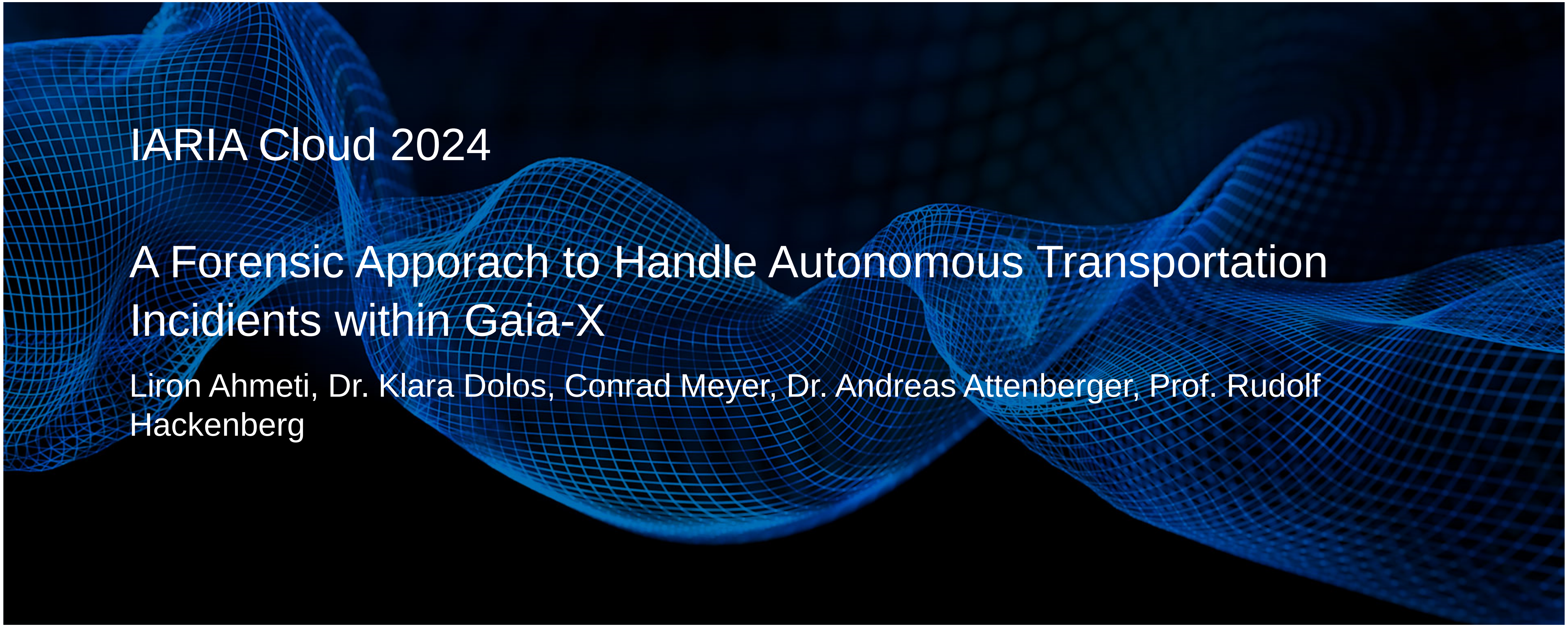
Zentrale Stelle
für Informationstechnik
im Sicherheitsbereich

Gaia-X 4 AMS

Ein Projekt der Gaia-X 4 Future Mobility Projektfamilie

ZITiS



IARIA Cloud 2024

A Forensic Apporach to Handle Autonomous Transportation Incidients within Gaia-X

Liron Ahmeti, Dr. Klara Dolos, Conrad Meyer, Dr. Andreas Attenberger, Prof. Rudolf Hackenberg

Agenda

- Autonomous Mobility and Gaia-X
- Criminal scenarios and their investigation
- Generalization of the forensic approach

Novel Challenges for Safety and Security

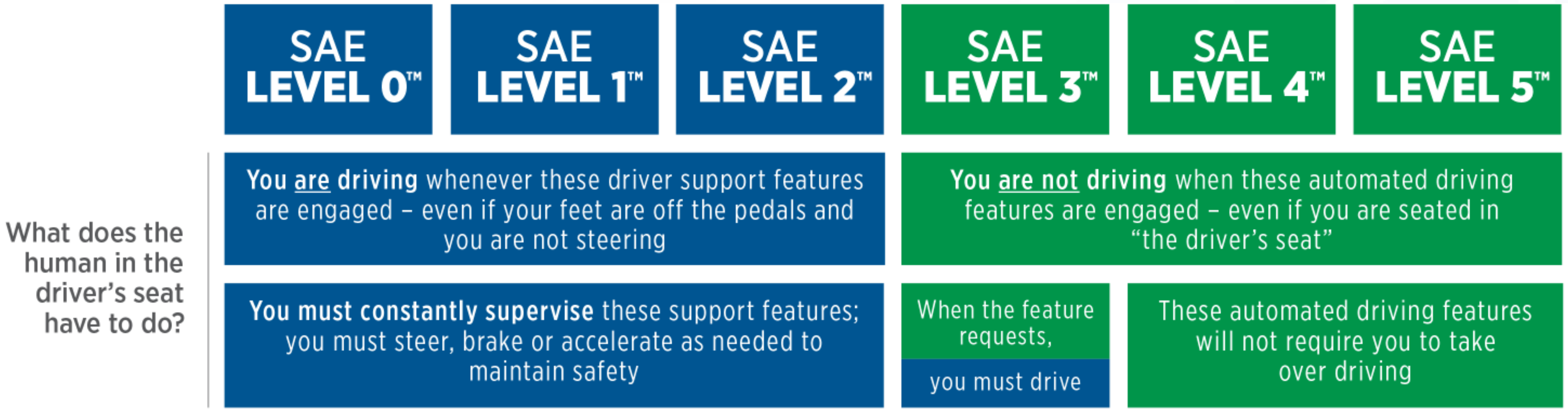
- Increasing complexity
  - Current vehicles: 1,2 x 10^8 lines of code
  - Autonomous vehicles: 10^{12} lines of code (forecast - Jaguar)

→ New types of incidents (accidents, criminal activities)!

- Forensic approach for newly occurring incidents in transportation

Autonomous Mobility

No human intervention is needed for navigation and control



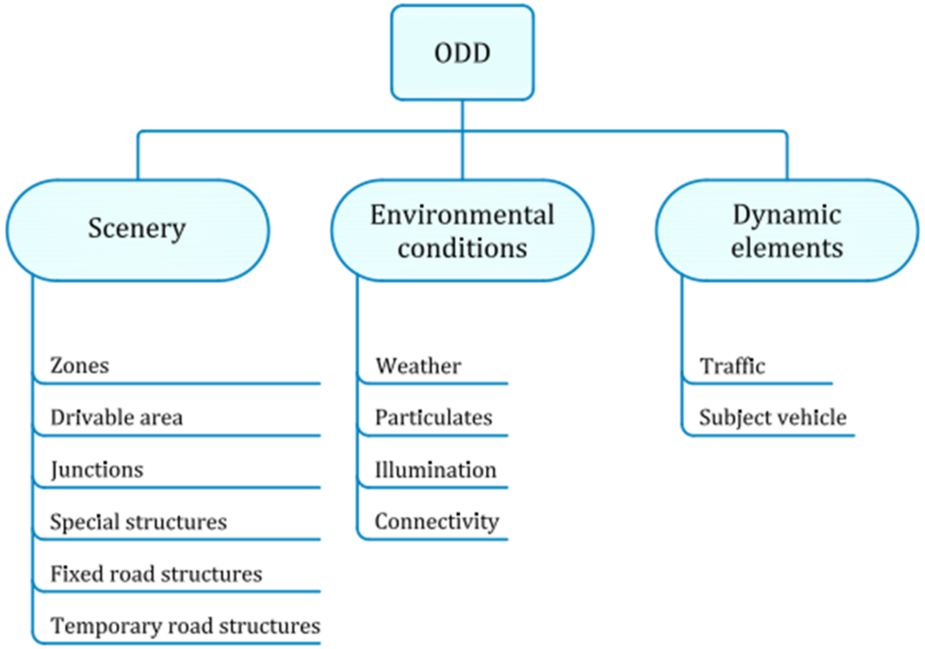
	SAE LEVEL 0™	SAE LEVEL 1™	SAE LEVEL 2™	SAE LEVEL 3™	SAE LEVEL 4™	SAE LEVEL 5™
What does the human in the driver's seat have to do?	**You <u>are</u> driving** whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			**You <u>are not</u> driving** when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	

SAE International, Levels of driving automation

Operational Design Domain (ODD)

- Limits and restrictions for autonomous driving (AD)
- Describes specific conditions e.g.
  - geographic areas, weather conditions, road infrastructure, traffic
- Vehicle-specific

- Example Mercedes
  - Autonomous driving (Level 4) only in a multi-storey car park in Stuttgart



ODD

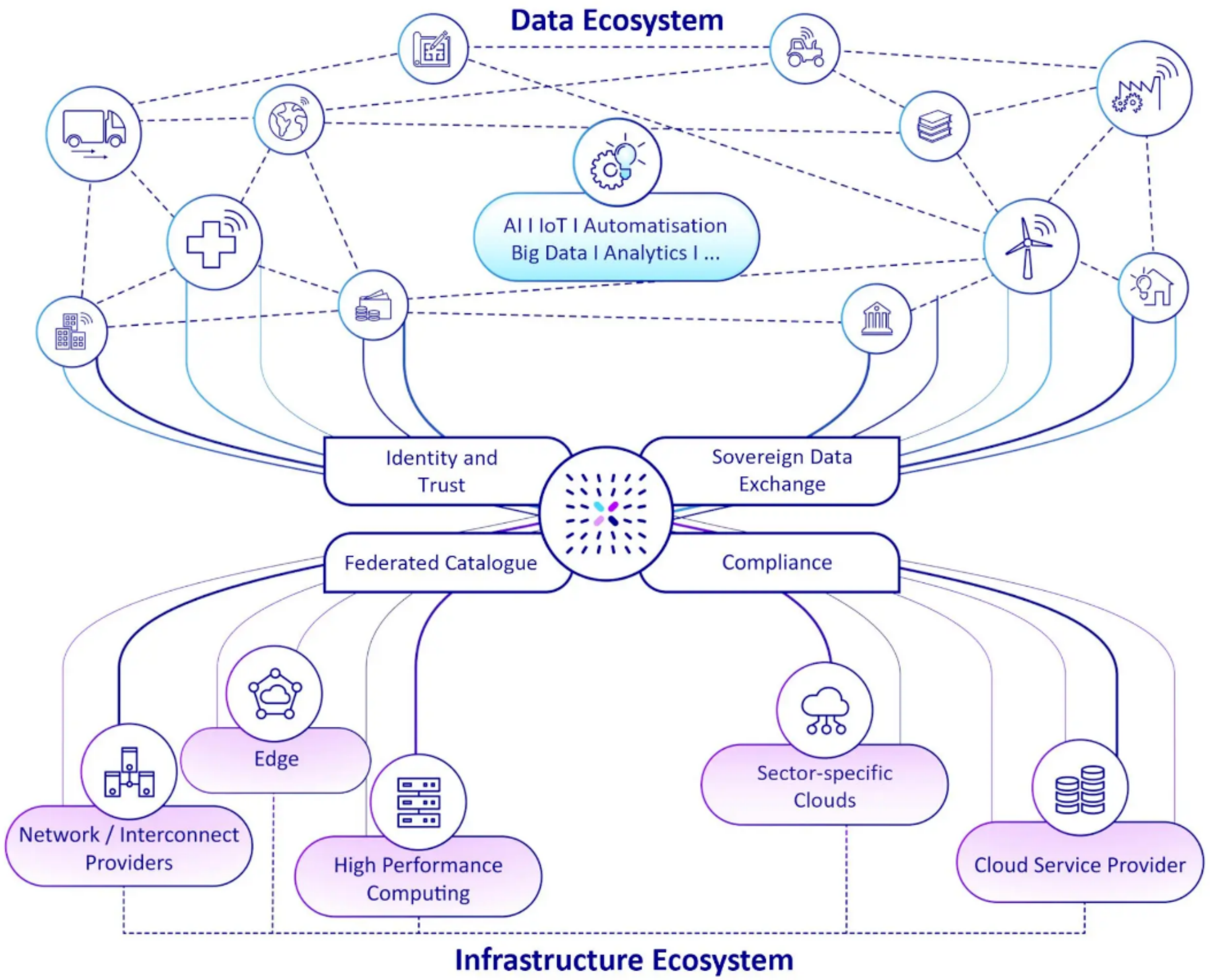
Scenery
- Zones
- Drivable area
- Junctions
- Special structures
- Fixed road structures
- Temporary road structures

Environmental conditions
- Weather
- Particulates
- Illumination
- Connectivity

Dynamic elements
- Traffic
- Subject vehicle

SAE International, standard J3016

Gaia-X



Gaia-X-Hub: Gaia-X explained

Zentrale Stelle
für Informationstechnik
im Sicherheitsbereich

Gaia-X 4 AMS
Ein Projekt der Gaia-X 4 Future Mobility Projektfamilie

Threat Modeling for Autonomous Vehicles

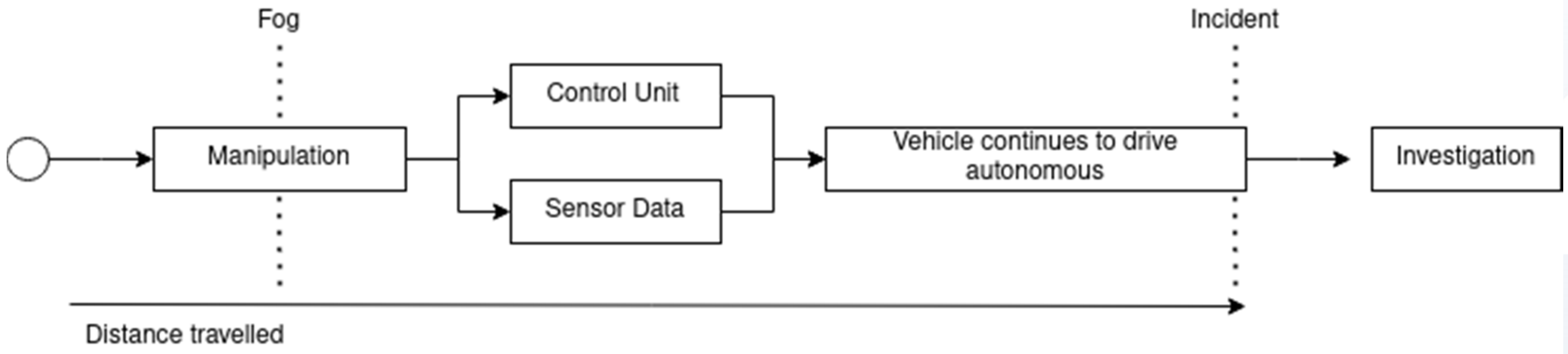
ZITiS

- 55% of surveyed risk assessment employees look at cyber security as the main concern for autonomous vehicles (Munich Re America 2016)
- Threats can be grouped into five categories:
  - Physical threats (side channels or debug interfaces)
  - Recording and manipulation of network traffic (interception threats)
  - Attacks against communication interfaces (DDoS)
  - Malicious code
  - Data threats (loss or leak of information)

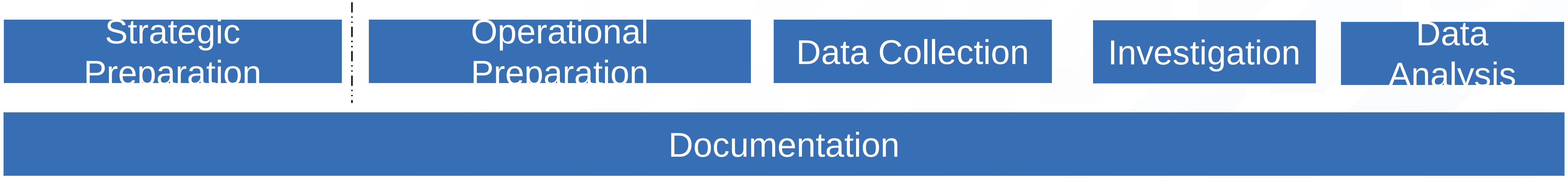
Forensics needed!

Criminal Scenario: „Vehicle Manipulation“

- Manipulation of the vehicle
  - Sensor values that disagree with autonomous driving are ignored
  - Enable autonomous driving in situations where it is not permitted



Investigation Process „Vehicle Manipulation“



Strategic Preparation

Operational Preparation

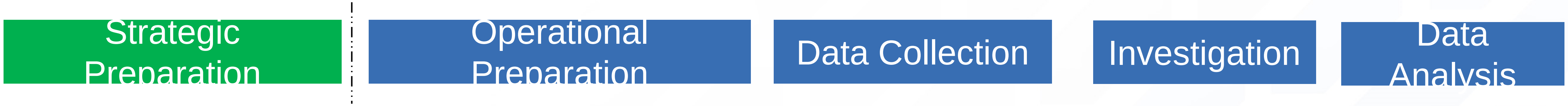
Data Collection

Investigation

Data Analysis

Documentation

Investigation Process „Vehicle Manipulation“

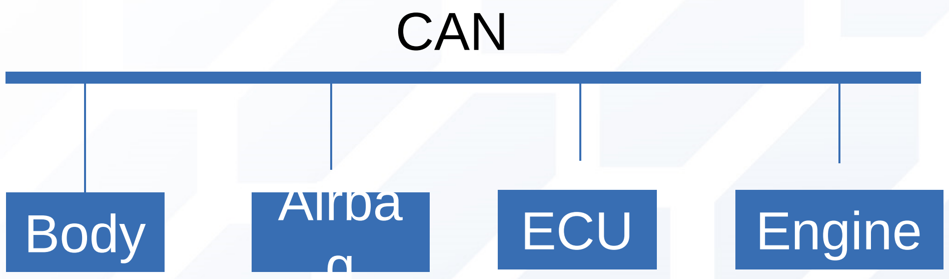


- Regulations
  - EU regulation 2019/2144:
    - Event-based data recording to store anonymized data
  - UN Regulation No. 157: Approval of Vehicles with Automatic Lane-Keeping System
    - Requirements for Data Storage Systems for Automated Driving
  - German Level 4 - Law
    - Storing condition of the vehicle

Investigation Process „Vehicle Manipulation“

Strategic Preparation | Operational Preparation | Data Collection | Investigation | Data Analysis

- Electronic Control Unit (ECU) Data
  - Access via Unifed Diagnostic Services (UDS)
  - Protocol for communication between the vehicle control units and diagnostic devices
- Communication
  - ODB-II
  - Vehicle units are communicate via Controller Area Network (CAN)



Zentrale Stelle für Informationstechnik im Sicherheitsbereich

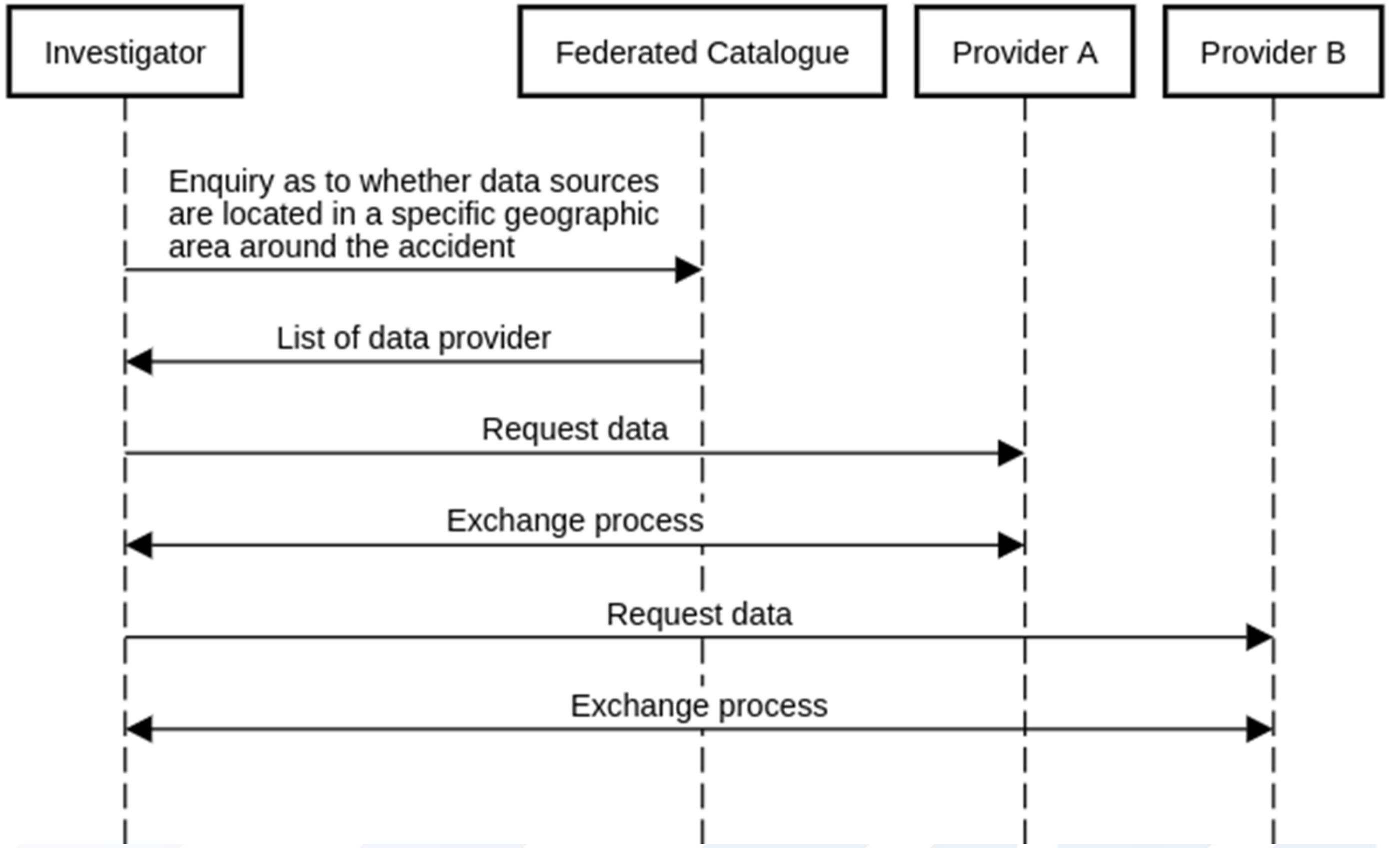
Gaia-X 4 AMS

Ein Projekt der Gaia-X 4 Future Mobility Projektfamilie

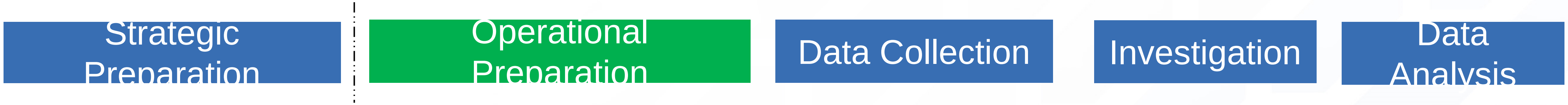
Investigation Process „Vehicle Manipulation“

Strategic Preparation | Operational Preparation | Data Collection | Investigation | Data Analysis

- Gaia-X Federated Catalogue serves as a instance for finding data providers
- Providers can be requested decentrally and standardised
- No prior contracts are required
- Providers are liable



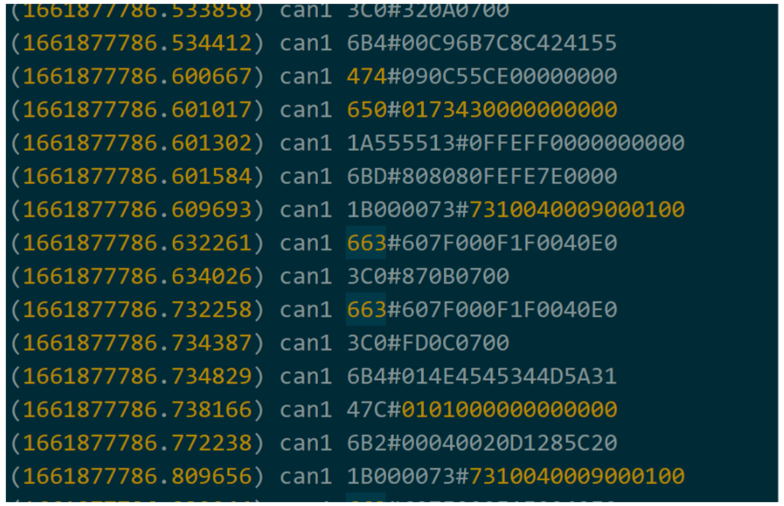
Investigation Process „Vehicle Manipulation“



- ODB-II
  - EDR/DSSAD
  - Communication dumbs
- UDS
  - Data from ECUs
- Gaia-X Federated Catalogue
  - Technical Supervisor
  - Data provider in Gaia-X

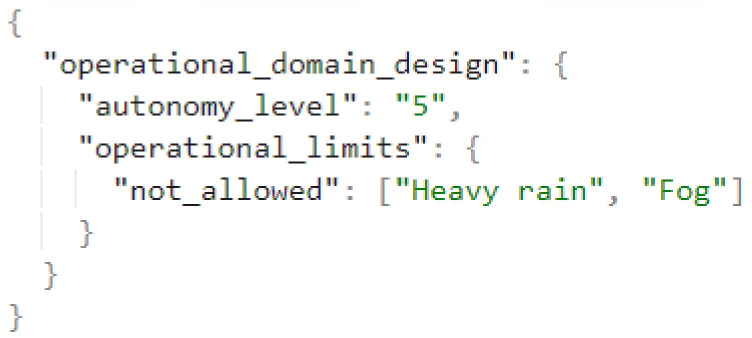
Investigation Process „Vehicle Manipulation“

Strategic Preparation | Operational Preparation | **Data Collection** | Investigation | Data Analysis



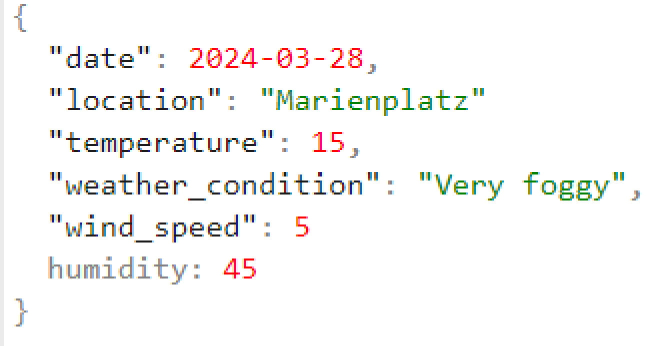
```
(1661877786.533858) can1 3C0#320A0700
(1661877786.534412) can1 6B4#00C96B7C8C424155
(1661877786.600667) can1 474#090C55CE00000000
(1661877786.601017) can1 650#0173430000000000
(1661877786.601302) can1 1A555513#0FFEFF0000000000
(1661877786.601584) can1 6BD#808080FEFE7E0000
(1661877786.609693) can1 1B000073#7310040009000100
(1661877786.632261) can1 663#607F000F1F0040E0
(1661877786.634026) can1 3C0#870B0700
(1661877786.732258) can1 663#607F000F1F0040E0
(1661877786.734387) can1 3C0#FD0C0700
(1661877786.734829) can1 6B4#014E4545344D5A31
(1661877786.738166) can1 47C#0101000000000000
(1661877786.772238) can1 6B2#00040020D1285C20
(1661877786.809656) can1 1B000073#7310040009000100
```

CAN dump



```
{
  "operational_domain_design": {
    "autonomy_level": "5",
    "operational_limits": {
      "not_allowed": ["Heavy rain", "Fog"]
    }
  }
}
```

Vehicle ODD configuration



```
{
  "date": 2024-03-28,
  "location": "Marienplatz"
  "temperature": 15,
  "weather_condition": "Very foggy",
  "wind_speed": 5
  humidity: 45
}
```

Weather provider response

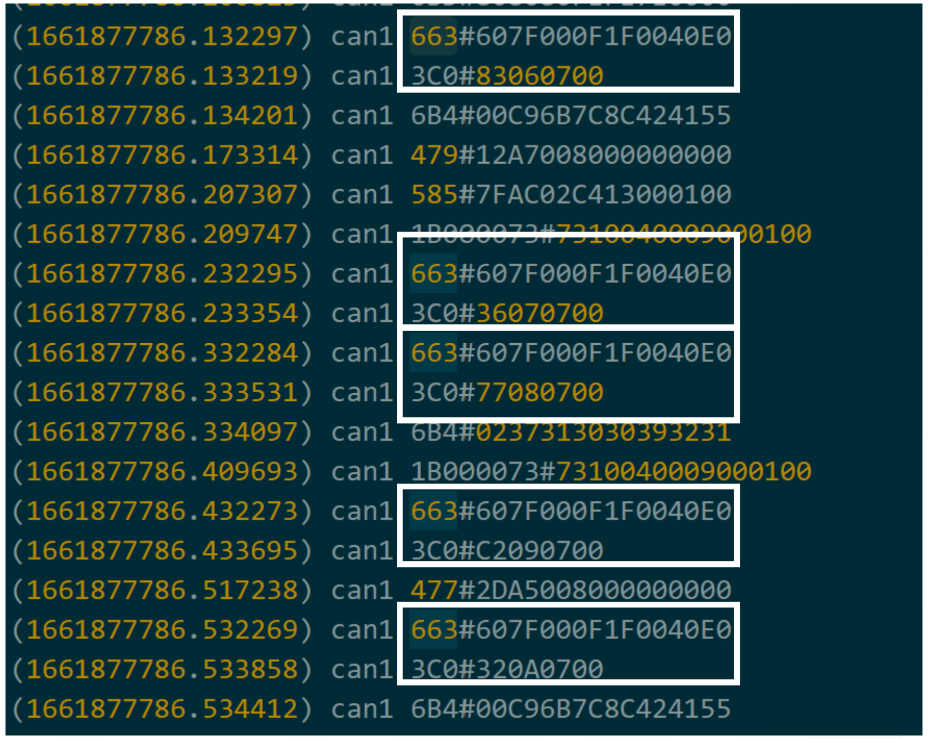
DSSAD Dump

ECU Software

Investigation Process „Vehicle Manipulation“

ZITiS

Strategic Preparation | Operational Preparation | Data Collection | Investigation | Data Analysis



```
(1661877786.132297) can1 663#607F000F1F0040E0
(1661877786.133219) can1 3C0#83060700
(1661877786.134201) can1 6B4#00C96B7C8C424155
(1661877786.173314) can1 479#12A7008000000000
(1661877786.207307) can1 585#7FAC02C413000100
(1661877786.209747) can1 1B000073#7310040009000100
(1661877786.232295) can1 663#607F000F1F0040E0
(1661877786.233354) can1 3C0#36070700
(1661877786.332284) can1 663#607F000F1F0040E0
(1661877786.333531) can1 3C0#77080700
(1661877786.334097) can1 6B4#0237313030393231
(1661877786.409693) can1 1B000073#7310040009000100
(1661877786.432273) can1 663#607F000F1F0040E0
(1661877786.433695) can1 3C0#C2090700
(1661877786.517238) can1 477#2DA5008000000000
(1661877786.532269) can1 663#607F000F1F0040E0
(1661877786.533858) can1 3C0#320A0700
(1661877786.534412) can1 6B4#00C96B7C8C424155
```

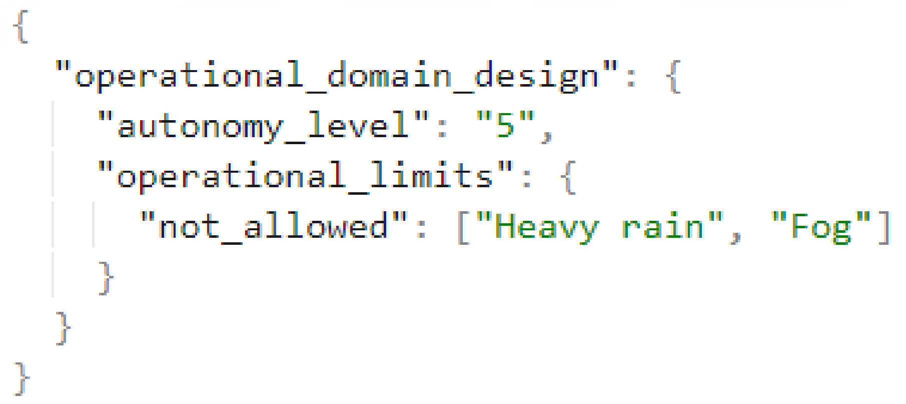
CAN dump

Investigation Process „Vehicle Manipulation“

Strategic Preparation | Operational Preparation | Data Collection | Investigation | Data Analysis

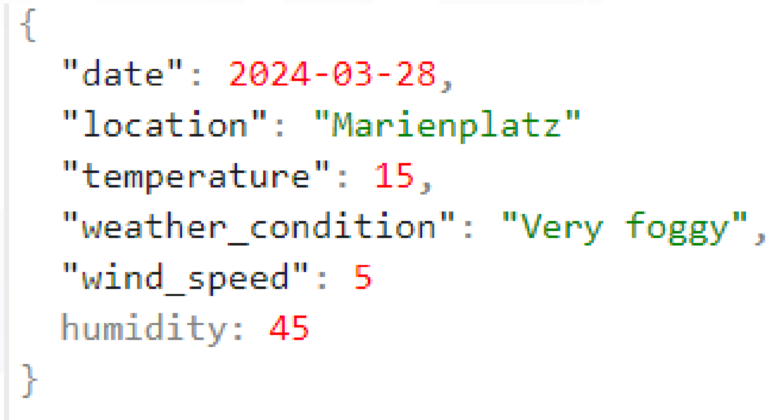
Time	System Activation
-5	True
-4	True
-3	True
-2	True
-1	True
0	True

Extract from DSSAD



```
{
  "operational_domain_design": {
    "autonomy_level": "5",
    "operational_limits": {
      "not_allowed": ["Heavy rain", "Fog"]
    }
  }
}
```

Vehicle ODD config



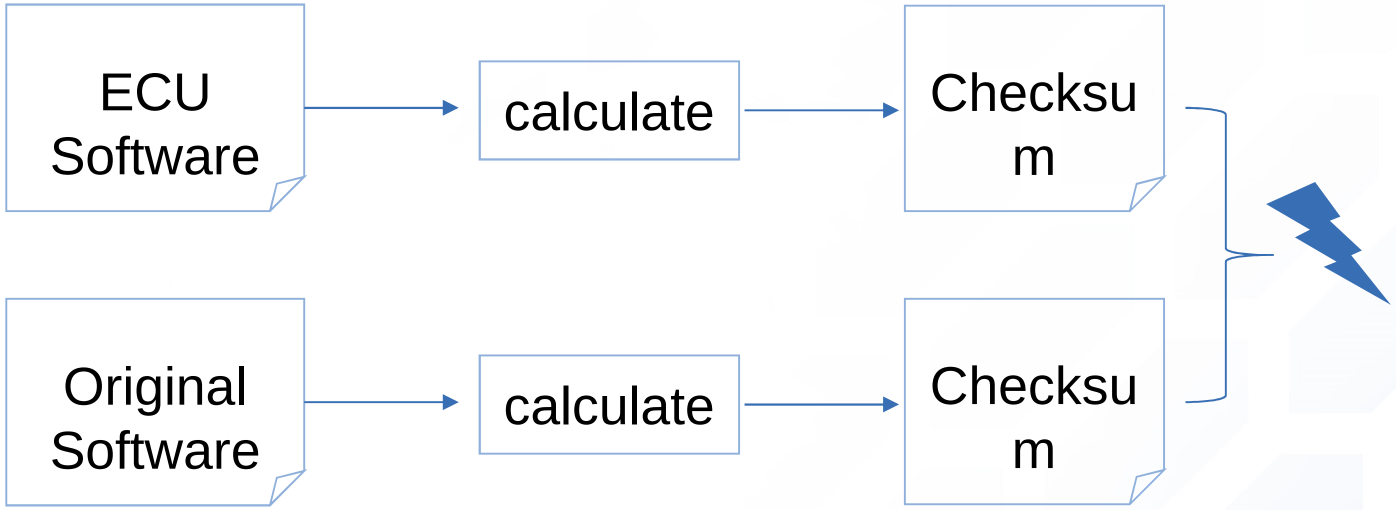
```
{
  "date": 2024-03-28,
  "location": "Marienplatz"
  "temperature": 15,
  "weather_condition": "Very foggy",
  "wind_speed": 5
  humidity: 45
}
```

Weather provider response

Investigation Process „Vehicle Manipulation“

ZITiS

Strategic Preparation | Operational Preparation | Data Collection | Investigation | Data Analysis



ECU Software

calculate

Checksum

Original Software

calculate

Checksum

Criminal Scenario „Denial of Service“

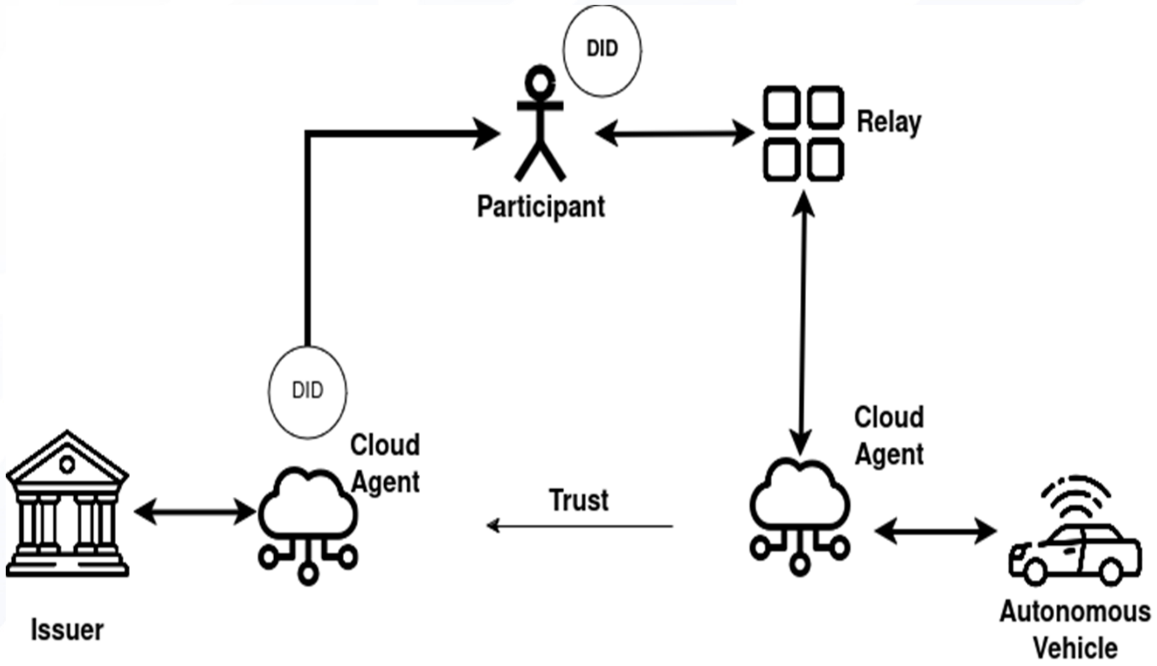
- Denial of Service Attack
  - Attack of the Communication Unit
  - Disrupt communication with Technical Supervisor
  - Failure of driving function (Level 5)

Investigation Process „Denial of Service“

ZITiS

Strategic Preparation | Operational Preparation | Data Collection | Investigation | Data Analysis

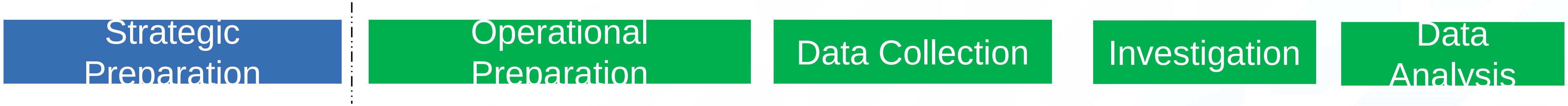
- Definition of mechanisms to prevent and identify attackers
- „Whitelisting“
  - Only process requests with valid Gaia-X participants
  - Digital identiy verified by Gaia-X Trust Framework
- Using Cloud Agents
  - Preprocessing of requests
  - Logging



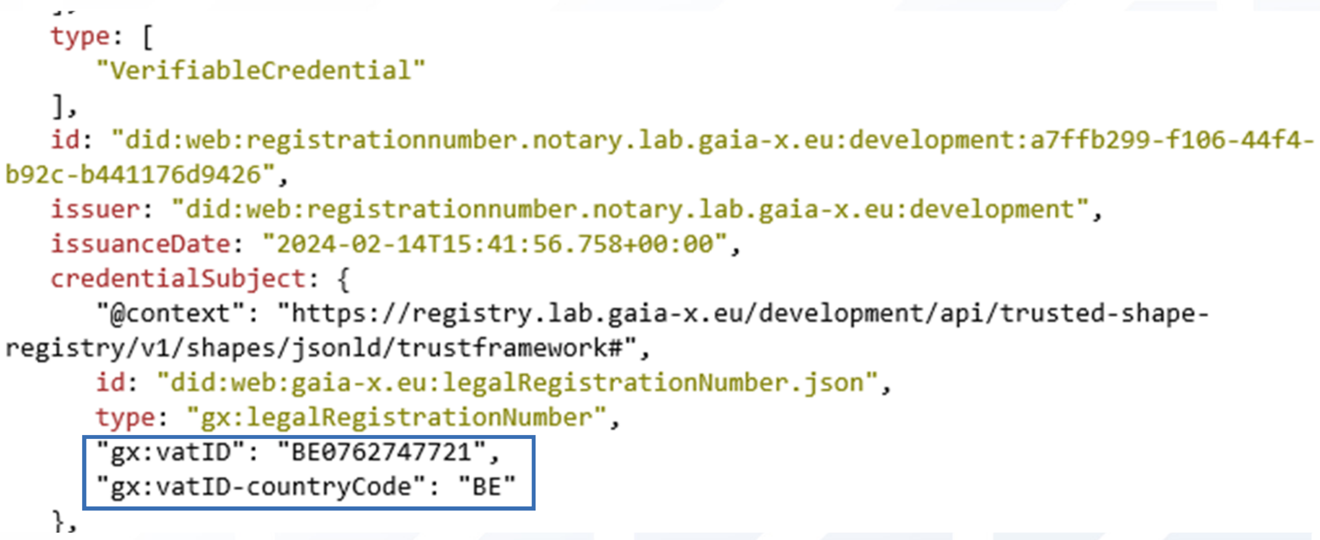
Zentrale Stelle für Informationstechnik im Sicherheitsbereich

Gaia-X 4 AMS
Ein Projekt der Gaia-X 4 Future Mobility Projektfamilie

Investigation Process „Denial of Service“



- Cloud Agent
- REST API



```
   type: [
      "VerifiableCredential"
   ],
   id: "did:web:registrationnumber.notary.lab.gaia-x.eu:development:a7ffb299-f106-44f4-
b92c-b441176d9426",
   issuer: "did:web:registrationnumber.notary.lab.gaia-x.eu:development",
   issuanceDate: "2024-02-14T15:41:56.758+00:00",
   credentialSubject: {
      "@context": "https://registry.lab.gaia-x.eu/development/api/trusted-shape-
registry/v1/shapes/jsonld/trustframework#",
      id: "did:web:gaia-x.eu:legalRegistrationNumber.json",
      type: "gx:legalRegistrationNumber",
      "gx:vatID": "BE0762747721",
      "gx:vatID-countryCode": "BE"
   },
```

Gaia-X, Verifiable Credentials