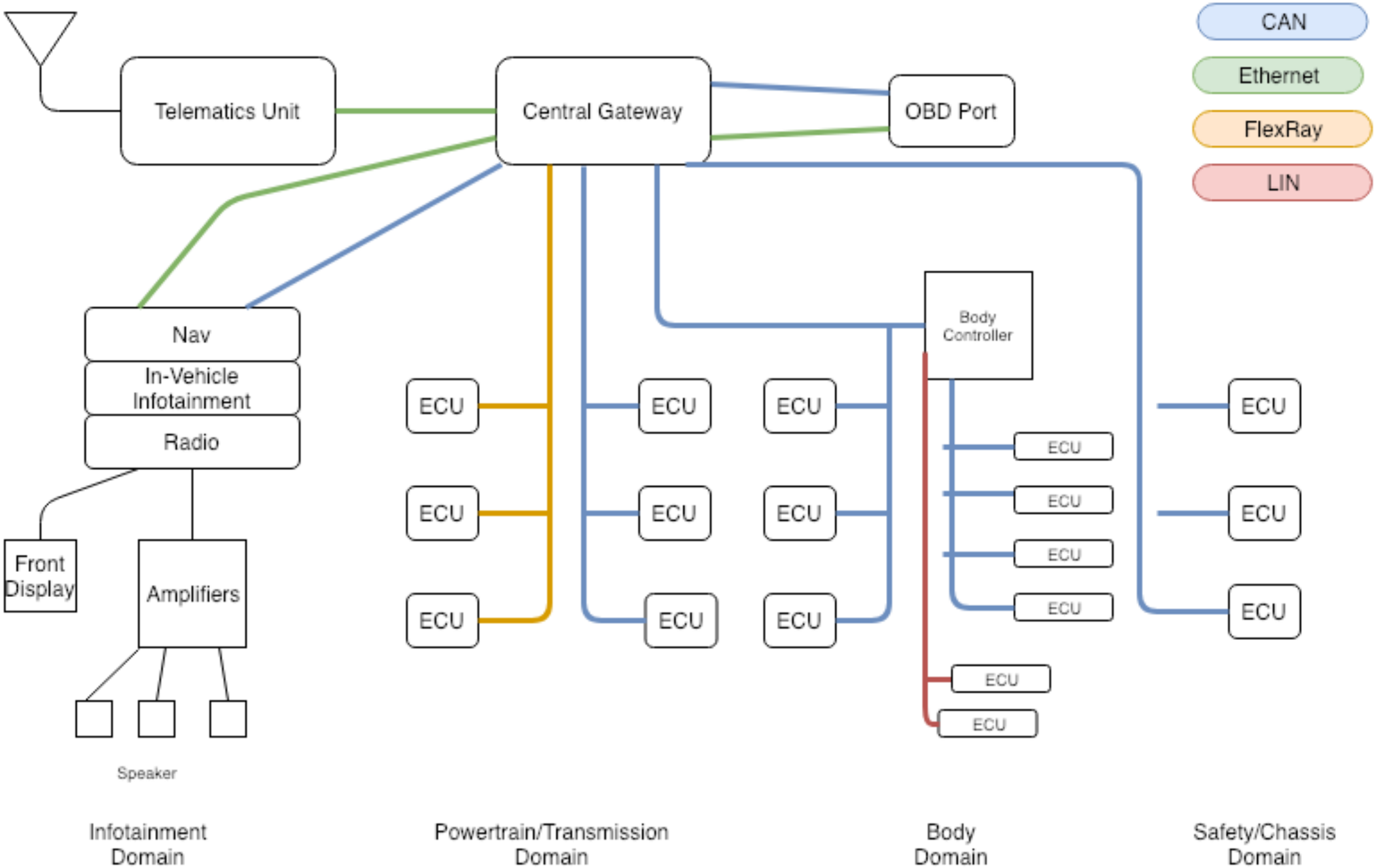
https://secvi.inet.haw-hamburg.de/

Anomaly Detection im Fahrzeugnetzwerk

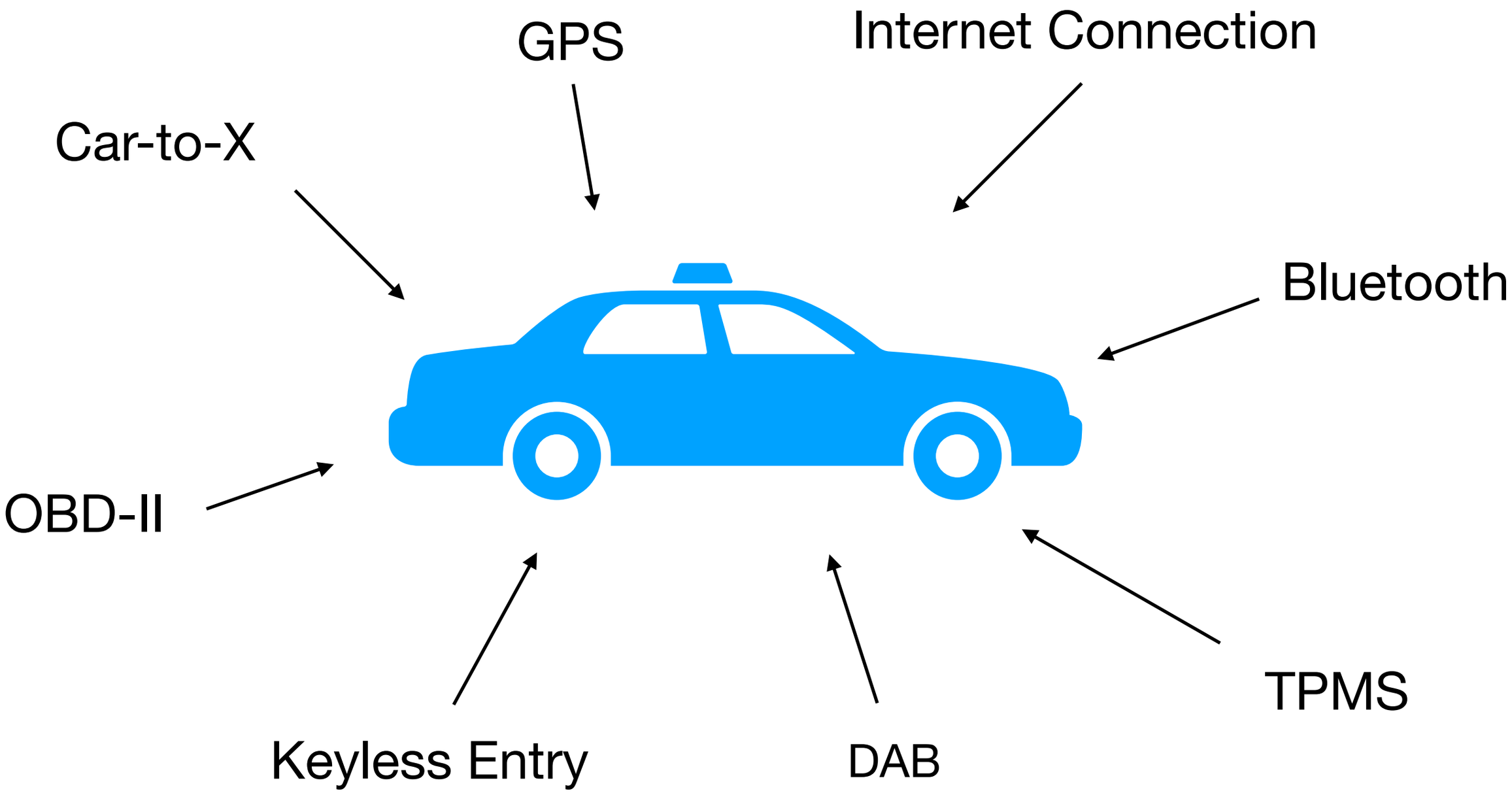
Hauptseminar Vortrag von Wilhelm Schumacher, gehalten am 6.12.2019 im Rahmen des Master Informatik an der HAW Hamburg

Im Grundseminar…



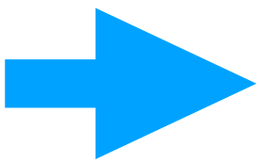
Erstellt auf Basis von https://www.iot-now.com/2017/02/27/59018-securing-automotive-air-updates

Attack Surface



Aktuelle Bedrohungen

- Viele neue Funktionen im **intelligenten** Auto möglich
- Kein abgeschottetes Netzwerk mehr
- Angreifbar durch externe Interfaces
- Neue Sicherheitskonzepte notwendig

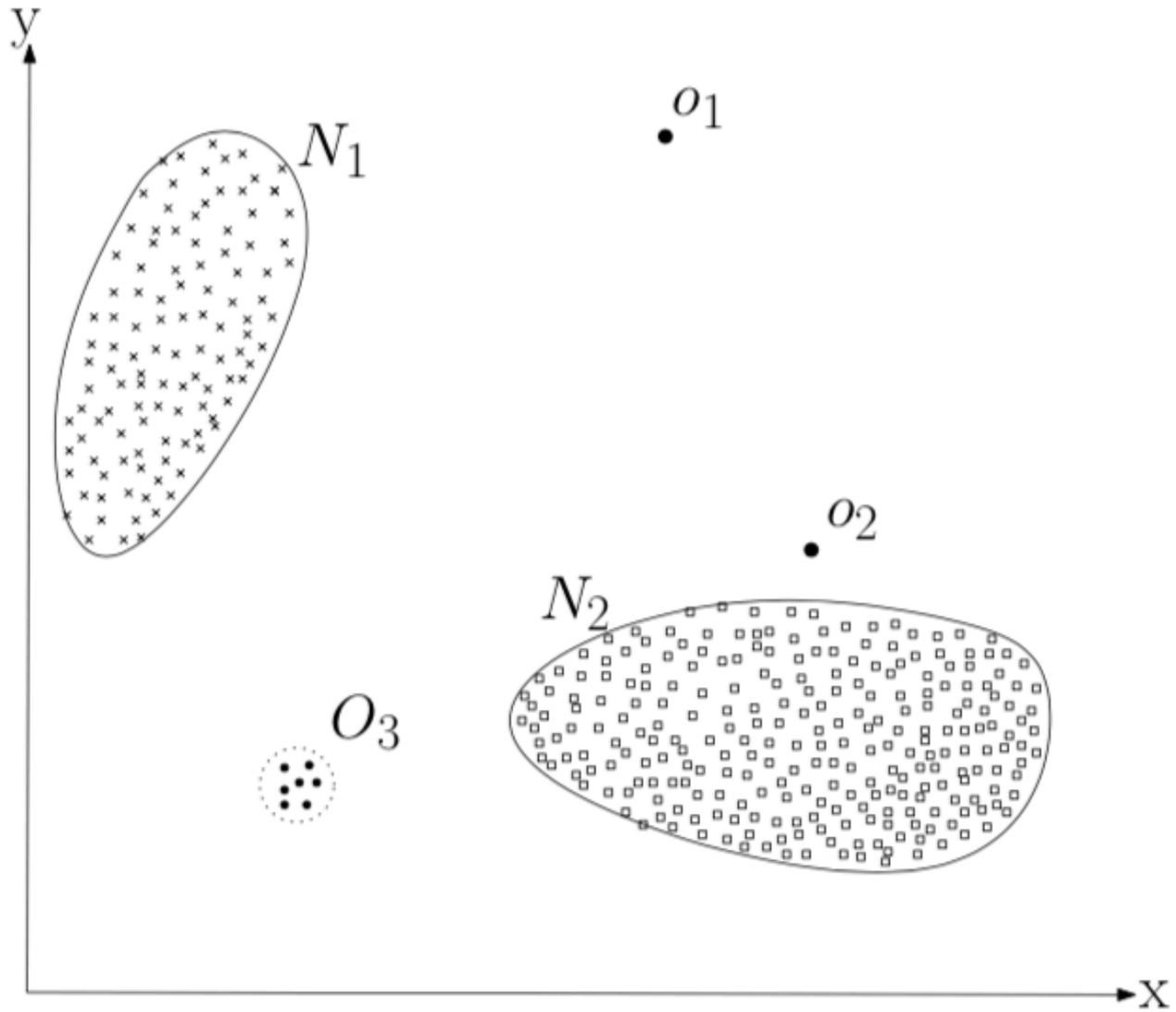


Schwerpunkt: Anomaly Detection im Fahrzeug

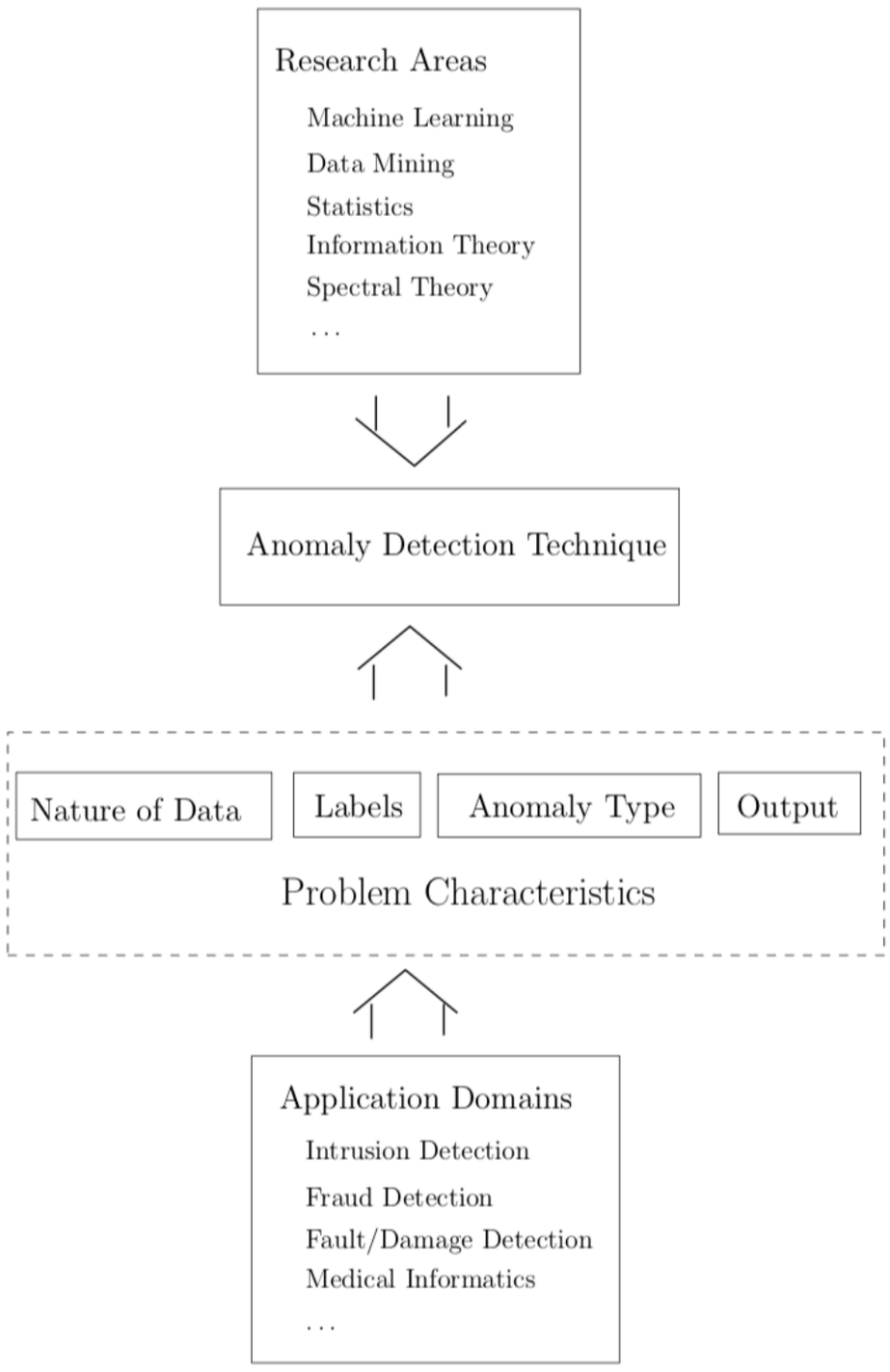
Agenda

1. Rückblick Grundseminar
2. Anomaly Detection im automotiven Umfeld
3. Methoden der Anomaly Detection
4. Grundprojekt: RecBarToZones Simulation
5. Ausblick

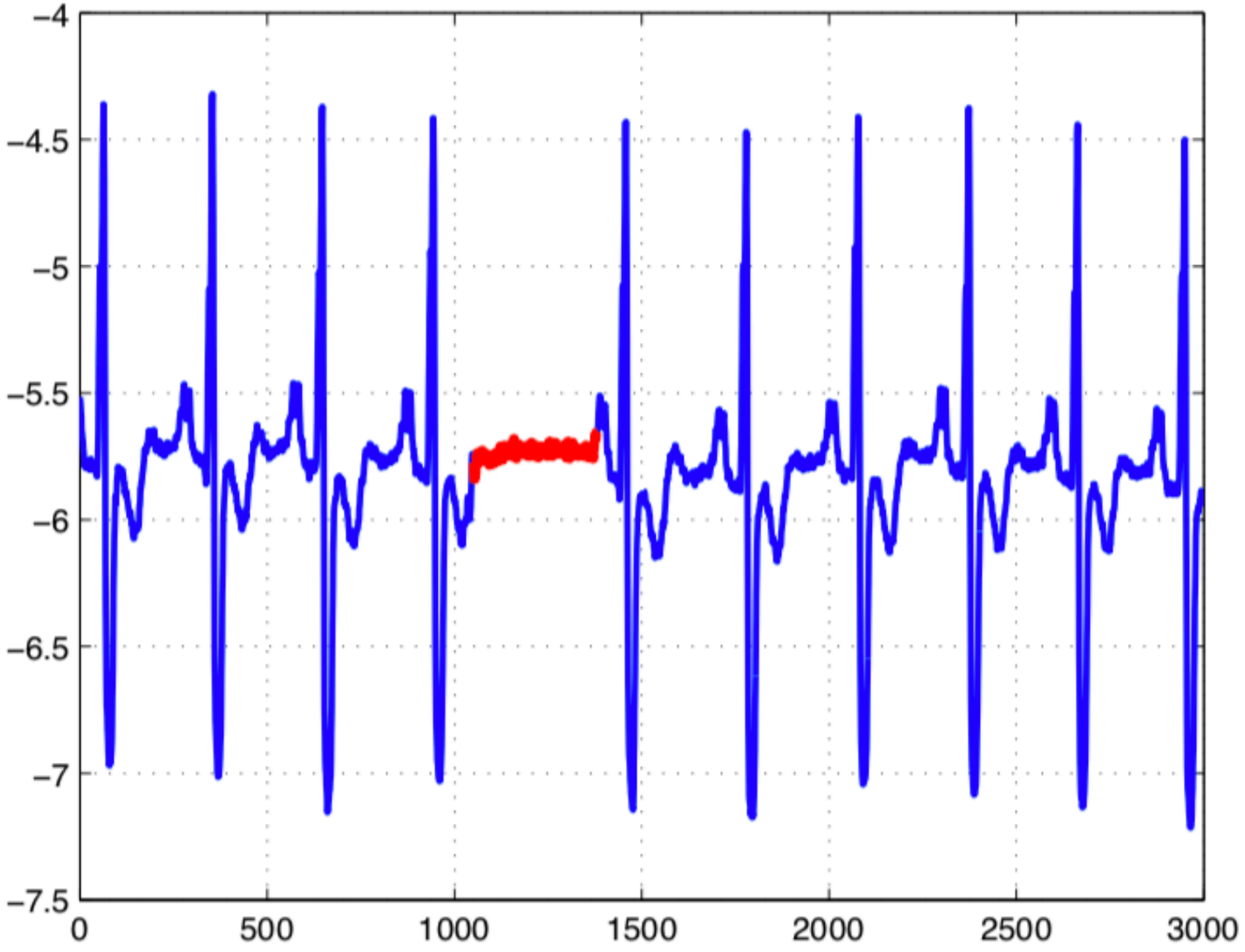
Anomaly Detection



https://dl.acm.org/citation.cfm?id=1541882 [6]



http://doi.acm.org/10.1145/1541880.15418822 [5]



http://doi.acm.org/10.1145/1541880.15418822 [5]

Kontext Fahrzeug

- Viele Verfahren in anderen Domänen bereits erfolgreich im Einsatz
- Das Fahrzeug ist ein sicherheitskritisches System
- Stellt nur eine Ebene des Sicherheitssystems dar
- Reguläre Updates sind schwierig bereitzustellen

Herausforderungen

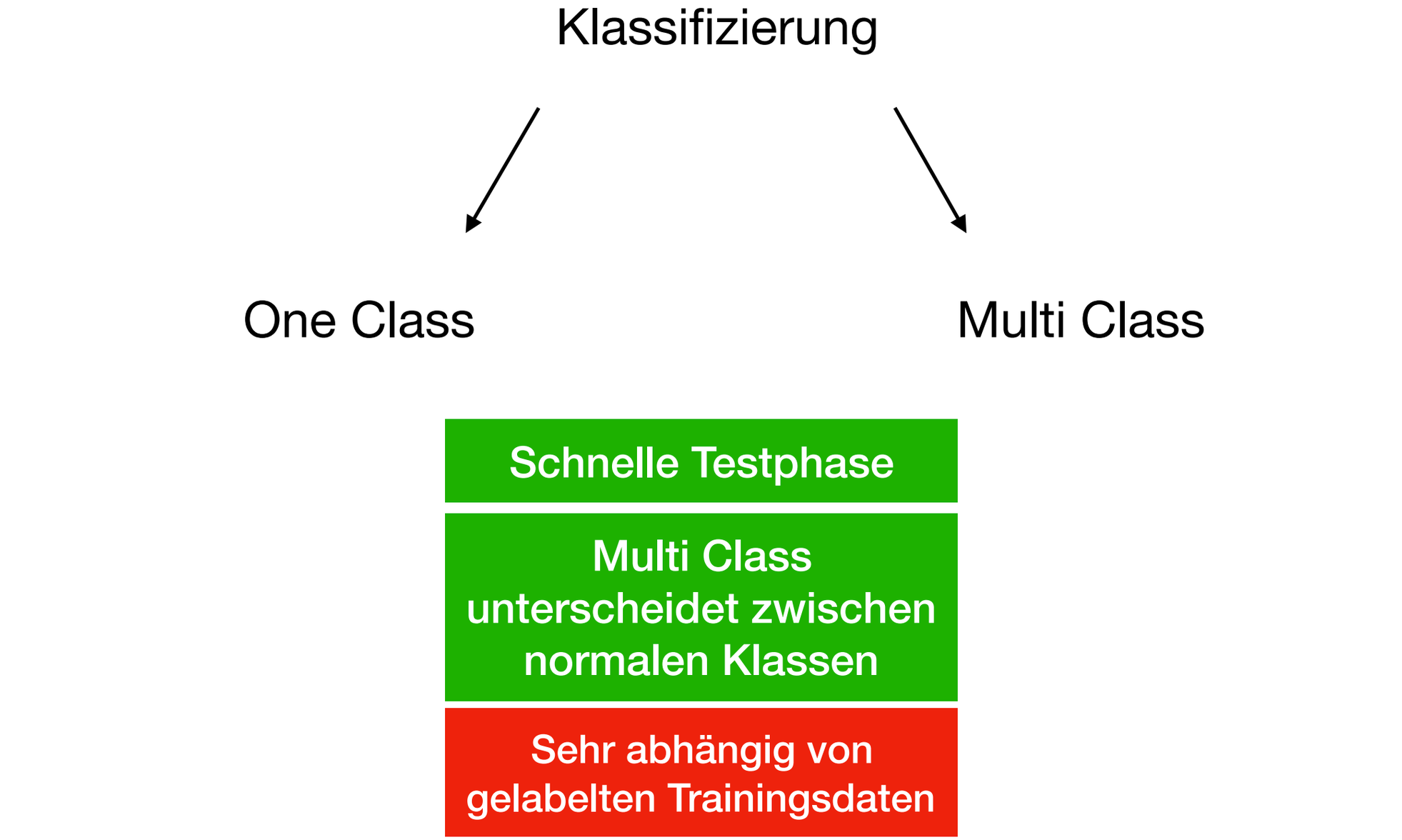
- Signature-based Detection hat große Nachteile
- Richtige Auswahl der Daten
- Intelligenz der Sensoren
- Echtzeitanforderungen
- Benachrichtigungen und Reaktionen

Methoden

Bhuyan et al.: Network Anomaly Detection: Methods, Systems and Tools	Chandola et al.: Anomaly Detection : A Survey	Anomaly-based network intrusion detection: Techniques, systems and challenges
1. Statistical	1. Statistical	1. Statistical
2. Classification Based	2. Classification Based	2. Machine Learning Based
3. Clustering and Outlier Based	3. Clustering Based	3. Knowledge Based
4. Soft Computing	4. Nearest Neighbor Based	-
5. Knowledge Based	5. Information Theoretic	-
6. Combination Learners	6. Spectral	-

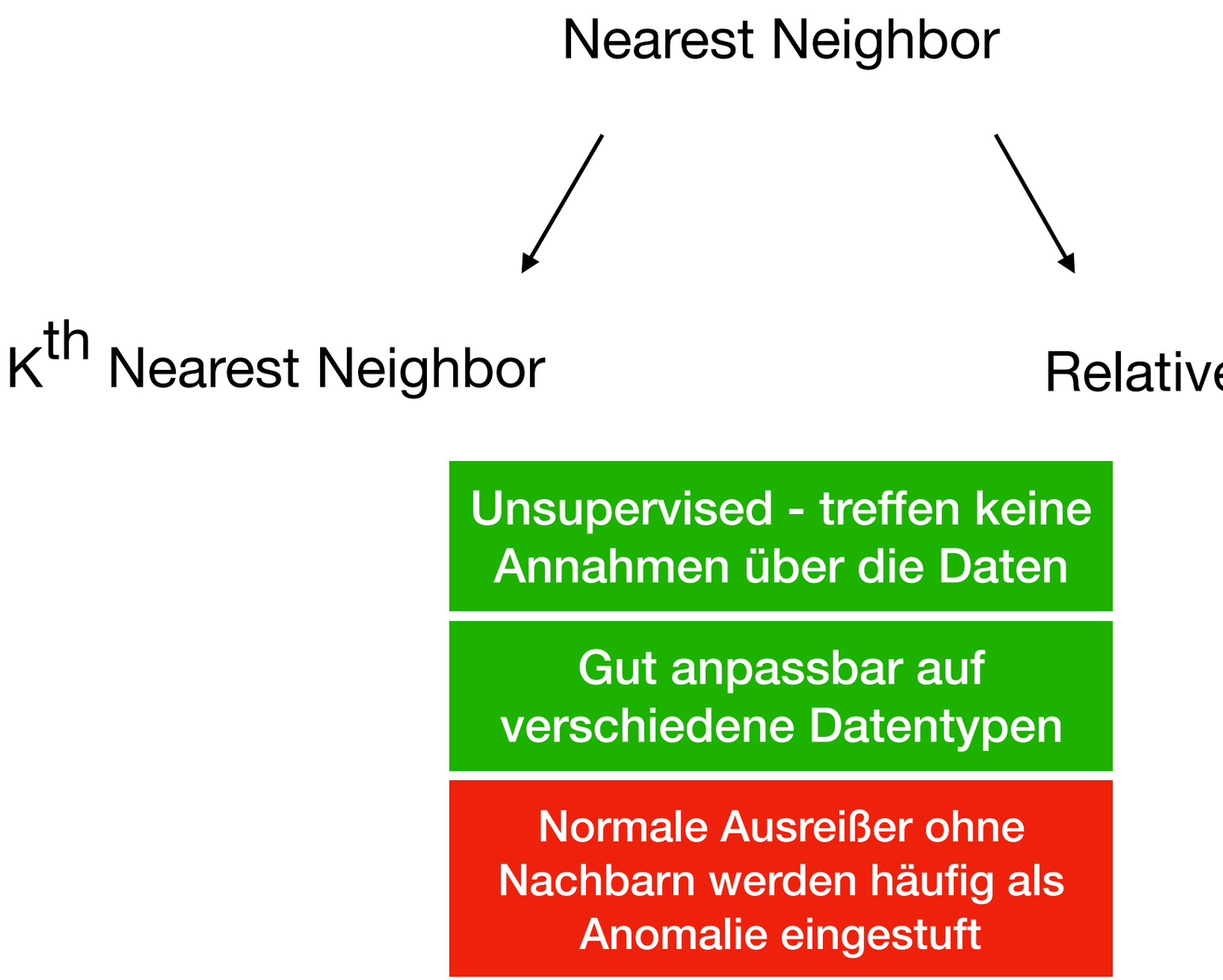
Tabelle 1 zeigt beispielhaft Kategorien in die Algorithmen/Methoden zur Anomalieerkennung eingeordnet werden können.

1. Klassifizierung

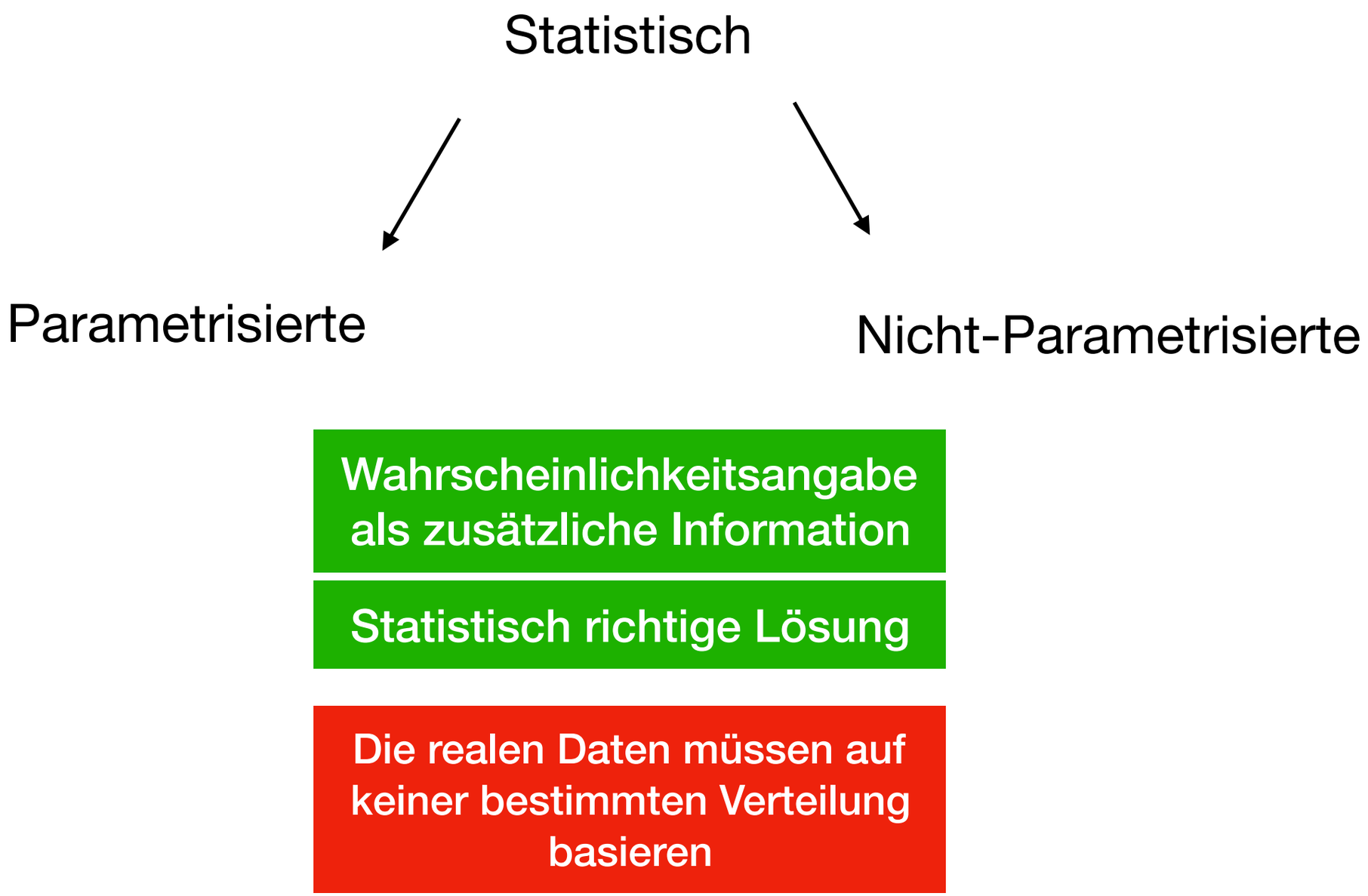


z.B. SVM, Neuronales Netz

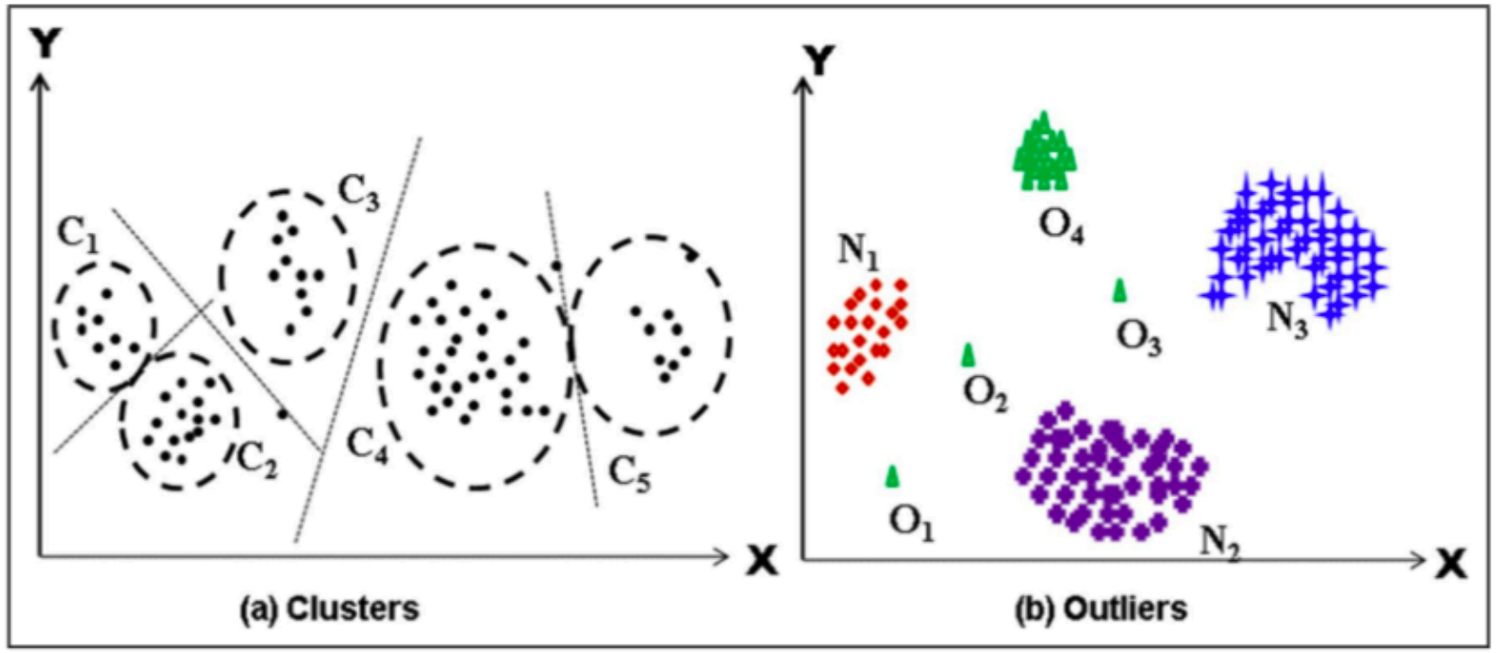
2. Nearest Neighbor



3. Statistisch



4. Clustering



https://ieeexplore.ieee.org/document/6524462 [5]

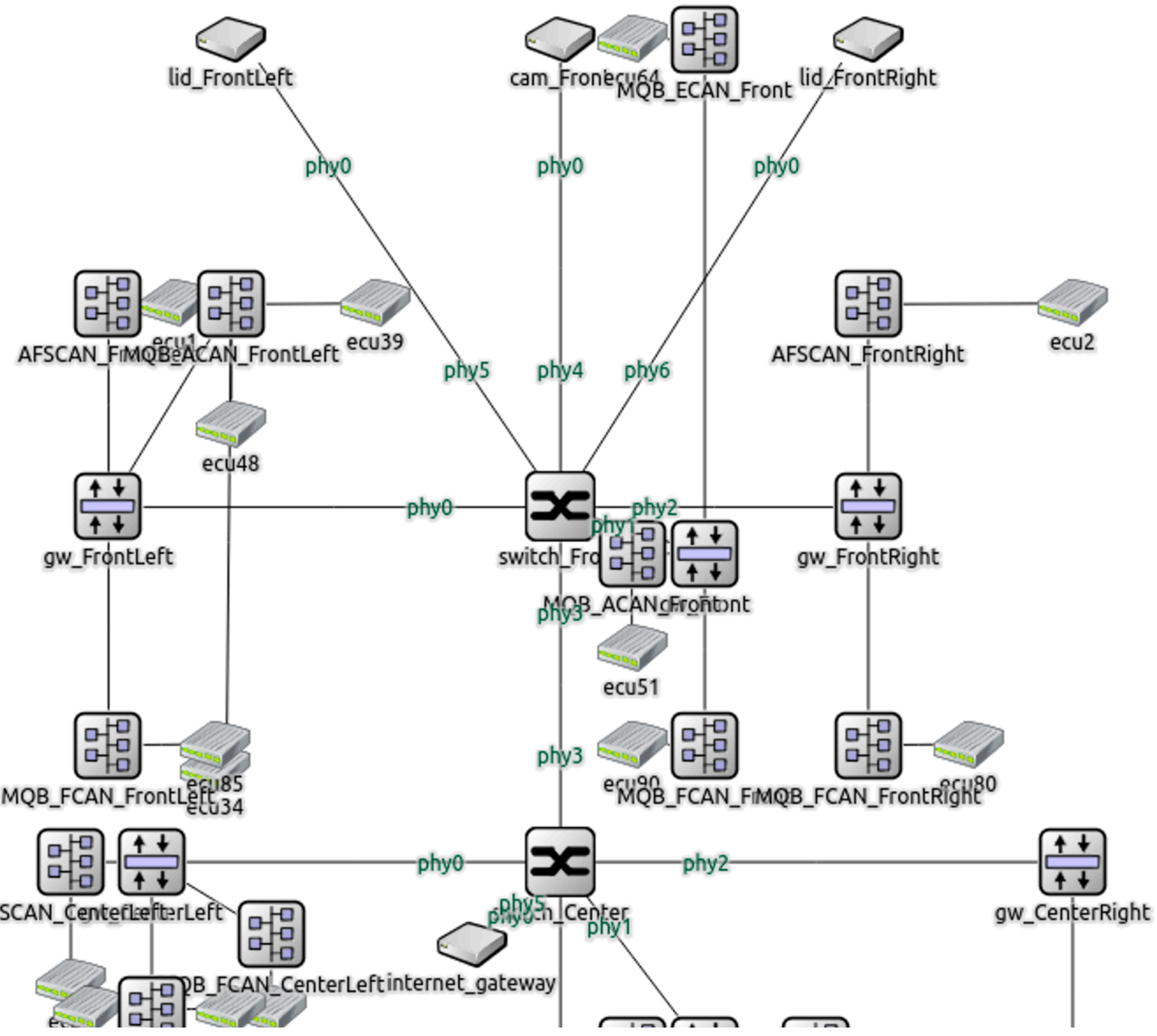
Einfache Clusterbildung wenn die Anzahl bekannt ist

Anomalien können auch ein Cluster bilden

z.B. k-Means, Mean shift

Grundprojekt

- Simulation OMNeT++ (Objective Modular Network Testbed in C++)
- Abbildung einer realen Kommunikationsmatrix
- Weiterleitung an Python Applikation
- Ziel: Vergleich von Algorithmen



Ausschnitt aus dem RecBarToZones Netzwerk

Simulationsparameter

- Metriken: Bandbreite, Paketgröße, durchschnittlicher Paketabstand, Jitter
- Algorithmen: SVM, Isolation Forest, k-Means, Mean shift, Histogram-based Outlier Detection, Elliptic Envelope
- Unterschiedliche Trainingszeiten und Trainingsintervalle
- Attacken: Increased Frequency, Message Flooding, Inaccuracy of Period, Port Scan

Ausblick

- Mehr Forschung mit simulierten Daten als Daten aus der echten Welt
- Safety weniger beachtet als Security
- Neue Methoden werden oft nicht gegen eine Basis verglichen
- Hauptprojekt: Tischaufbau mit echter Hardware
- Masterarbeit: Prototyp eines Fahrzeuges

Quellen

- [1] https://secvi.inet.haw-hamburg.de/
- [2] A structured approach to anomaly detection for in-vehicle networks: - https://ieeexplore.ieee.org/abstract/document/5604050
- [3] A Distributed Anomaly Detection System for In-Vehicle Network Using HTM: - https://ieeexplore.ieee.org/abstract/document/8274979
- [4] A Survey of Anomaly Detection for Connected Vehicle Cybersecurity and Safety: - https://ieeexplore.ieee.org/abstract/document/8500383
- [5] Network Anomaly Detection: Methods, Systems and Tools: - https://ieeexplore.ieee.org/document/6524462/
- [6] Anomaly detection: A survey: - https://dl.acm.org/citation.cfm?id=1541882
- [7] Anomaly-based network intrusion detection: Techniques, systems and challenges: - https://www.sciencedirect.com/science/article/pii/S0167404808000692
- [8] Comprehensive Experimental Analyses of Automotive Attack Surfaces: - http://www.autosec.org/pubs/cars-usenixsec2011.pdf

Vielen Dank für die Aufmerksamkeit