Automotive Forensics

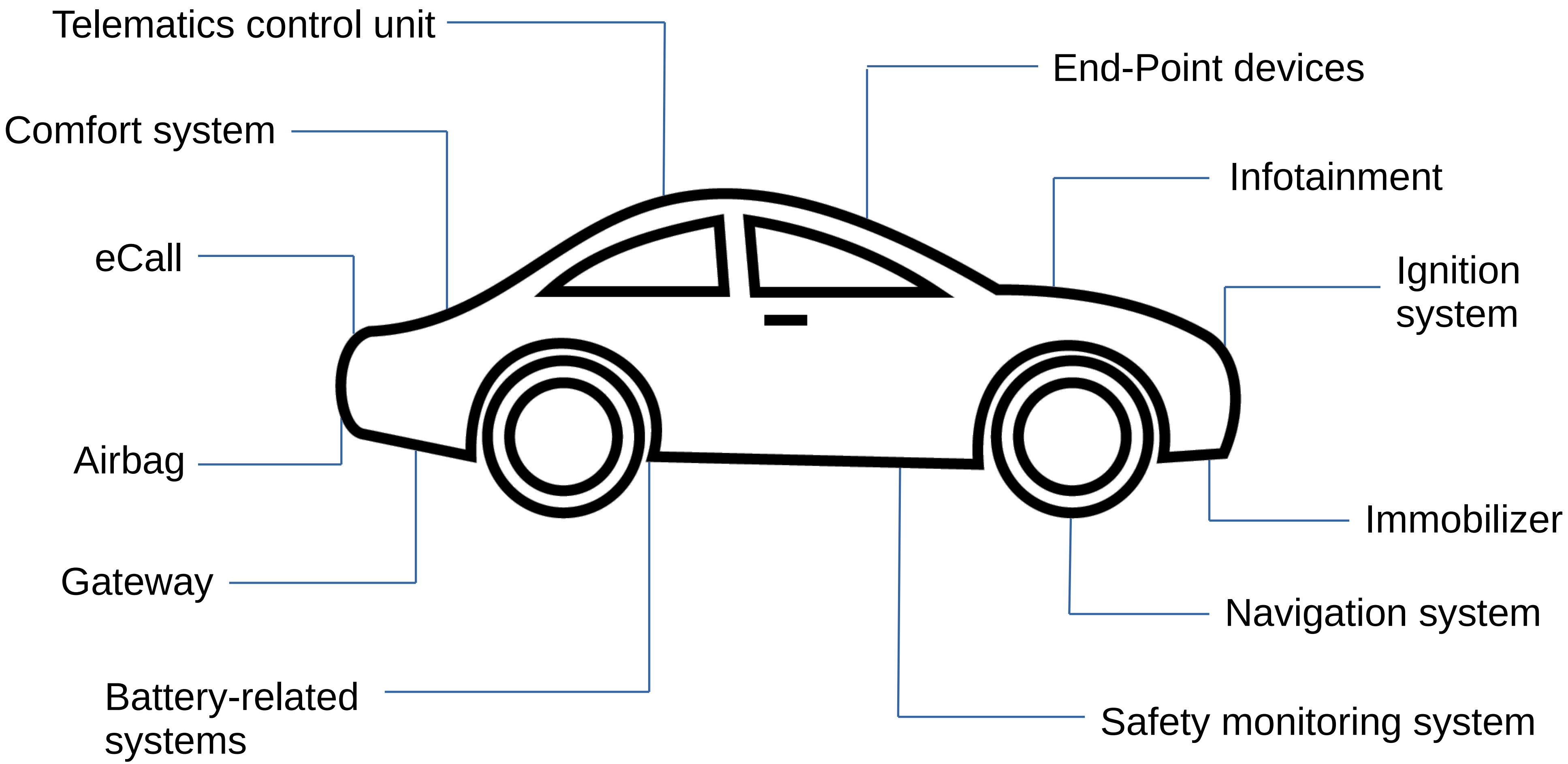
A hands-on showcase

Kevin Gomez Buquerin

Tutorial at SECURWARE 2021

extern.kevinklaus.gomezbuquerin@thi.de

Automotive Fundamentals



Telematics control unit

Comfort system

eCall

Airbag

Gateway

Battery-related systems

End-Point devices

Infotainment

Ignition system

Immobilizer

Navigation system

Safety monitoring system

Backend-Services

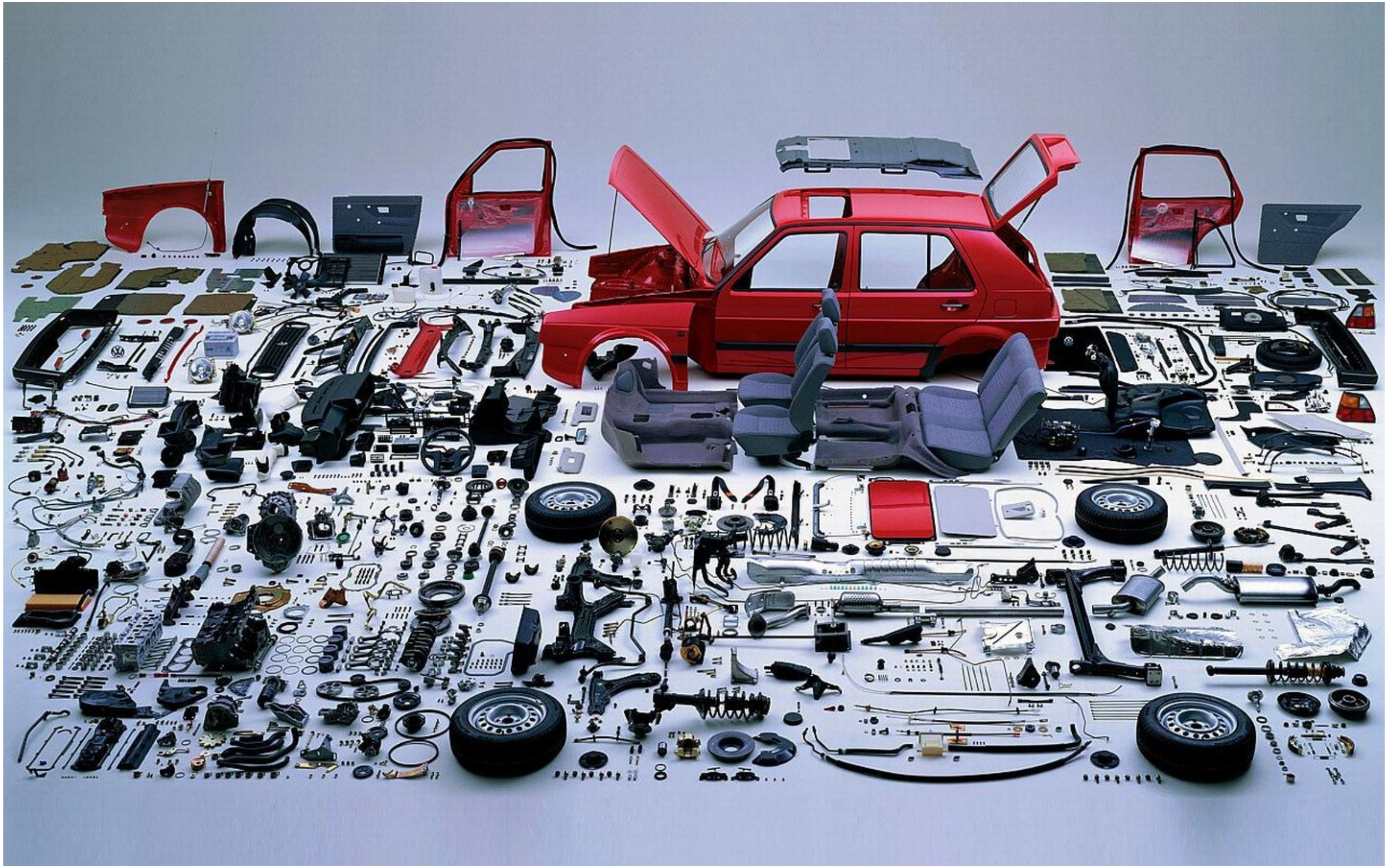
Smartphones

OBD-Dongles

Smart-Home

Car-To-X

Traffic lights



Digital Forensics Fundamentals

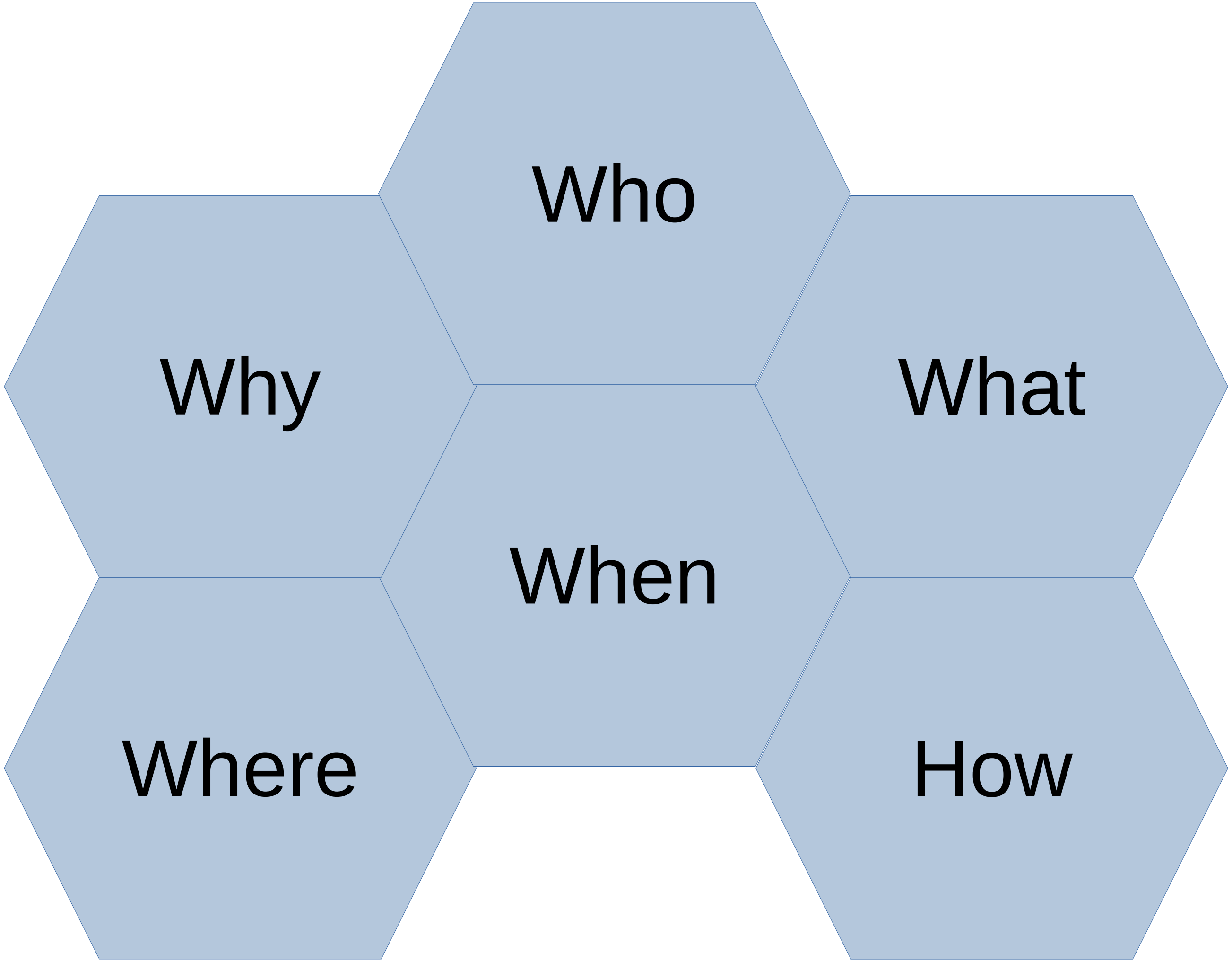
Goal

Reconstruction of events

1) Forensic Readiness
2) Extraction
3) Analysis
4) Interpretation
5) Reporting

“***Any action*** *of an individual, and obviously the violent action constituting a crime, cannot occur without* ***leaving a trace****.*”

- Dr. Edmond Locard (1934)



Who

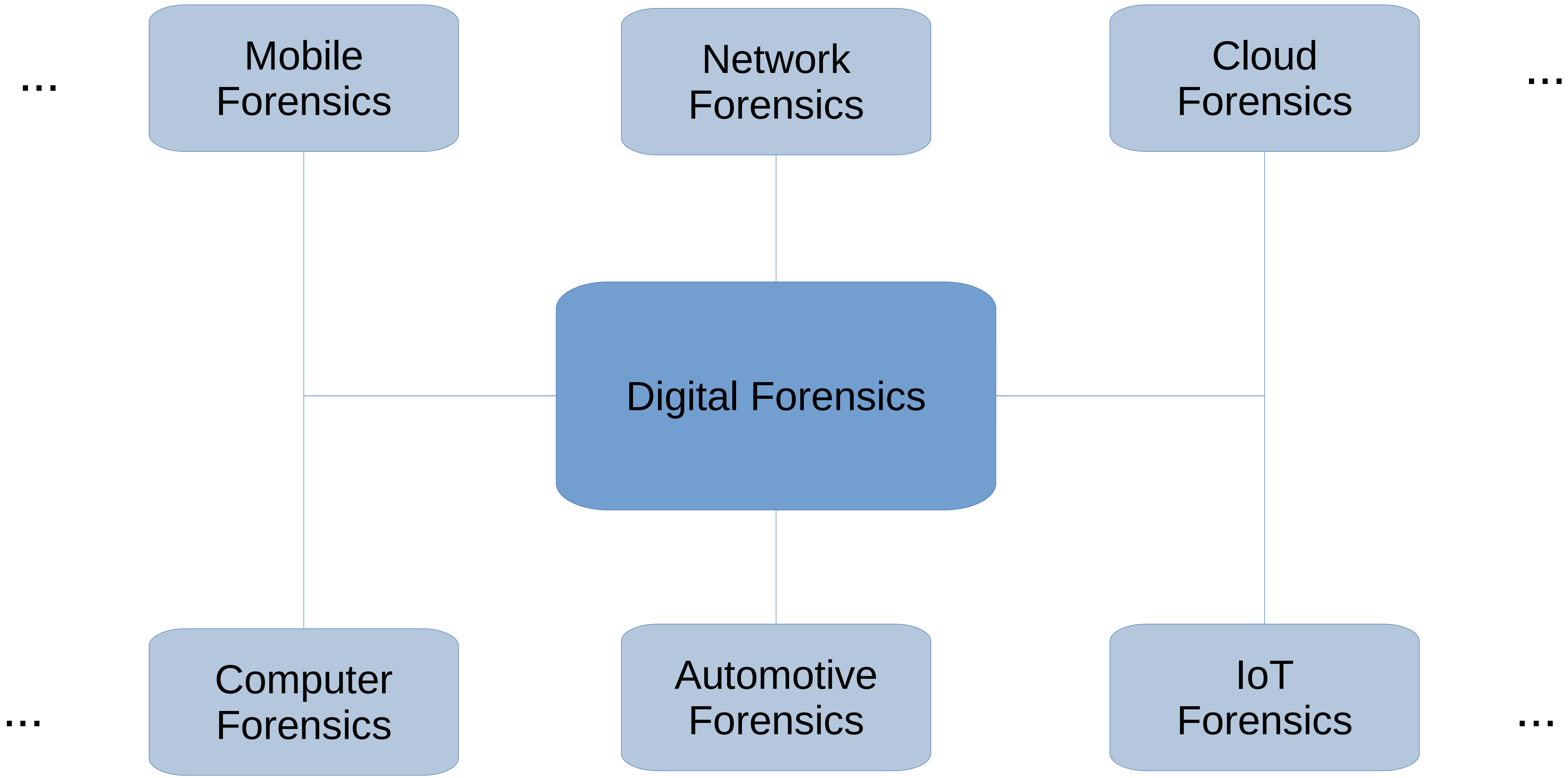
Why

What

When

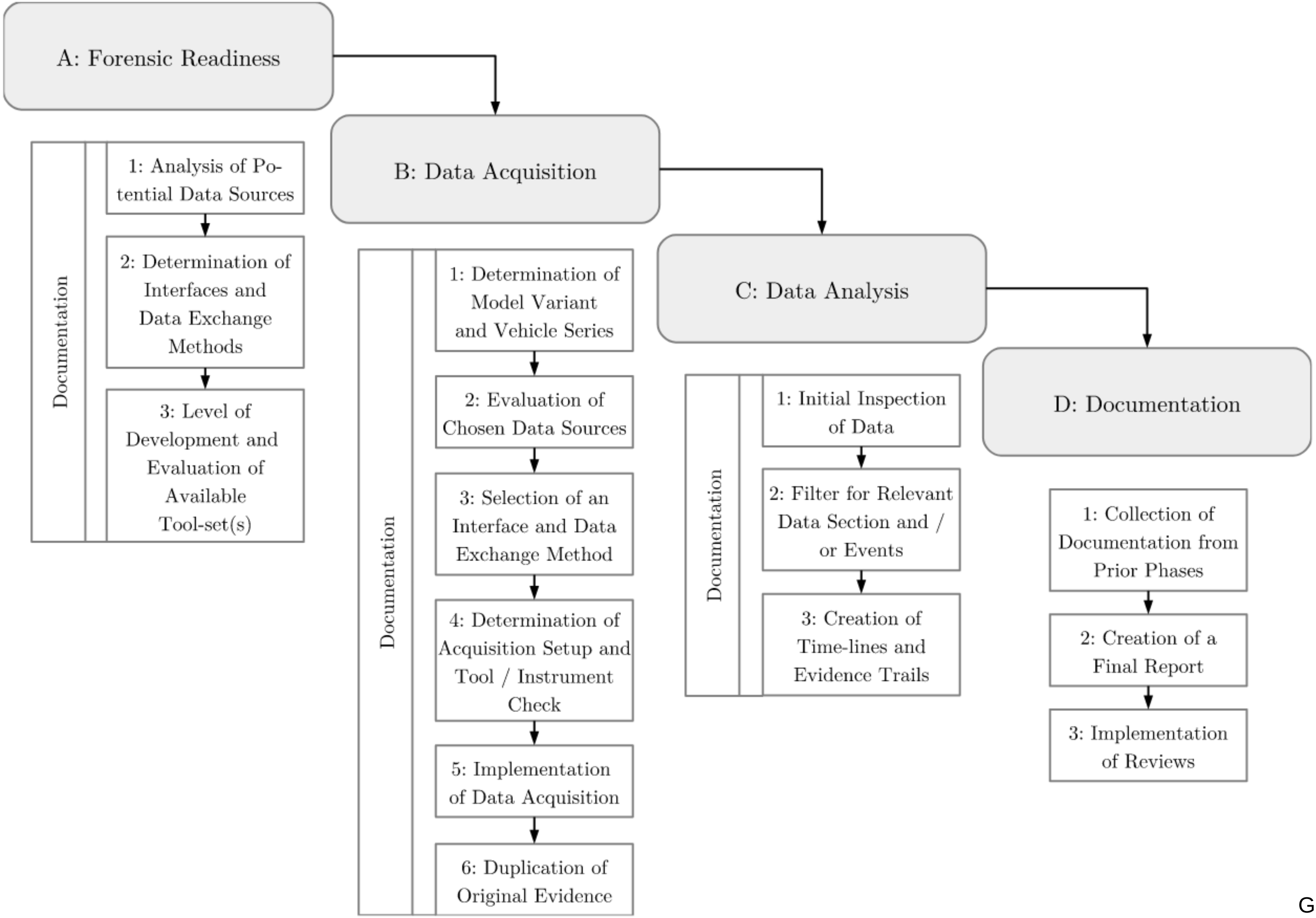
Where

How


...
Mobile Forensics
Network Forensics
Cloud Forensics
...
Digital Forensics
...
Computer Forensics
Automotive Forensics
IoT Forensics
...

Automotive Digital Forensics Fundamentals

“*ADF is the implementation of **technologies**, **processes**, and **methodologies** from **DF science** to the automotive domain. It includes **in-vehicle components** and **components connected to the vehicle** (ecosystem) such as Smartphones, OBD-Dongles as well as the supporting infrastructure.*”



A: Forensic Readiness

Documentation

1: Analysis of Potential Data Sources

2: Determination of Interfaces and Data Exchange Methods

3: Level of Development and Evaluation of Available Tool-set(s)

B: Data Acquisition

Documentation

1: Determination of Model Variant and Vehicle Series

2: Evaluation of Chosen Data Sources

3: Selection of an Interface and Data Exchange Method

4: Determination of Acquisition Setup and Tool / Instrument Check

5: Implementation of Data Acquisition

6: Duplication of Original Evidence

C: Data Analysis

Documentation

1: Initial Inspection of Data

2: Filter for Relevant Data Section and / or Events

3: Creation of Time-lines and Evidence Trails

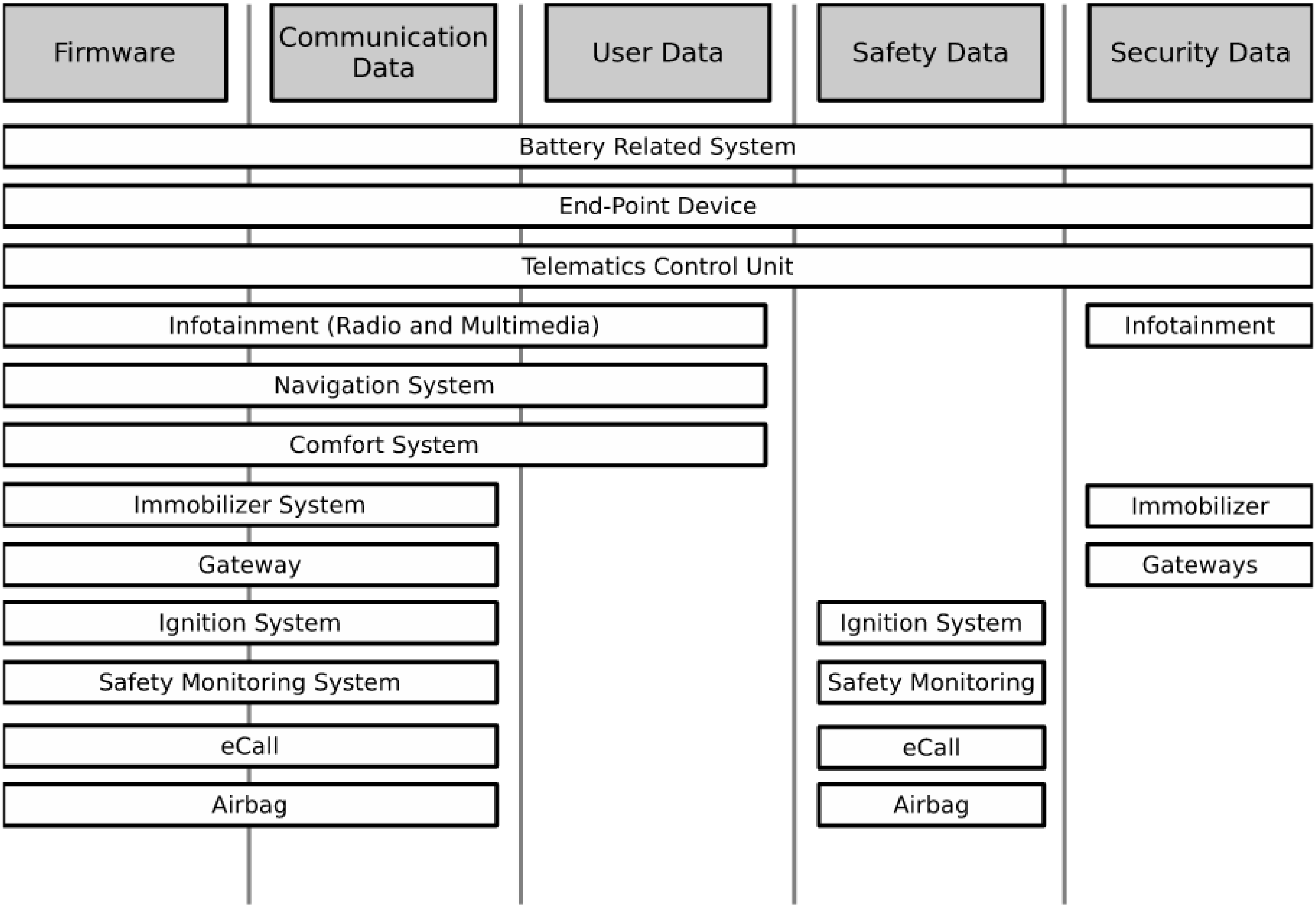
D: Documentation

1: Collection of Documentation from Prior Phases

2: Creation of a Final Report

3: Implementation of Reviews

Gomez2021DFRWS



Firmware

Communication Data

User Data

Safety Data

Security Data

Battery Related System

End-Point Device

Telematics Control Unit

Infotainment (Radio and Multimedia)

Infotainment

Navigation System

Comfort System

Immobilizer System

Immobilizer

Gateway

Gateways

Ignition System

Ignition System

Safety Monitoring System

Safety Monitoring

eCall

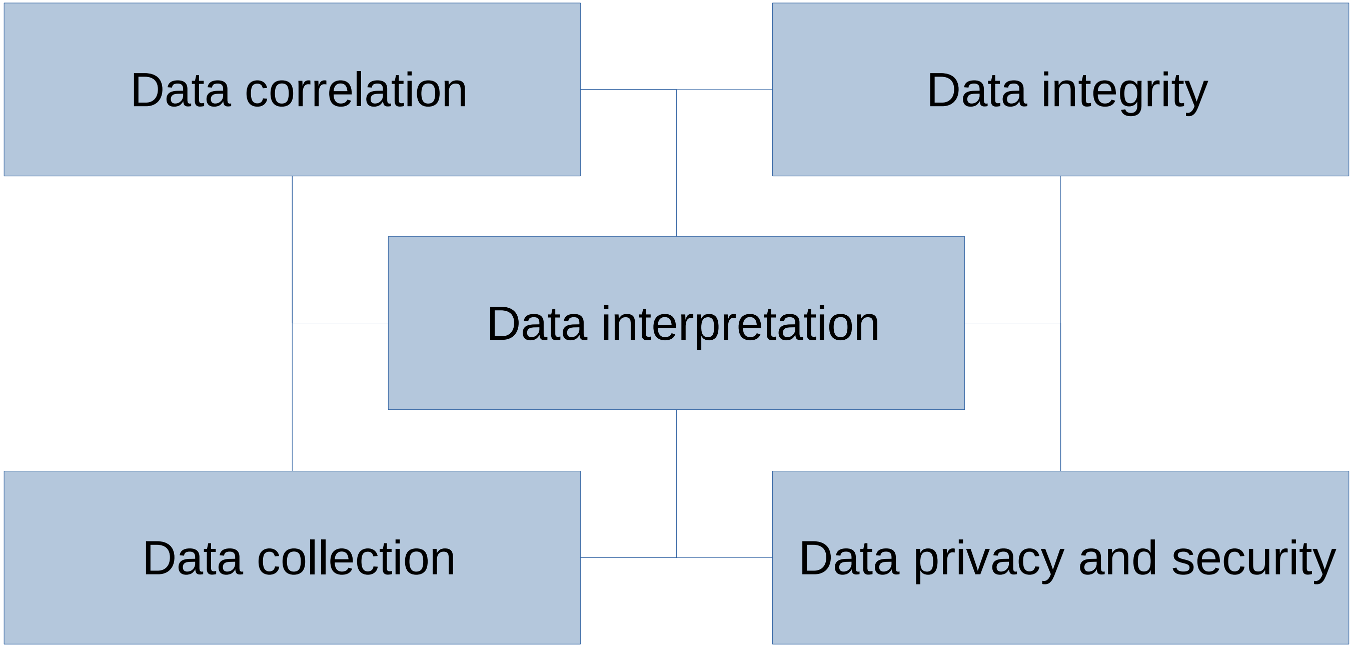
eCall

Airbag

Airbag

Gomez2021ESCAR

Challenges



Data correlation

Data integrity

Data interpretation

Data collection

Data privacy and security

The Case

www.tesla.com

Airbag ECU

www.ebay.de

What could we do?

Airbag ECU

www.ebay.de

What could we do?

- Analysis of the ECU
- Install into another Tesla

Airbag ECU

www.ebay.de

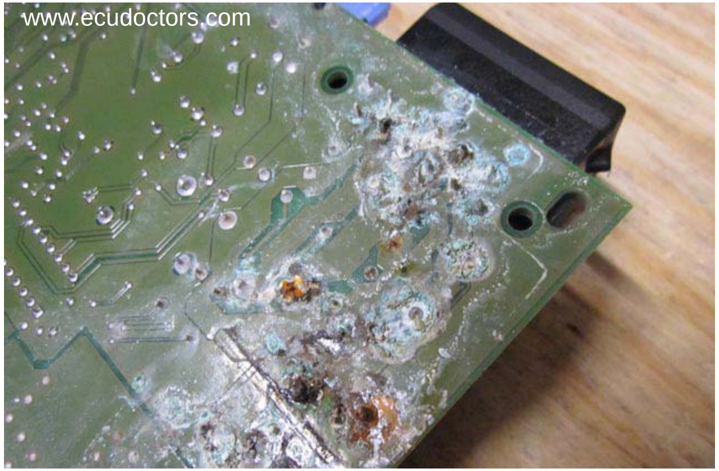
What could we do?

- Analysis of the ECU
- ~~Install into another Tesla~~

→ Disassemble the ECU

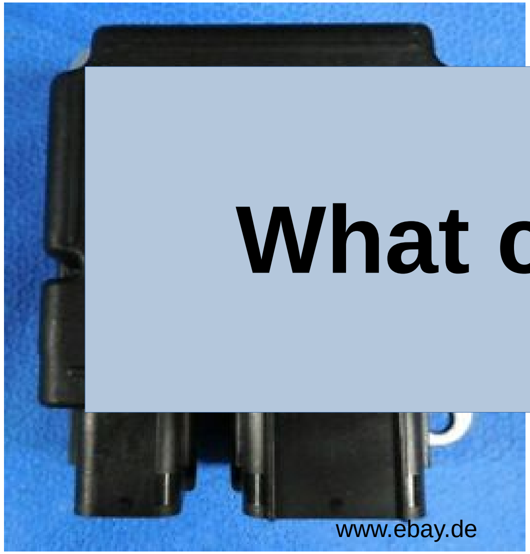
Airbag ECU

www.ebay.de



www.ecudoctors.com

Airbag ECU



www.ebay.de

www.ecudoctors.com

What could we do?

www.crashdatagroup.com

- Try Telsa EDR Tool

www.crashdatagroup.com

- ~~Try Telsa EDR Tool~~ → Not working

www.crashdatagroup.com

- ~~Try Telsa EDR Tool~~ → Not working
- Desoldering of storage devices

www.crashdatagroup.com

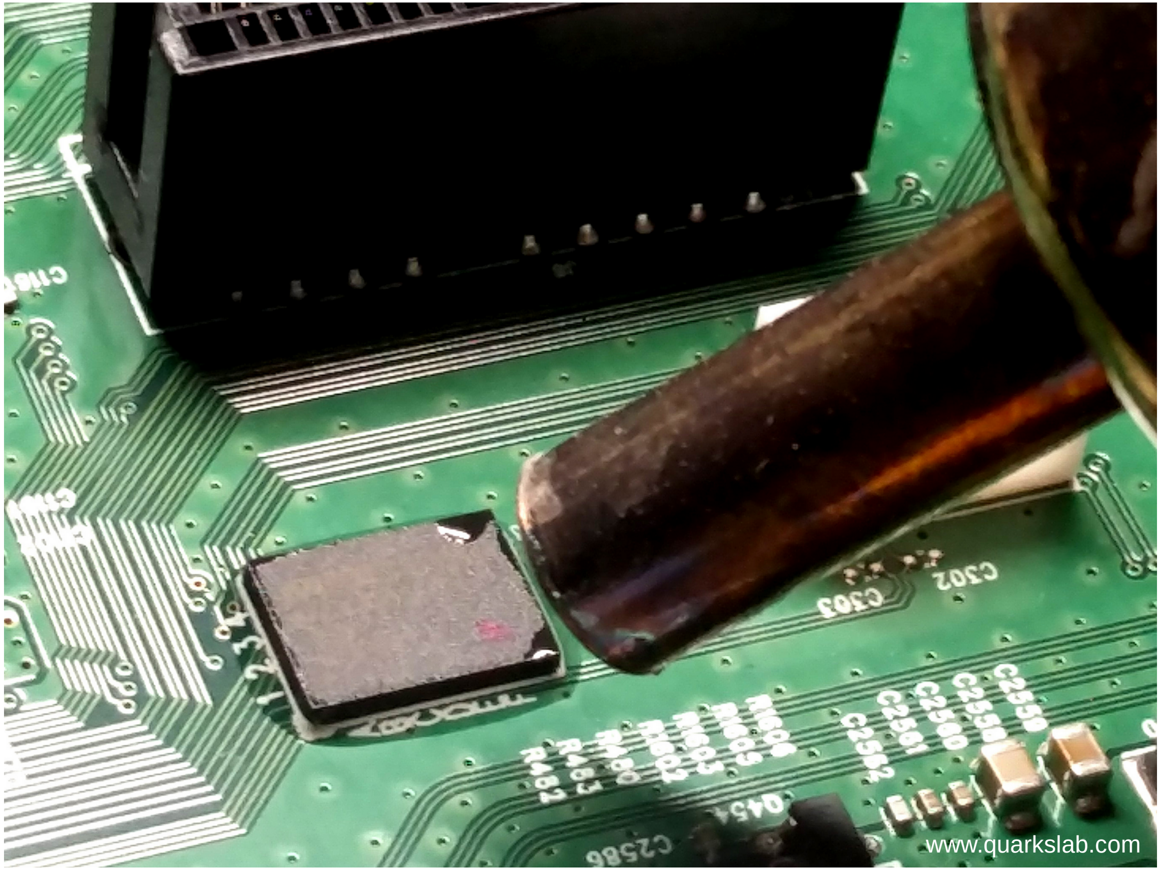
- ~~Try Telsa EDR Tool~~ → Not working
- Desoldering of storage devices
- Read flash with external adapter

www.crashdatagroup.com

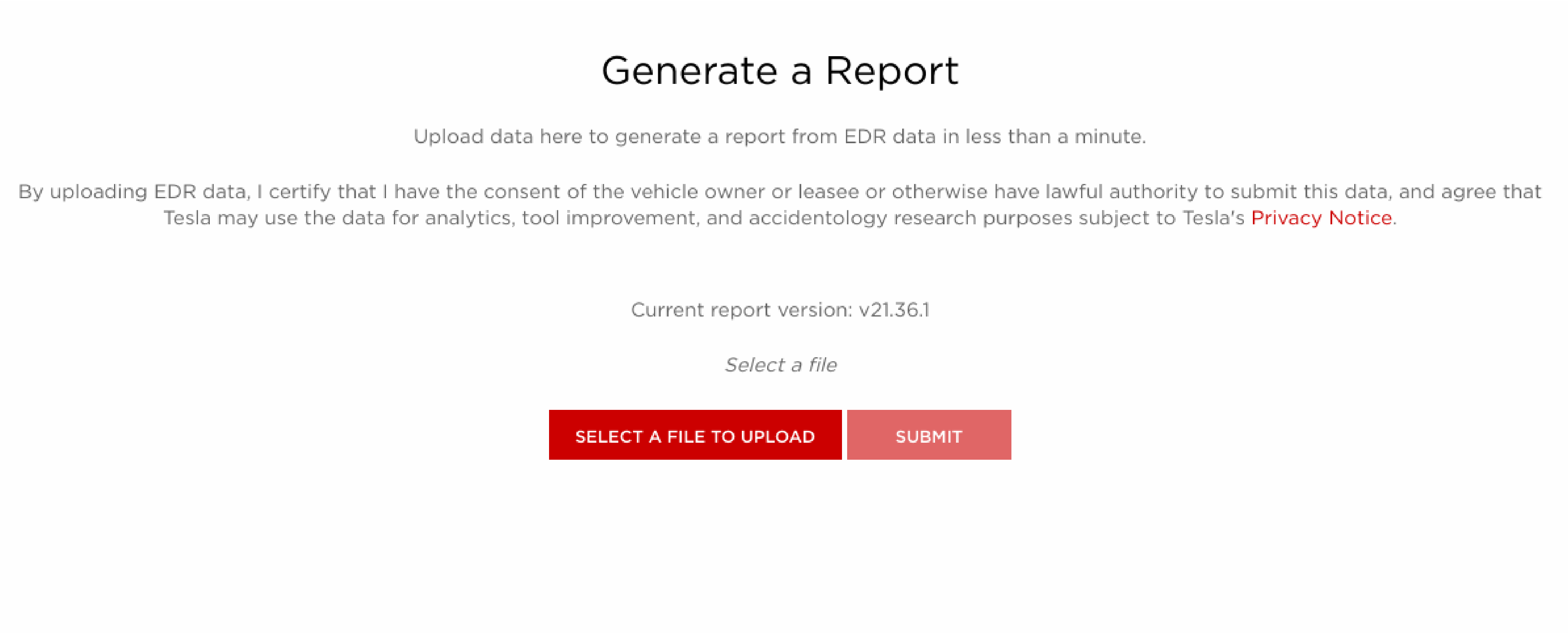
- ~~Try Telsa EDR Tool~~ → Not working
- Desoldering of storage devices
- ~~Read flash with external adapter~~ → Interpetation

www.crashdatagroup.com

- ~~Try Telsa EDR Tool~~ → Not working
- Desoldering of storage devices
- ~~Read flash with external adapter~~ → Interpetation
- Build into working Airbag ECU


www.quarkslab.com

Ingenieurbüro Kneifel
IB Kneifel
MacBook
www.kneifel.de



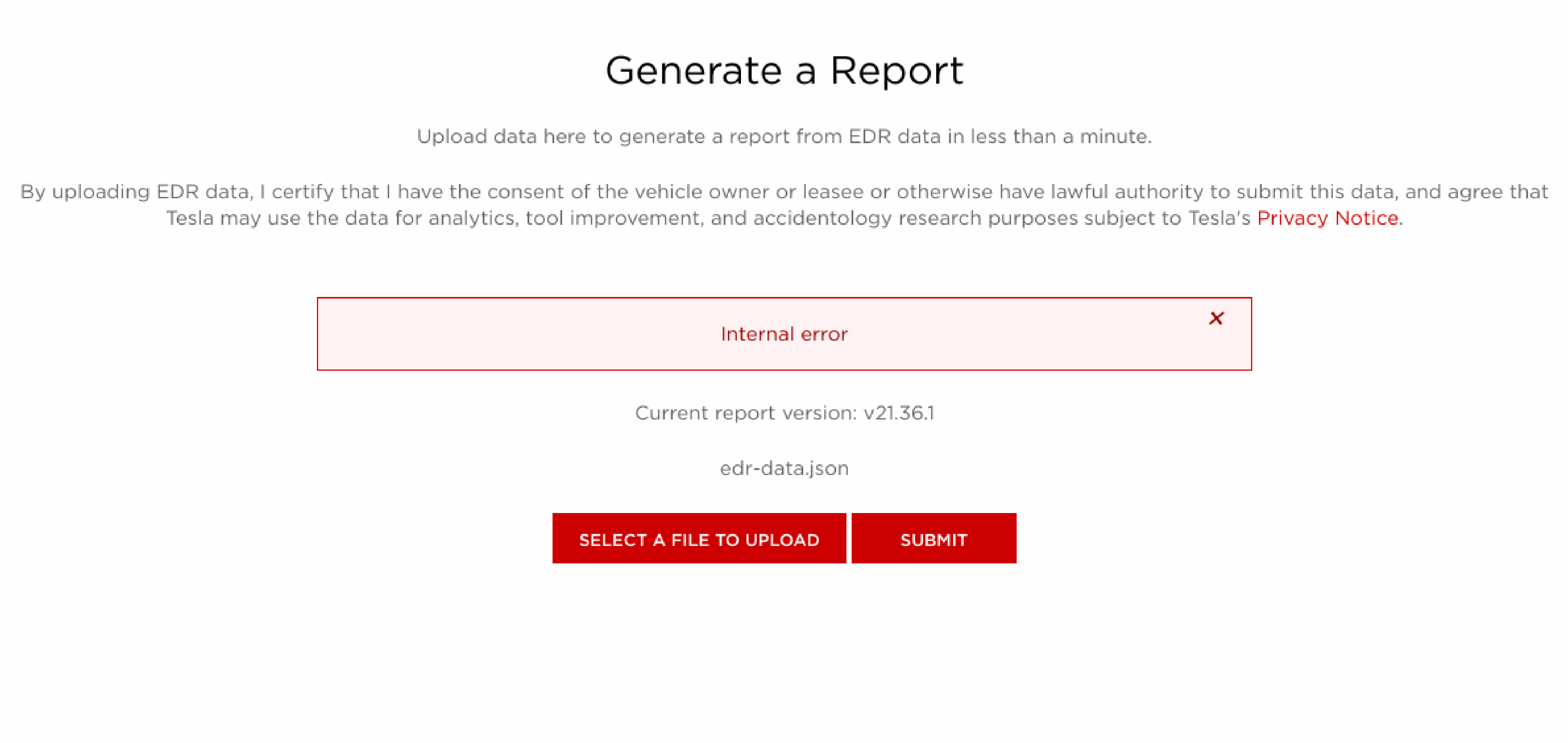
Generate a Report

Upload data here to generate a report from EDR data in less than a minute.

By uploading EDR data, I certify that I have the consent of the vehicle owner or leasee or otherwise have lawful authority to submit this data, and agree that Tesla may use the data for analytics, tool improvement, and accidentology research purposes subject to Tesla's Privacy Notice.

Current report version: v21.36.1

Select a file



Generate a Report

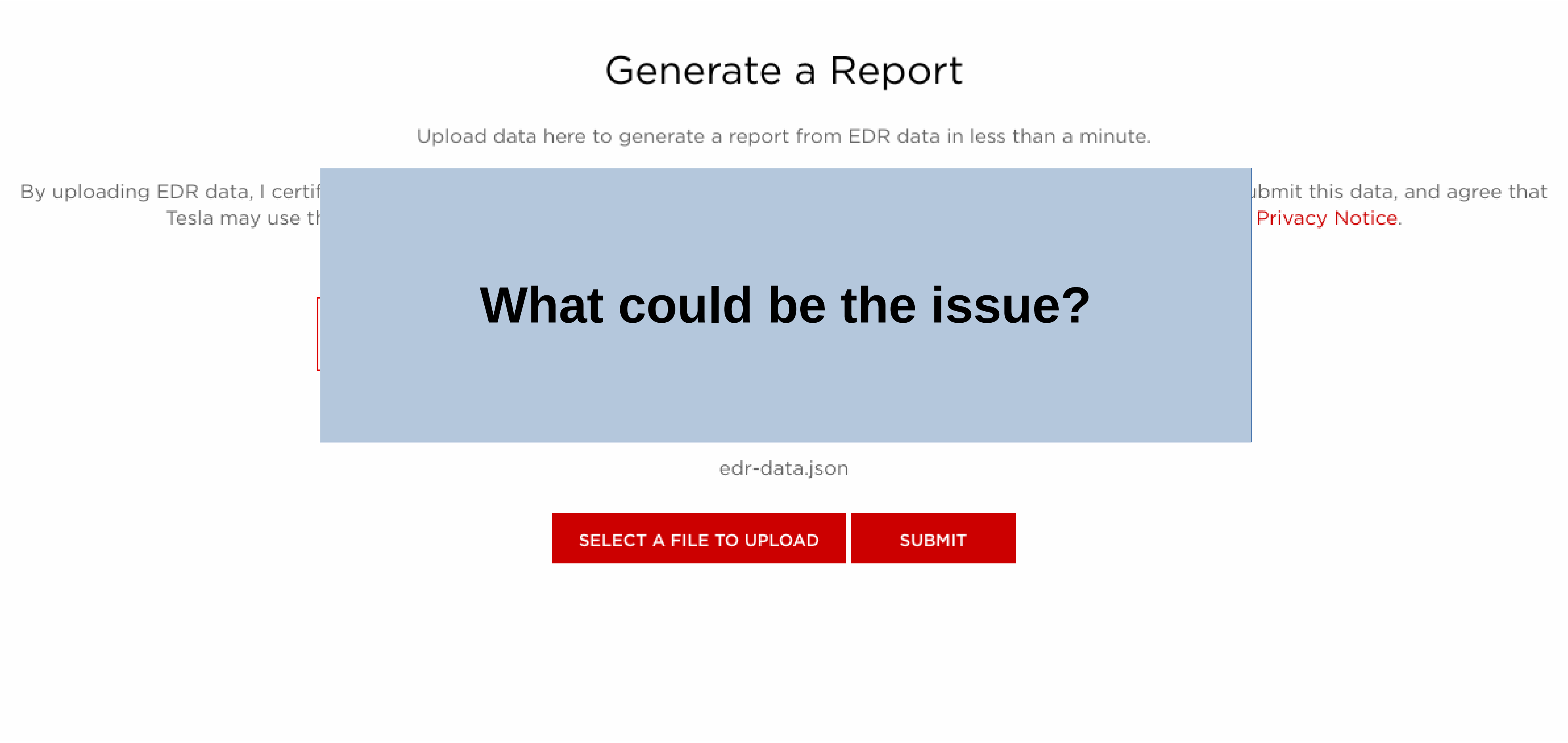
Upload data here to generate a report from EDR data in less than a minute.

By uploading EDR data, I certify that I have the consent of the vehicle owner or leasee or otherwise have lawful authority to submit this data, and agree that Tesla may use the data for analytics, tool improvement, and accidentology research purposes subject to Tesla's Privacy Notice.

Internal error

Current report version: v21.36.1

edr-data.json



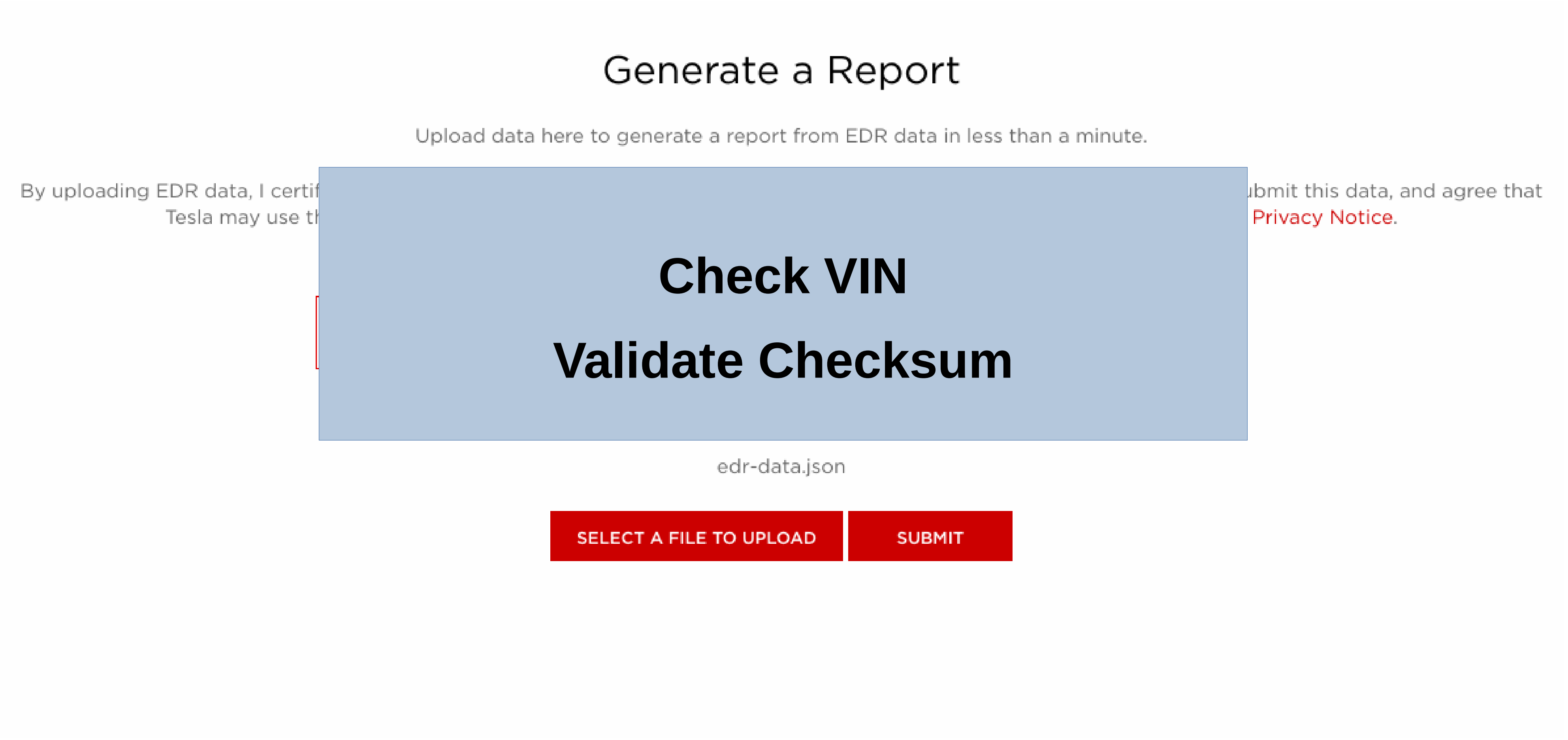
Generate a Report

Upload data here to generate a report from EDR data in less than a minute.

By uploading EDR data, I certif ubmit this data, and agree that
Tesla may use th Privacy Notice.

edr-data.json

What could be the issue?



Generate a Report

Upload data here to generate a report from EDR data in less than a minute.

By uploading EDR data, I certif ubmit this data, and agree that
Tesla may use th Privacy Notice.

edr-data.json

Check VIN

Validate Checksum

We forgot something at the beginning!

We forgot something at the beginning!

Forensic question from stakeholder

Q1 Can you reconstruct events?

Q2 Can you get the report?

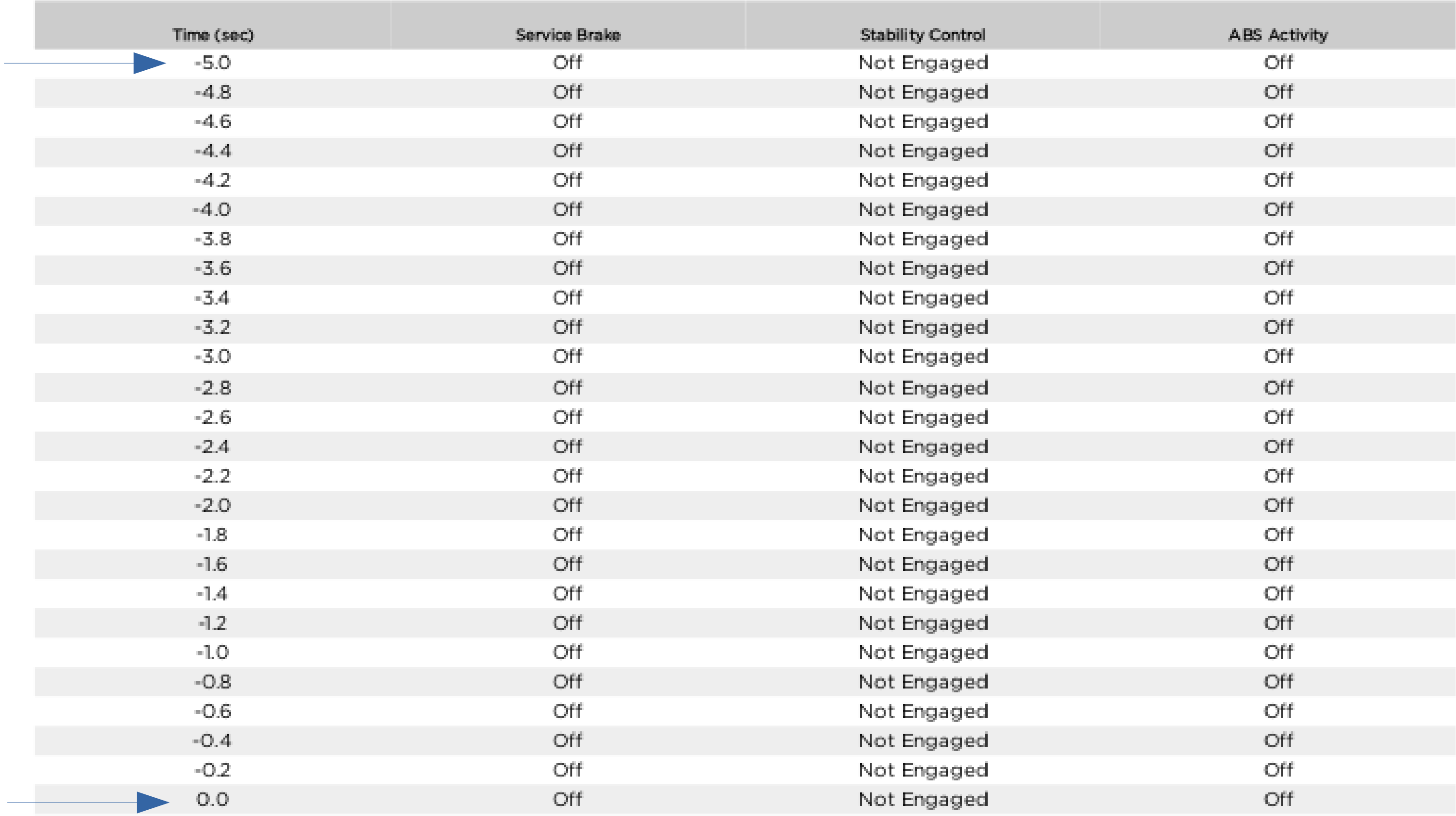
Q3 Did the vehicle accelerate by itself?

Q1 Can you reconstruct events?

✓ **Q2** Can you get the report?

Q3 Did the vehicle accelerate by itself?

before the event



Time (sec)	Service Brake	Stability Control	ABS Activity
-5.0	Off	Not Engaged	Off
-4.8	Off	Not Engaged	Off
-4.6	Off	Not Engaged	Off
-4.4	Off	Not Engaged	Off
-4.2	Off	Not Engaged	Off
-4.0	Off	Not Engaged	Off
-3.8	Off	Not Engaged	Off
-3.6	Off	Not Engaged	Off
-3.4	Off	Not Engaged	Off
-3.2	Off	Not Engaged	Off
-3.0	Off	Not Engaged	Off
-2.8	Off	Not Engaged	Off
-2.6	Off	Not Engaged	Off
-2.4	Off	Not Engaged	Off
-2.2	Off	Not Engaged	Off
-2.0	Off	Not Engaged	Off
-1.8	Off	Not Engaged	Off
-1.6	Off	Not Engaged	Off
-1.4	Off	Not Engaged	Off
-1.2	Off	Not Engaged	Off
-1.0	Off	Not Engaged	Off
-0.8	Off	Not Engaged	Off
-0.6	Off	Not Engaged	Off
-0.4	Off	Not Engaged	Off
-0.2	Off	Not Engaged	Off
0.0	Off	Not Engaged	Off

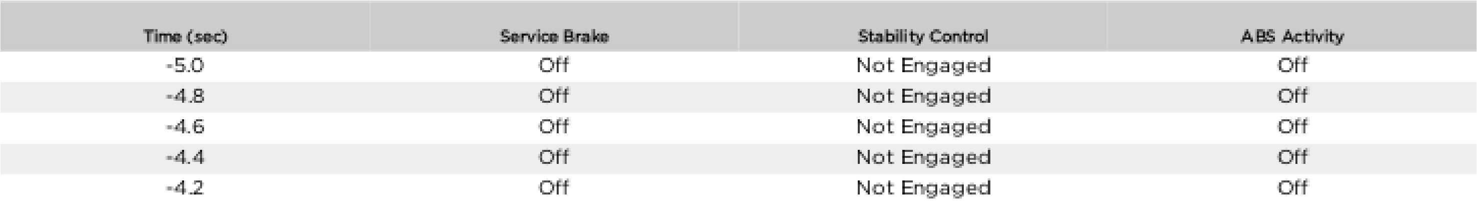
Time of event

Time (sec)	Service Brake	Stability Control	ABS Activity
-5.0	Off	Not Engaged	Off
-4.8	Off	Not Engaged	Off
-4.6	Off	Not Engaged	Off
-4.4	Off	Not Engaged	Off
-4.2	Off	Not Engaged	Off

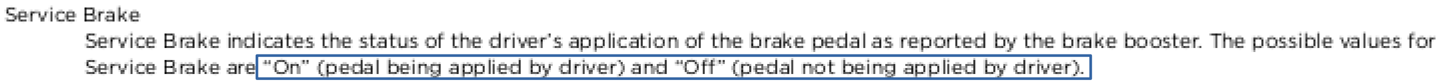
Service Brake

Service Brake indicates the status of the driver's application of the brake pedal as reported by the brake booster. The possible values for Service Brake are "On" (pedal being applied by driver) and "Off" (pedal not being applied by driver).

-1.2	Off	Not Engaged	Off
-1.0	Off	Not Engaged	Off
-0.8	Off	Not Engaged	Off
-0.6	Off	Not Engaged	Off
-0.4	Off	Not Engaged	Off
-0.2	Off	Not Engaged	Off
0.0	Off	Not Engaged	Off

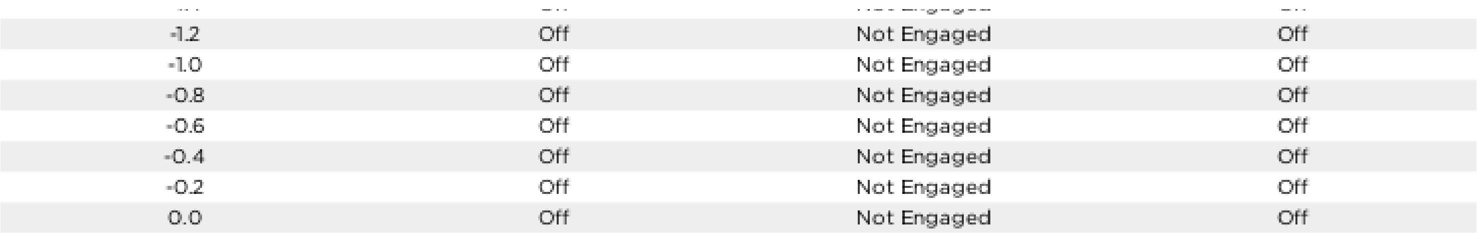


Time (sec)	Service Brake	Stability Control	ABS Activity
-5.0	Off	Not Engaged	Off
-4.8	Off	Not Engaged	Off
-4.6	Off	Not Engaged	Off
-4.4	Off	Not Engaged	Off
-4.2	Off	Not Engaged	Off

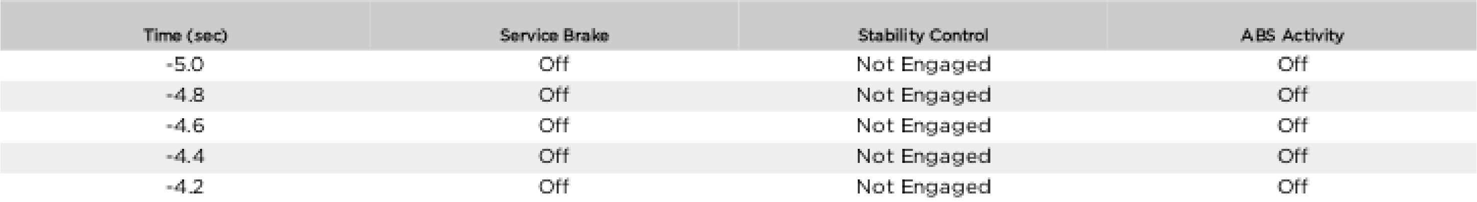


Service Brake

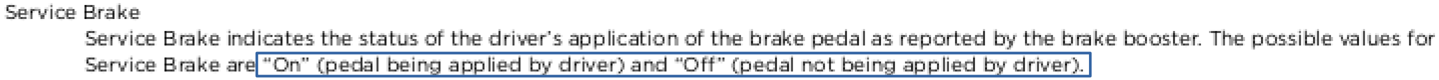
Service Brake indicates the status of the driver's application of the brake pedal as reported by the brake booster. The possible values for Service Brake are "On" (pedal being applied by driver) and "Off" (pedal not being applied by driver).



-1.2	Off	Not Engaged	Off
-1.0	Off	Not Engaged	Off
-0.8	Off	Not Engaged	Off
-0.6	Off	Not Engaged	Off
-0.4	Off	Not Engaged	Off
-0.2	Off	Not Engaged	Off
0.0	Off	Not Engaged	Off

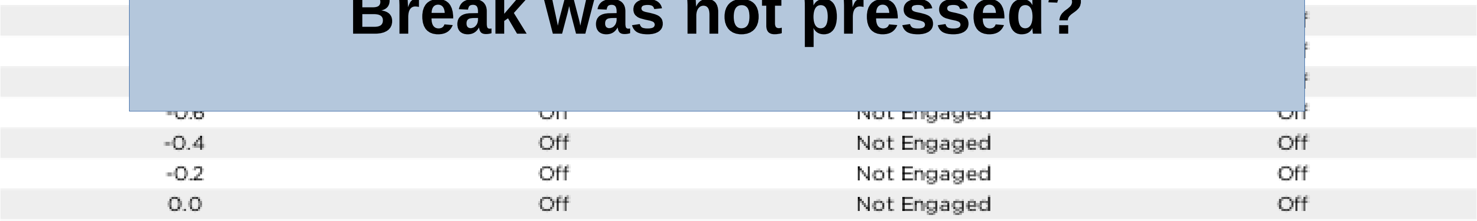


Time (sec)	Service Brake	Stability Control	ABS Activity
-5.0	Off	Not Engaged	Off
-4.8	Off	Not Engaged	Off
-4.6	Off	Not Engaged	Off
-4.4	Off	Not Engaged	Off
-4.2	Off	Not Engaged	Off



Service Brake

Service Brake indicates the status of the driver's application of the brake pedal as reported by the brake booster. The possible values for Service Brake are "On" (pedal being applied by driver) and "Off" (pedal not being applied by driver).



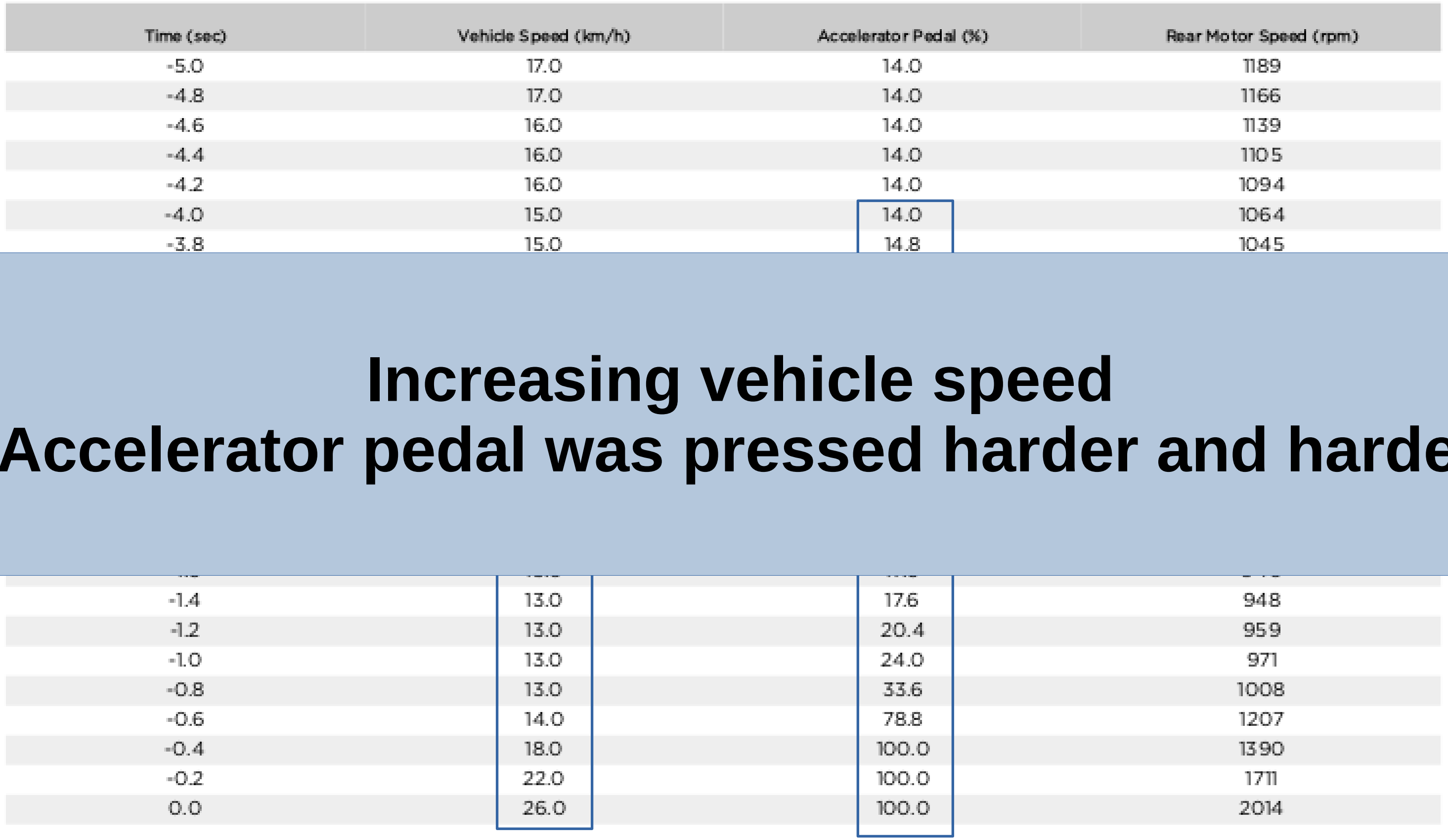
-0.6	Off	Not Engaged	Off
-0.4	Off	Not Engaged	Off
-0.2	Off	Not Engaged	Off
0.0	Off	Not Engaged	Off

Break was not pressed?

Time (sec)	Vehicle Speed (km/h)	Accelerator Pedal (%)	Rear Motor Speed (rpm)
-5.0	17.0	14.0	1189
-4.8	17.0	14.0	1166
-4.6	16.0	14.0	1139
-4.4	16.0	14.0	1105
-4.2	16.0	14.0	1094
-4.0	15.0	14.0	1064
-3.8	15.0	14.8	1045
-3.6	15.0	15.6	1026
-3.4	15.0	16.8	1014
-3.2	14.0	16.8	1005
-3.0	14.0	16.8	994
-2.8	14.0	16.8	992
-2.6	14.0	17.6	971
-2.4	14.0	17.2	977
-2.2	14.0	17.6	953
-2.0	14.0	17.6	950
-1.8	14.0	17.6	951
-1.6	13.0	17.6	940
-1.4	13.0	17.6	948
-1.2	13.0	20.4	959
-1.0	13.0	24.0	971
-0.8	13.0	33.6	1008
-0.6	14.0	78.8	1207
-0.4	18.0	100.0	1390
-0.2	22.0	100.0	1711
0.0	26.0	100.0	2014

Time (sec)	Vehicle Speed (km/h)	Accelerator Pedal (%)	Rear Motor Speed (rpm)
-5.0	17.0	14.0	1189
-4.8	17.0	14.0	1166
-4.6	16.0	14.0	1139
-4.4	16.0	14.0	1105
-4.2	16.0	14.0	1094
-4.0	15.0	14.0	1064
-3.8	15.0	14.8	1045
-3.6	15.0	15.6	1026
-3.4	15.0	16.8	1014
-3.2	14.0	16.8	1005
-3.0	14.0	16.8	994
-2.8	14.0	16.8	992
-2.6	14.0	17.6	971
-2.4	14.0	17.2	977
-2.2	14.0	17.6	953
-2.0	14.0	17.6	950
-1.8	14.0	17.6	951
-1.6	13.0	17.6	940
-1.4	13.0	17.6	948
-1.2	13.0	20.4	959
-1.0	13.0	24.0	971
-0.8	13.0	33.6	1008
-0.6	14.0	78.8	1207
-0.4	18.0	100.0	1390
-0.2	22.0	100.0	1711
0.0	26.0	100.0	2014

Time (sec)	Vehicle Speed (km/h)	Accelerator Pedal (%)	Rear Motor Speed (rpm)
-5.0	17.0	14.0	1189
-4.8	17.0	14.0	1166
-4.6	16.0	14.0	1139
-4.4	16.0	14.0	1105
-4.2	16.0	14.0	1094
-4.0	15.0	14.0	1064
-3.8	15.0	14.8	1045
-3.6	15.0	15.6	1026
-3.4	15.0	16.8	1014
-3.2	14.0	16.8	1005
-3.0	14.0	16.8	994
-2.8	14.0	16.8	992
-2.6	14.0	17.6	971
-2.4	14.0	17.2	977
-2.2	14.0	17.6	953
-2.0	14.0	17.6	950
-1.8	14.0	17.6	951
-1.6	13.0	17.6	940
-1.4	13.0	17.6	948
-1.2	13.0	20.4	959
-1.0	13.0	24.0	971
-0.8	13.0	33.6	1008
-0.6	14.0	78.8	1207
-0.4	18.0	100.0	1390
-0.2	22.0	100.0	1711
0.0	26.0	100.0	2014



Time (sec)	Vehicle Speed (km/h)	Accelerator Pedal (%)	Rear Motor Speed (rpm)
-5.0	17.0	14.0	1189
-4.8	17.0	14.0	1166
-4.6	16.0	14.0	1139
-4.4	16.0	14.0	1105
-4.2	16.0	14.0	1094
-4.0	15.0	14.0	1064
-3.8	15.0	14.8	1045
[illegible]	[illegible]	[illegible]	[illegible]
-1.4	13.0	17.6	948
-1.2	13.0	20.4	959
-1.0	13.0	24.0	971
-0.8	13.0	33.6	1008
-0.6	14.0	78.8	1207
-0.4	18.0	100.0	1390
-0.2	22.0	100.0	1711
0.0	26.0	100.0	2014

Increasing vehicle speed

Accelerator pedal was pressed harder and harder

- Break was not pressed
- Vehicle speed was increased
- Accelerator pedal was pressed harder and harder

What could have happened?

✓ **Q1** Can you reconstruct events?

✓ **Q2** Can you get the report?

Q3 Did the vehicle accelerate by itself?

- ✓ **Q1** Can you reconstruct events?
- ✓ **Q2** Can you get the report?
- ? **Q3** Did the vehicle accelerate by itself?

Autopilot enabled?

✓ **Q1** Can you reconstruct events?

✓ **Q2** Can you get the report?

? **Q3** Did the vehicle accelerate by itself?

Autopilot enabled? → **No access to autopilot logs**

Open Questions

- EDR Data **trustworthy**?

Open Questions

- EDR Data **trustworthy**?
- **Access** to evidence not given

Open Questions

- EDR Data **trustworthy**?
- **Access** to evidence not given
- **No correlation** of different data-sources

Open Questions

- EDR Data **trustworthy**?
- **Access** to evidence not given
- **No correlation** of different data-sources
- **No validation** of data-sources possible

We need changes and new proposals!

- **Generalized** approaches
- **Correlation** of events
- **Normalized** data
- New and better **tools**
- View **vehicle + ecosystem** as a whole