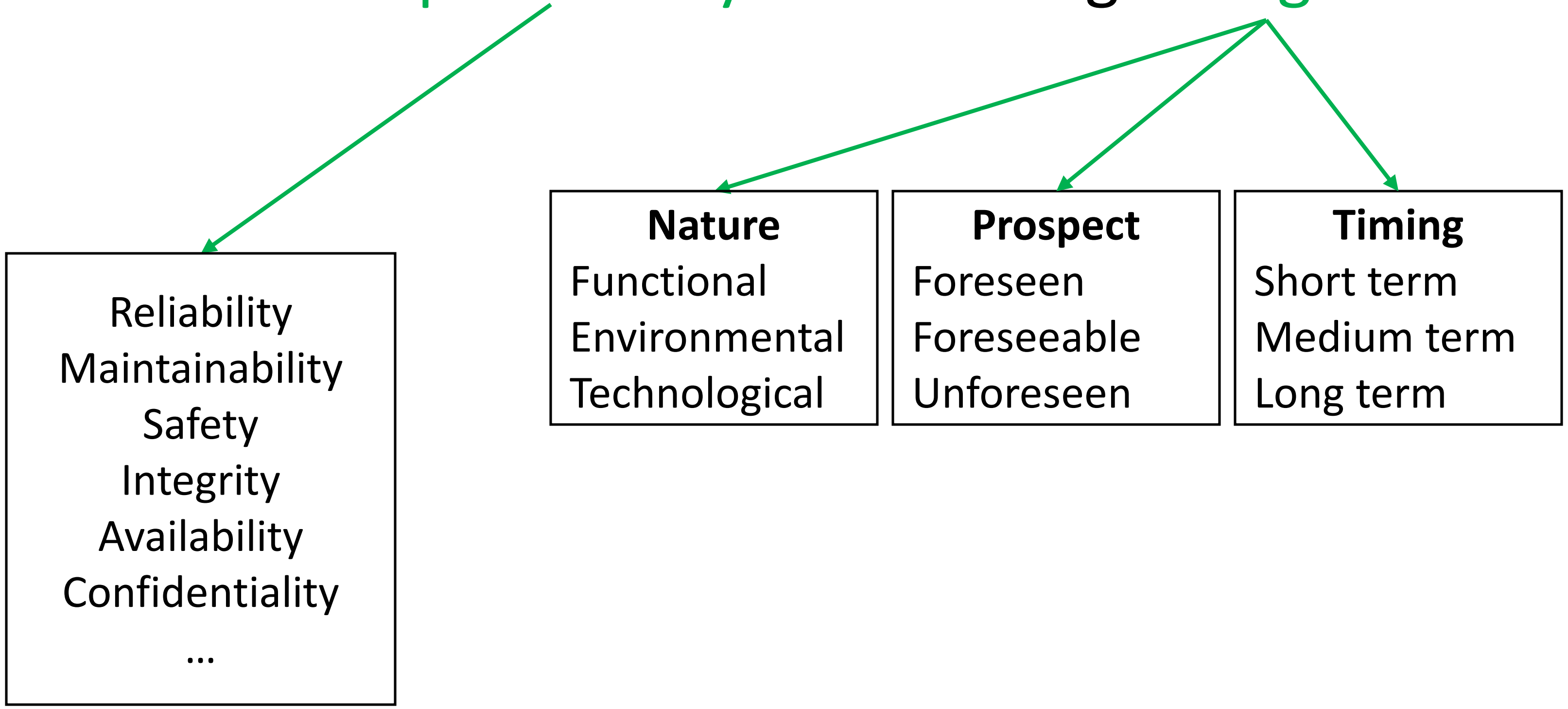
2019-10-10

VOLVO VOLVO VOLVO GROUP RISE ASSURED SECURITY CONSULTANTS CHALMERS COMBITECH VINNOVA FFI

CyReV Cyber Resilience for Vehicles

Resilience (Laprie 2008)

- Persistence of dependability when facing changes



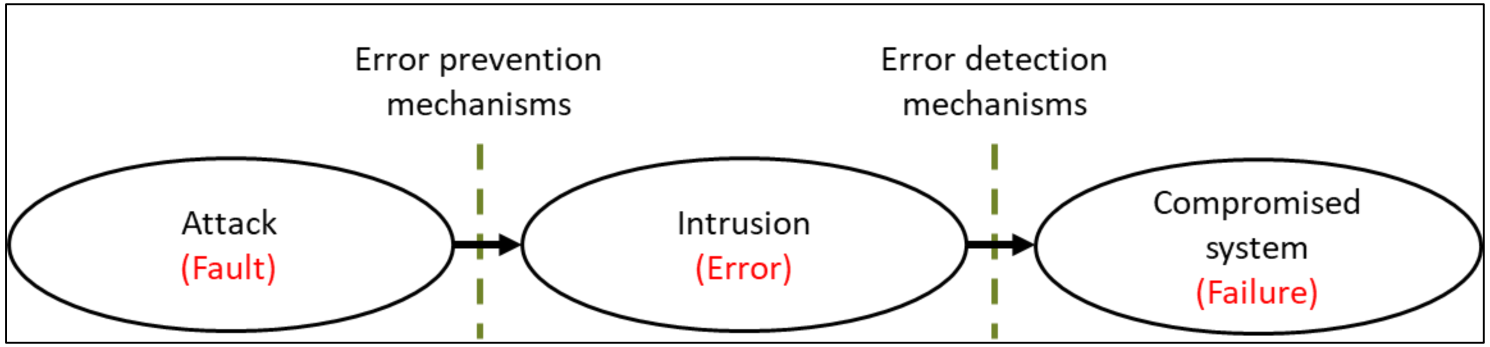
Reliability
Maintainability
Safety
Integrity
Availability
Confidentiality
…

Nature
Functional
Environmental
Technological

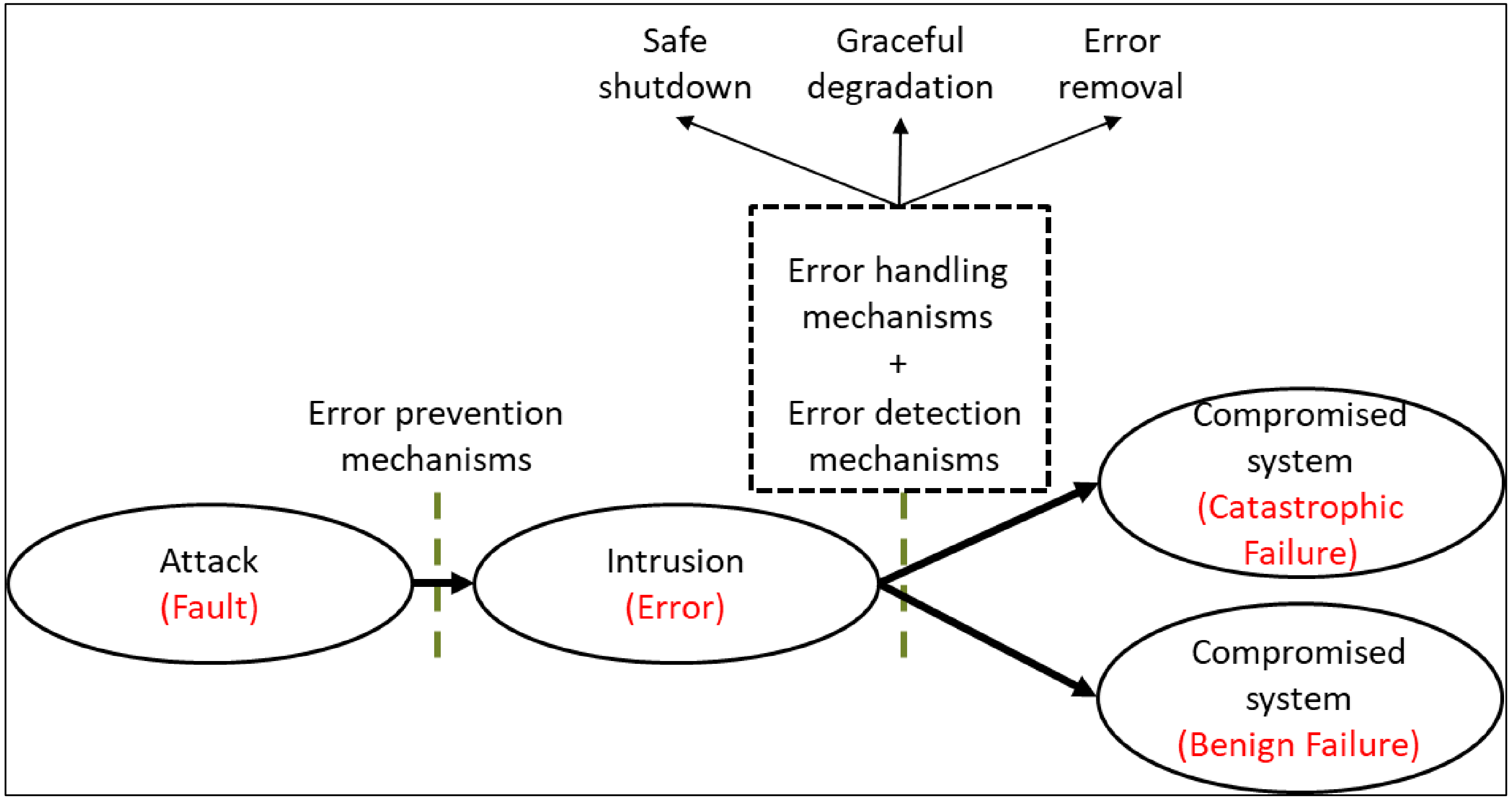
Prospect
Foreseen
Foreseeable
Unforeseen

Timing
Short term
Medium term
Long term

Threats to Dependability



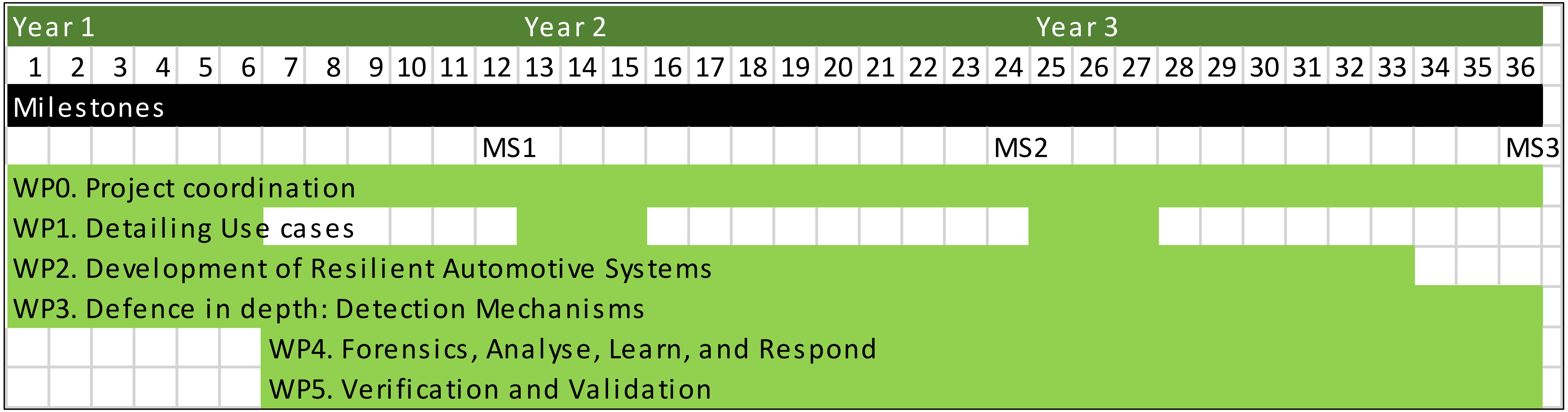
Threats to Dependability



Objectives and Expected Results

- Principles and techniques for resilient vehicle design and smart repair
- A reference architecture for resilient In-Vehicle Network (IVN)
- Several relevant use cases that are mapped to the IVN
- Mechanisms to detect security incidents
  - Cloud-based Intrusion Detection Mechanisms
  - In-vehicle intrusion detection
  - Hybrid intrusion detection
- Collaborative attack response
- Post attack forensics for post attacks investigations
- Design and implementation of evaluation methods that can be used to test and evaluate resilient IVN architectures.
- An interplay analysis between safety and security

WP Structure



	Year 1												Year 2												Year 3											
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
Milestones																																				
												MS1												MS2												MS3
WP0. Project coordination	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
WP1. Detailing Use cases	🟩	🟩	🟩	🟩	🟩	🟩							🟩	🟩	🟩										🟩	🟩	🟩									
WP2. Development of Resilient Automotive Systems	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩			
WP3. Defence in depth: Detection Mechanisms	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
WP4. Forensics, Analyse, Learn, and Respond							🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
WP5. Verification and Validation							🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Cyber Resilience for Vehicles

WP1. Detailing Use cases

- Study of major challenges and Identification of relevant use cases
  - Components for a vehicle architecture to detect and respond to cyber-attacks
  - Detection of anomalies in vehicular system behaviour
  - Pre and post data collection and data analysis
  - Interplay between safety and security and handling the conflicting requirements
  - Degrading the vehicle operation during an attack/incident
  - There is the need for degrading the operation during an attack/incident

Anomaly detection on the CAN bus	**Event and Log Management**
Honeypot	**Root cause analysis based on data collected from the system**
Defense in depth	**Attack path identification through source detection**
Detection of GNSS spoofing/jamming attacks	**Corrective and Recovery controls in case of breach**
Attack detection and protection on fleet-level	**…**

CyReV Cyber Resilience for Vehicles

WP2. Development of Resilient Automotive Systems

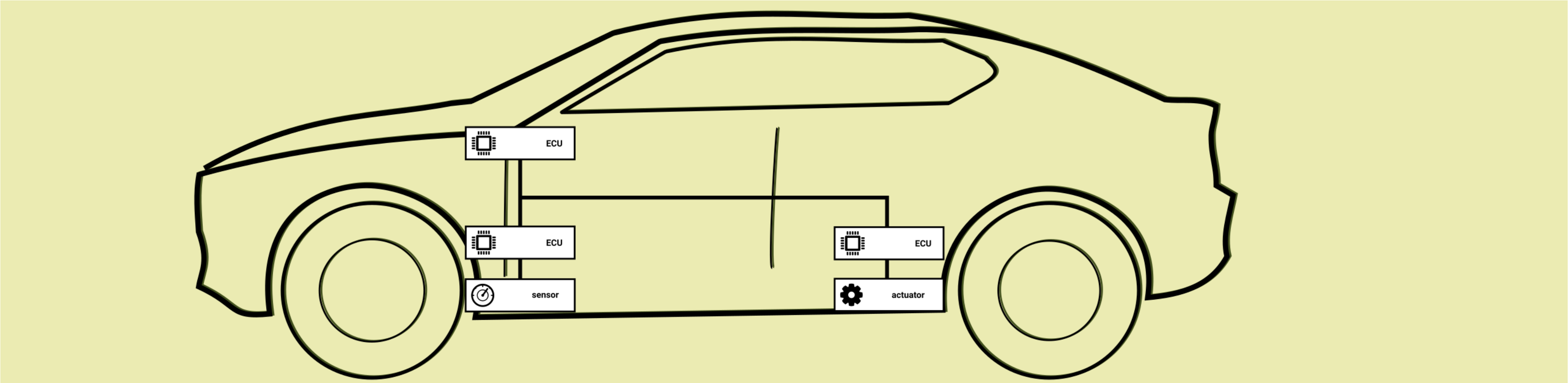
- Principles for Resilient Vehicles and smart repairs
  - Investigate how a resilient vehicle system can be built.
  - Identify components to be used to simulate security problems.
  - Investigate different levels of response

Raising an alarm that should later be checked by OEMs	**Enforcing stricter firewall/gateway rules**
Shutting down or disconnecting internal functions	**Limiting or disabling some subsystem functionality**
Disconnecting the vehicle from external communications or even initiating a complete shutdown	

- Reference architecture for Resilient Vehicles
  - Prevent, detect and respond to cyber-attacks while continuing to offer the intended service.
  - Investigate the components in which a reference architecture should contain.
- Performance of resilient vehicle design
  - Define metrics to evaluate the effectiveness of a resilient vehicle design.
    - Pros, cons, and performance implications

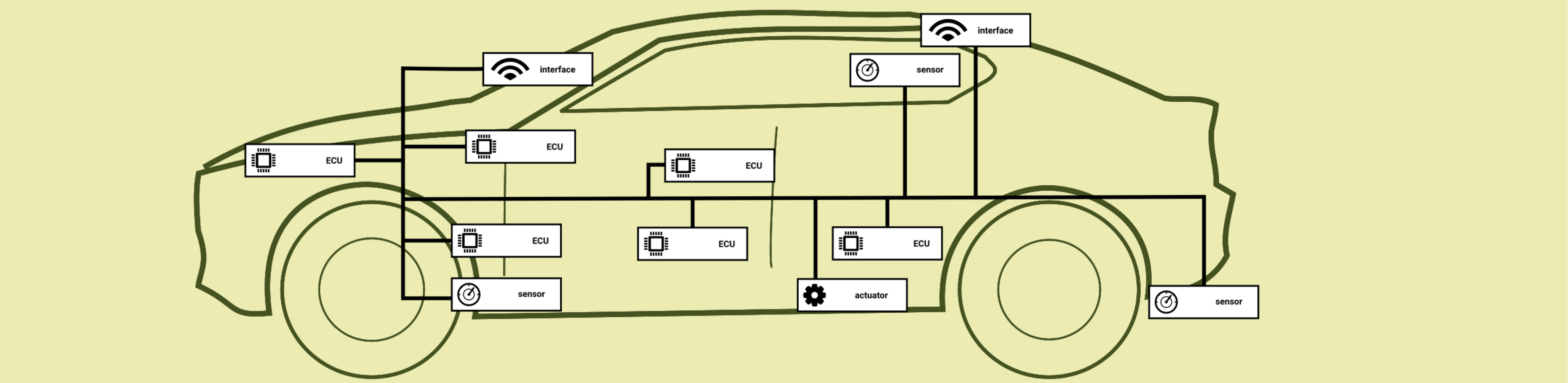
WP2. Development of Resilient Automotive Systems

- Vehicle Electronic Architecture
  - Past



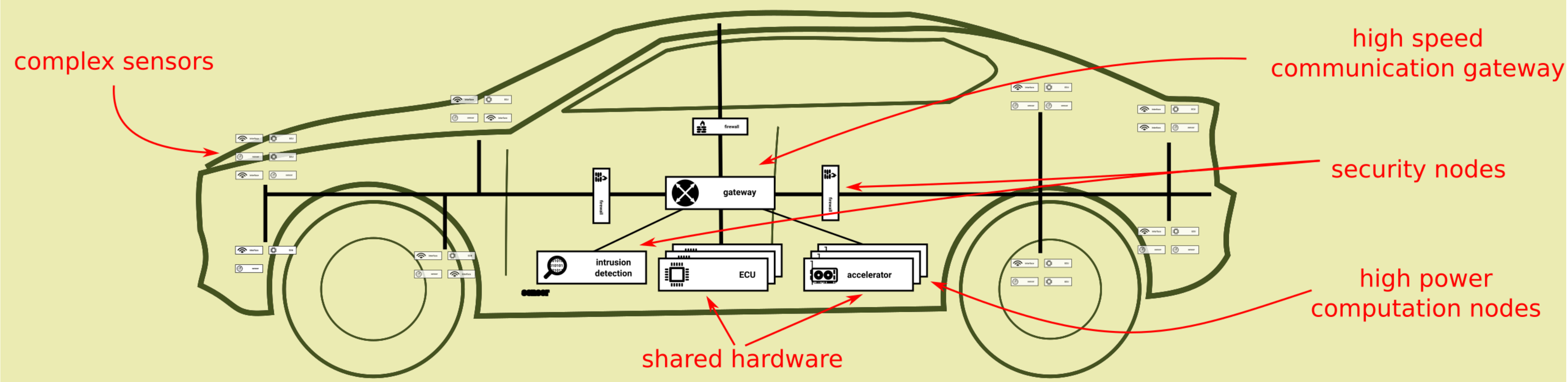
WP2. Development of Resilient Automotive Systems

- Vehicle Electronic Architecture
  - Present



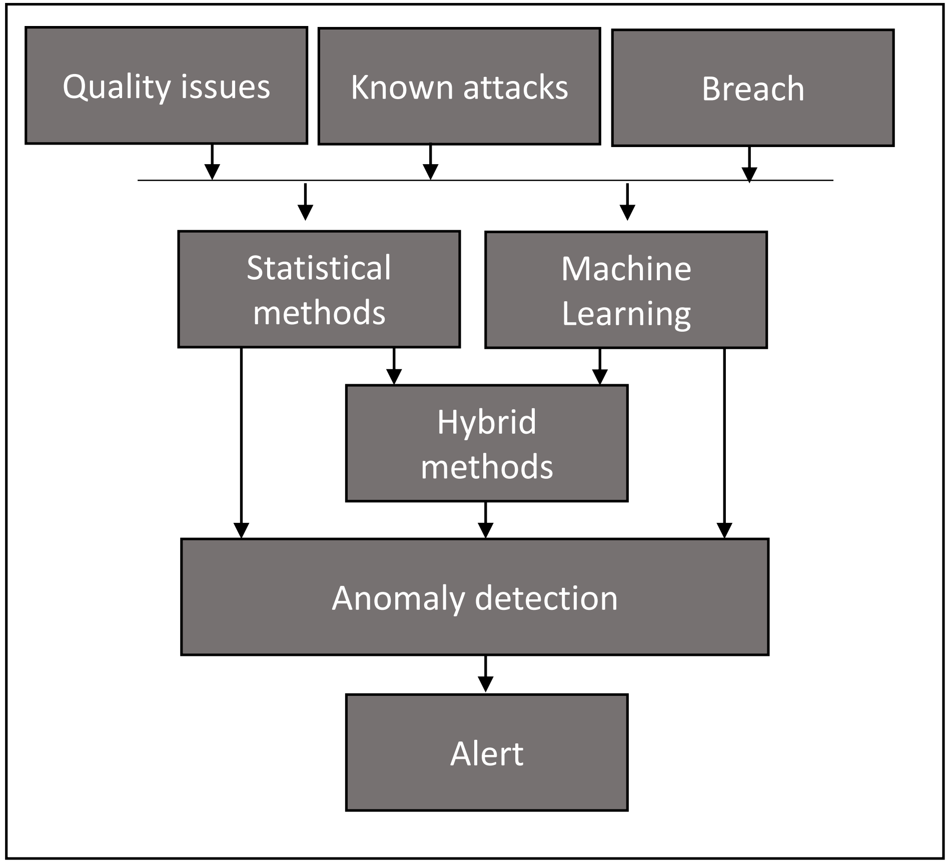
WP2. Development of Resilient Automotive Systems

- Vehicle Electronic Architecture
  - Future



WP3. Defence in depth: Detection Mechanisms

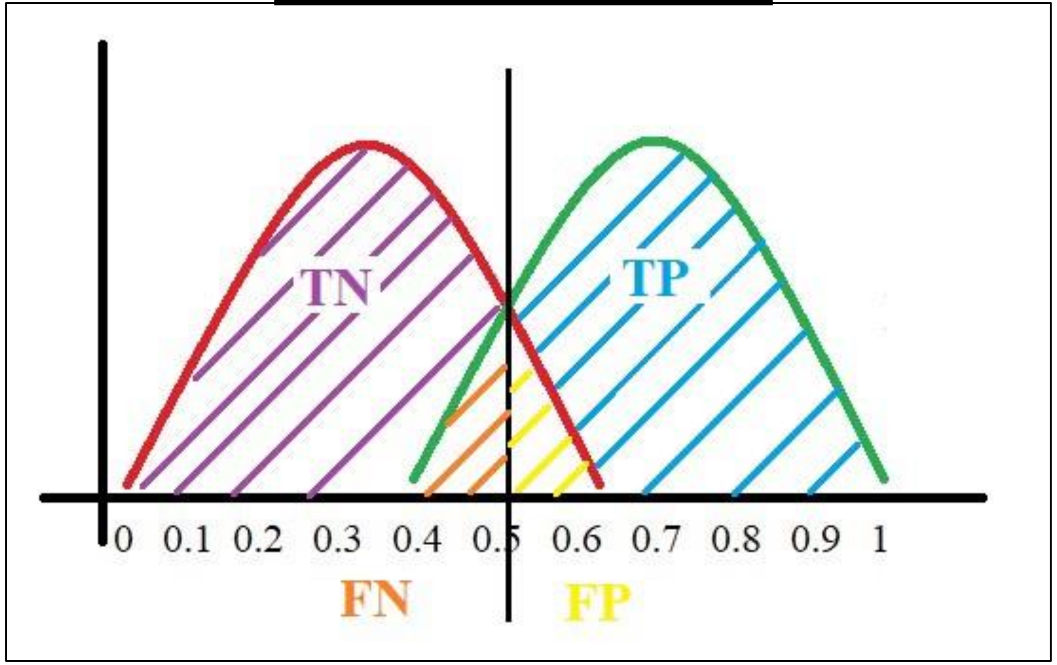
- Cloud-based Intrusion detection mechanisms
  - Challenge
  - Methodology
  - Results
  - Combining statistical and machine learning methods to detect intrusions in the cloud.



WP3. Defence in depth: Detection Mechanisms

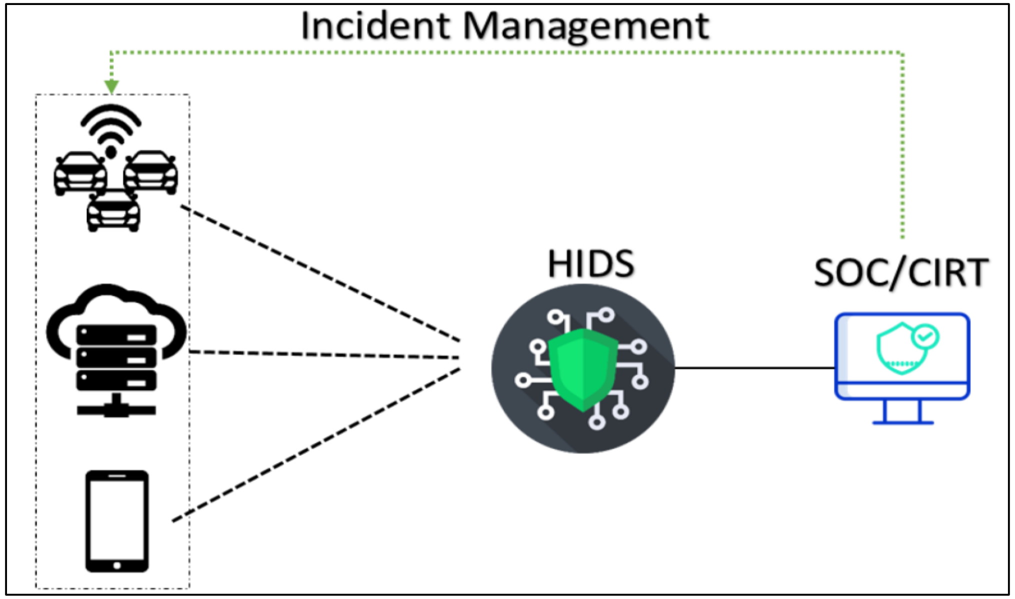
- In-vehicle intrusion detection
  - In-vehicle monitoring and detection mechanisms, investigate their effect on resilient architectures and quality of the generated event data.
  - Investigate different types of alarms that can be raised by an IDS.
  - Another important issue is the trustworthiness of the IDS and the event data in a partially compromised environment.

IDS alarms



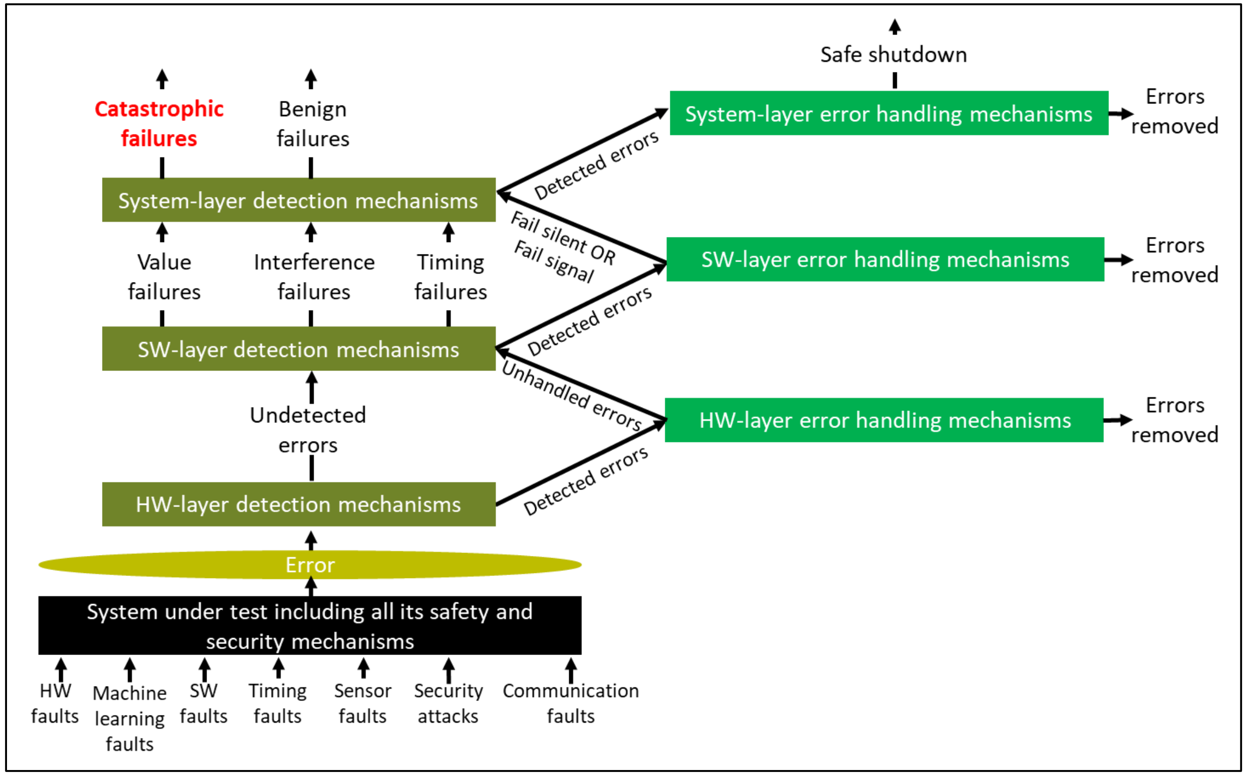
WP3. Defence in depth: Detection Mechanisms

- Hybrid intrusion detection
  - Propose a framework for developing Hybrid Intrusion Detection Systems (HIDS)
  - HIDS provides greater visibility into security events by
    - inspecting correlated information from multiple attack vectors; and
    - utilizing a combination of detection methods that collectively achieve higher detection accuracy.



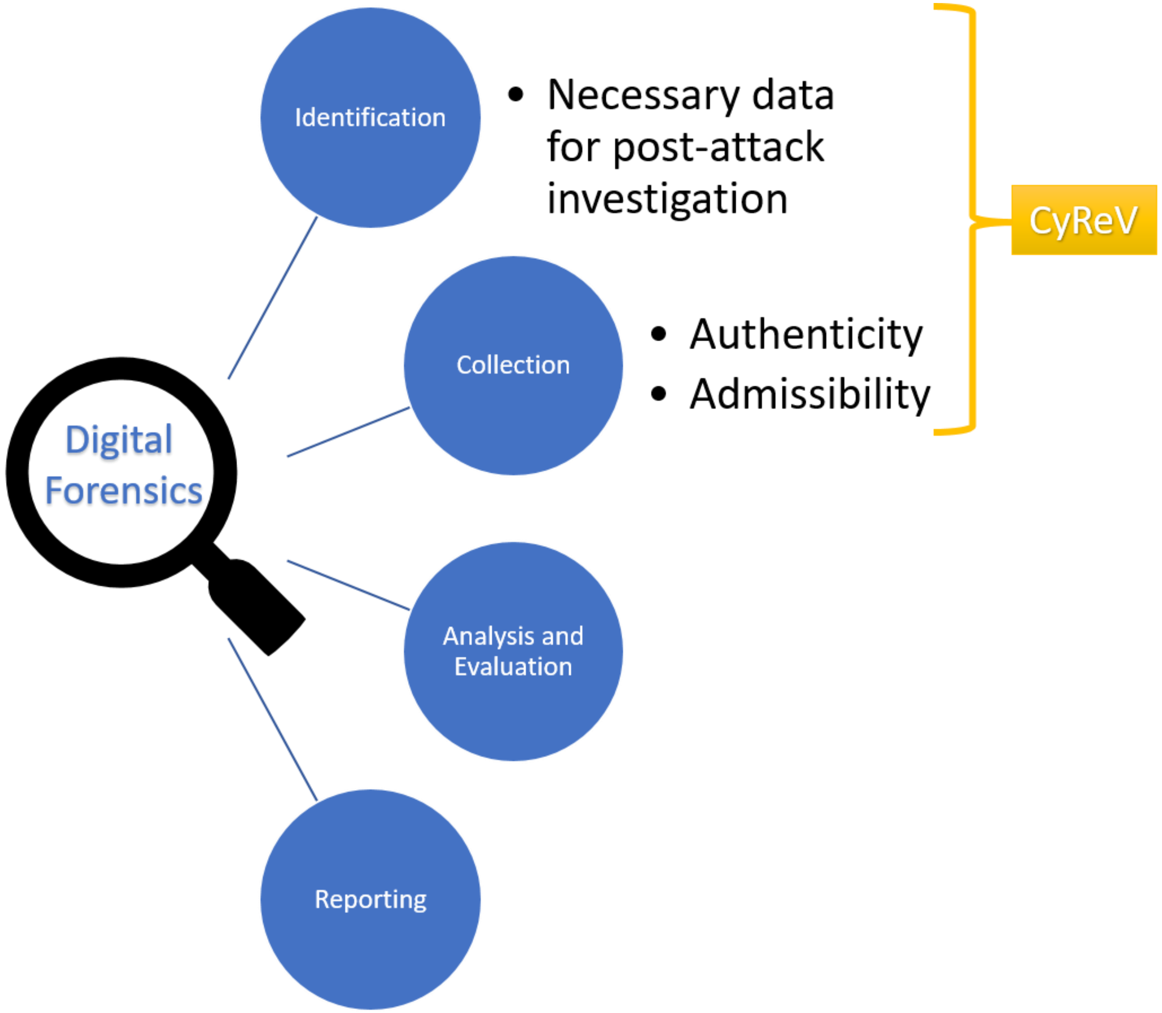
WP3. Defence in depth: Detection Mechanisms

- Interplay between error/intrusion detection/handling mechanisms
  - An analytical interplay analysis based on the layered resilience framework



WP4. Forensics, Analyse, Learn, and Respond

- Pre and post attack data collection for forensics
  - What data is necessary to save for future analysis and who is legally responsible to collect them?
  - How can authenticity of the collected electronic evidence be guaranteed?
  - How can the chain of custody be preserved?



- Necessary data for post-attack investigation
- Authenticity
- Admissibility

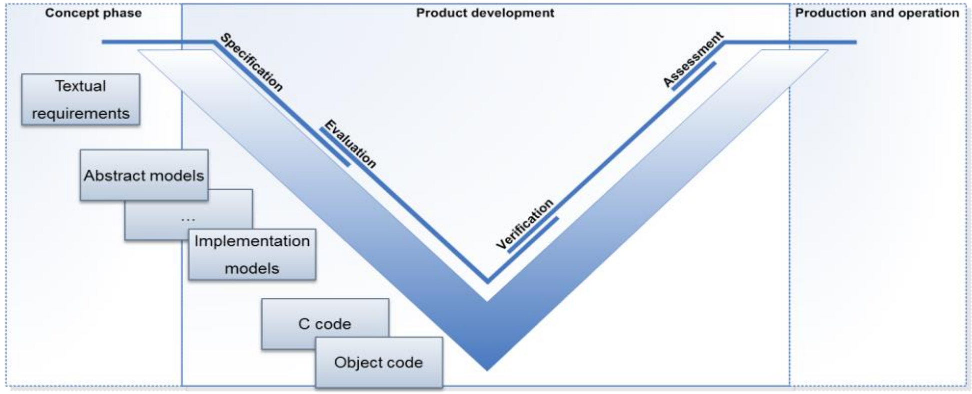
CyReV Cyber Resilience for Vehicles

WP4. Forensics, Analyse, Learn, and Respond

- On-line attack analysis
  - Monitor on-board SW
  - Understand attack root causes
- On-line collaborative attack response
  - Define safe response techniques
  - Share results of resilience strategy

WP5. Verification and Validation

- V&V of cyber resilient vehicles
  - Identify and list V&V strategies that are suitable for evaluating resilient vehicles.
  - Generic strategies as well as strategies aligned with ISO 26262, ISO/SAE 21434, ISO 21448.
- Proof of Value (PoV)
  - Implement proof of concepts by means of methods and tools to demonstrate the proposed architectural.
- Interplay between safety and security using experimental V&V methods
  - Conducting fault- and attack injection
  - Exploring multiple attack vectors by performing sequential attack injection campaigns.
  - Studying the use of pre-injection analyses.



CyReV Cyber Resilience for Vehicles

CYReV

Cyber Resilience for Vehicles

Thank you!

Q&A!

CYReV Cyber Resilience for Vehicles