Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Decentralized Anomaly Detection with unused Computing Power in Avionic and Automotive Applications

DEGGENDORF INSTITUTE OF TECHNOLOGY

Prof. Dr.- Ing. Andreas Grzemba

Deggendorf Institute of Technology

- Founded in 1994
- 8 Faculties
- 7000 Students
- 20 % International
- 99 Nationalities
- 142 Professors
- 500 Staff

DIT & Cyber Security

- Education
  - Bachelor Cyber Security
  - Extra-occupational Master Cyber Security
- Applied Research
  - Institute ProtectIT
- Consulting
  - Spin-off ProtectEM GmbH

Decentralized Anomaly Detection with unused Computing Power in Avionic and Automotive Applications

Agenda

- Architecture
- Generic Detection / Reaction System
- Incident Detection Algorithms

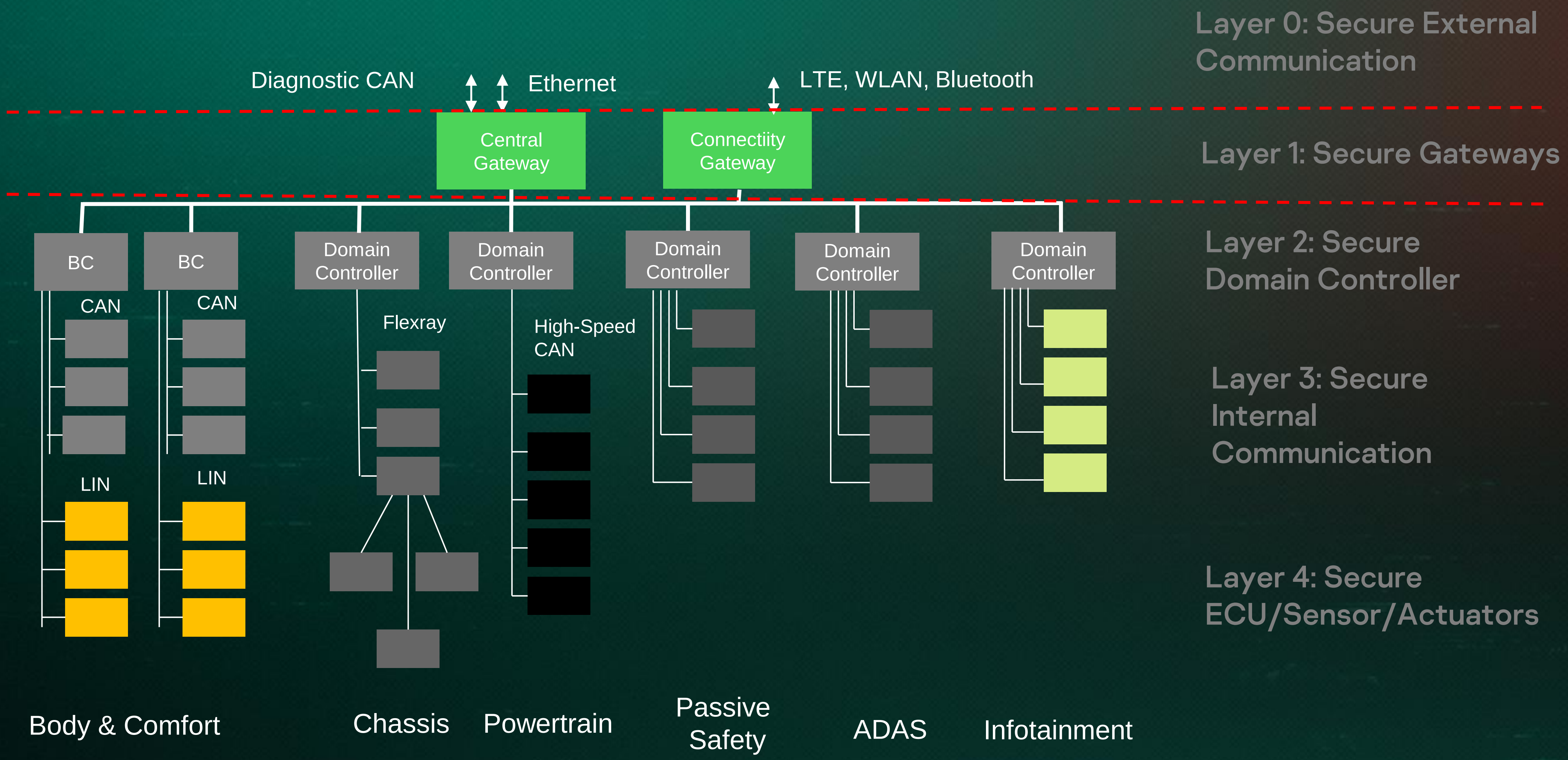
Joint Research Project between Universities and Industry

Architecture	Privacy	Generic Detection Reaction Center	Automotive Detection Reaction Center	Algorithmic

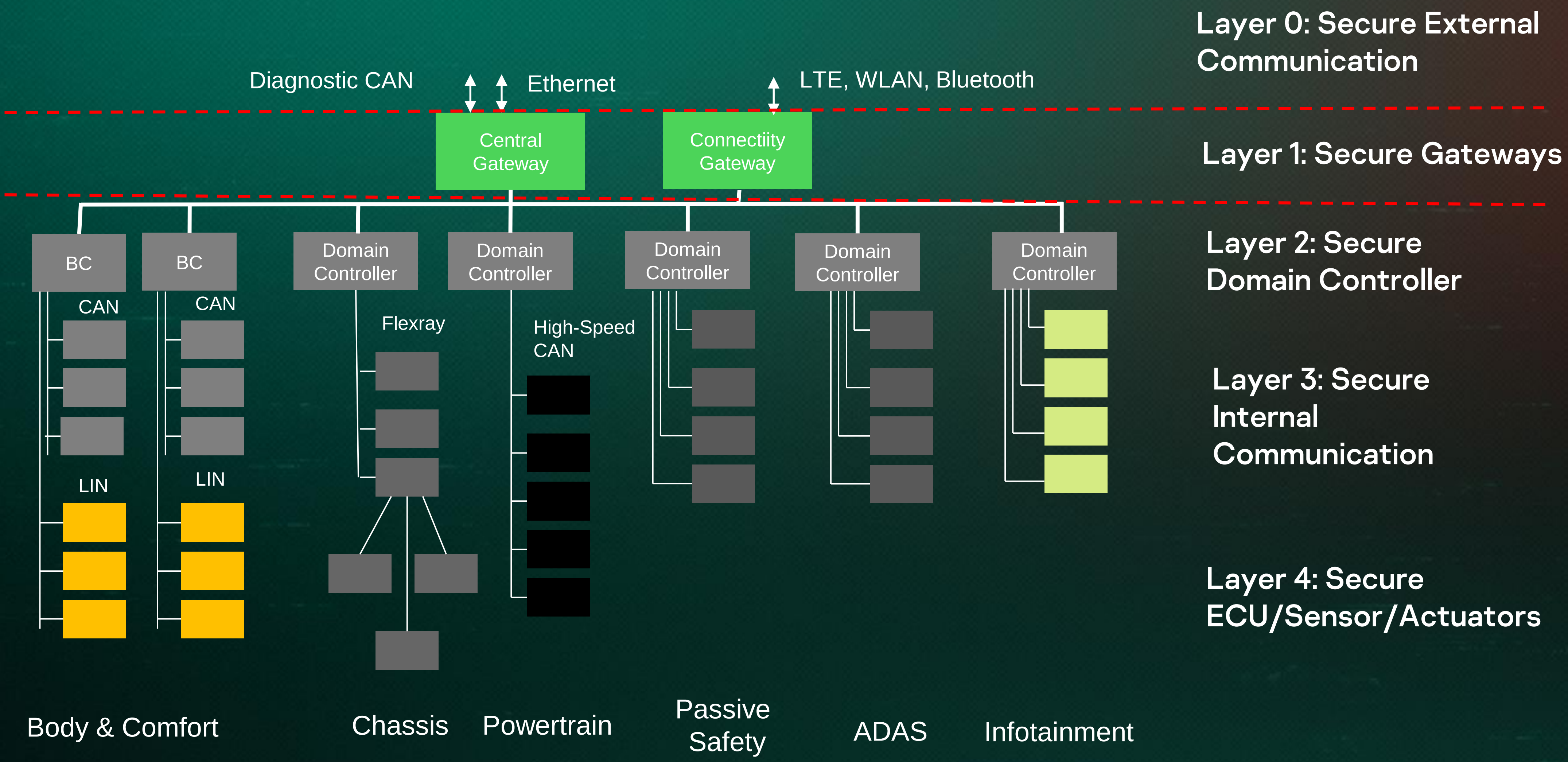
Issue :

Electronic architectures of aircraft and automotive are complex

Automotive Communication Architecture

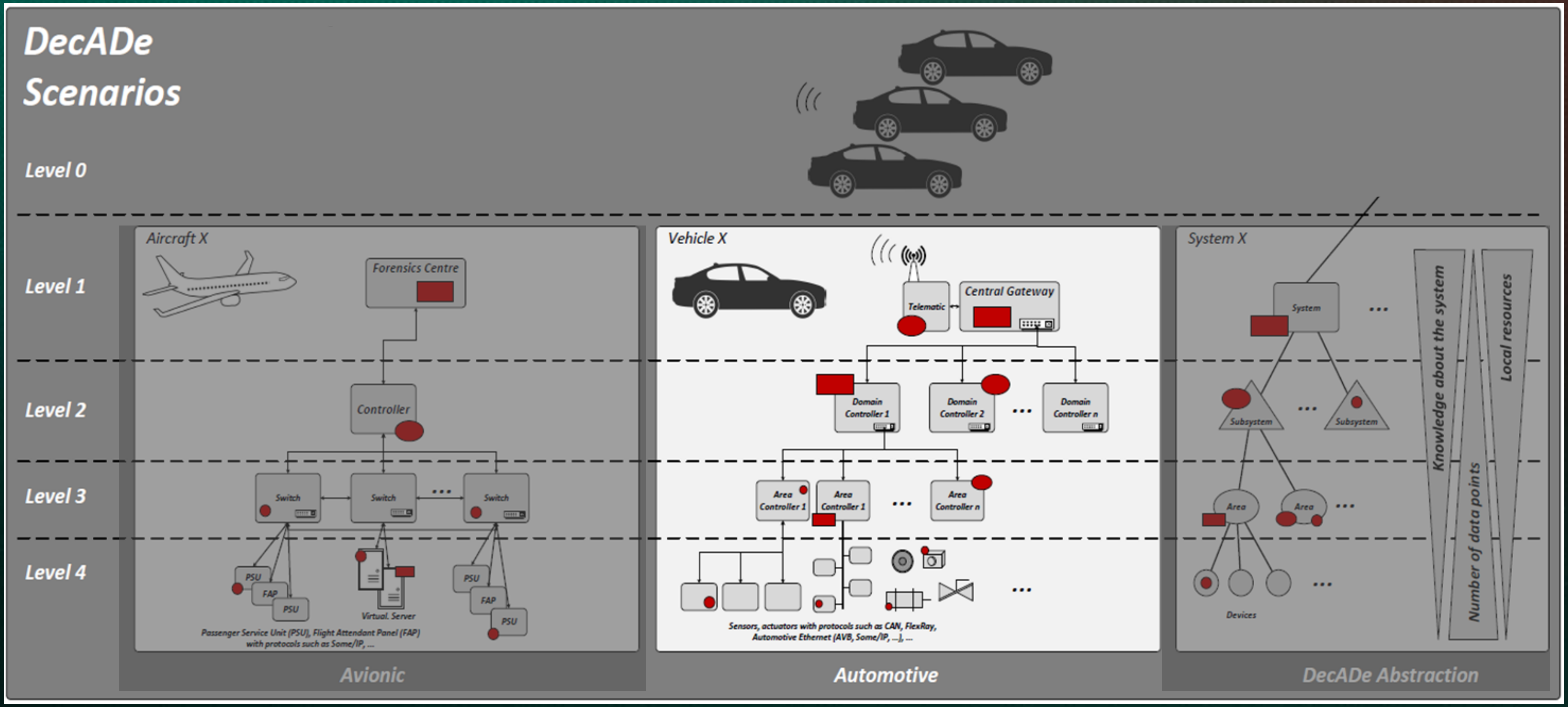


Automotive Communication Architecture

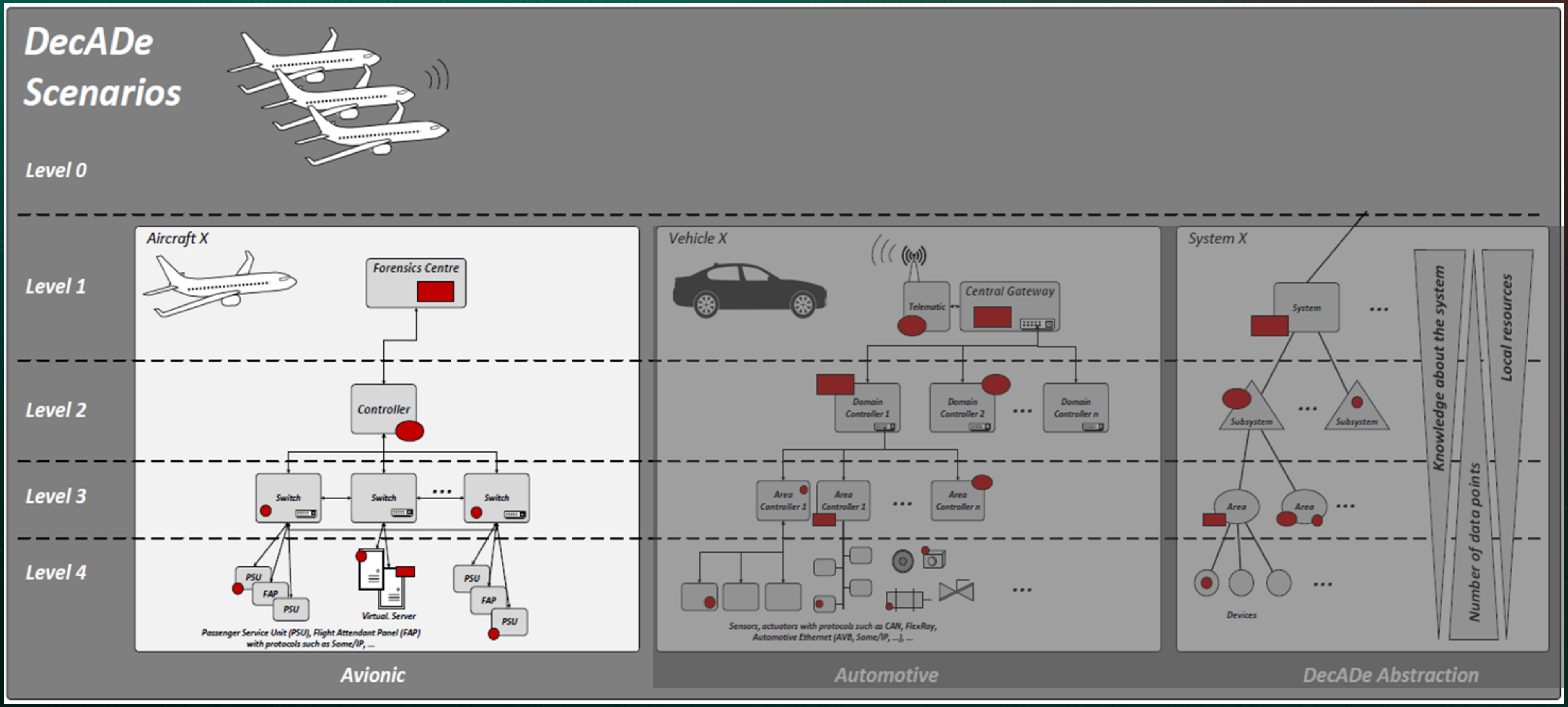


Kaspersky Industrial Cybersecurity Conference 2019 – Prof. Dr.-Ing. Andreas Grzemba; Deggendorf Institute of Technology

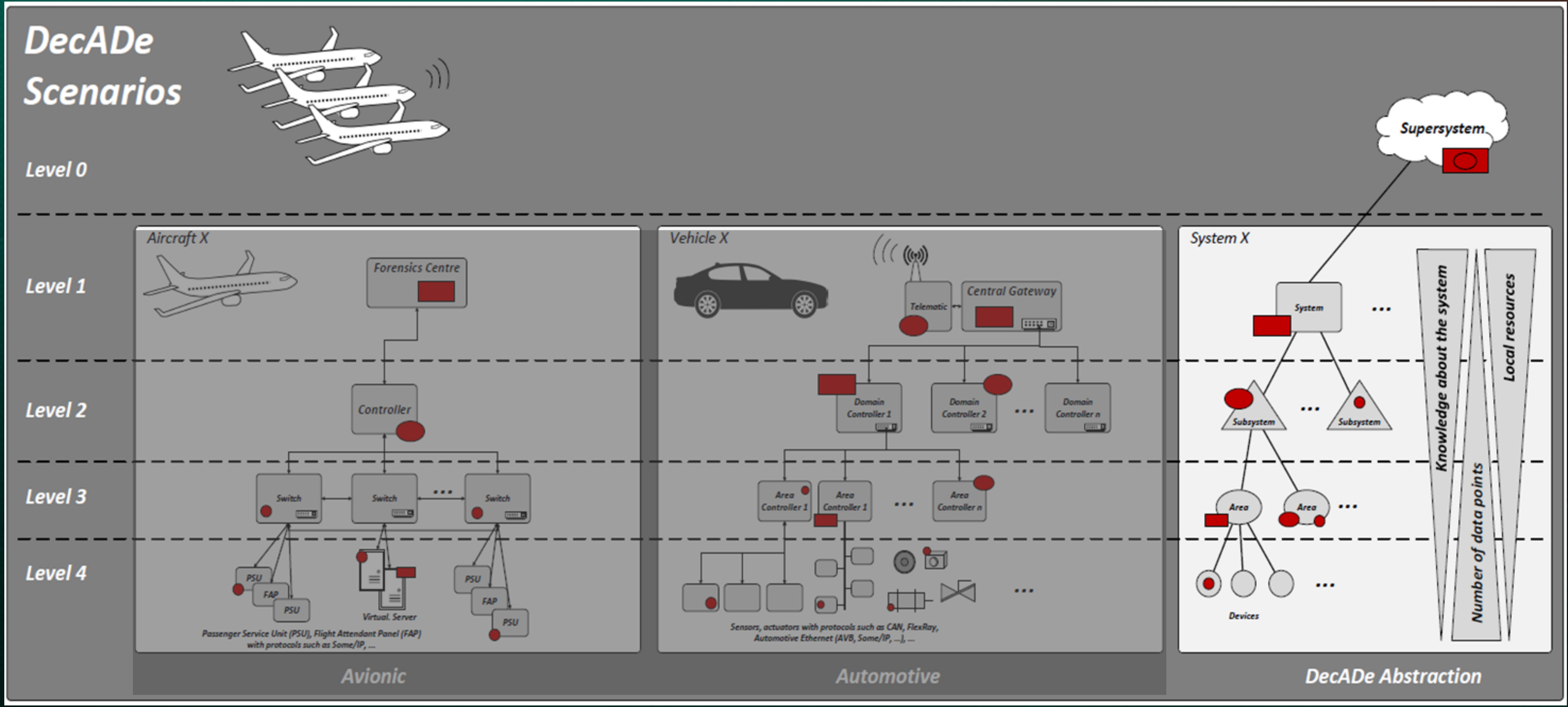
Generic Architecture



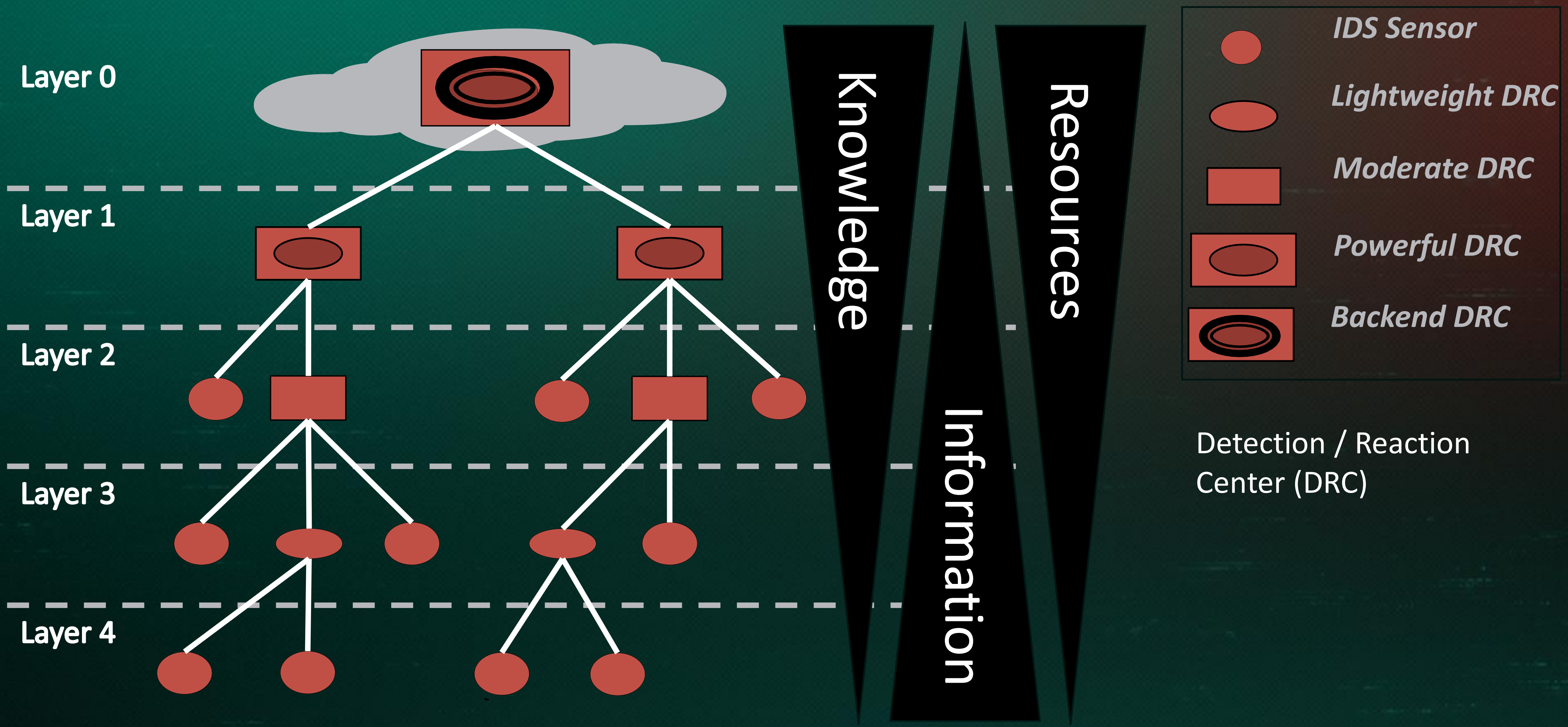
Generic Architecture



Generic Architecture

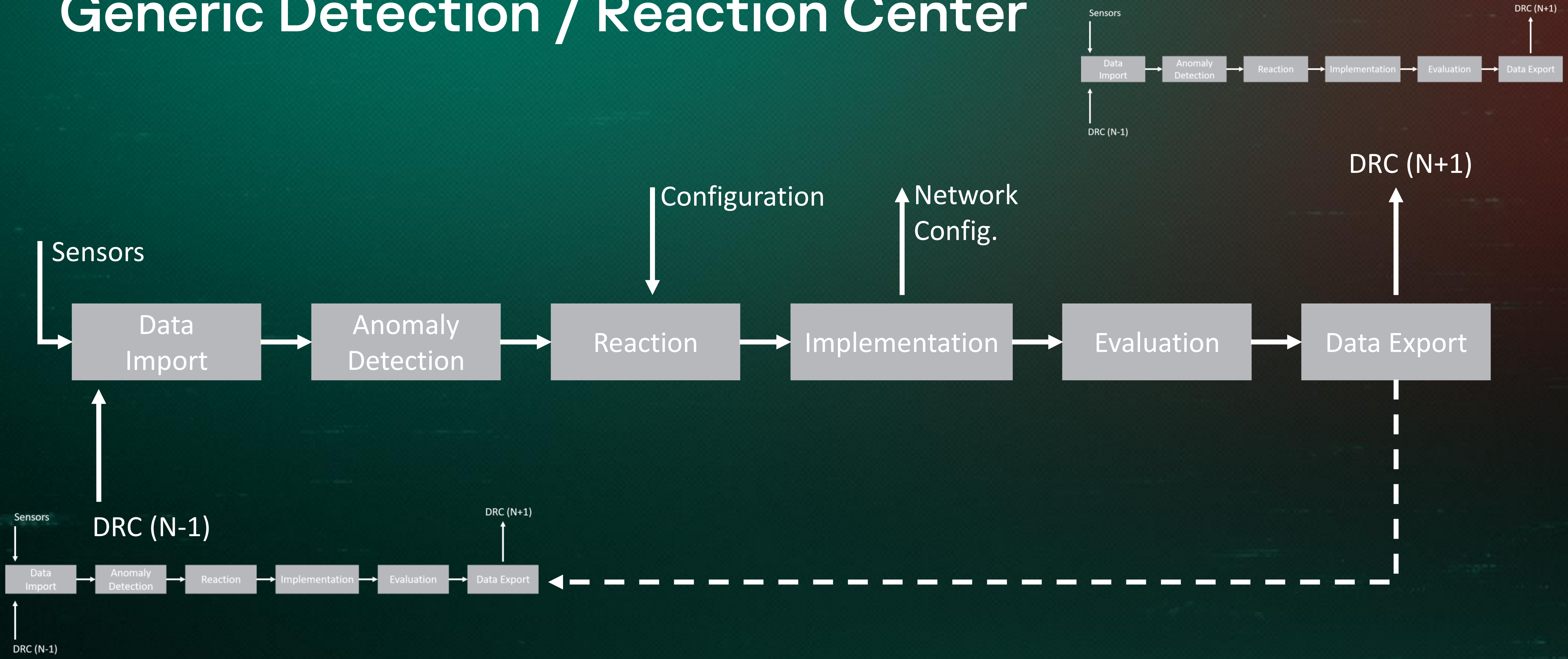


Hierarchic Detection / Reaction System



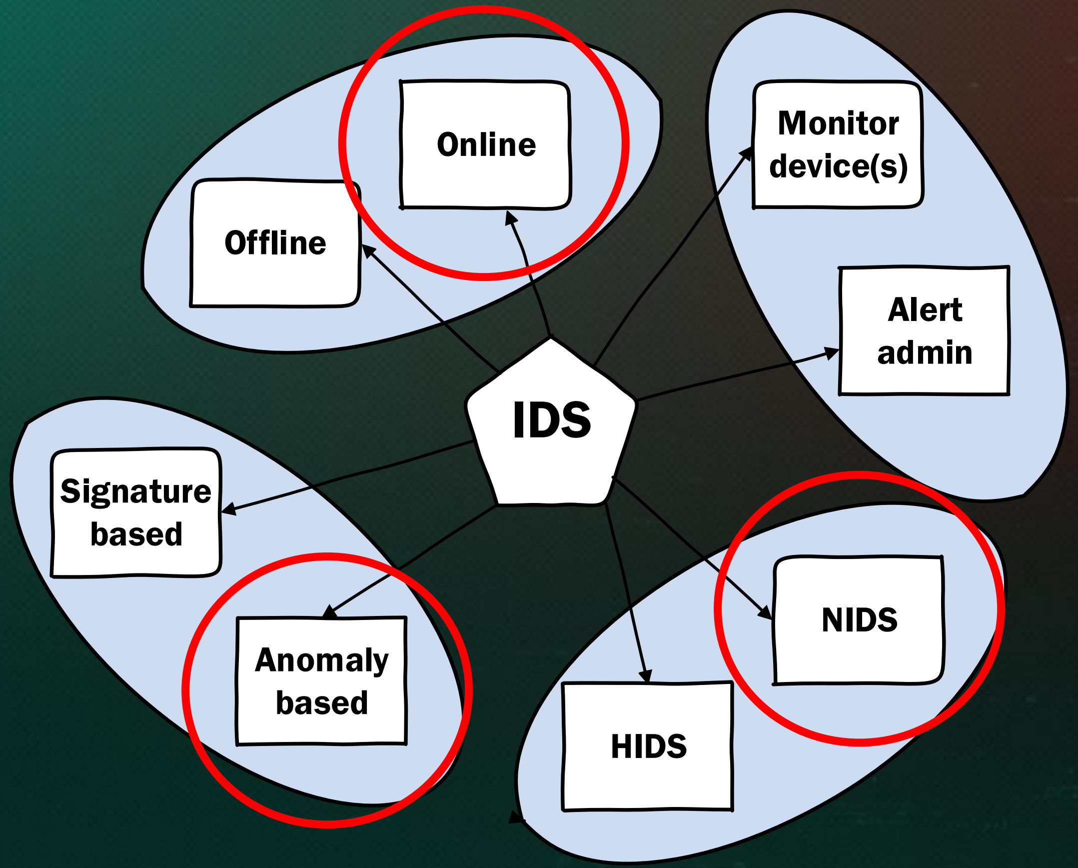
Detection / Reaction Center (DRC)

Generic Detection / Reaction Center



Incident Detection

Multiple Suitable Algorithms



Incident Detection Algorithms

Many possibilities

- Data sets, feature sets, model
- Supervised, semi-supervised, unsupervised anomaly detection
- Rule-based systems
- Logistic regression
- Neural networks
- (One class) support vector machines

Evaluated approaches:

- Variational Autoencoder (Neural network)
  - Detection of anomalies in respect of the trained data based on classification
  - Issue: theoretical infinite anomlies possible; not resource efficient

Our approach: Outlier Detection with Machine Learning

Incident Detection Algorithms

A lot of possibilities

- Data sets, feature sets, model
- Supervised, semi-supervised, unsupervised anomaly detection
- Rule-based systems
- Logistic regression
- Neural networks
- (One class) support vector machines

Evaluated approaches:

- Variational Autoencoder (Neural network)
  - Detection of anomalies in respect of the trained data based on classification
  - Issue: theoretical infinite anomlies possible; not resource efficient

Our approach: Outlier Detection with Machine Learning

Incident Detection Algorithms

A lot of possibilities

- Data sets, feature sets, model
- Supervised, semi-supervised, unsupervised anomaly detection
- Rule-based systems
- Logistic regression
- Neural networks
- (One class) support vector machines

Evaluated approaches:

- Variational Autoencoder (Neural network)
  - Detection of anomalies in respect of the trained data based on classification
  - Issue: theoretical infinite anomlies possible; not resource efficient

Our approach: Outlier Detection with Machine Learning

Incident Detection

Anomaly Detection with Machine Learning

Selection: **Isolation Forest** and **Loda** outlier detection algorithms

Properties for anomaly detection in network communication:

- Operation without knowledge of data labels
- Possibility of online (real-time) detection
- Detection of previously unknown, distributed and advanced attacks
- Detection of point and context anomalies
- Scalable, flexible and resource-preserving (Training, Classification) in use

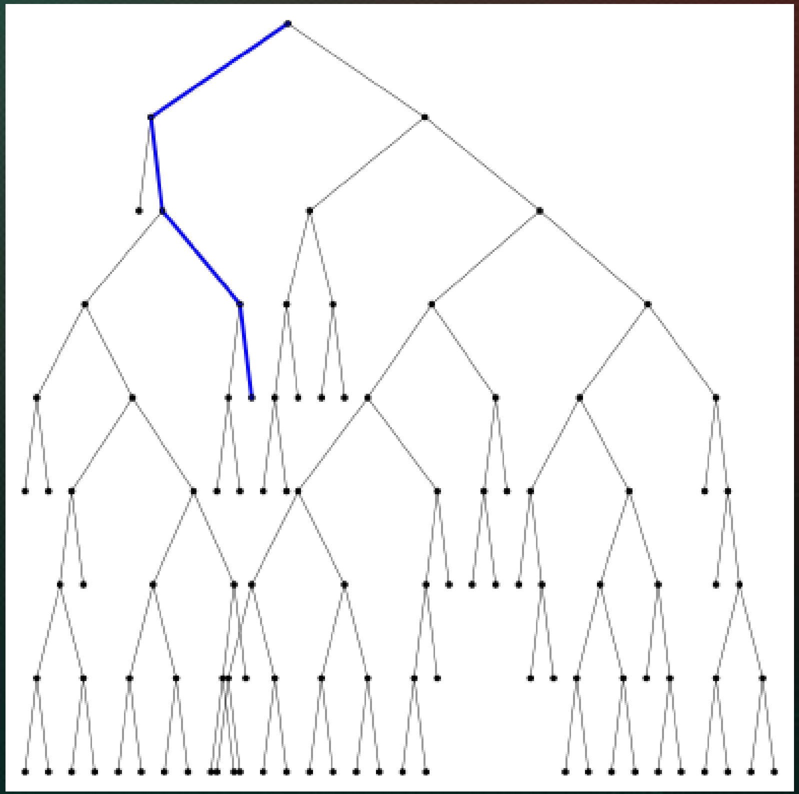
Isolation Forest

Data is separated in smaller subsets

iForest consists of iTrees, that are generated by the subsets

Process of training (modelling)

- Nodes of the binary tree have attributes ***q*** and ***p***
- ***q*** is a randomly chosen feature of the data set
- ***p*** is a randomly chosen separation point (between min. and max.)
- ***p*** < ***q*** → left node
- ***p*** > ***q*** → right node



Testing the model

- Path length provides information about normality / abnormality
- A anomaly score is calculated for a data set, that runs through all iTrees

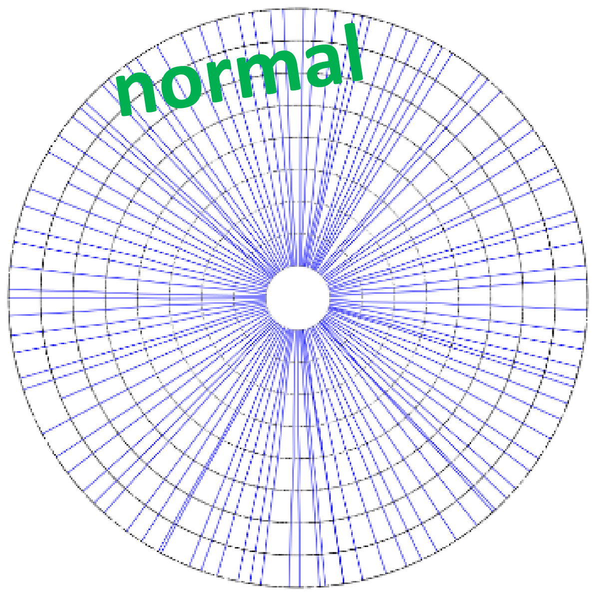
Isolation Forest

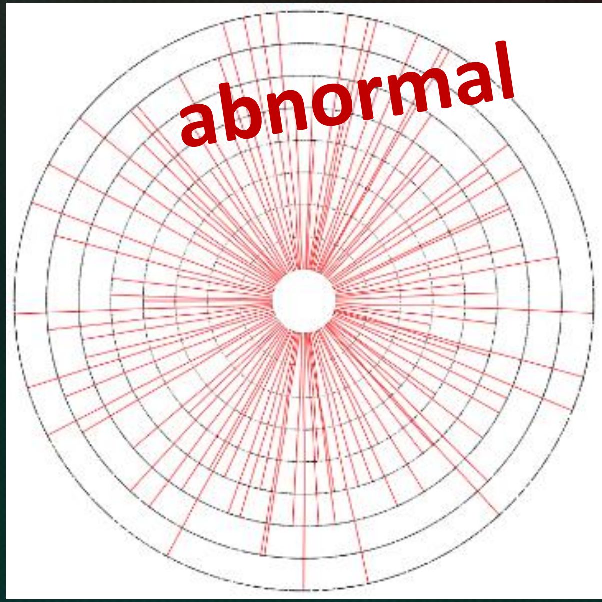
Data is separated in smaller subsets

iForest consists of iTrees, that are generated by the subsets

Process of training (modelling)

- Nodes of the binary tree have attributes *q* and *p*
- *q* is a randomly chosen feature of the data set
- *p* is a randomly chosen separation point (between min. and max.)
- $p < q \rightarrow$ left node
- $p > q \rightarrow$ right node





Testing the model

- Path length provides information about normality / abnormality
- A anomaly score is calculated for a data set, that runs through all iTrees

Loda

Lightweight on-line Detector of Anomalies

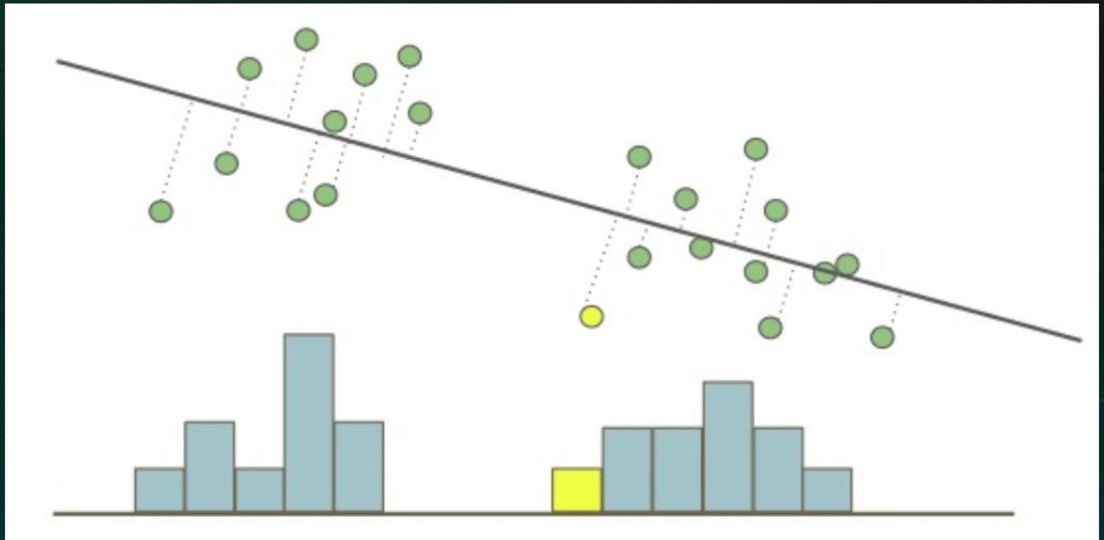
Ensemble of k one-dimensional histograms

Each histogram is generated by a random projection vector of the probability density of the input data

Output: Score value, the higher the more likely to be an anomaly

„Benefits“ compared to Isolation Forest

- Online mode without modification
- Reduced complexity



Loda

Lightweight on-line Detector of Anomalies

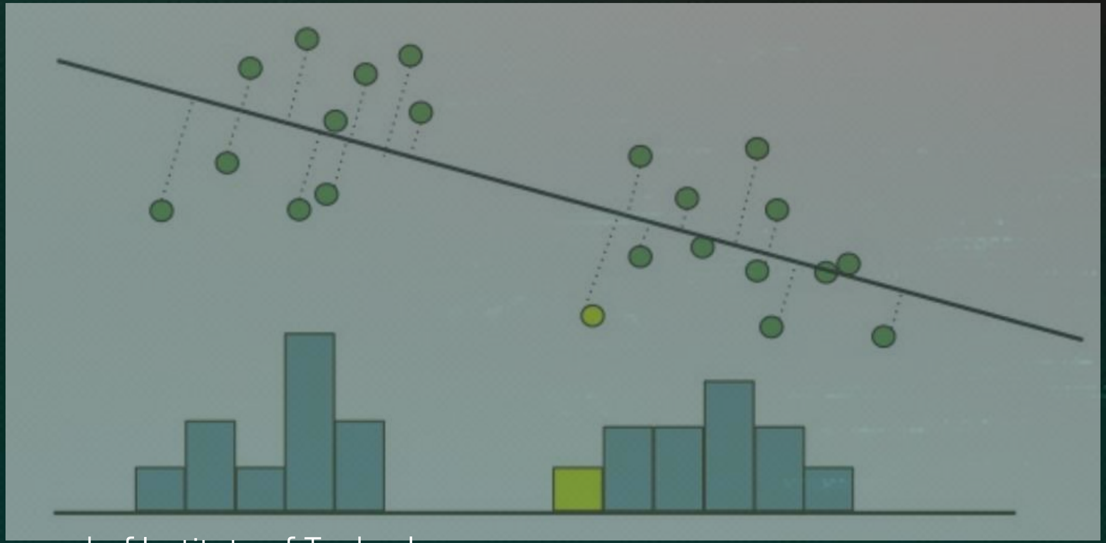
Ensemble of one-dimensional histograms

Each histogram is generated by a random projection vector of the probability density of the input data

Output: Score value, the higher the more likely to be an anomaly

„Benefits" compared to Isolation Forest

- Online mode without modification
- Reduced complexity



Time Complexity

	Time complexity		Space complexity
	Training	Classification	
Isolation Forest	$\mathcal{O}(kl \log l)$	$\mathcal{O}(k \log l)$	$\mathcal{O}(kl)$
Loda (1)	$\mathcal{O}(nkd^{-1/2})$	$\mathcal{O}(k(d^{-1/2} + b))$	$\mathcal{O}(k(d^{-1/2} + b))$
Loda (2)	$\mathcal{O}(nkd^{-1/2})$	$\mathcal{O}(kd^{-1/2})$	$\mathcal{O}(k(d^{-1/2} + b + l))$

Hierarchic Incident Detection

Issue: model needs many resources

- Small resources (CPU, RAM, etc.) on the lower layers
- The entire network doesn't need complete knowledge

Solution: Using a hierarchic system architecture

Layer *n* collects data for modelling (**Training**) on layer *n+1*

The trained model is transferred back to *n* for **Classification**

Hierarchic Incident Detection

Issue: model needs many resources

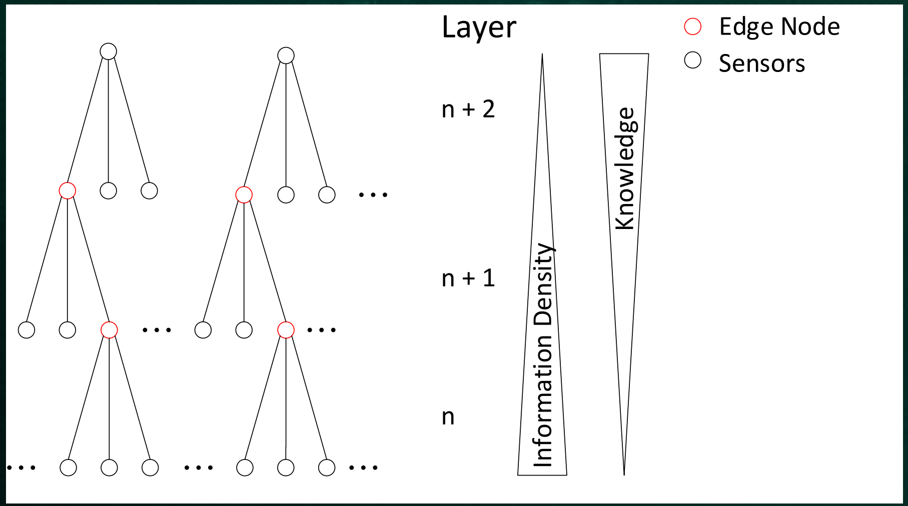
Small resources (CPU, RAM, etc.) on the lower layers

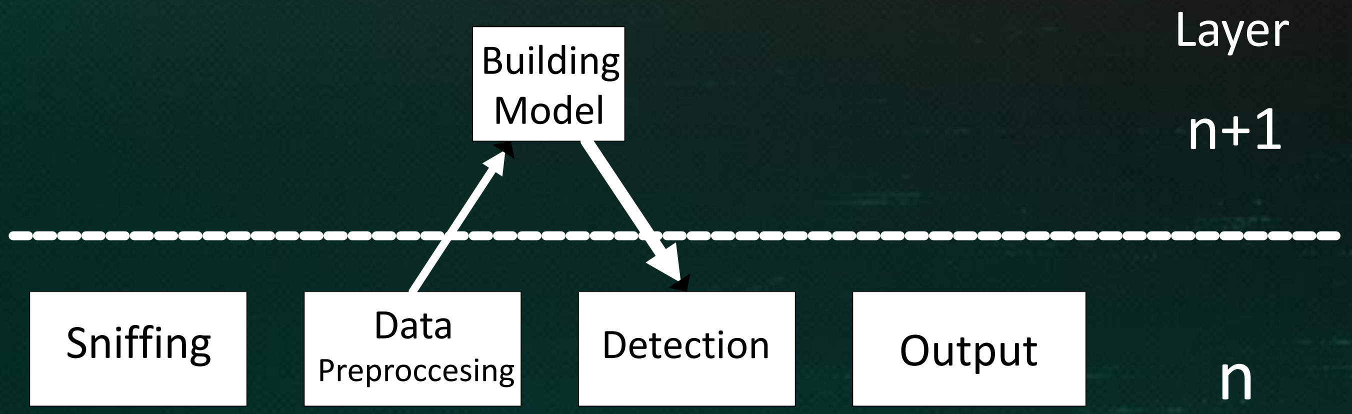
The entire network doesn't need complete knowledge

Solution: Using a hierarchic system architecture

Layer *n* collects data for modelling (Training) on layer *n+1*

The trained model is transferred back to *n* for Classification





Huge amount of alerts … and now?

Handling of Alerts

Goal :

Handling of a huge amount of alerts

Reduction of False Positives

Approaches :

Similarity-based: Reduction of the amount of alerts with aggregation and clustering in respect of analogy, attribute, …

Sequential-based: recognition of causal correlation, definition of pre- und postconditions

Case-based: using of knowledge-base (training data sets, expert-rules)

Handling of Alerts

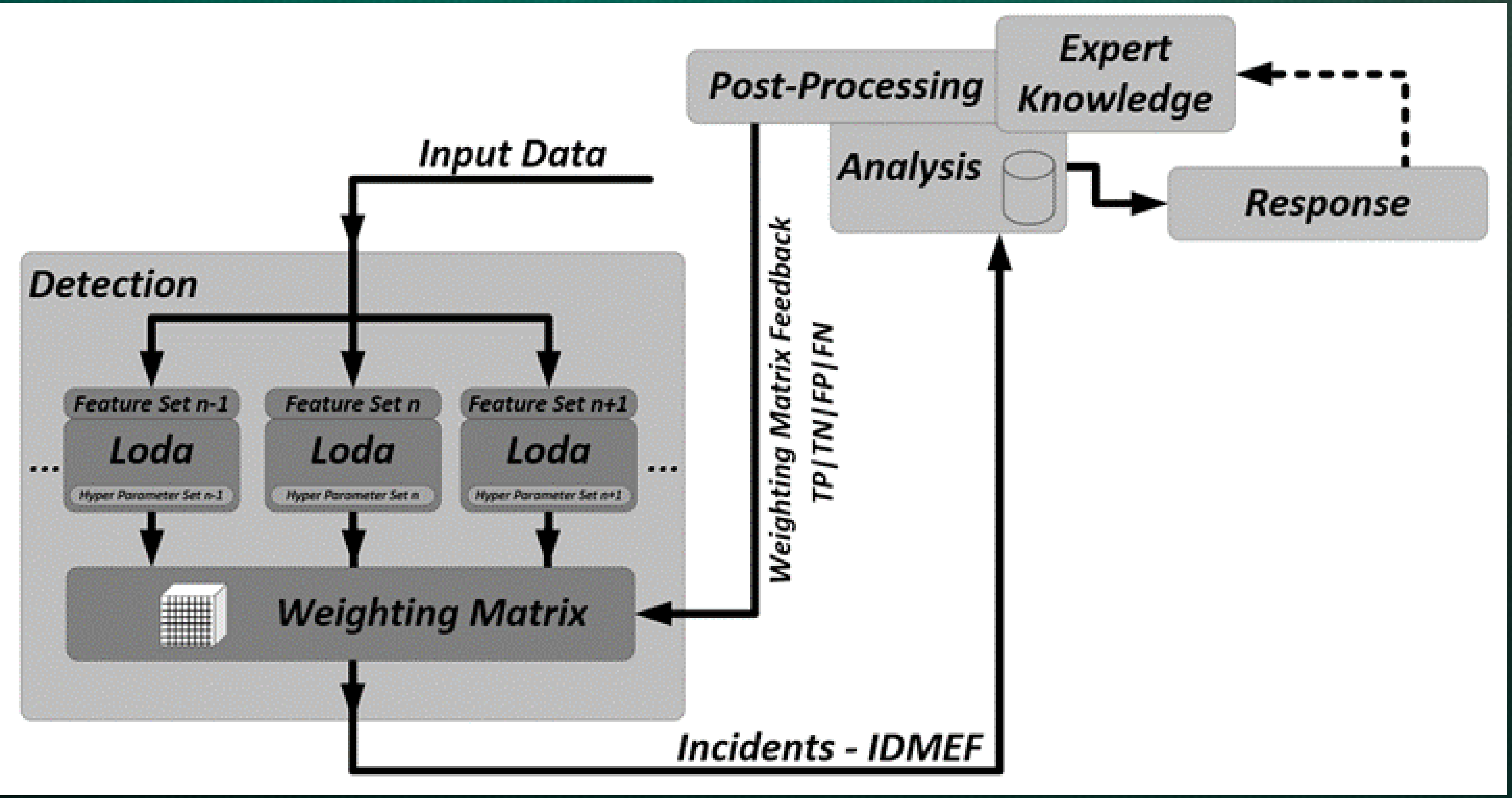
Goal :

Handling of a huge amount of alerts
Reduction of False Positives

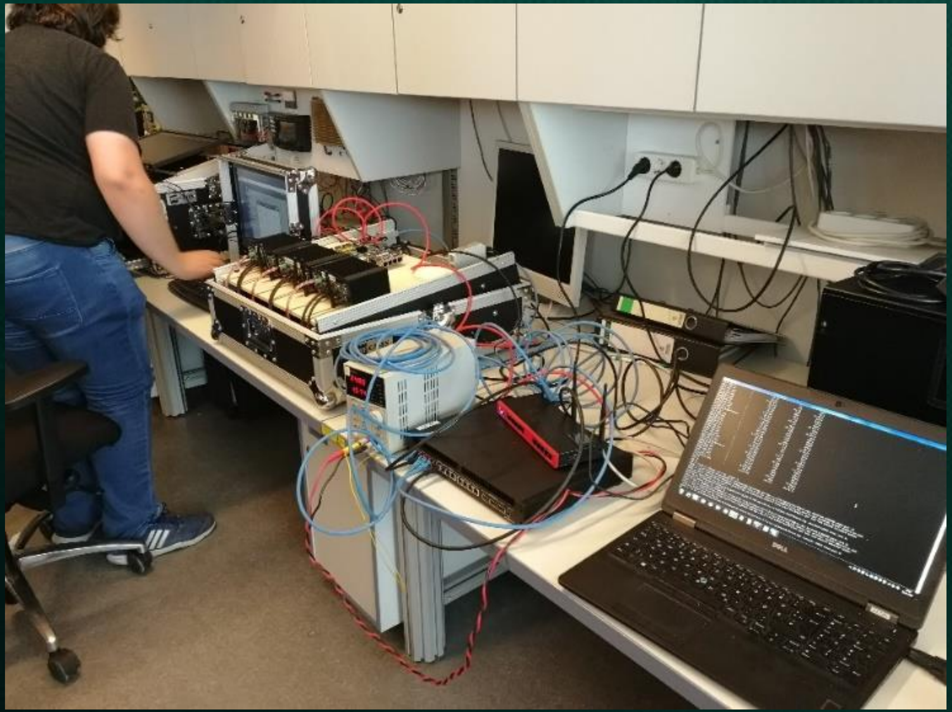
Approaches :

Similarity-based: Reduction of the amount of alerts with aggregation and clustering in respect of analogy, attribute, …
Sequential-based: recognition of causal correlation, definition of pre- und postconditions
Case-based: using of knowledge-base (training data sets, expert-rules)

Handling of Alerts



Demonstrator Set-Up



Summary

One IDS/DRC on the upper layer in not sufficient

Isolated Forest is more complex as Loda

The false-positive rate is for both algorithms similar

Very import is the feature set

The reaction is very dependent to the application

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

DEGGENDORF INSTITUTE OF TECHNOLOGY

Thank you!

Deggendorf Institute of Technology
Institute ProtectIT

Faculty of Computer Engineering
Dieter-Görlitz-Platz 1, 94469 Deggendorf

andreas.grzemba@th-deg.de
Phone: +49 (0) 991 3615-512
https://www.th-deg.de/en/protectit