automotive engineering iav

Incident Response for Vehicular Systems

More than online updates

Prof. Dr. Falk Langer, Lukas Stahlbock

esCar2020 - November 2020

Cyber security is like swimming with sharks

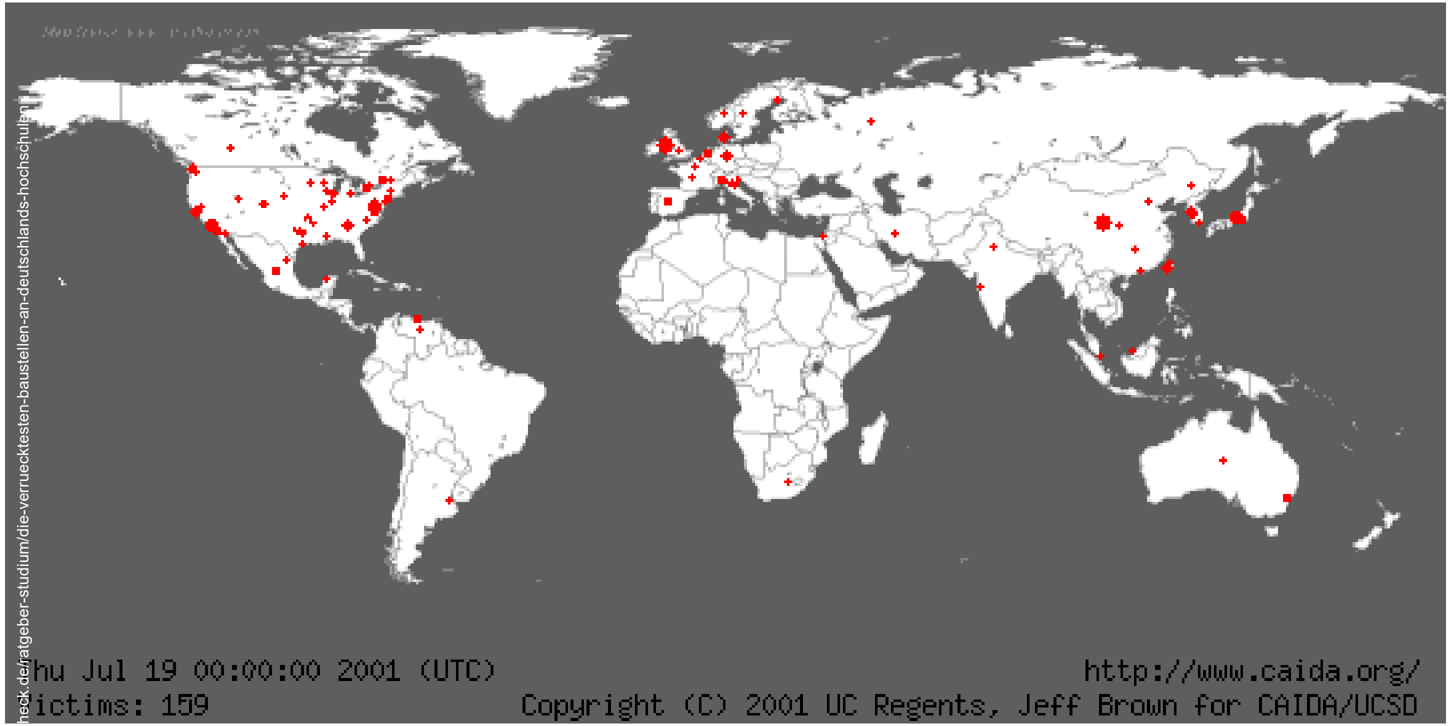
Quelle: https://www.infoworld.com/article/3385128/how-to-eliminate-the-security-risk-of-redundant-data.htm

If you are not wounded nothing happens

But one drop of blood and you will be attacked from everywhere

(Joshua Corman)

Cyber security and the risk of extensive spread


Thu Jul 19 00:00:00 2001 (UTC)
Victims: 159
http://www.caida.org/
Copyright (C) 2001 UC Regents, Jeff Brown for CAIDA/UCSD

heck.de/ratgeber-studium/die-verruecktesten-baustellen-an-deutschlands-hochschulen

Code-Red Worm (07/2001) Quelle: https://www.caida.org/research/security/code-red/

Code-Red Worm:

- **Started on Juli 19th 2001**
- **After 14 hours, 359,104 victims were compromised**

Wannacry:

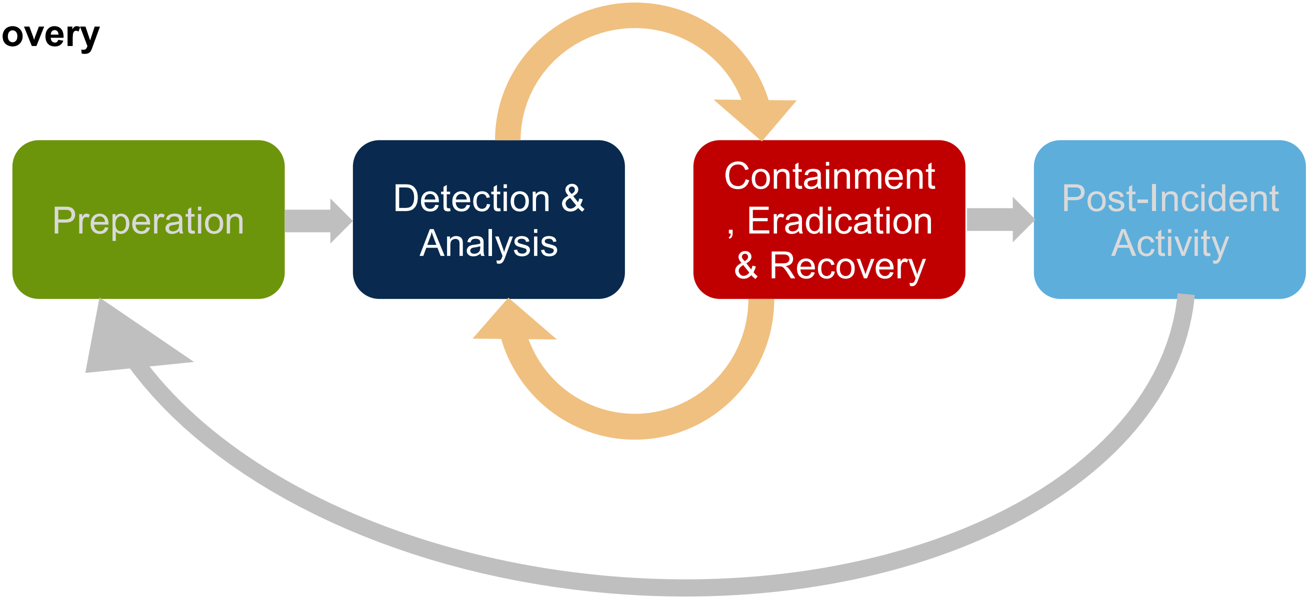
- **Started on May 12th 2017**
- **After 24 hours, 230,000 hosts were infected**

→ If you get attaked, things can go pretty fast

Incident response life cycle after NIST

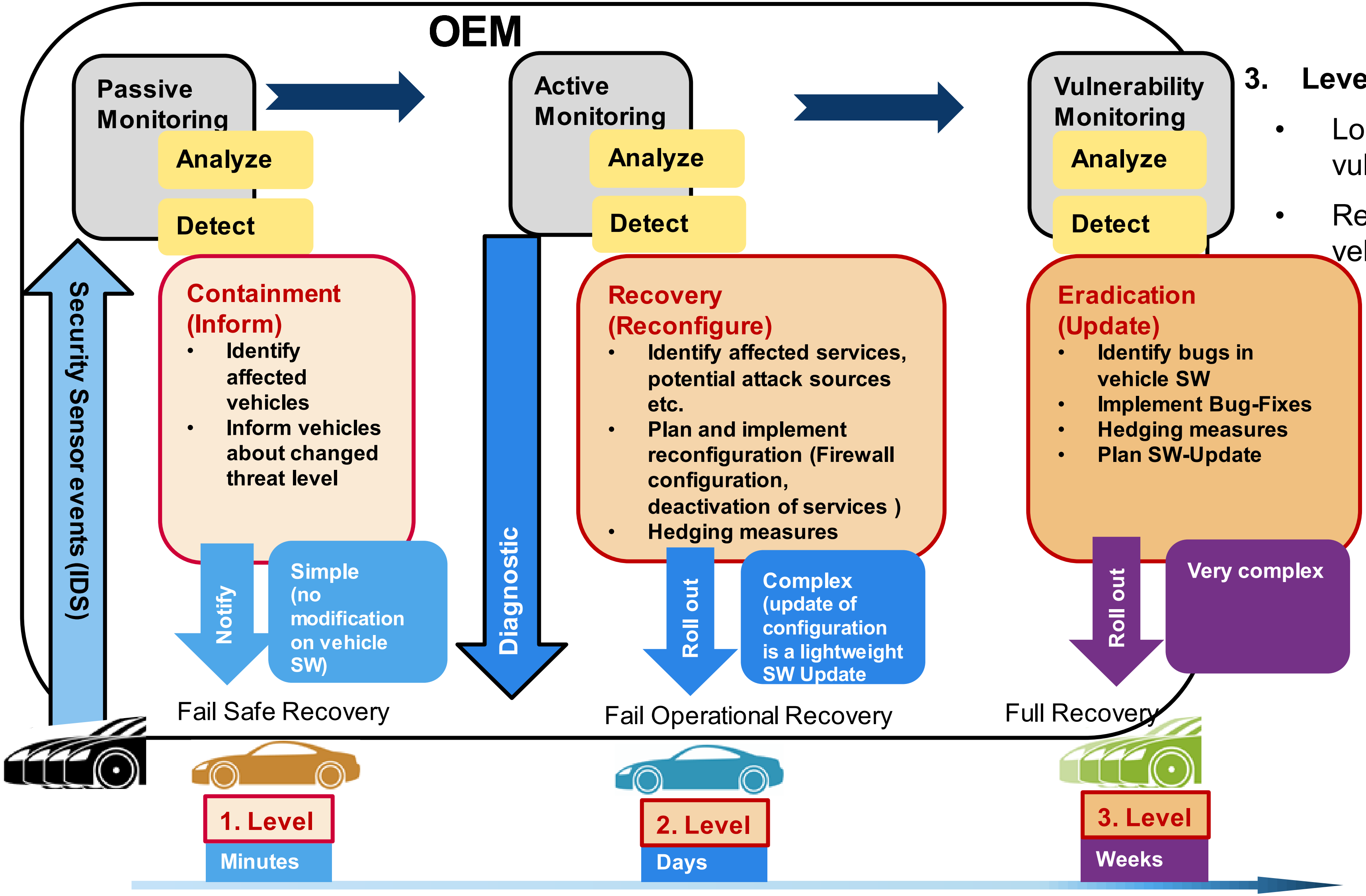
US National Institute of Standards and Technology defines within Computer Security Incident Handling Guide following steps:

1. Preparation
2. **Detection and Analyses**
3. **Containment, Eradication & Recovery**
4. Post-Incident Activity



US National Institute of Standards and Technology defines within Computer Security Incident Handling Guide (SP 800-61) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3. Level – Full Recovery – Online SW Update



OEM

Passive Monitoring

Analyze

Detect

Active Monitoring

Analyze

Detect

Vulnerability Monitoring

Analyze

Detect

Security Sensor events (IDS)

Containment (Inform)

- Identify affected vehicles
- Inform vehicles about changed threat level

Notify

Simple (no modification on vehicle SW)

Fail Safe Recovery

Diagnostic

Recovery (Reconfigure)

- Identify affected services, potential attack sources etc.
- Plan and implement reconfiguration (Firewall configuration, deactivation of services)
- Hedging measures

Roll out

Complex (update of configuration is a lightweight SW Update

Fail Operational Recovery

Eradication (Update)

- Identify bugs in vehicle SW
- Implement Bug-Fixes
- Hedging measures
- Plan SW-Update

Roll out

Very complex

Full Recovery

1. Level

Minutes

2. Level

Days

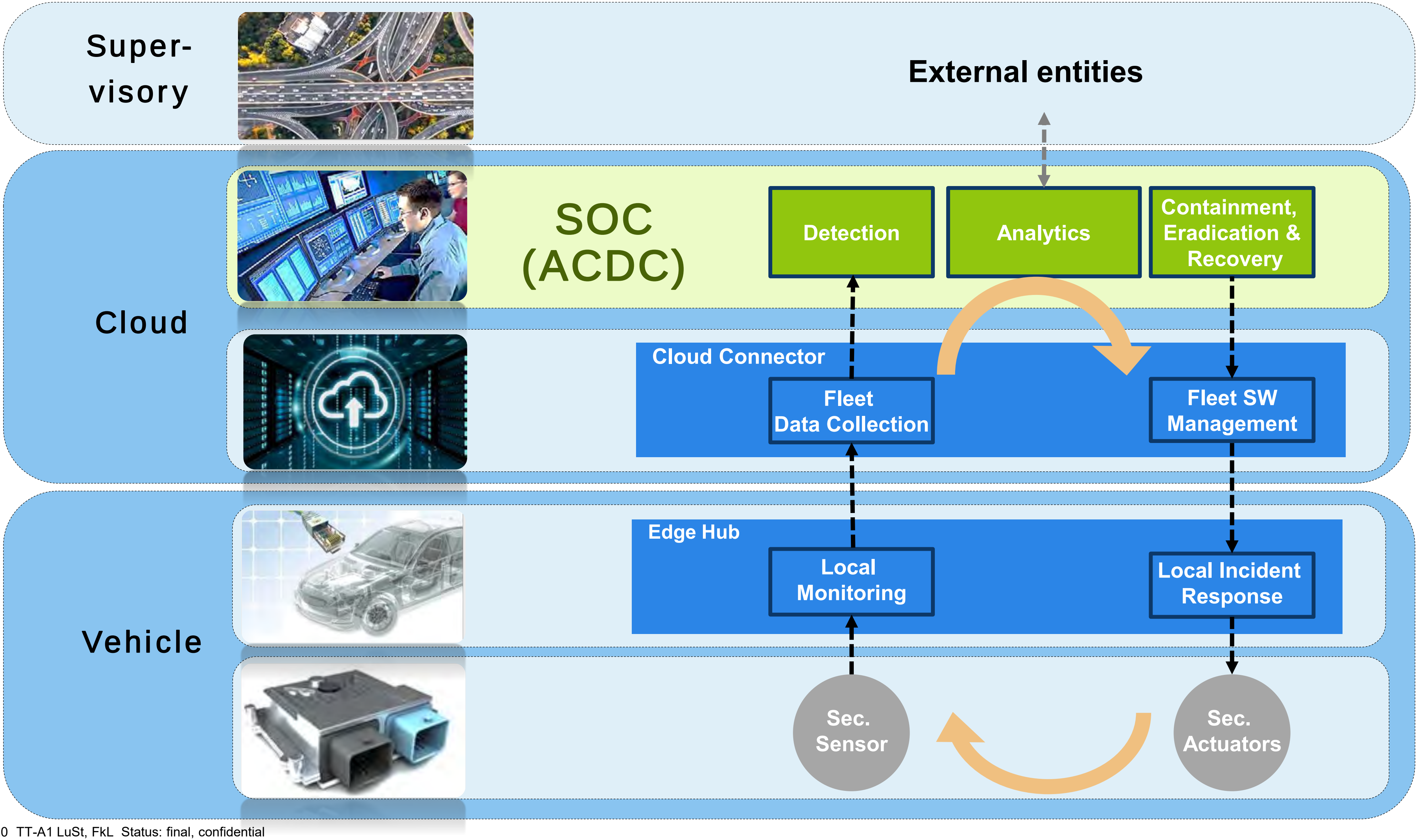
3. Level

Weeks

3. **Level of Response**

- Longterm process of vulnerability monitoring
- Results in update of vehicle software

Technical Stages ACDC



Super-visory

External entities

Cloud

SOC (ACDC)

Detection

Analytics

Containment, Eradication & Recovery

Cloud Connector

Fleet Data Collection

Fleet SW Management

Vehicle

Edge Hub

Local Monitoring

Local Incident Response

Sec. Sensor

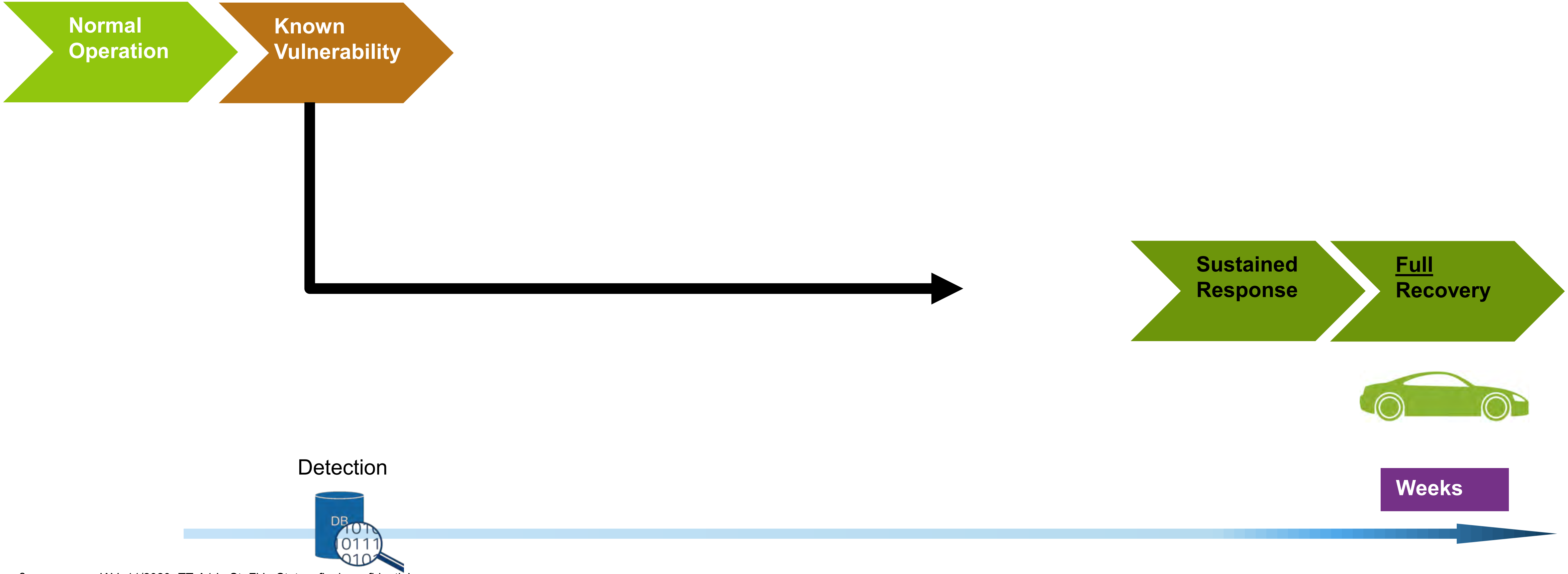
Sec. Actuators

Structure

- Who we are
- Introduction Incident Response for Vehicles
- **Response Stages for Safety-Critical Systems**
- Response in Detail
- Summary

Timeline Incident Response – The good case

- **Known Vulnerability triggers SW update that leads to full Recovery**



Normal Operation

Known Vulnerability

Sustained Response

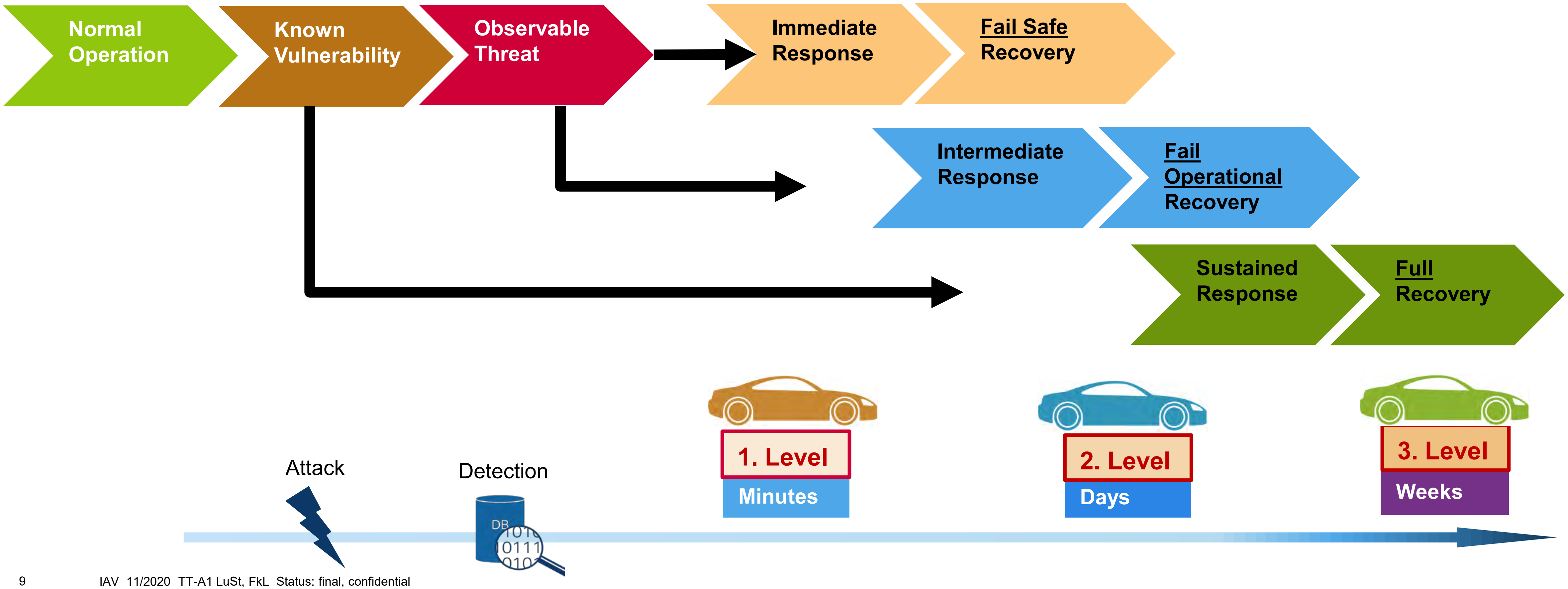
<u>Full</u> Recovery

Detection

Weeks

Timeline Incident Response with Respect Safety Critical Applications

- **Attacker often use uncovered vulnerabilitiesoften uncovered vulnerabilities**
- **Safe operation of vehicles must be ensured over time**
- **Observable Threat triggers Fail-Safe and Fail-Operational Recovery**



Normal Operation

Known Vulnerability

Observable Threat

Immediate Response

<u>Fail Safe</u> Recovery

Intermediate Response

<u>Fail Operational</u> Recovery

Sustained Response

<u>Full</u> Recovery

1. Level

Minutes

2. Level

Days

3. Level

Weeks

Attack

Detection

Phases of Incident Response for Safety Critical Applications (comp. to NIST)

Proposed Steps in Safety-Critical Automotive Applications

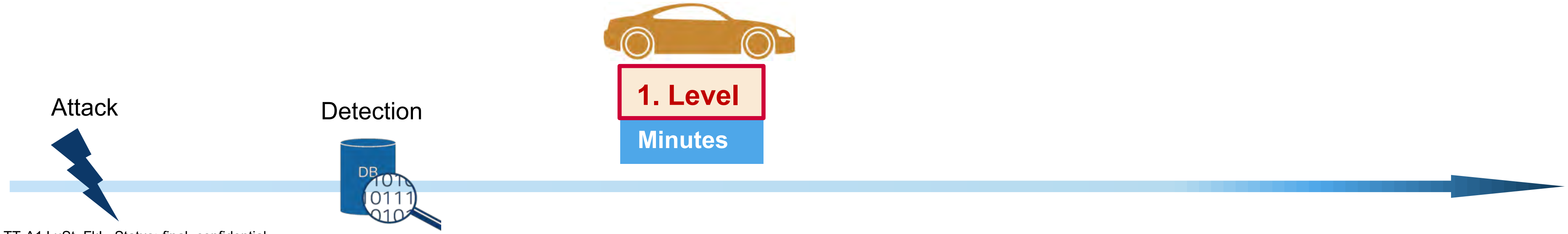
1. Preparation
2. **Detection and Analyses**
3. **Containment → Fail Safe Recovery**

Vehicles neednedeeds to be in a safe operation every time

- **Fail Safe means that operations need to be disabled if they are not secure**

Containment

→ Fail Safe Recovery



Phases of Incident Response for Safety Critical Applications (comp. to NIST)

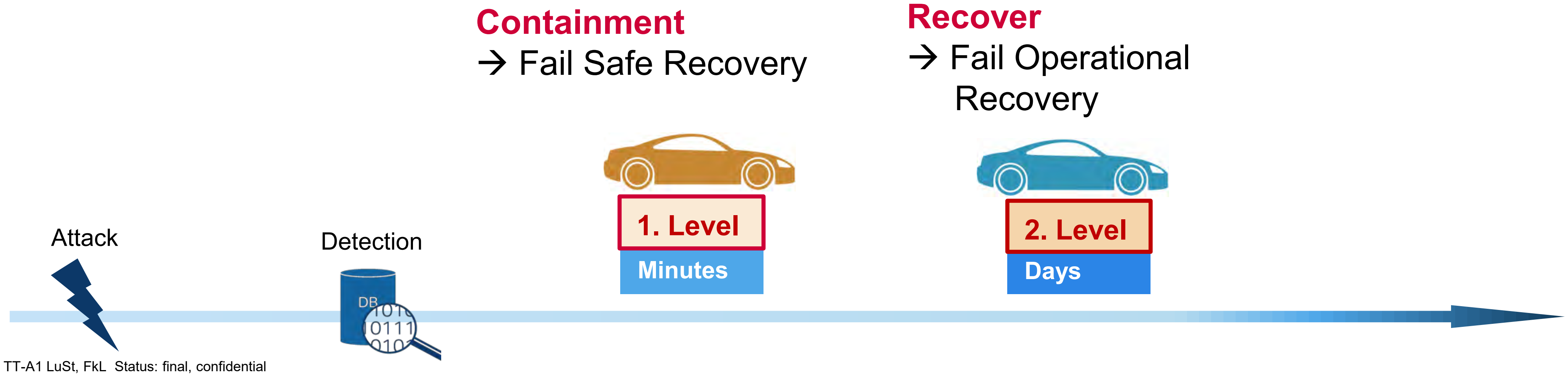
Proposed Steps in Safety-Critical Automotive Applications

1. Preparation
2. **Detection and Analyses**
3. **Containment → Fail Safe Recovery**

   Recovery → Fail Operational Recovery

Vehicles need needs to be in a safe operation every time

- **Fail Safe means that operations need to be disabled if they are not secure**
- **Fail operational means that provided functions must be recoveredrecoverd after an incident**



Containment
→ Fail Safe Recovery

Recover
→ Fail Operational Recovery

Phases of Incident Response for Safety Critical Applications (comp. to NIST)

Proposed Steps in Safety-Critical Automotive Applications

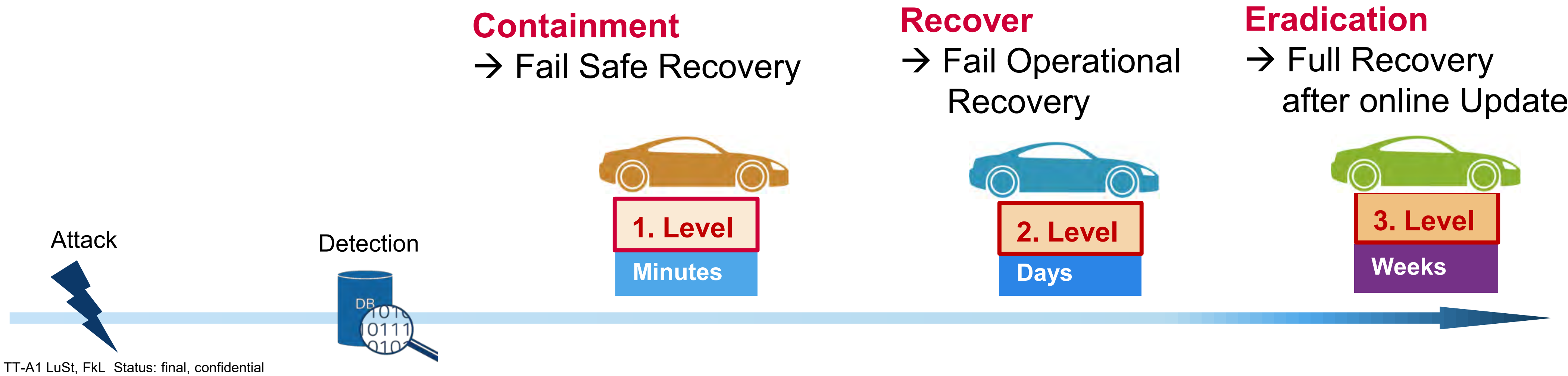
1. Preparation
2. **Detection and Analyses**
3. **Containment → Fail Safe Recovery**

   Recovery → Fail Operational Recovery

   Eradication → Full Recovery after online Update
4. Post-Incidence Activity

Vehicles need to be in a safe operation every time

- **Fail Safe means that operations need to be disabled if they are not secure**
- **Fail operational means that provided functions must be recovered after an incident**
- **Full recovery means that operations are working as usual again**

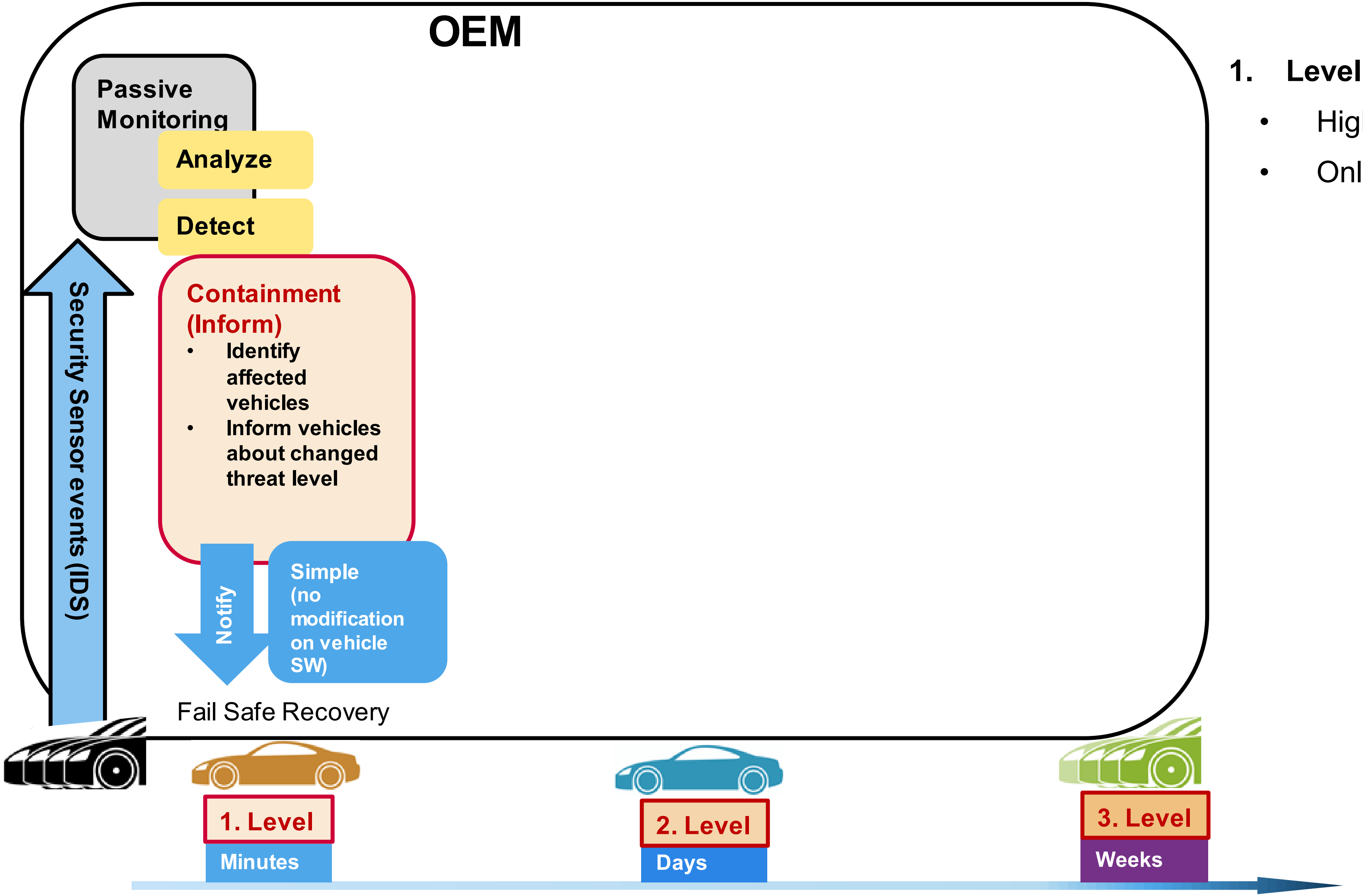


Containment
→ Fail Safe Recovery

Recover
→ Fail Operational Recovery

Eradication
→ Full Recovery after online Update

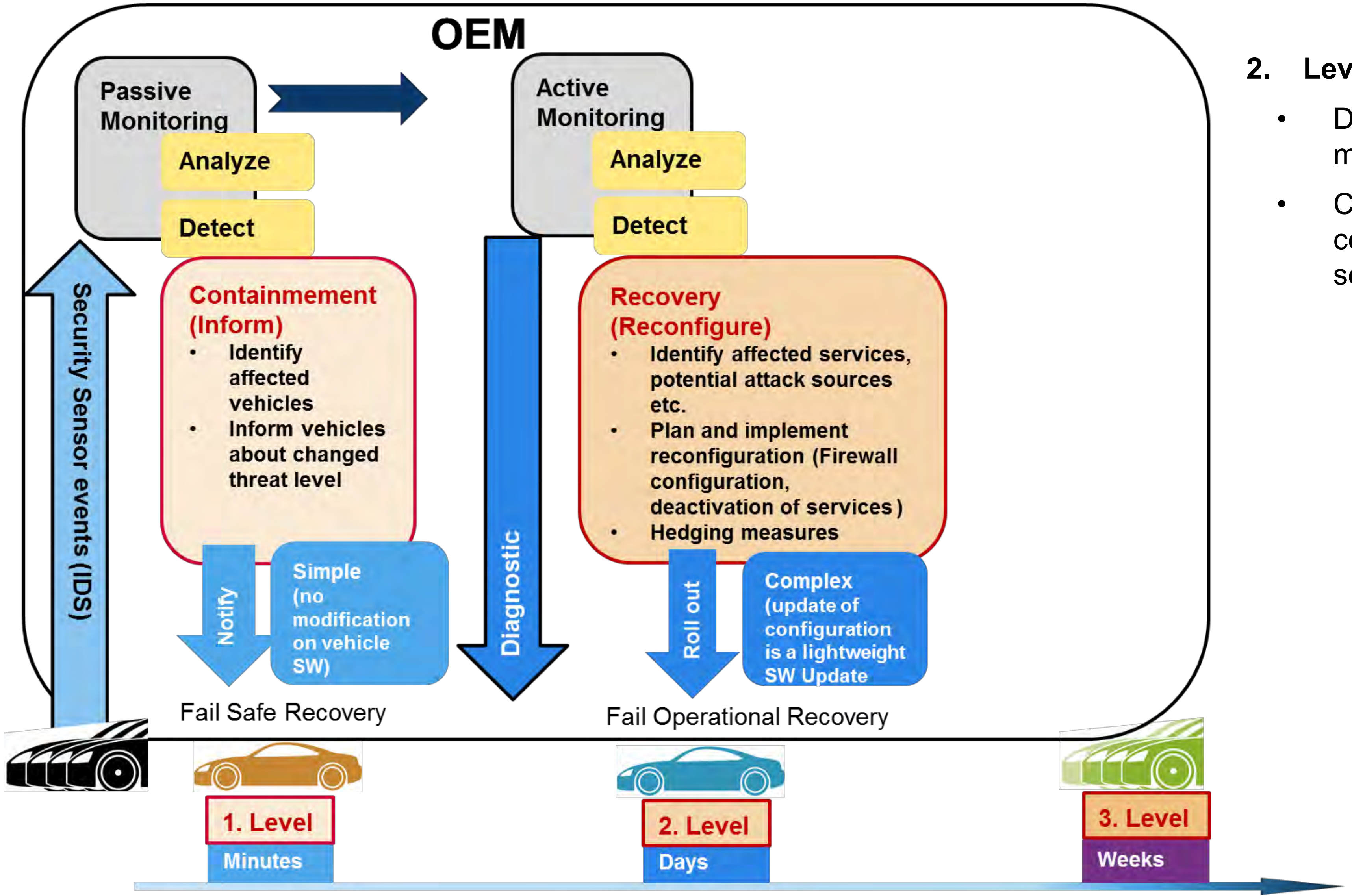
1. Level – Fail Safe Recovery



OEM
Passive Monitoring
Analyze
Detect
Security Sensor events (IDS)
Containment (Inform)
• Identify affected vehicles
• Inform vehicles about changed threat level
Notify
Simple (no modification on vehicle SW)
Fail Safe Recovery
1. Level
Minutes
2. Level
Days
3. Level
Weeks

1. **Level of Response**
   - Highly automated
   - Only notification to vehicle

2. Level – Fail Operational Recovery


OEM
Passive Monitoring
Analyze
Detect
Active Monitoring
Analyze
Detect
Security Sensor events (IDS)
Containmement (Inform)
• Identify affected vehicles
• Inform vehicles about changed threat level
Diagnostic
Recovery (Reconfigure)
• Identify affected services, potential attack sources etc.
• Plan and implement reconfiguration (Firewall configuration, deactivation of services)
• Hedging measures
Notify
Simple (no modification on vehicle SW)
Roll out
Complex (update of configuration is a lightweight SW Update
Fail Safe Recovery
Fail Operational Recovery
1. Level
Minutes
2. Level
Days
3. Level
Weeks

2. **Level of Response**
   - Deep inspection (active monitoring of vehicles)
   - Changes in configuration of vehicle software

Structure

- Who we are
- Introduction Incident Response for Vehicles
- Response Stages for Safety-Critical Systems
- Response in Detail
- Summary

Jeep Hack 2015

https://twitter.com/kaspersky/status/624291836996284418/photo/1

First hack:

- WiFi passwords generated based on production time
- Limited control of IVI system (e.g. changing radio station or volume)

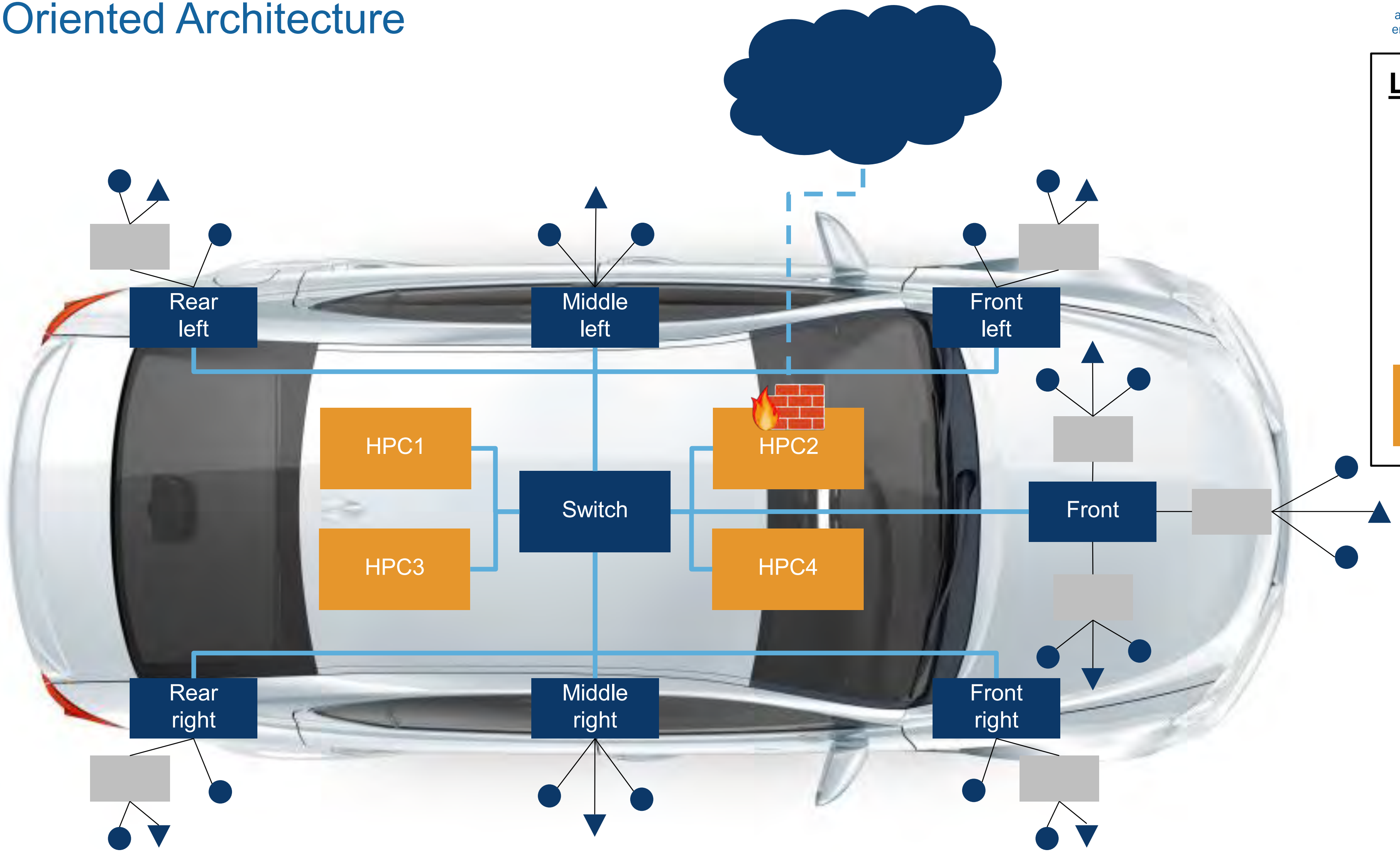
Second hack:

- Vulnerability: open port 6667 for D-Bus services with authentication as anonymous enabled
- Using a femtocell to gain full control of linux based IVI system
- IVI system to flash an controller connected to CAN bus
- Manipulate CAN messages to control steering wheel, engine, …

http://illmatics.com/Remote%20Car%20Hacking.pdf

→ **Fiat Chrysler had to recall 1.4 million vehicles**

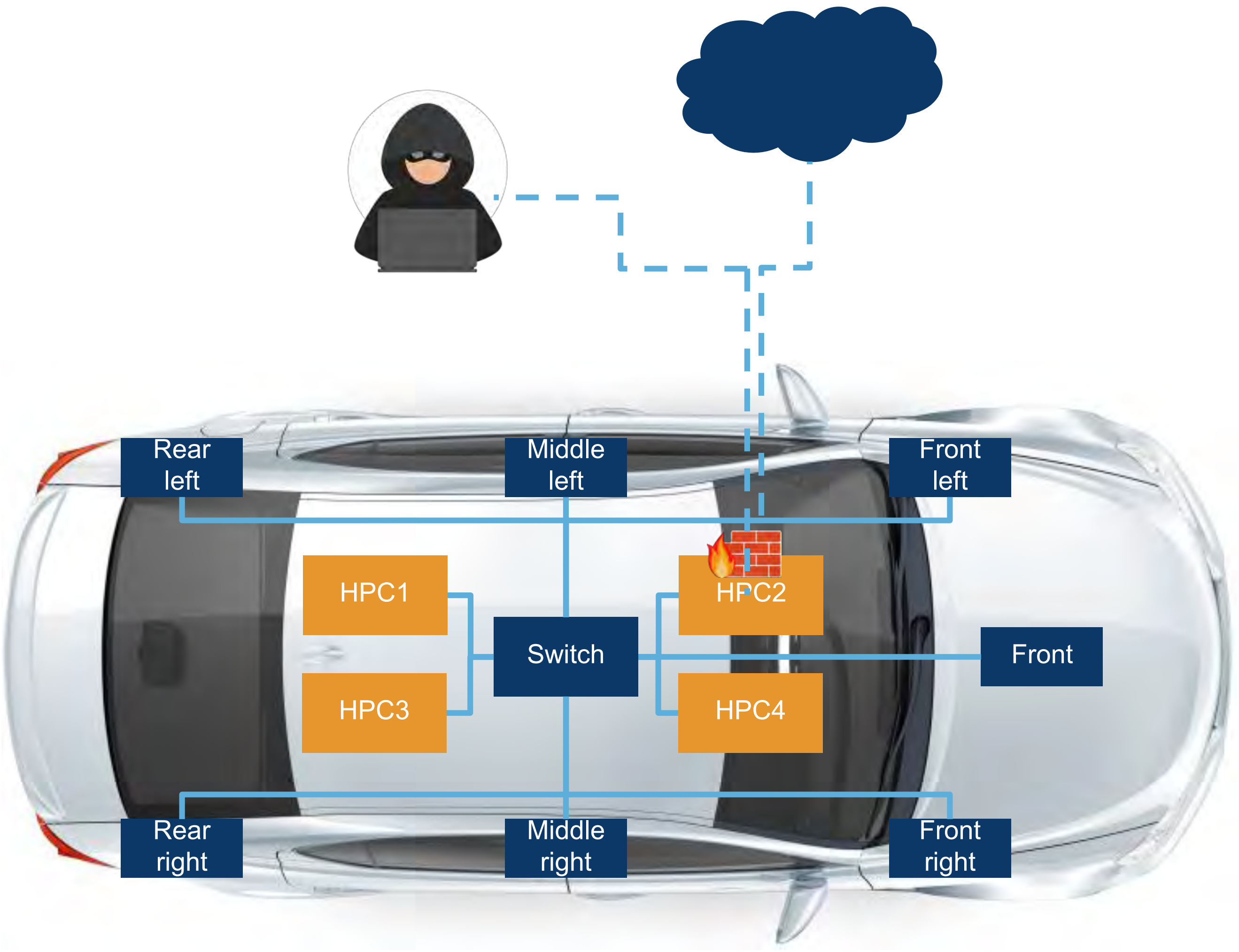
Zone-Oriented Architecture



Legend

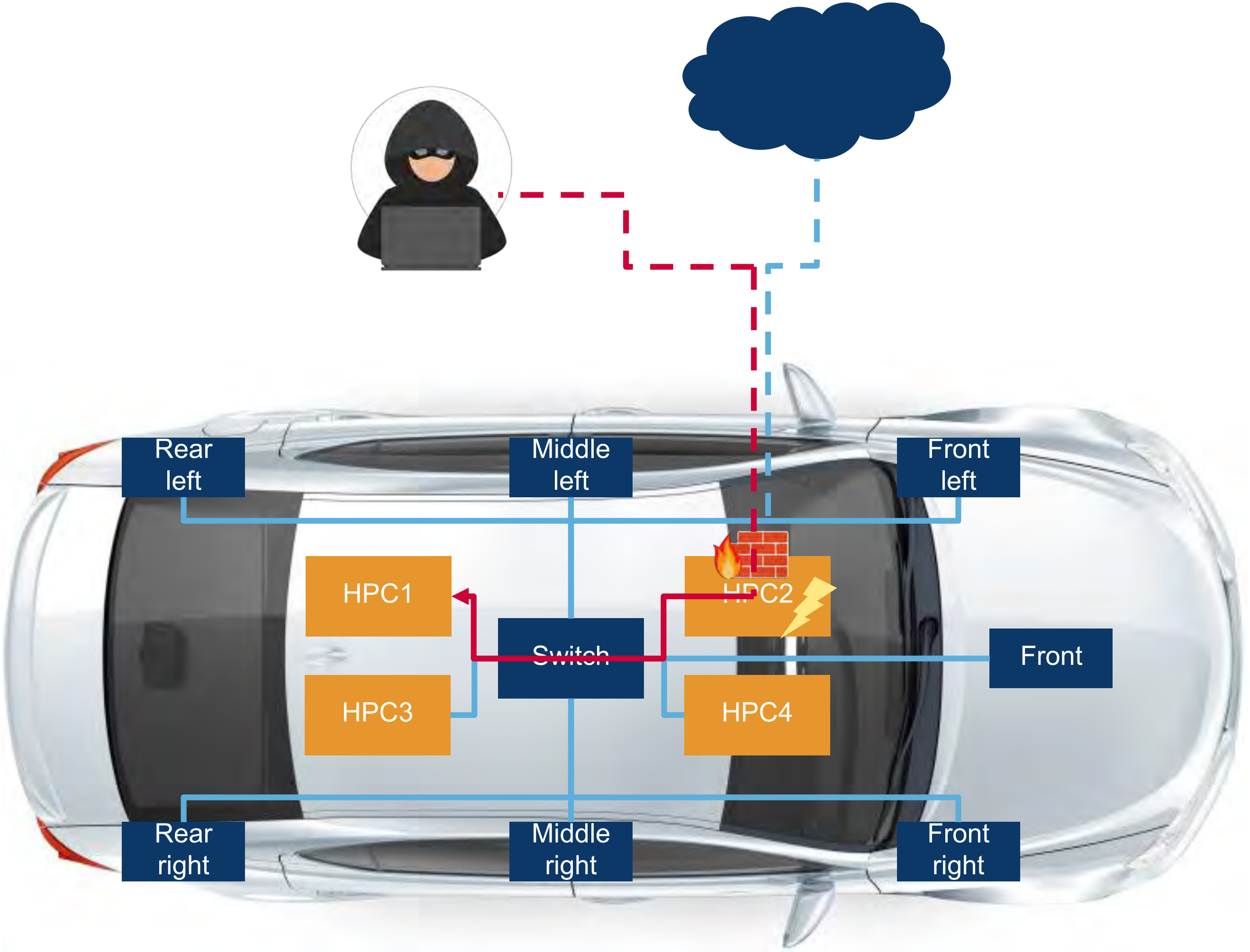
- ● Sensor
- ▲ Actuator
- ECU
- Zone Controller
- High Performance Controller

Fail Safe Recovery



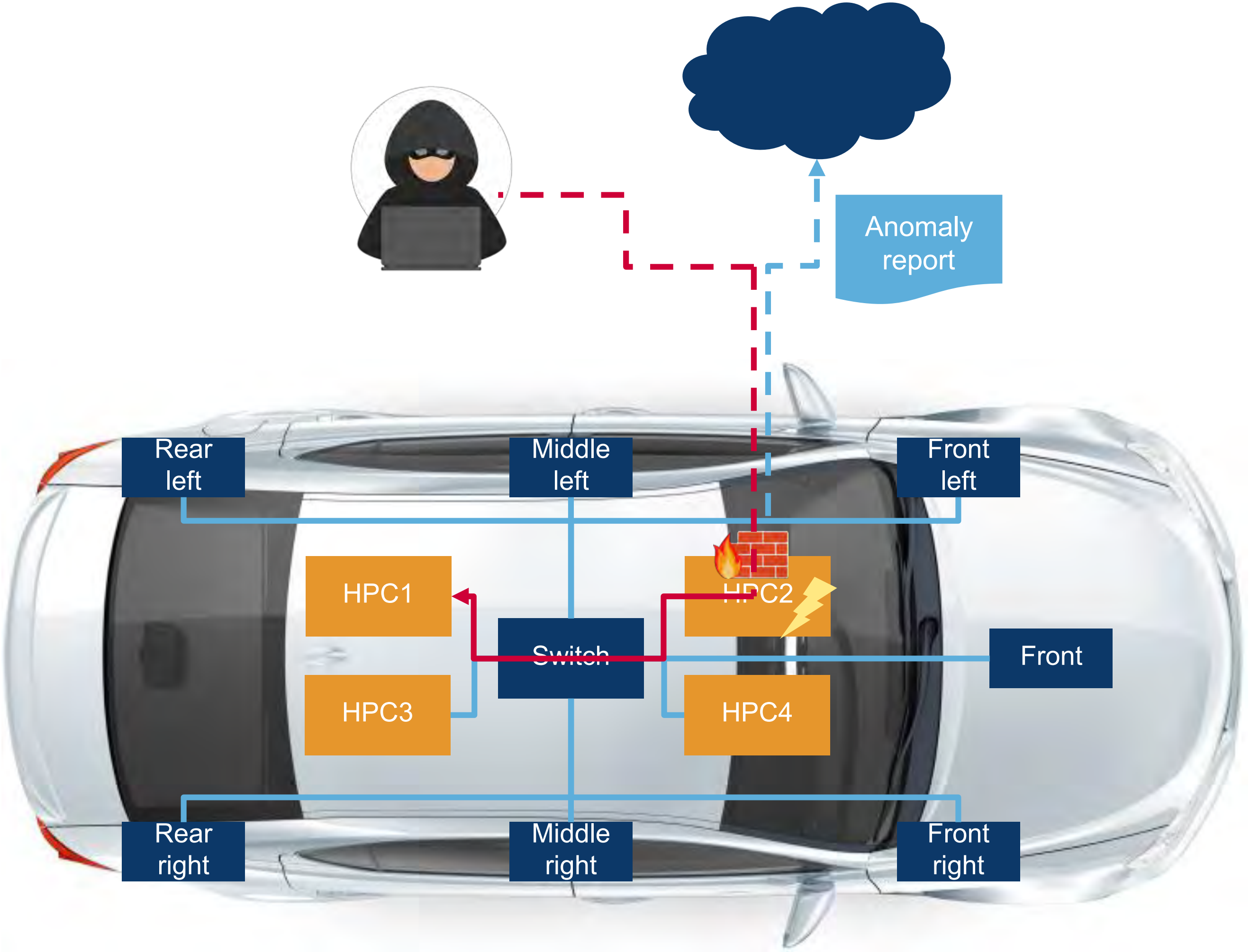
- **Attacker gained access via open port for D-Bus service without authentication**

Fail Safe Recovery



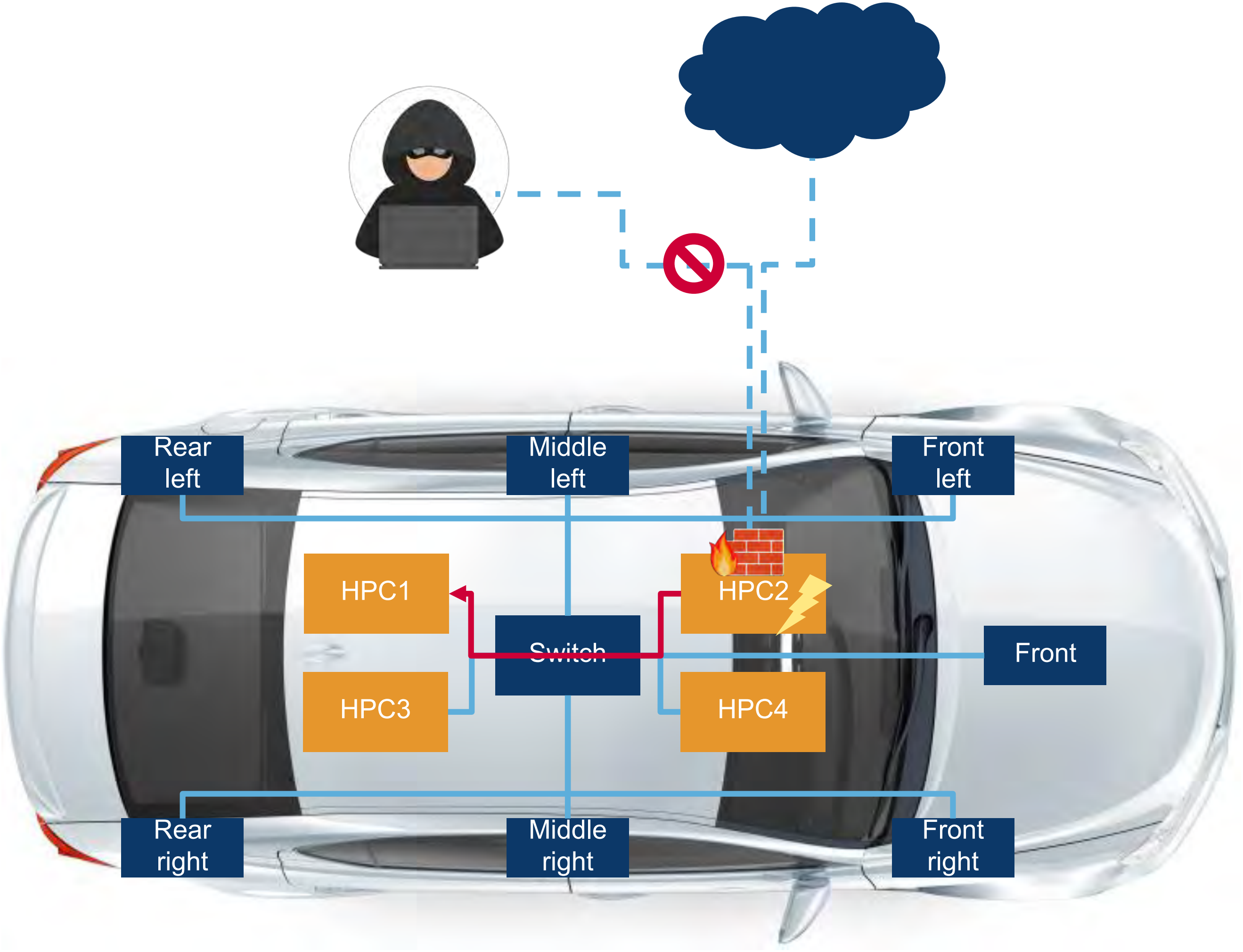
- Attacker gained access via open port for D-Bus service without authentication
- Attacker manipulates in-vehicle communication

Fail Safe Recovery



- Attacker gained access via open port for D-Bus service without authentication
- Attacker manipulates in-vehicle communication
- Anomaly detection notices manipulated network flows
- Anomaly gets reported to ACDC

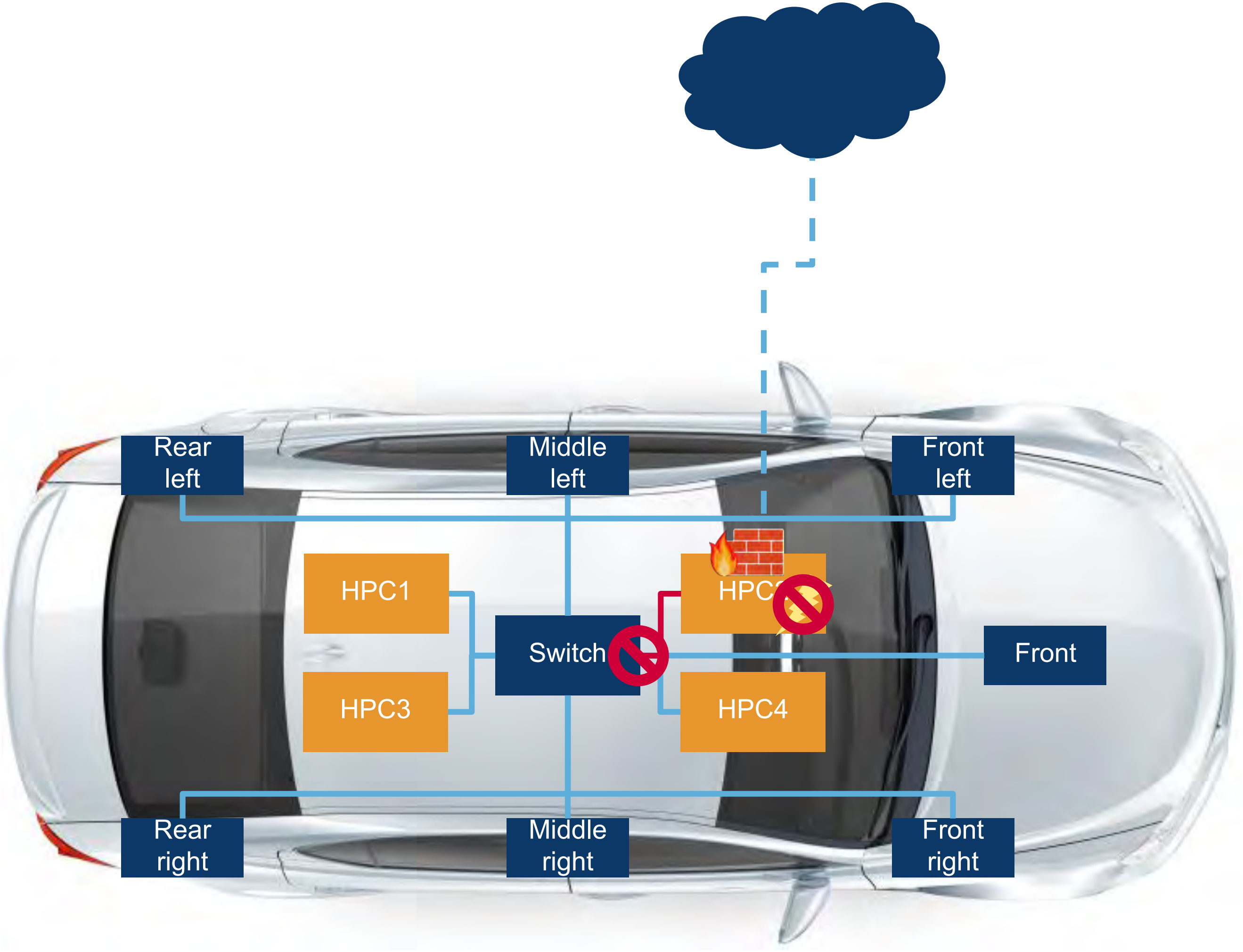
Fail Safe Recovery



- Attacker gained access via open port for D-Bus service without authentication
- Attacker manipulates in-vehicle communication
- Anomaly detection notices manipulated network flows
- Anomaly gets reported to ACDC
- Anomaly detection identified the attack but not its cause
- Containment action:
  - Fail safe firewall configuration with only opened port for further updates or even complete blockage of external interfaces

→ **Attacker has no access anymore**

Fail Operational Recovery

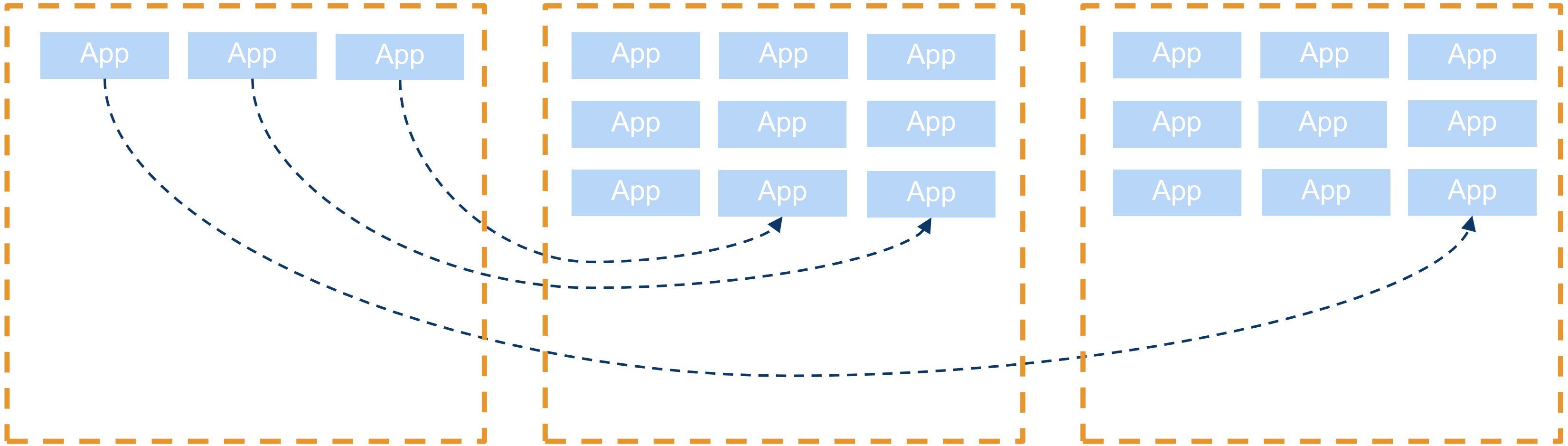


- **Analysis:**
  - Attacker used open port 6667 to access system
  - Attacker may already have inserted malicious code
- **Recovery action:**
  - [Fleet] Update firewall configuration to block port 6667
  - [Vehicle] Reallocate applications from HPC2 to the other HPCs
  - [Vehicle] Update switch configuration

→ **Malicious code cannot harm applications on HPC2**

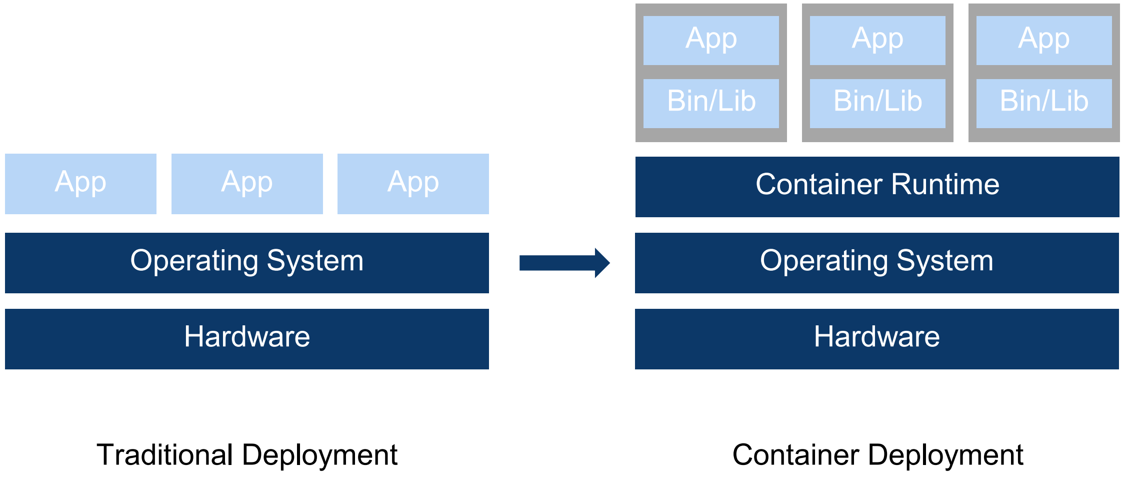
Basic idea

- **Service Oriented Architecture**
- **Services can be reallocated and rescheduled during runtime**
- **Enhances availability and flexibility**



Technical requirements

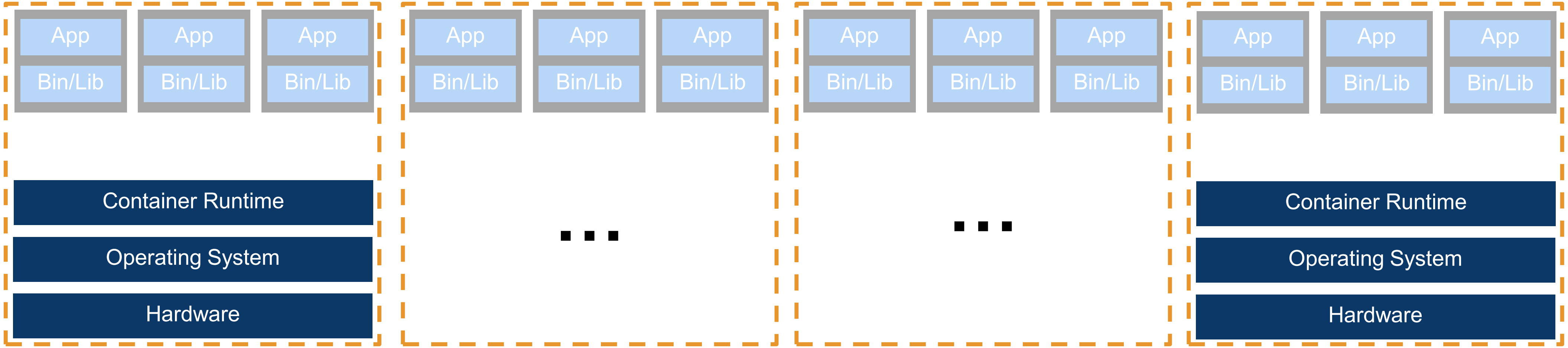
- **Services must be portable**
- **Integration as application containers (e.g. Docker)**
- **Use namespaces, cgroups, chroot to isolate processes**



→ Container based applications can be moved across HPCs

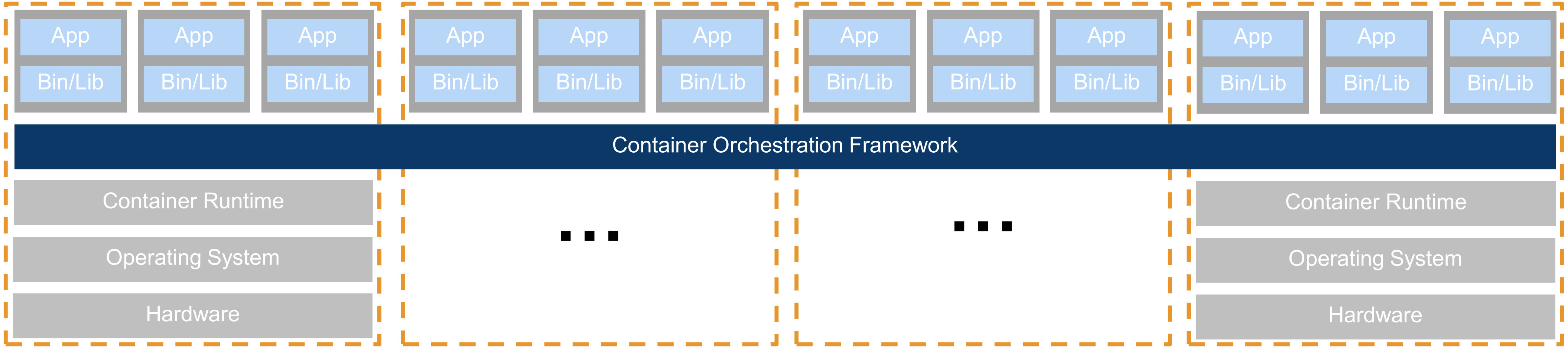
Container Orchestration

- **Orchestration: Composition of services**
- **State of the art in IT systems**
  - Application containers to deploy microservices
  - Orchestration framework to manage containers



Container Orchestration

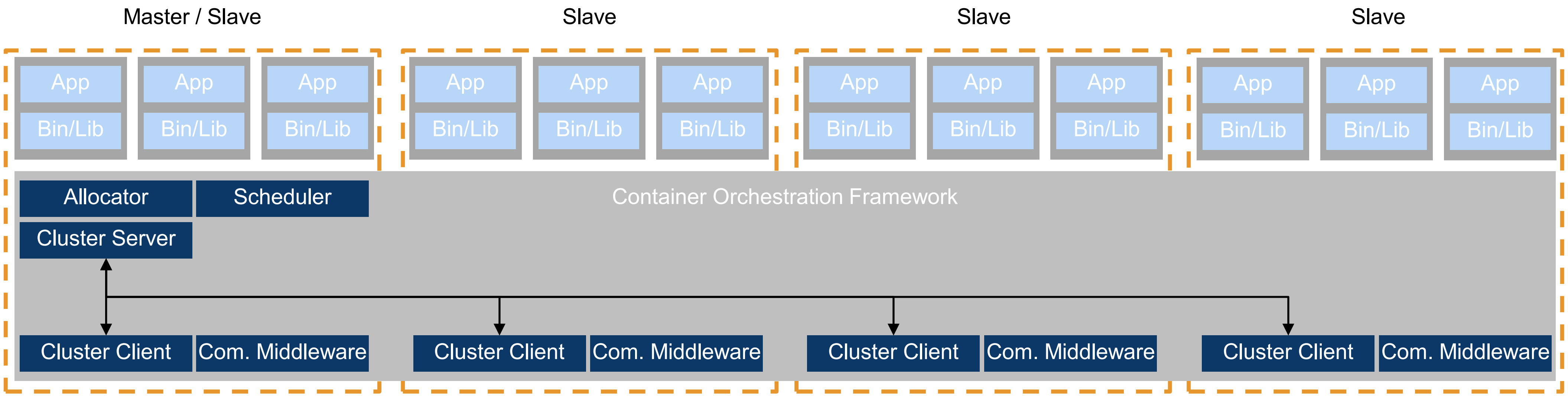
- **Orchestration: Composition of services**
- **State of the art in IT systems**
  - Application containers to deploy microservices
  - Orchestration framework to manage containers



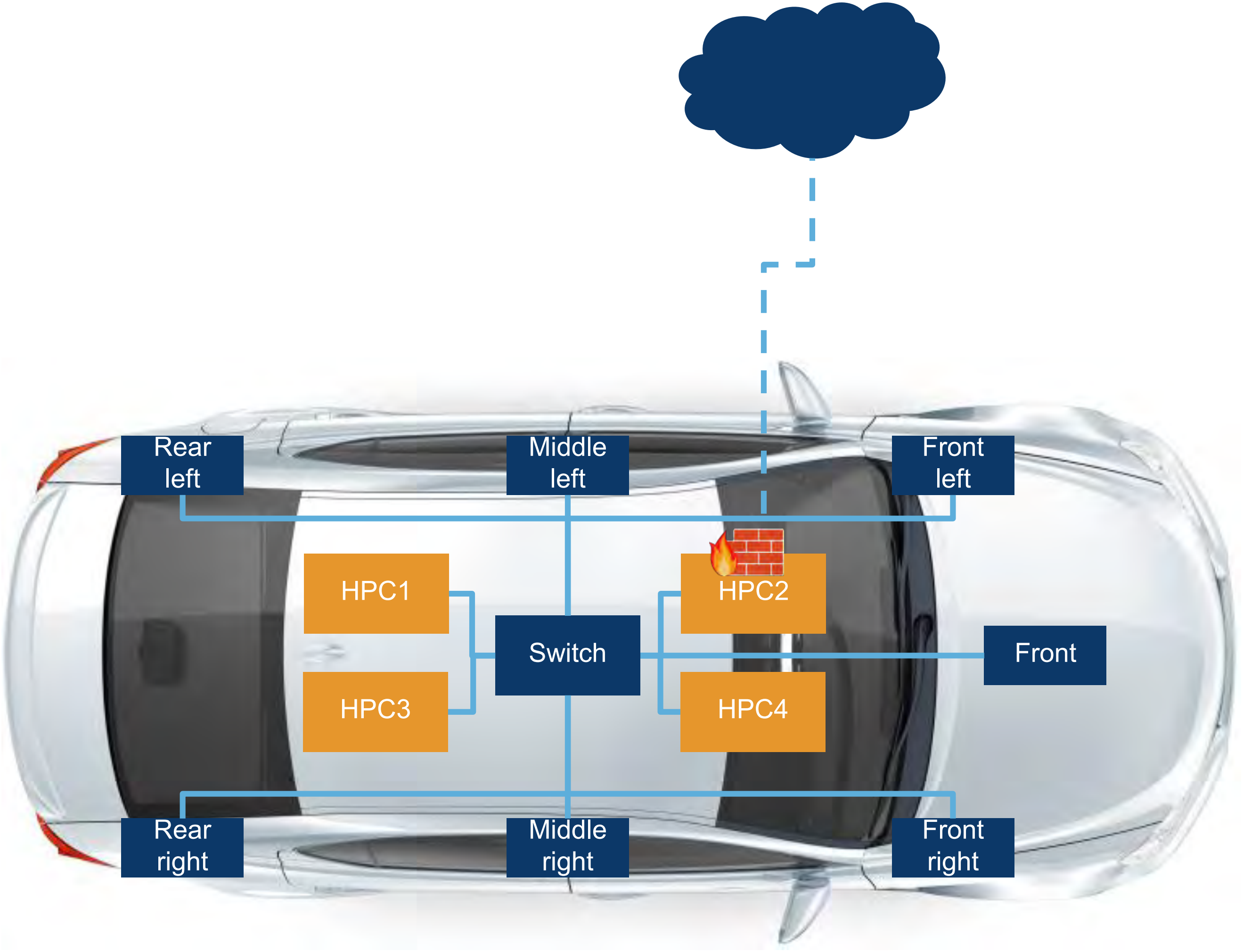
→ **Integration of orchestration framework on all HPCs**

Container Orchestration Framework

- **Master-Slave architecture**
- **Master**
  - Manages container deployment
  - Monitors health and state of slave nodes
- **Multiple synchronized master nodes possible**
- **Slave**
  - Monitors health and state of containers
  - Changes container states to desired states from Master
- **A node may act as master and slave simultaneously**



Full Recovery



- **Team of expert:**
  - Analysis logs and IDS reports
  - Identify weak spot: "No authentication required for D-Bus service on port 6667"
- **OEM and Tier-X:**
  - Build a new firmware for HPC2 that requires authentication for D-Bus service
- **Eradication action:**
  - [Fleet] Rollout of firmware update for HPC2
  - [Vehicle] Reallocate applications back to HPC2
  - [Vehicle] Update switch configuration

→ Vulnerability fixed in vehicle fleet

Structure

- Who we are
- Introduction Incident Response for Vehicles
- Response Stages for Safety-Critical Systems
- Response in Detail
- **Summary**

Summary

Summary:

- **Incident response strategies required for future vehicles**
  - Safety requirements need to be fulfilled at every time
  - Software updates → take to much time
- **Different response stages are introduced**
  1. Fail Safe Recovery: Information
  2. Fail Operational Recovery: Reconfiguration
  3. Full Recovery: Software update
- **Example response stage actions with special regards to system reconfiguration**
  - Containerized services
  - Dynamic reallocation and rescheduling of containers

Thank you

Services

Engineering

Consulting

Products

Contact

Prof. Dr.-Ing Falk Langer

IAV GmbH

Carnotstraße 1, 10587 Berlin
Telefon +49 371-237 33 264

Falk.Langer@iav.de

www.iav.com

Lukas Stahlbock

IAV GmbH

Carnotstraße 1, 10587 Berlin
Telefon +49 5371-80 54 263

Lukas.Stahlbock@iav.de

www.iav.com