University of Stuttgart
Institute of Industrial Automation and
Software Engineering

AI-based Anomaly Detection for Technical Systems

Andrey Morozov and Sheng Ding

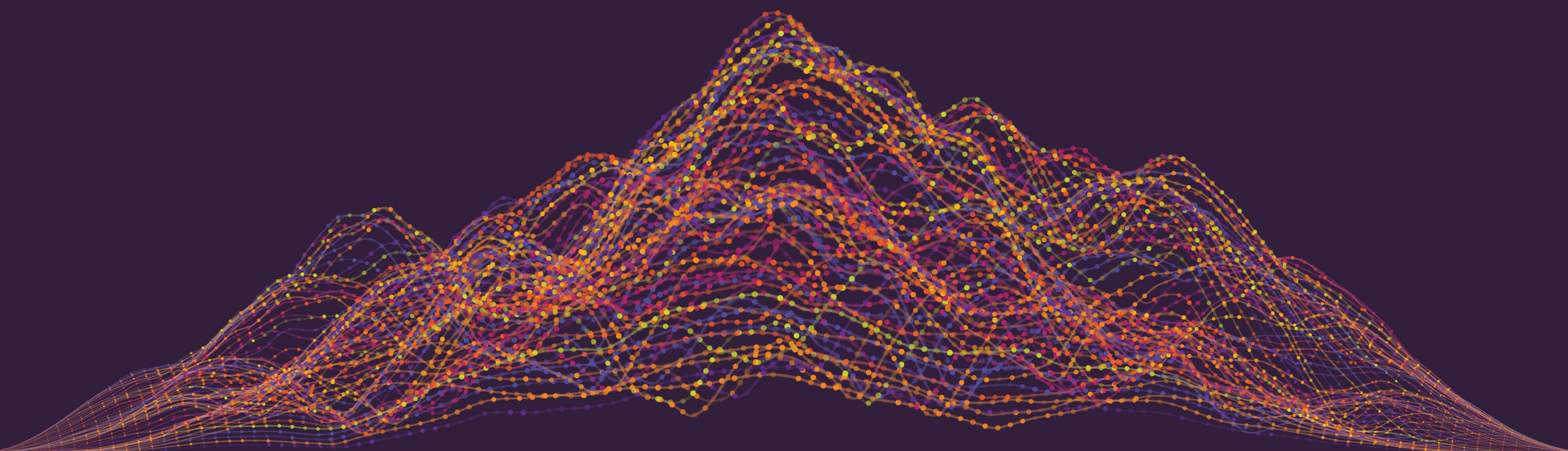
ASME TEC Talk, 19.07.2022

Outline

- Part 1: Safety-critical systems, system states, faults, errors, failures.
- Part 2: Anomalies and anomaly detection methods.
- Part 3: Example of a DL-based anomaly detector (Kraken).
- Part 4: Challenges and solutions.

Part 1

Faults, errors, failures



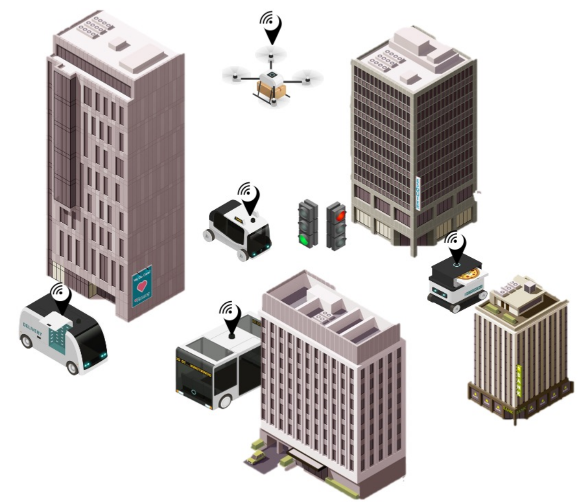
Faults, errors, failures

Examples of safety-critical systems

Medical
exo-skeleton

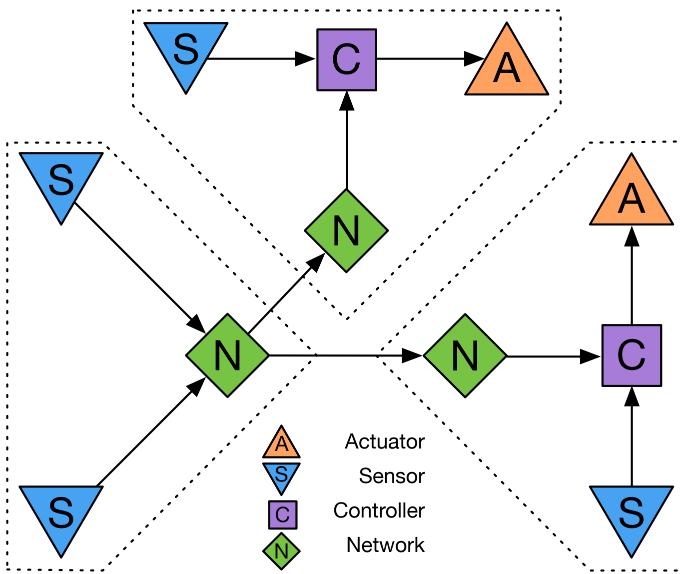
Flexible
production line

Intelligent
transportation



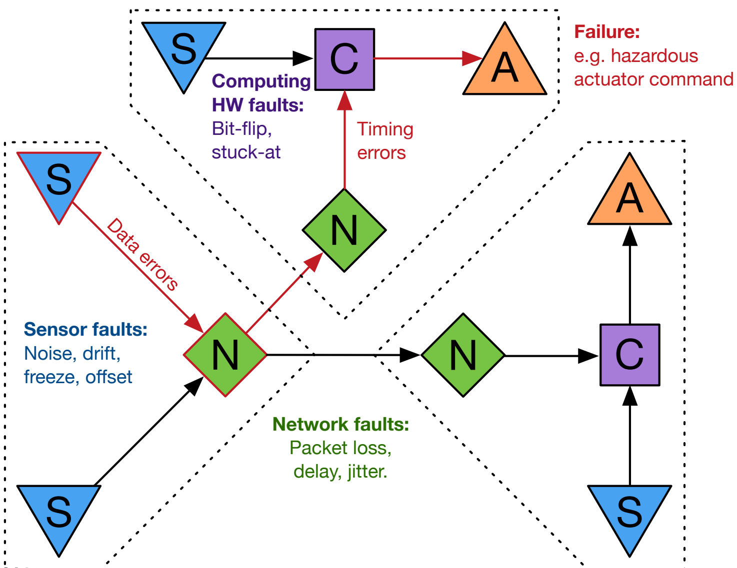
Faults, errors, failures

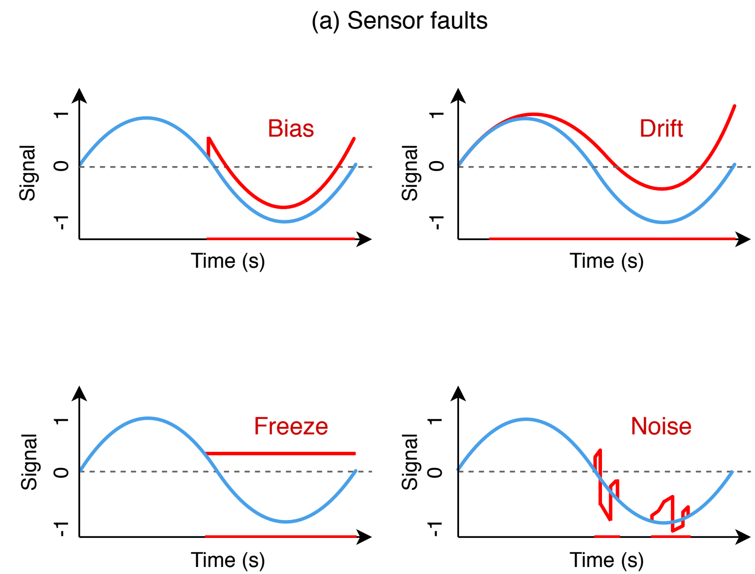
Networked heterogenous components



Faults, errors, failures

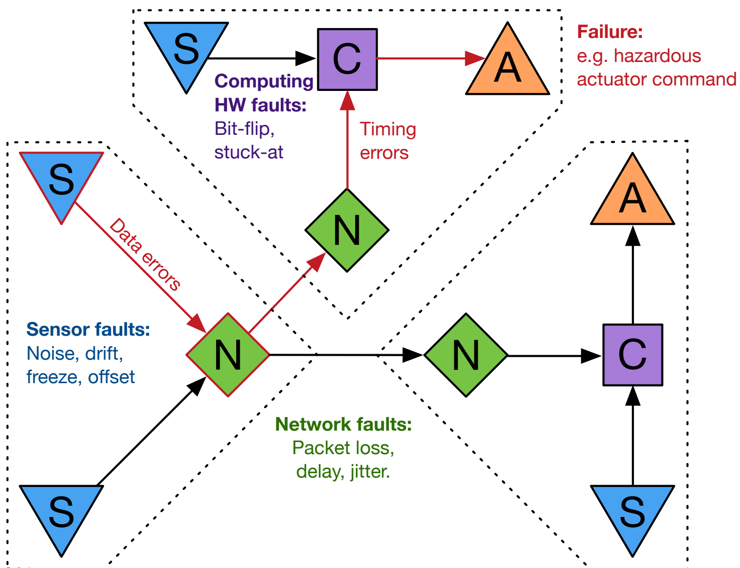
Examples of internal faults





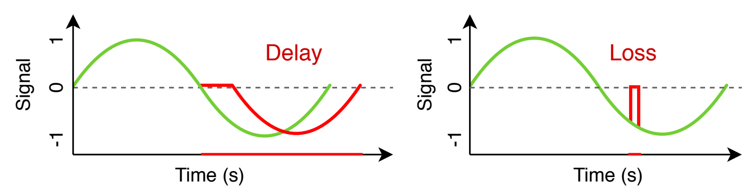
Faults, errors, failures

Examples of internal faults



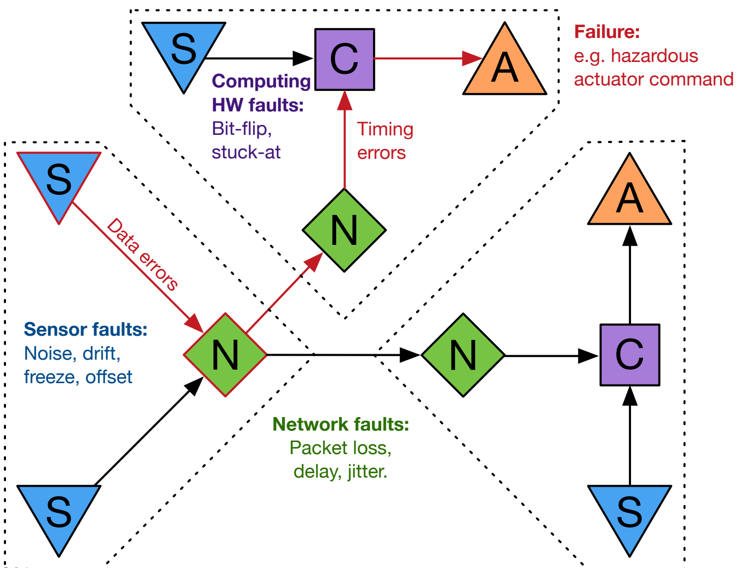
(b) Computing hardware faults

(c) Network faults



Faults, errors, failures

Examples of external faults



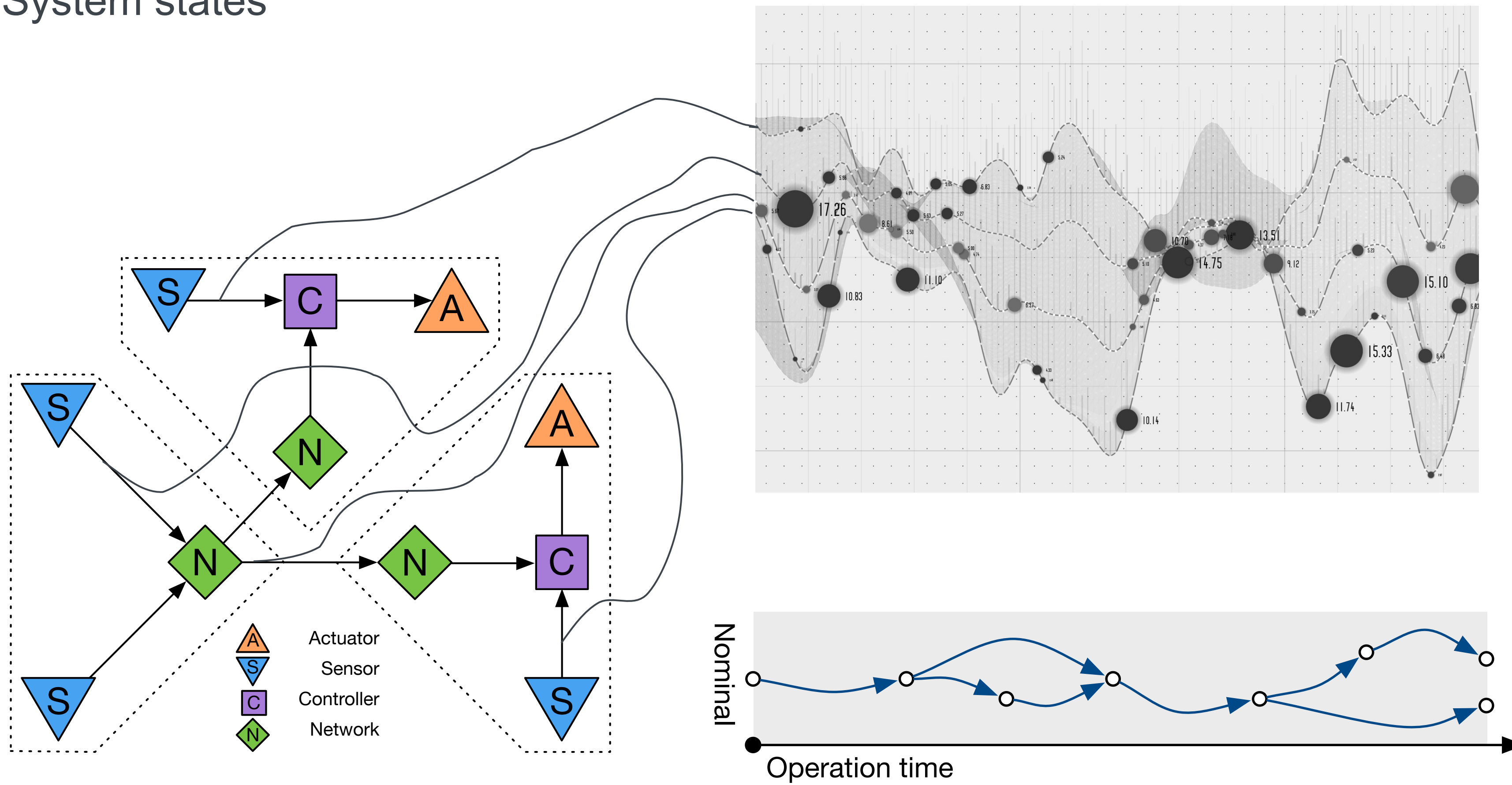
(d) Hacker attacks

(e) Environmental conditions

https://innovate.ieee.org/innovation-spotlight/vehicle-detection/

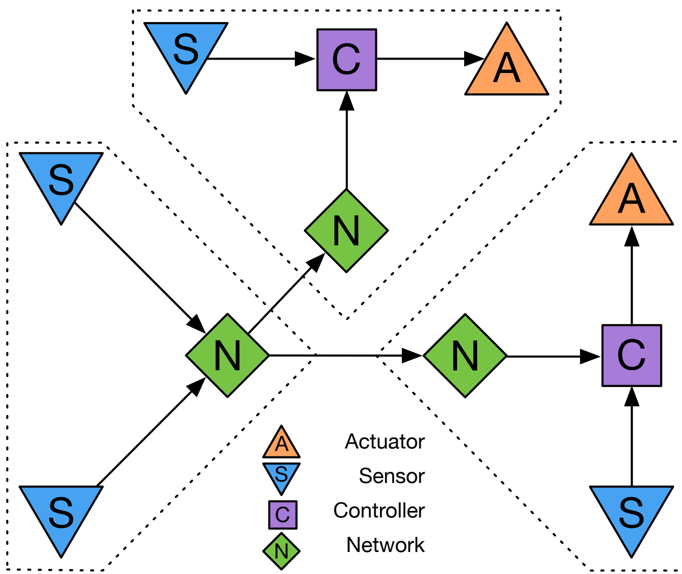
Faults, errors, failures

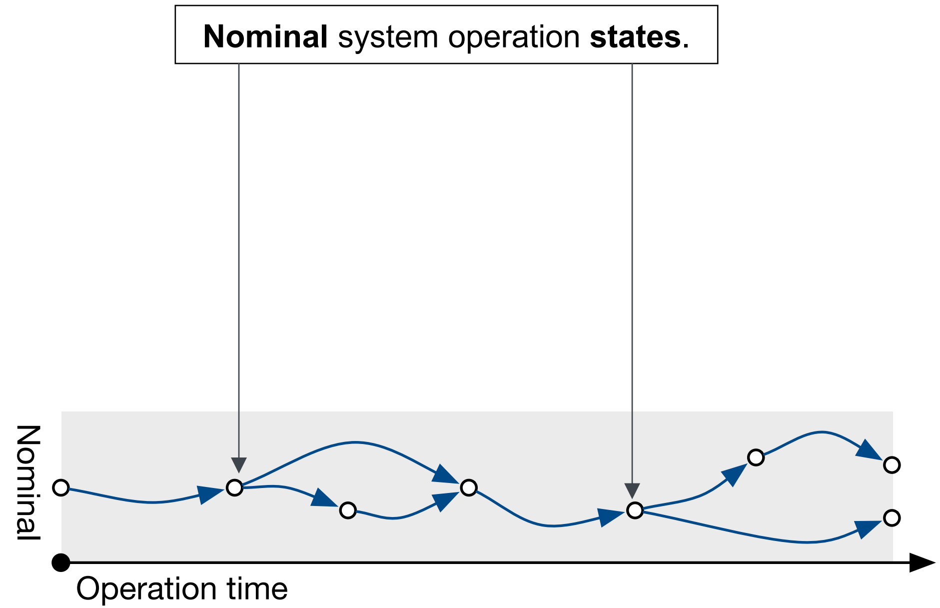
System states



Faults, errors, failures

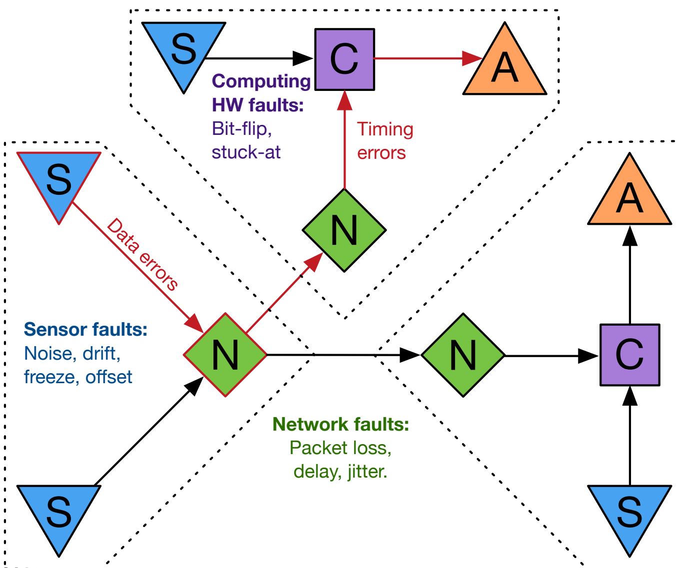
System states

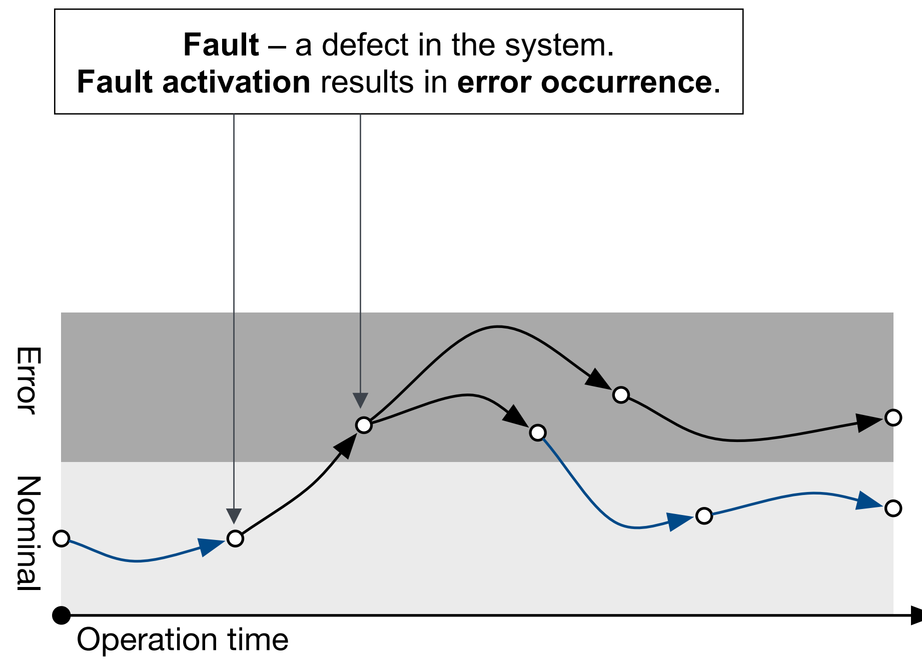




Faults, errors, failures

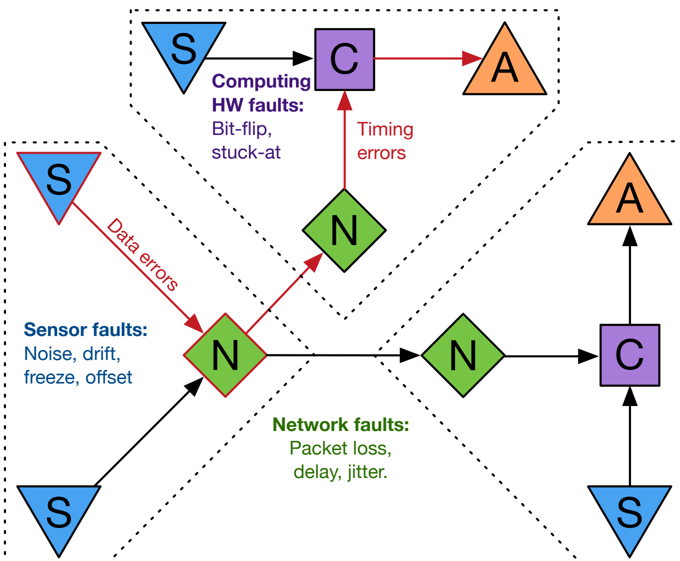
System errors

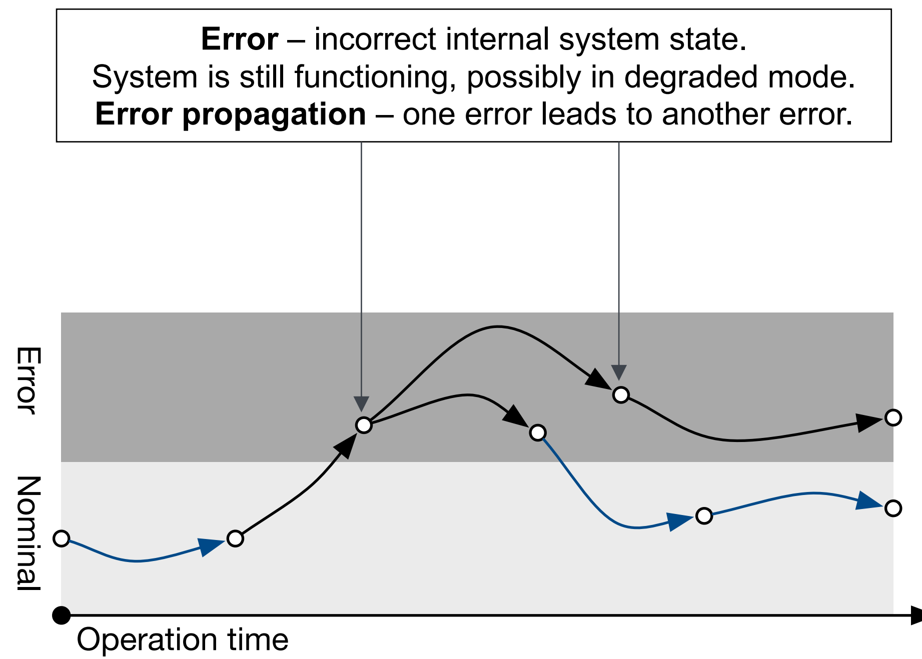




Faults, errors, failures

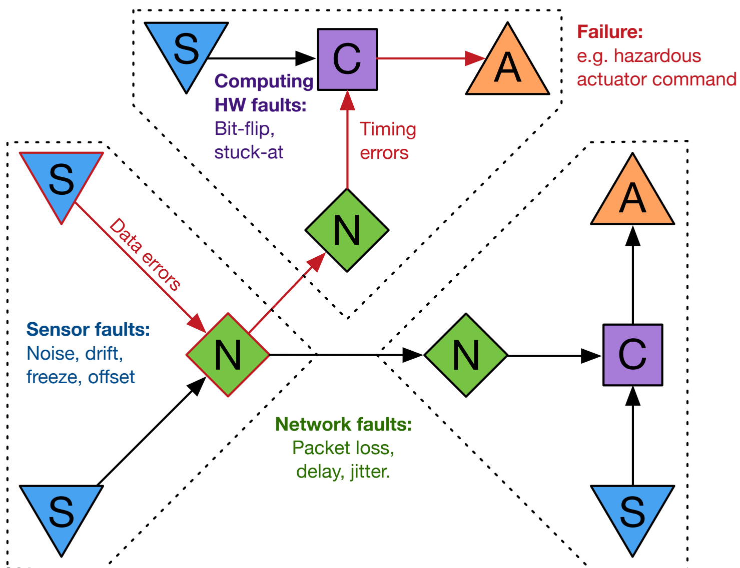
Error propagation

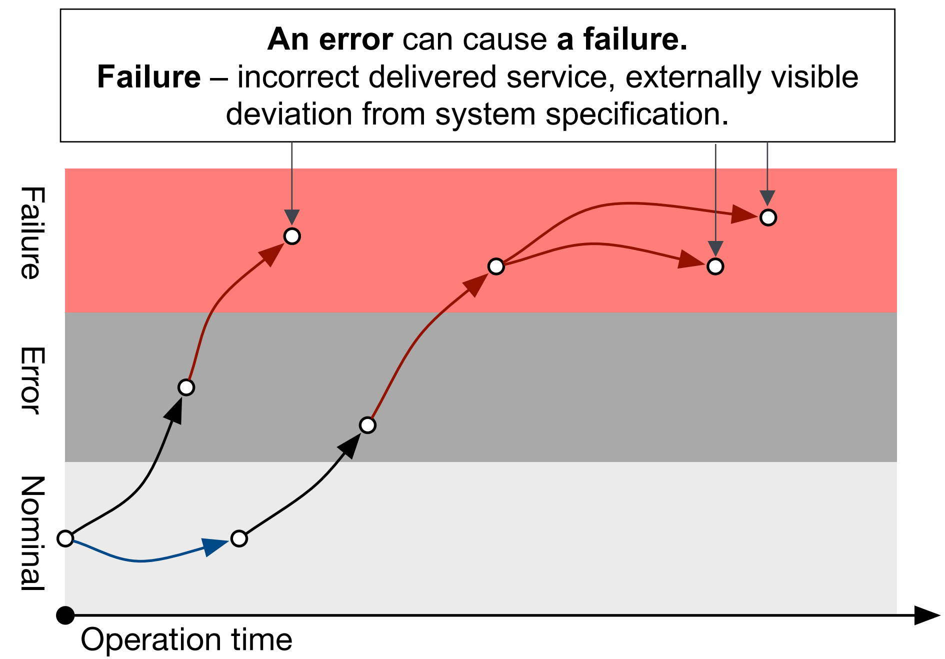




Faults, errors, failures

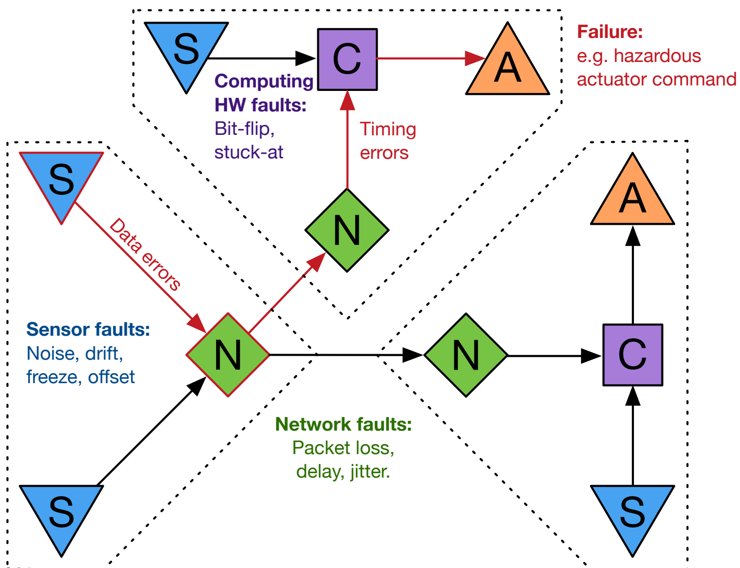
System failures

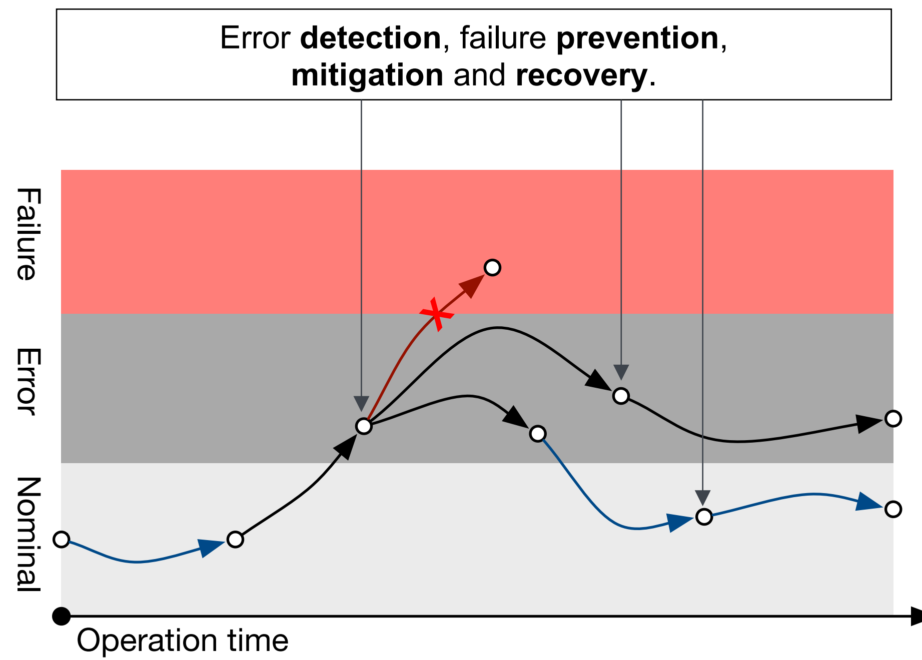




Faults, errors, failures

Error detection





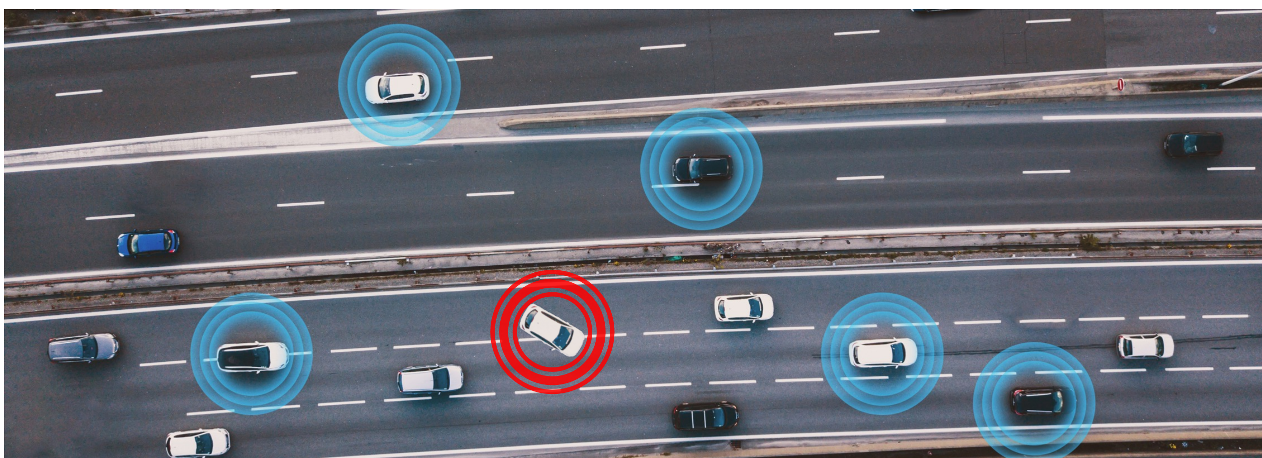
Part 2

Anomalies

Anomalies

What is an anomaly?

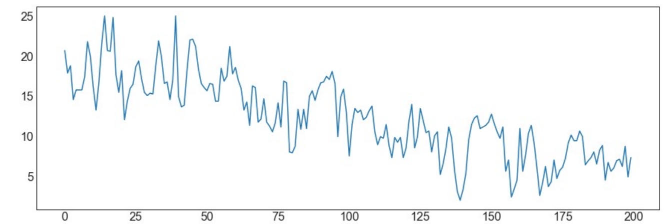
- An anomaly is an observation or a sequence of observations which deviates remarkably from the general distribution of data.
- The set of the anomalies form a very small part of the dataset.



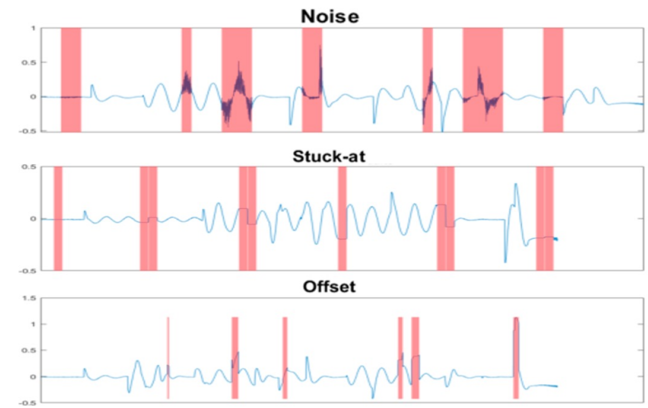
Anomalies

Data types

- **Time series** is a series of data points indexed in time order.
- **Temporal** data include time-series, but also data with timestamps of unequal interval.
- **Univariate** data takes only one dimension, e.g., single sensor readings.
- **Multivariate** data contains multiple dimensions, e.g., images or time-series of several sensors.
- **Labelled dataset**: an annotation exists for each element, which determines if it is a normal or anomalous.



Example of temporal (time-series), multivariate, laballed data:

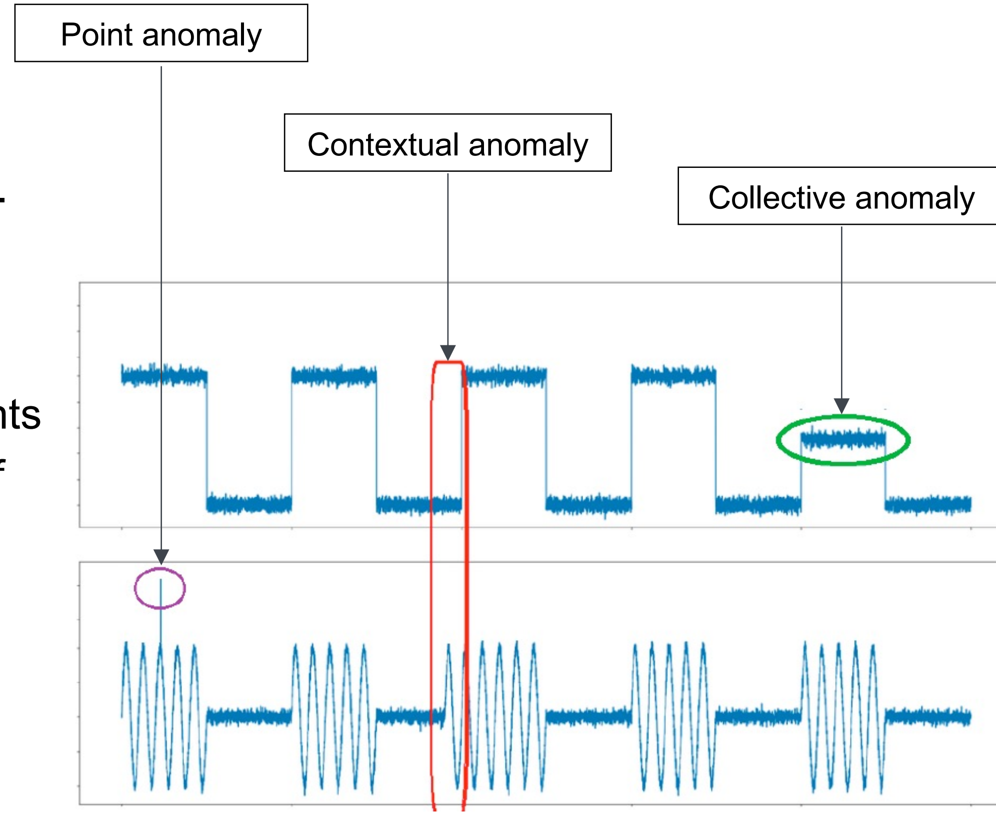


Anomalies

Anomaly classification

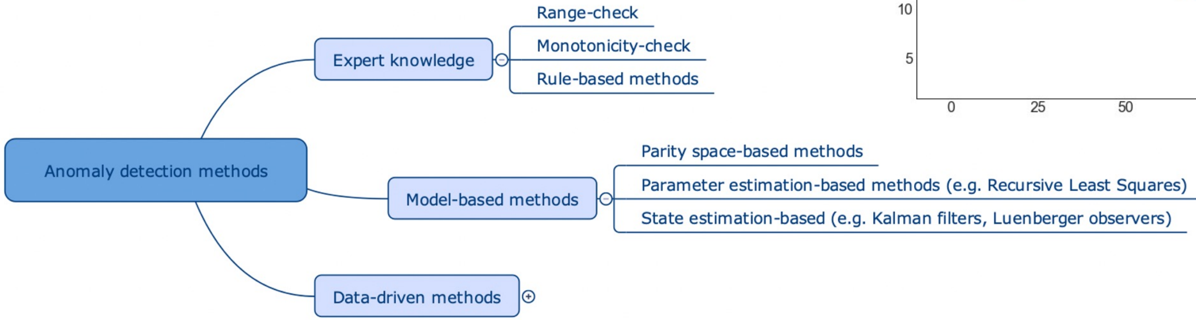
Three different types of anomalies exist.

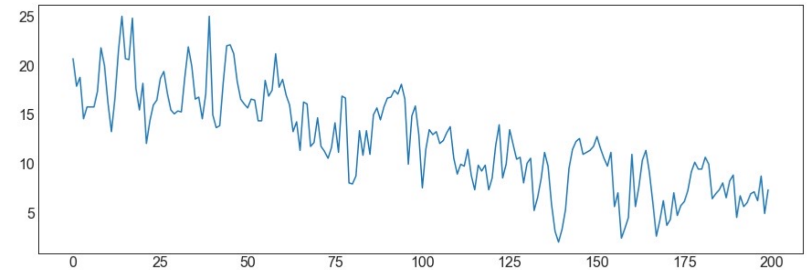
- **Point anomalies:** If a point deviates significantly from the rest of the data.
- **Collective anomalies:** Individual points are not anomalous, but a sequence of points are labelled as an anomaly.
- **Contextual anomalies:** Some points can be normal in a certain context, while detected as anomaly in another context.

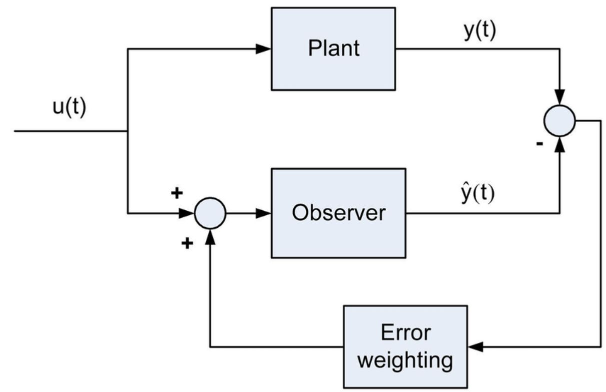


Anomalies

Classification of detection methods

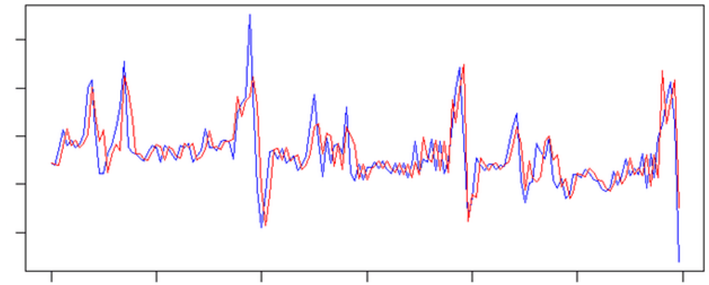




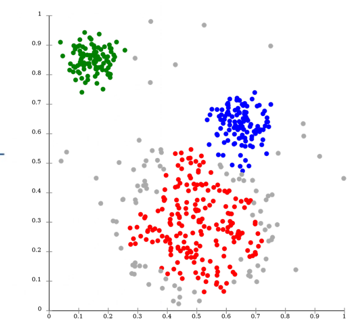


Anomalies

Classification of detection methods



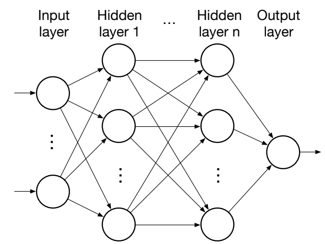
- Anomaly detection methods
  - Expert knowledge
  - Model-based methods
  - Data-driven methods
    - Statistical methods
      - Statistical process control
        - Multivariate CUmulated SUMs control chart (MCUSUM)
        - Multivariate Exponential Weighted Moving Average (MEWMA)
      - Prediction methods
        - Vector Autoregressive (VAR) method
        - Autoregressive Moving Average Model (ARIMA)
        - Prediction Confidence Interval (PCI)
        - Simple/Double/Triple Exponential Smoothing (SES, DES, TES)
      - Decomposition methods
        - Principal Component Analysis (PCA)
        - Singular Spectrum Analysis (SSA)
        - Independent Component Analysis (ICA)
      - Simillarity-search (e.g. Matrix-Profile (MP))
    - Machine Learning methods
      - K-Means Clustering
      - Density-Based Spatial Clustering of Applications with Noise (DBSCAN)
      - Local Outlier Factor (LOF)
      - Isolation Forest (IF)
      - One-Class Support Vector Machines (OC-SVM)
      - Extreme Gradient boosting (XGBoost)
    - Deep learning methods

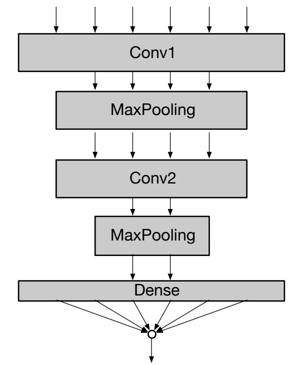


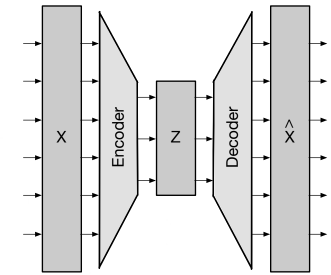
https://community.rstudio.com/t/forecasting-regression-model-with-arima-errors/75951
https://commons.wikimedia.org/wiki/File:DBSCAN-Gaussian-data.svg

Anomalies

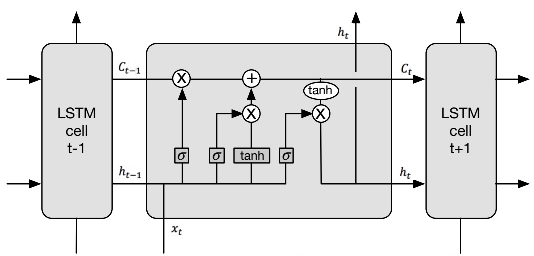
Classification of detection methods







- Anomaly detection methods
  - Expert knowledge
  - Model-based methods
  - Data-driven methods
    - Statistical methods
    - Machine Learning methods
    - Deep learning methods
      - Multiple Layer Perceptron (MLP)
      - Recurrent Neural Networks (RNN)
        - Long Short Term Memory (LSTM) network
        - Gated Recurrent Unit (GRU)
      - Convolutional Neural Networks (CNN)
        - Residual Neural Network (ResNet)
        - WaveNet
        - Deep Unsupervised Anomaly Detection (DeepAnT)
      - Auto-Encoders (AE)
        - MLP-UAE (univariate)
        - MLP-MAE (multivariate)
        - LSTM-AE
        - Variational AE (VAE)
      - Transformers
        - Transformer for Anomaly Detection in multivariate time series data (TranAD)
        - Transformers with Association Discrepancy
      - Generative Adversarial Networks
        - Multivariate Anomaly Detection with GAN (MAD-GAN)
        - Time series Anomaly Detector using GAN (TadGAN)

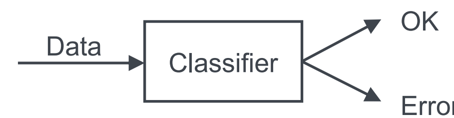


Anomalies

Approaches to DL-based anomaly detection

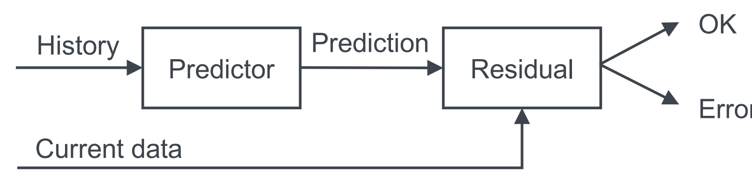
1) Classification (MLP, CNN):

- Supervised learning, good performance.
- Requires sufficient labeled erroneous instances.



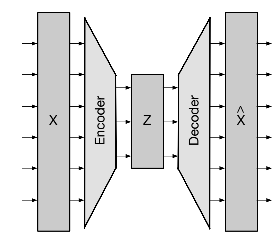
2) Prediction (LSTM):

- Unsupervised learning, labels are not required.
- On-line localization, and mitigation.



3) Reconstruction (AE):

- Based on encoder-decoder architecture.
- Not so efficient.



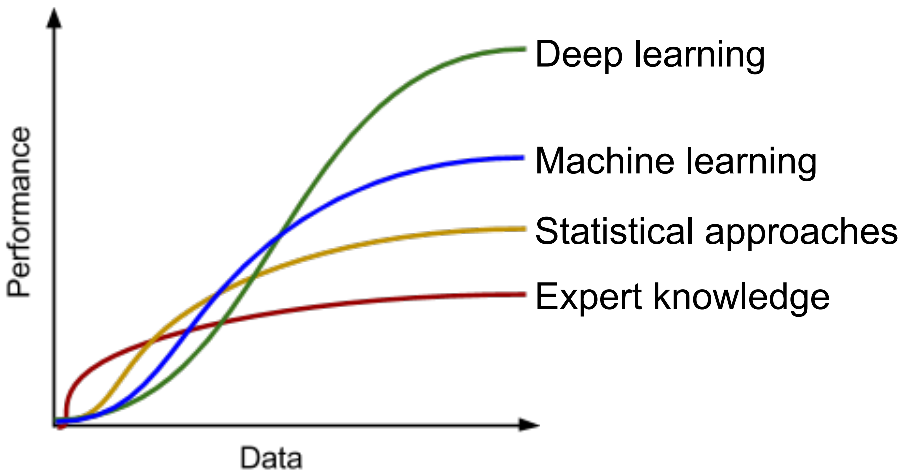
Anomalies

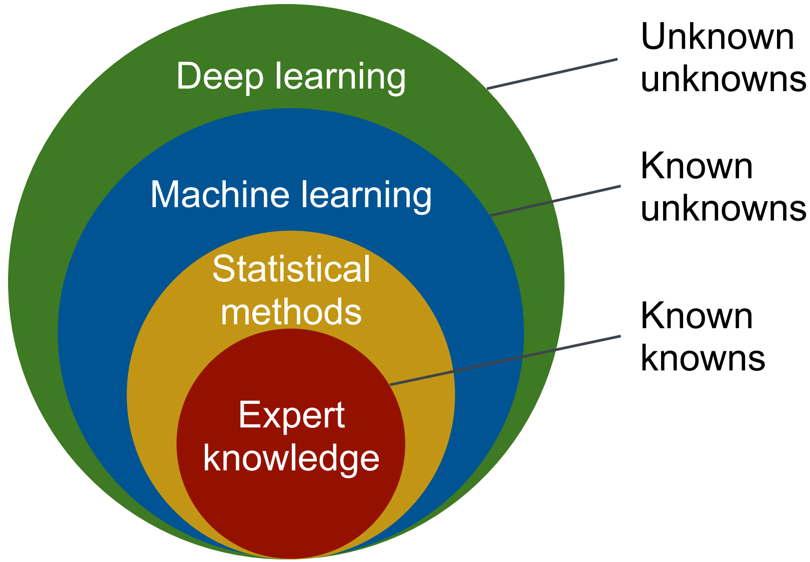
Perfromance of detection methods

Paper	Year	Conclusion
Anomaly Detection in Univariate Time-series: A Survey on the State-of-the-Art	2020	- DL are flawed (statistical methods are better than ML and DL)
Current time series anomaly detection benchmarks are flawed and are creating the illusion of progress.	2021	- DL are flawed (95% published results can‘t be trusted, AD can be solved good enough with older methods)
An Evaluation of Anomaly Detection and Diagnosis in Multivariate Time Series	2021	- UAE is best (fancy DNN design might not work as they promised, trivial NN might be better than them)
Do Deep Neural Networks Contribute to Multivariate Time Series Anomaly Detection?	2022	+ No fit for all solution (positive evidence that DL do prove real advantage in some circumstances)
Anomaly Detection in Time Series: A Comprehensive Evaluation	2022	+ No fit to all solution (there is no clear winner, no one-size-fits-all solution)

Anomalies

Perfromance of detection methods





Deep Learning: e.g. LSTM, Transformer, Autoencoder.

Machine Learning: K-Means, DBSCAN, Isolation Forest.

Statistical Approaches: ARIMA-Model, SES/DES/TES.

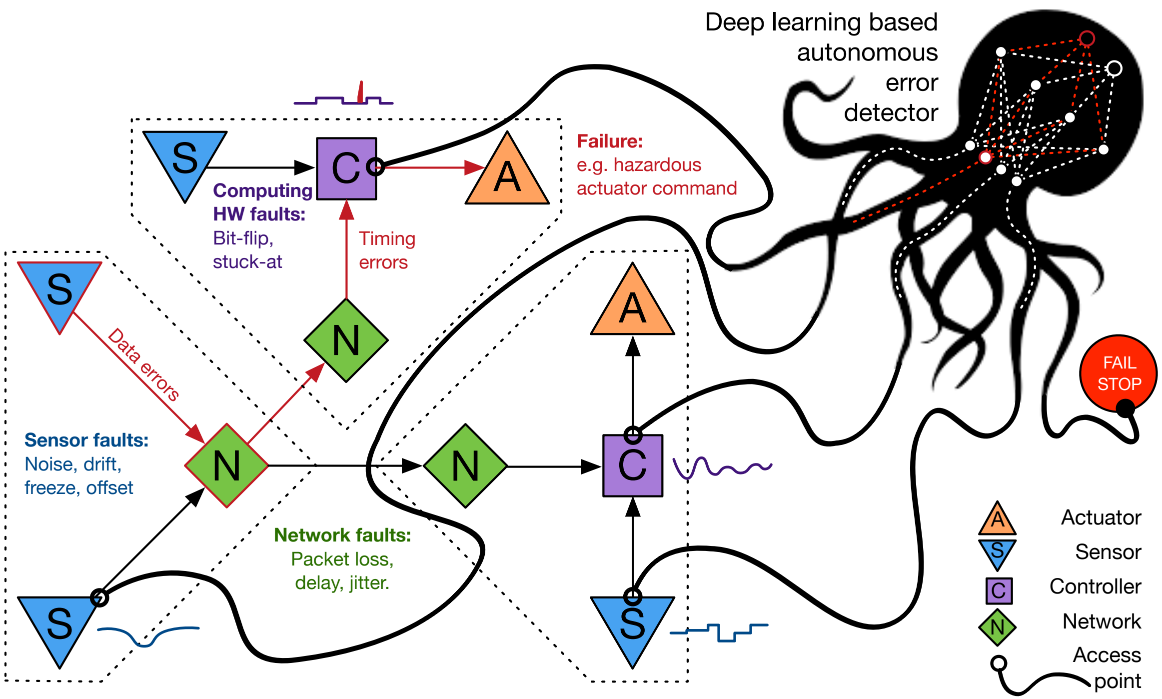
Expert knowledge: e.g. rules, range-check.

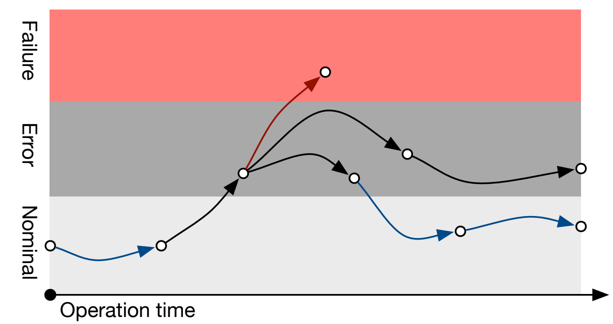
Part 3

Kraken

Kraken

Deep-learning based anomaly detector



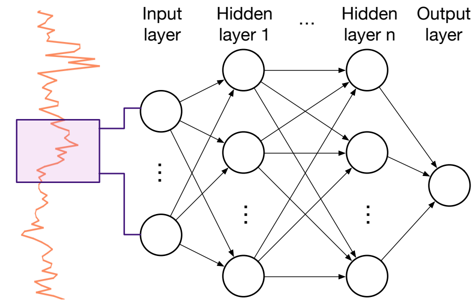


Kraken

Deep-learning based anomaly detector

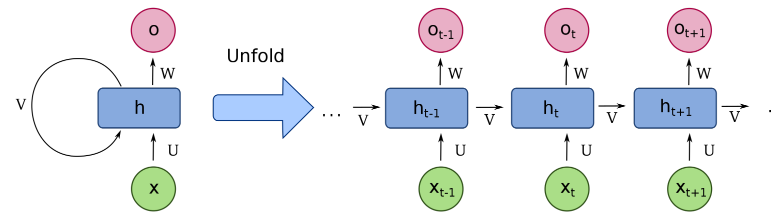
1) Muti-Layer Perceptron (MLP)

- Low performance for time series.



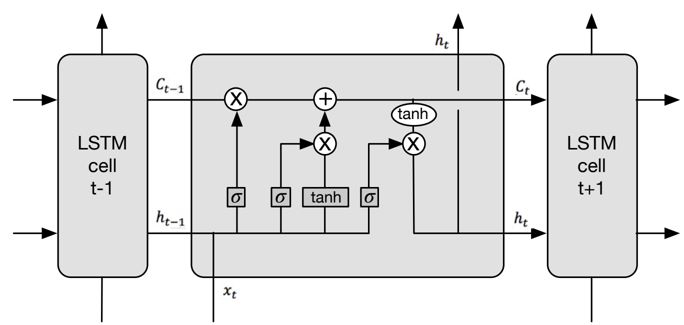
2) Recurrent Neural Network (RNN)

- Has memory to process sequences of inputs.
- Can learn temporal dynamic behavior.
- Fail to capture the context as time steps increase (*vanishing gradient problem*).



3) Long Short Term Memory (LSTM)

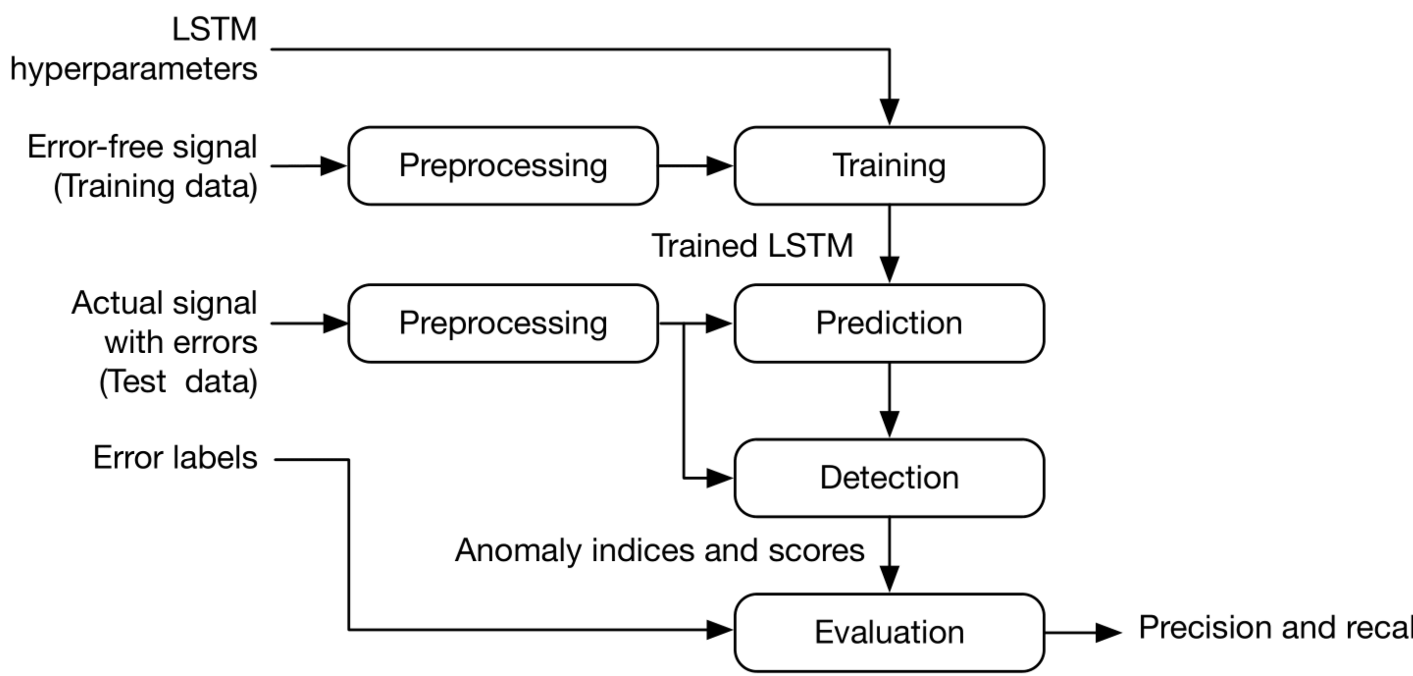
- Designed to avoid the vanishing gradient problem.



Kraken

Deep-learning based anomaly detector

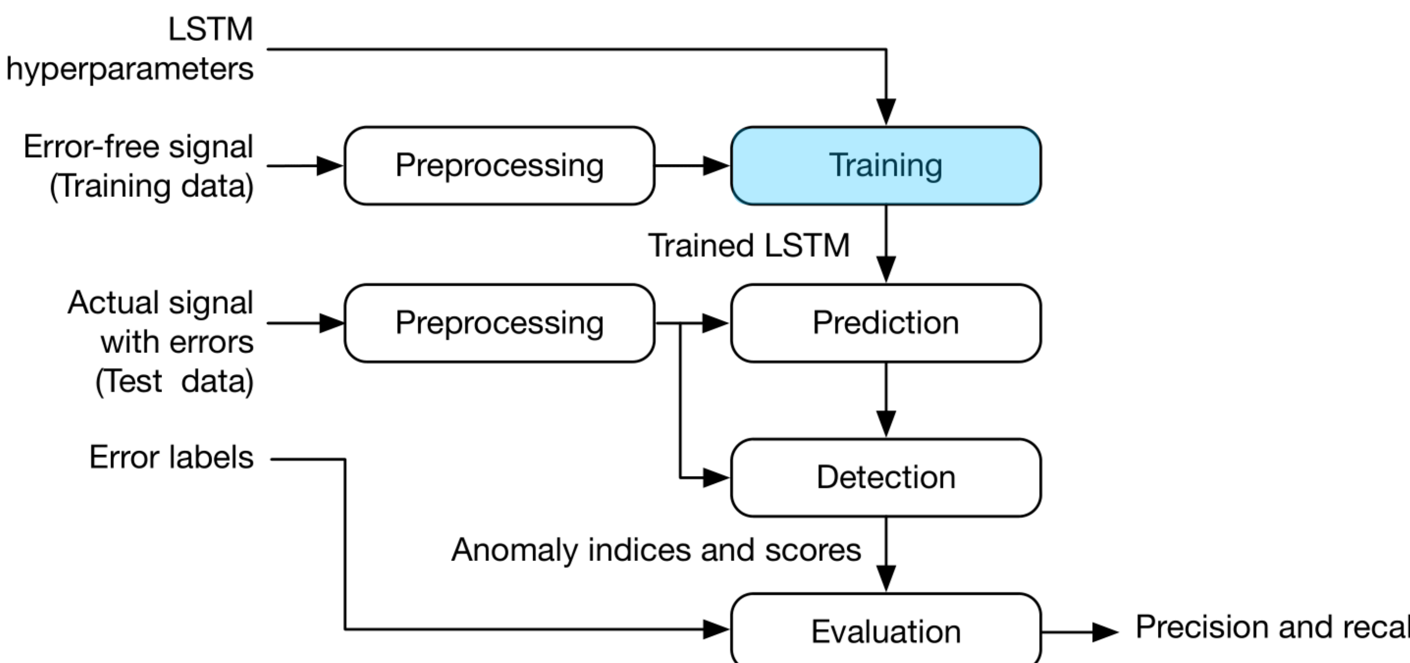
Workflow



Kraken

Deep-learning based anomaly detector

Workflow



Kraken

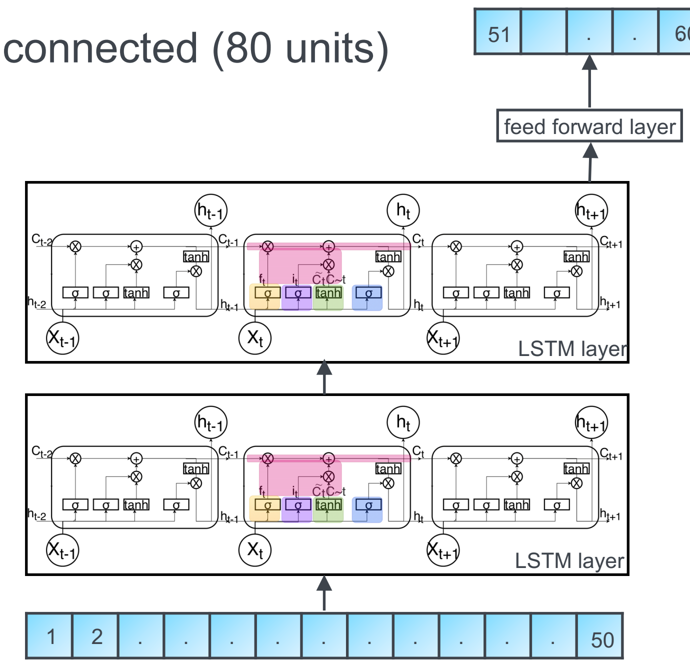
Deep-learning based anomaly detector

Stacked LSTM Architecture:

- Layers: two consecutive hidden LSTM layers fully connected (80 units)
- Look-back: 50 steps.
- Look-ahead: 1 steps.
- Dropout: 0.3

Training-parameters:

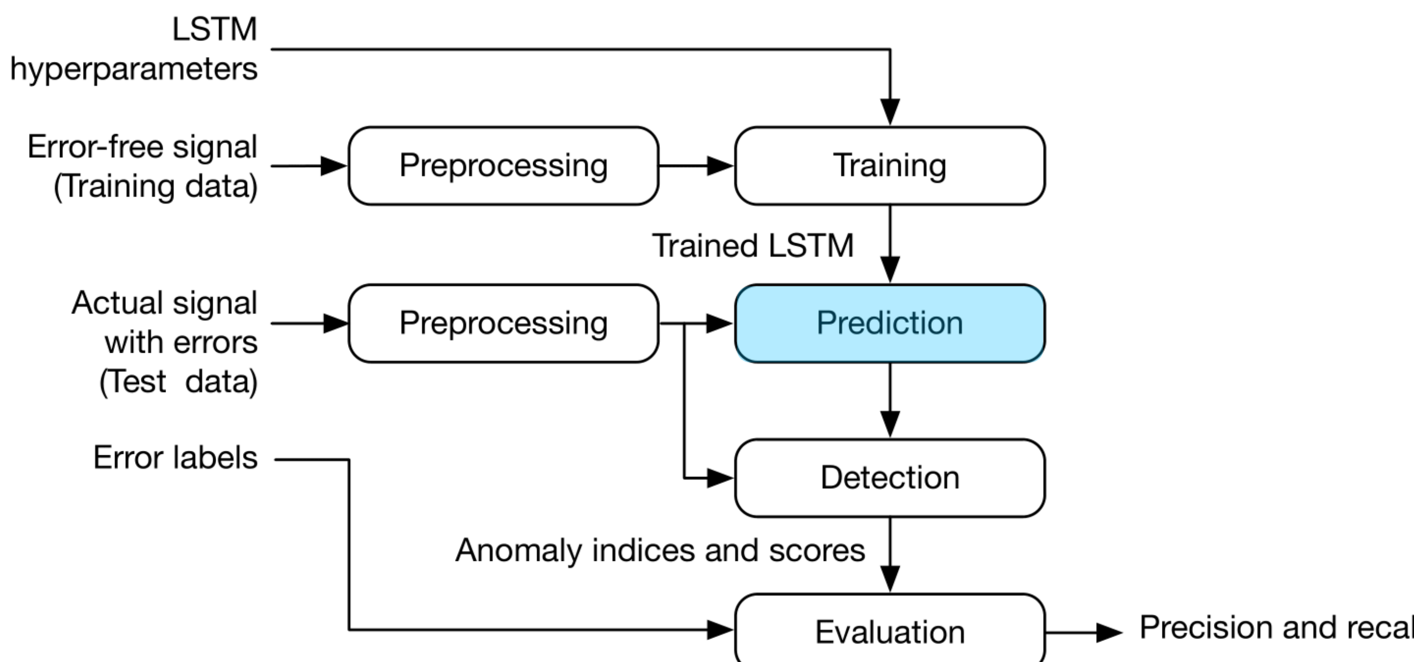
- Batch size: 70
- Optimizer: Adam
- Epochs: 35 epochs with early stopping.



Kraken

Deep-learning based anomaly detector

Workflow

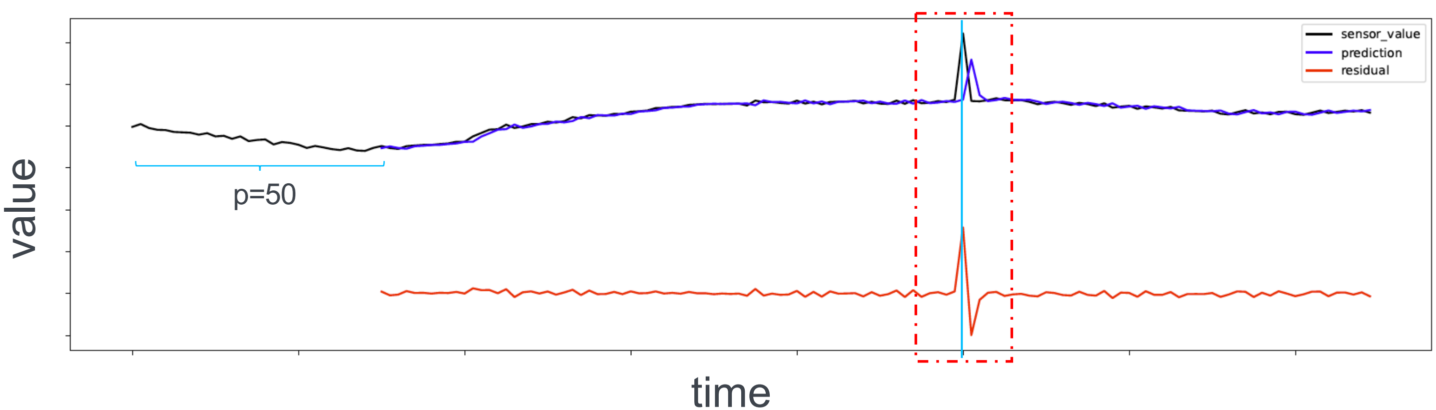


Kraken

Deep-learning based anomaly detector

Prediction:

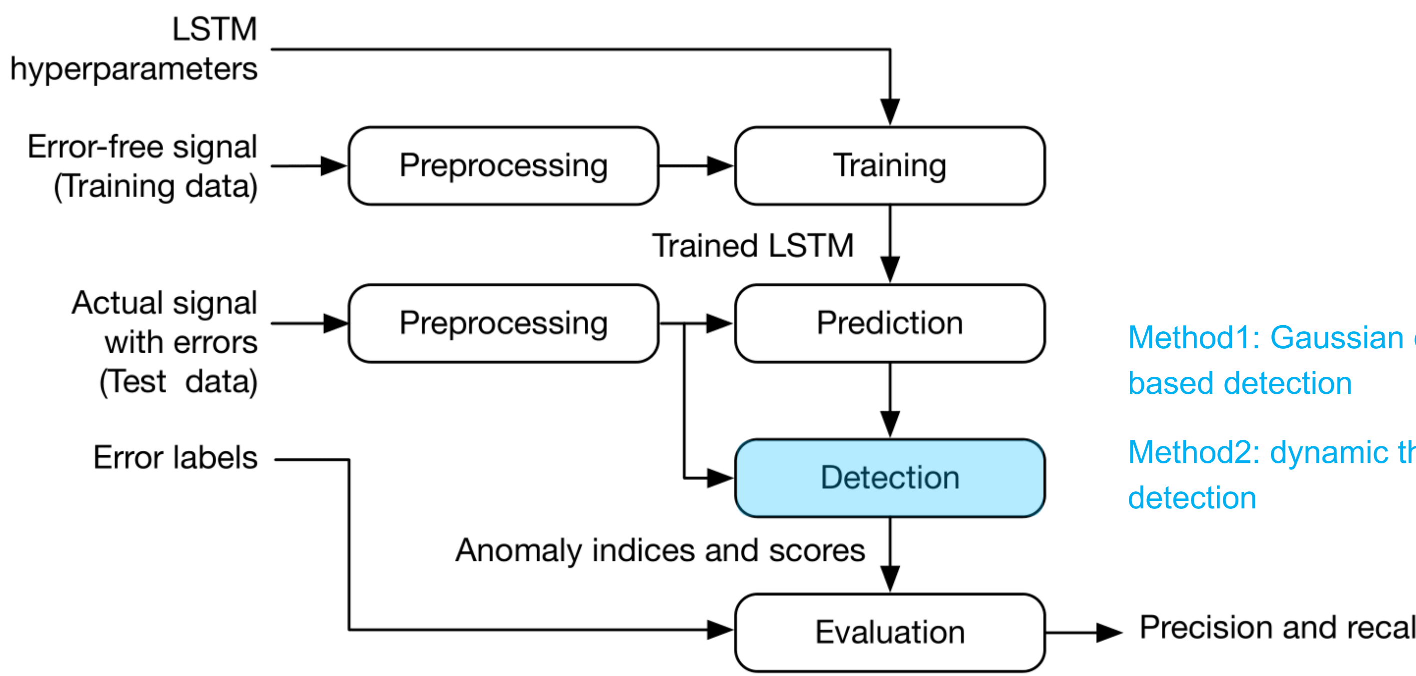
- The LSTM network predicts the next value (lookahead $q = 1$)
- based on the previous 50 time steps (lookback $p = 50$).



Kraken

Deep-learning based anomaly detector

Workflow



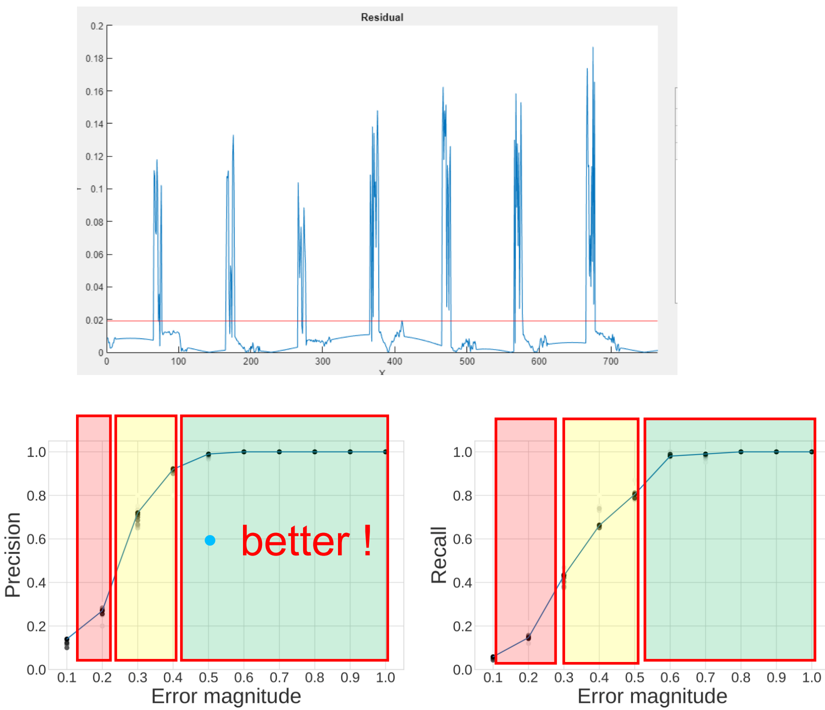
Method1: Gaussian distribution based detection

Method2: dynamic threshold based detection

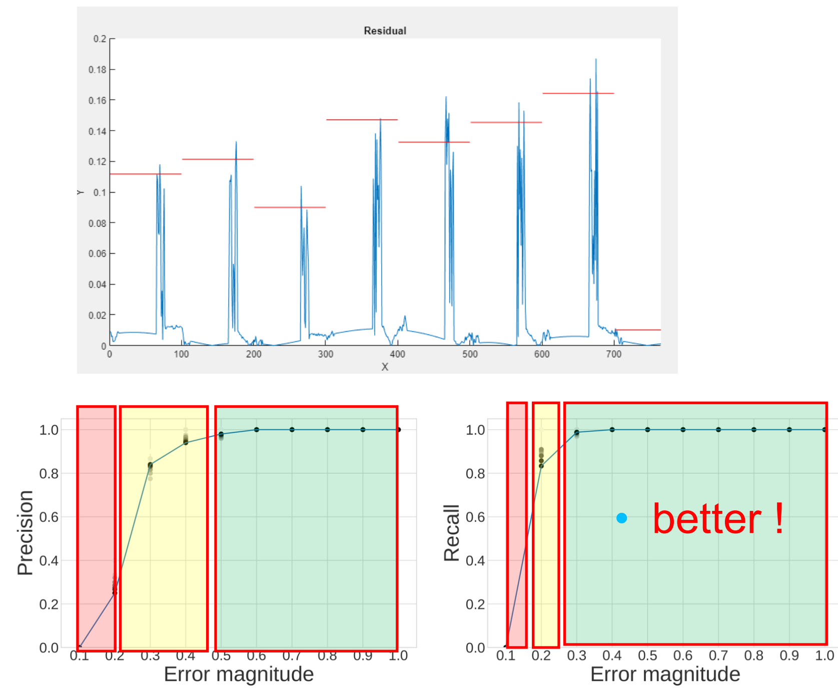
Kraken

Deep-learning based anomaly detector

Gaussian distribution based threshold



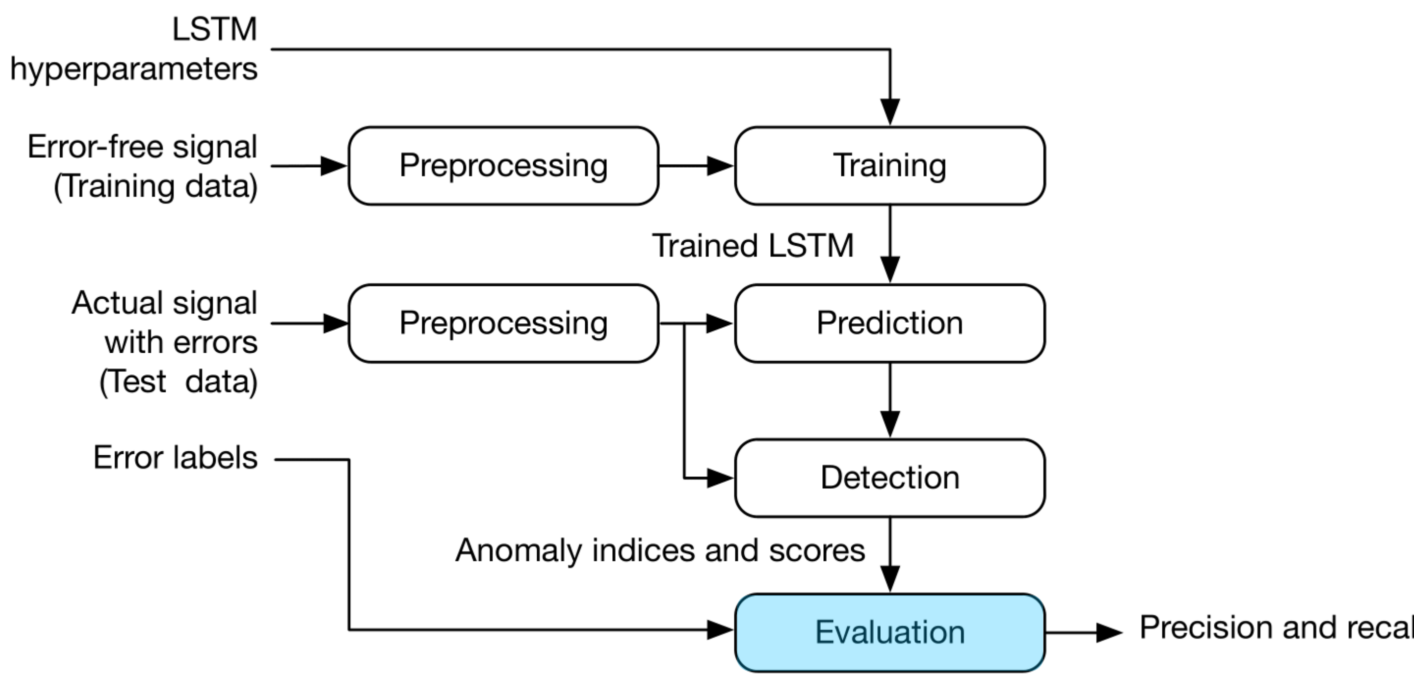
Dynamic threshold



Kraken

Deep-learning based anomaly detector

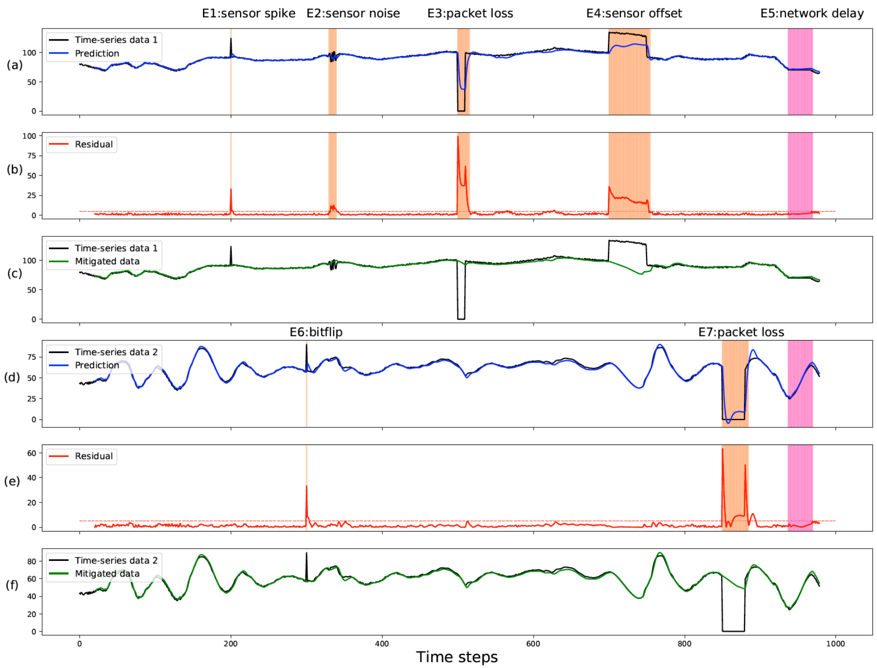
Workflow

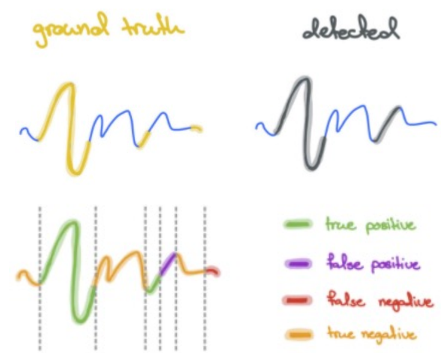


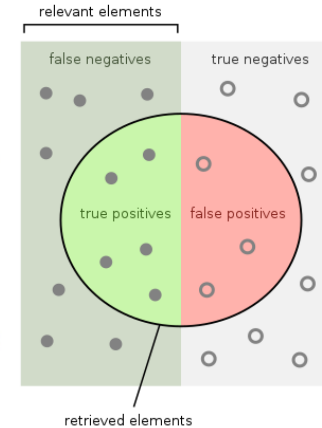
Kraken

Deep-learning based anomaly detector

Evaluation

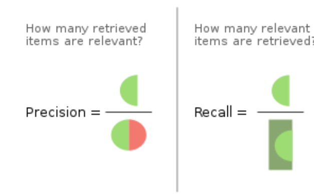






$$Precision = \frac{TP}{TP+FP}, \quad Recall = \frac{TP}{TP+FN}$$

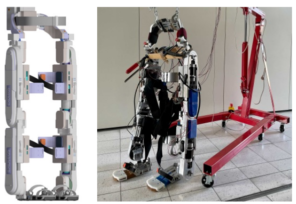
$$F_\beta = (1+\beta^2)\frac{Precision \cdot Recall}{(\beta^2 \cdot Precision) + Recall}$$



F1: recall and precision equally important
F2: recall twice as important as precision
F0.5: recall half as important as the precision

Kraken

Other use cases

		Simulink Model Description	Collected Data	Detector	Publications
	Robotic Colabartive Manipulators	Emulation of manufacturing process with two manipulators sharing a tool. • One robot takes the tool from tool holder A with randomized waypoints and puts it to tool holder B. • Another robot takes the tool from tool holder B and put it back to tool holder A	• Time series data • Collected from the sensors of the joints • Saved as CSV files	• MLP • Auto Encoder • Stacked GRU • Stacked LSTM • Transformer	• KrakenBox: Deep Learning based Error Detector for Industrial Cyber-Physical Systems (IMECE2021) • Anomaly Detection for Cyber Physical Systems using Transformers (IMECE2021) • Model-Based Error Detection for Industrial Automation Systems Using LSTM Networks (IMBSA2020) • Deep Learning-basierter Fehlerdetektor für industrielle Cyber-Physische Systeme (Industrie 4.0 Management) • On-line error detection and mitigation for time-series data of cyber-physical systems using deep learning based methods (EDCC2019)
	Robotic Exo-skeleton	Supportive exoskeleton system that assists elderly users in day-to-day activities. • Lower-limb 6-DOF supportive exoskeleton system. • The high-level controller is realized on a single-board computer connected to the joint controllers via the CAN bus using CANopen protocol. • The system along with the Simulink model is courtesy of KIT, Dr. Ilshat Mamaev.	• Time series data • Representing the signals collected from the joint • Saved as CSV files	• Stacked GRU • Stacked LSTM	• Deep Learning-based Error Mitigation for Assistive Exoskeleton with Computational-Resource-Limited Platform and Edge Tensor Processing Unit (IMECE2021) • Model-based Fault Injection Experiments for the Safety Analysis of Exoskeleton System (IMECE2020)
	Autonomous Vehicle System	Our simulation allows users to develop automated driving algorithms and assess their safety and performance. With the help of this, the safety of the implemented component or algorithm can be measured on both the vehicle level and the traffic level. We collected data from a scenario built under a simple scenario: • A front vehicle capable of sharing its position and speed • While another vehicle following it using adaptive cruise control system	• Time series data • Representing the speed and accleration of the vehicles • Transformed through wavelet filter into figures • Saved as figures in jpg form	• Random Forest • Gradient Boosting • CNN	• Tool Paper: Time Series Anomaly Detection Platform for MATLAB Simulink (IMBSA2022)
	Unmanned Aerial Vehicle	Emulation of parrot minidrone with four main components: • Flight Control System • Multicopter Model • Sensor Model • Environment Model	• Time series data • Representing the acceleration and gyroscope of the UAV • Saved as CSV files	• Random Forest • Bidirectional LSTM • CNN-LSTM	• IMU Sensor Faults Detection for UAV using Machine Learning (ESREL2022)

Kraken

Other use cases

Table 7. Performance of Machine Learning and Deep Learning models based on Test Dataset for Accelerometer

Architecture	Test Accuracy	F1 Score	Precision	Recall
Random Forest w/o Feature Engg.(baseline model)	89.0%	87.0%	88.0%	87.0%
Random Forest with Feature Engg.	98%	98%	97%	99%
Hybrid CNN-LSTM w/o Feature Engg.	**99.22%**	**99.0%**	**99.0%**	**99.0%**
BiLSTM w/o Feature Engg.	95%	94%	95%	94%

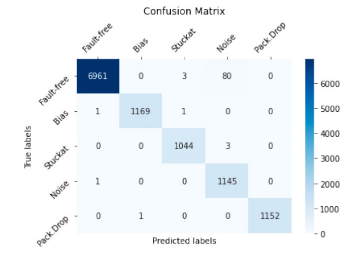


Fig. 12. Confusion Matrix of Hybrid CNN-LSTM model based on Test Dataset for Accelerometer.

Table 8. Performance of Machine Learning and Deep Learning models based on Test Dataset for Gyroscope

Architecture	Test Accuracy	F1 Score	Precision	Recall
Random Forest w/o Feature Engg. (baseline model)	82.0%	82.0%	82.0%	81.0%
Random Forest with Feature Engg.	**97%**	**96%**	**96%**	**97%**
Hybrid CNN-LSTM w/o Feature Engg.	90.0%	90.0%	91.0%	90.0%
Hybrid CNN-LSTM with Feature Engg.	93.0%	92.0%	92.0%	93.0%
BiLSTM w/o Feature Engg.	84.0%	83.0%	82.0%	83.0%

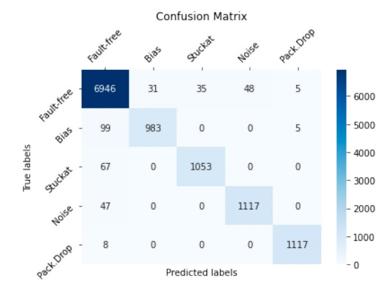
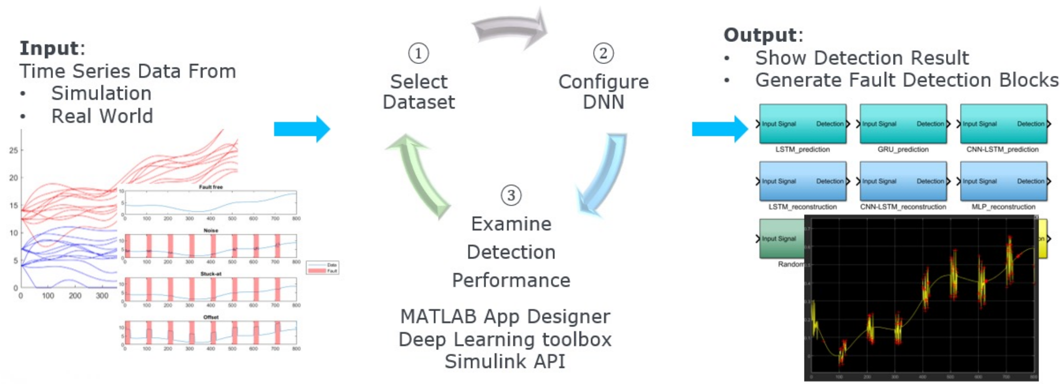


Fig. 13. Confusion Matrix of Random Forest model based on Test Dataset for Gyroscope.

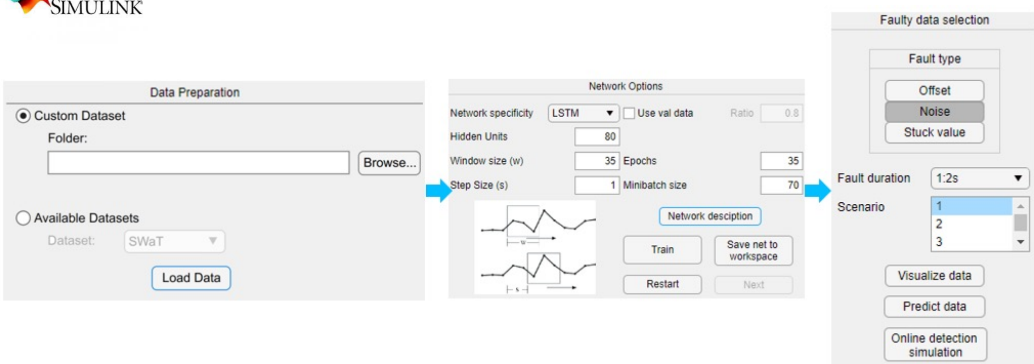
Unmanned Aerial Vehicle	Emulation of parrot minidrone with four main components: • Flight Control System • Multicopter Model • Sensor Model • Environment Model	• Time series data • Representing the acceleration and gyroscope of the UAV • Saved as CSV files	• Random Forest • Bidirectional LSTM • CNN-LSTM	• IMU Sensor Faults Detection for UAV using Machine Learning (ESREL2022)

Kraken

Time Series Anomaly Detection for Simulink



MATLAB SIMULINK



①Select Dataset and Preprocessing ② Configure DNN ③ Examine Detection Performance

Features:

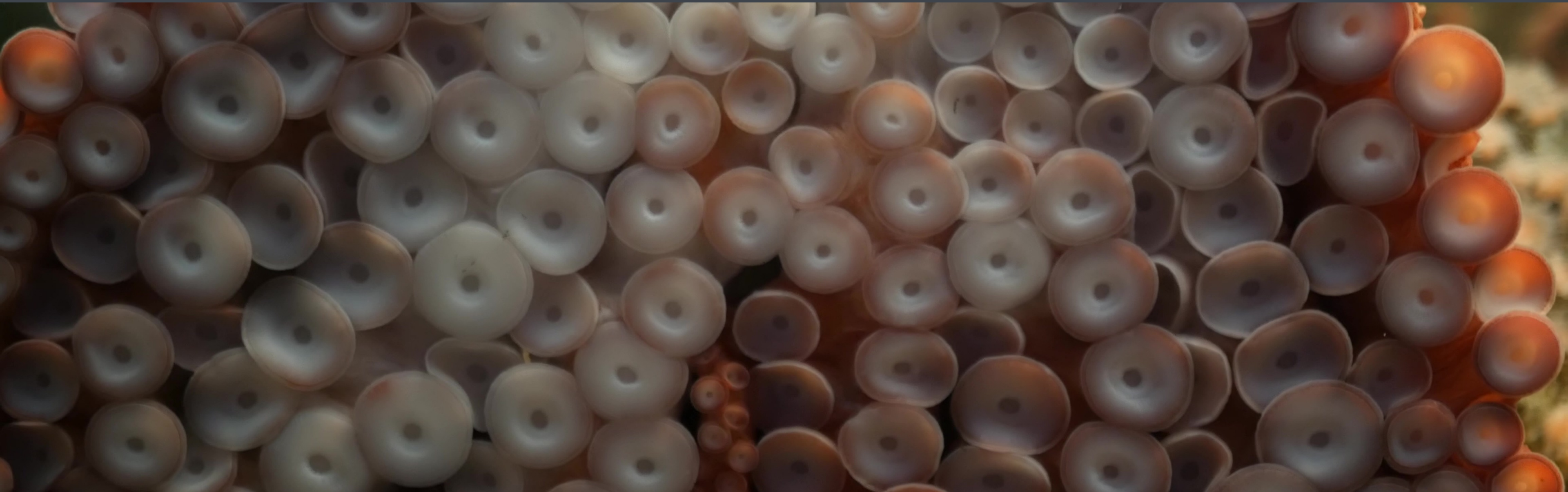
- Multiple DNN architectures
- Customizable hyper-parameters
- Several detection approaches
- Several evaluation methods
- Multiple fault types
- Multiple fault injection methods

“Tool Paper: Time Series Anomaly Detection Platform for MATLAB Simulink”, **Accepted to I**MBSA 2022

Open source:
https://github.com/mbsa-tud/tsad_platform

Part 4

Challenges

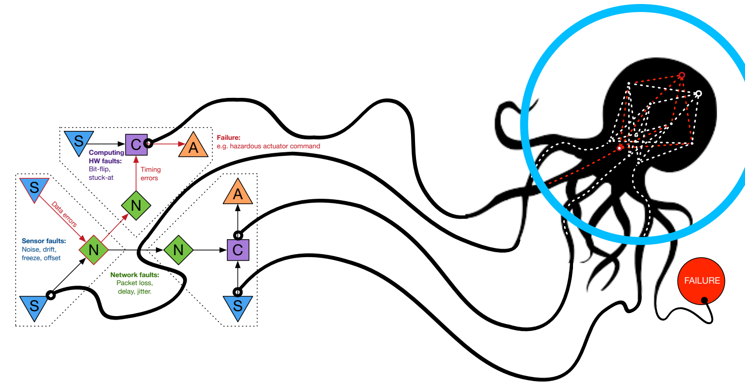


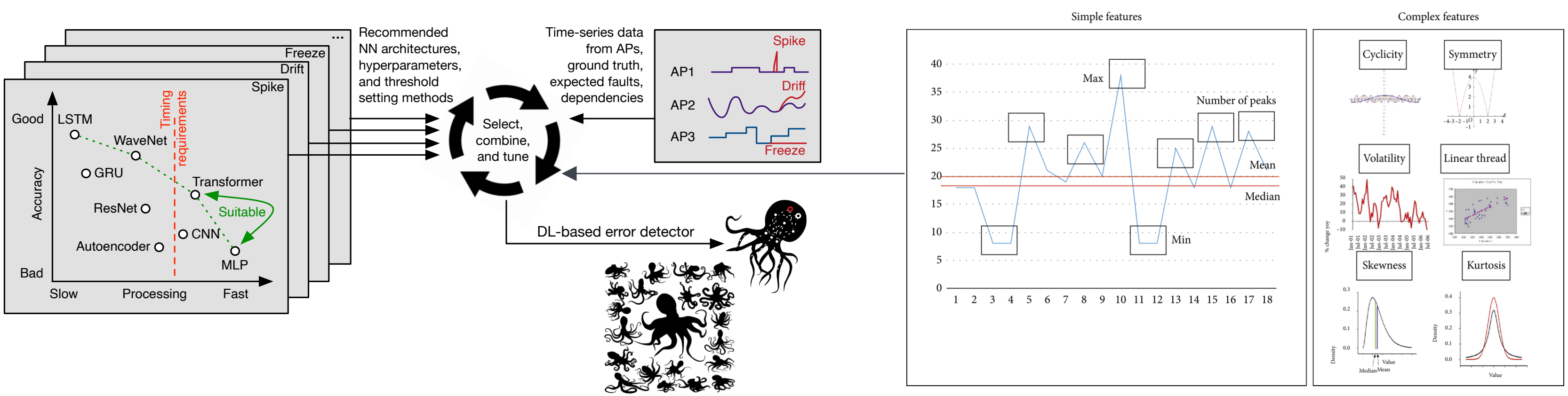
Challenges

How to select a suitable anomaly detector?

Context-aware anomaly detector:

- Search for optimal detection approach, deep learning architecture, hyperparameters;
- Combination (Ensemble) of several detectors;
- Dynamic switch of the detectors.

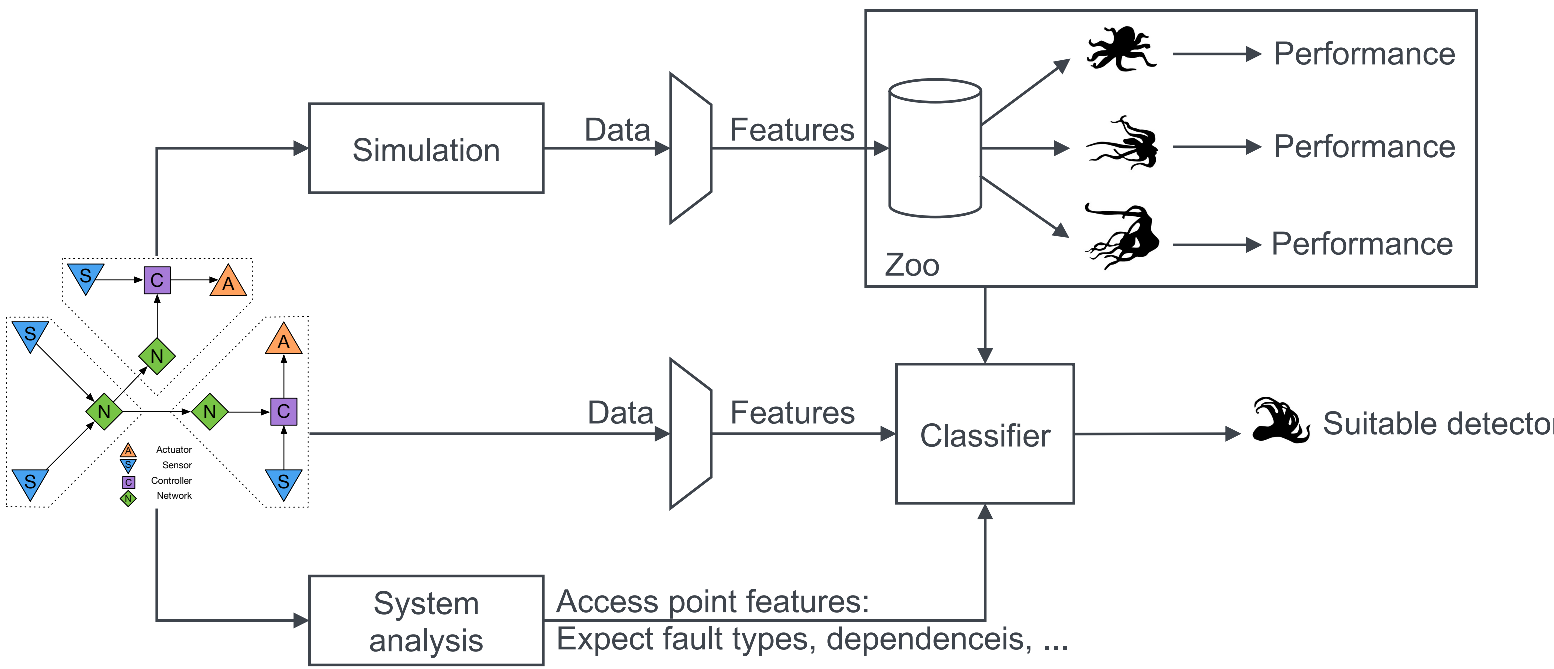




Challenges

How to select a suitable anomaly detector?

Context-aware anomaly detector:

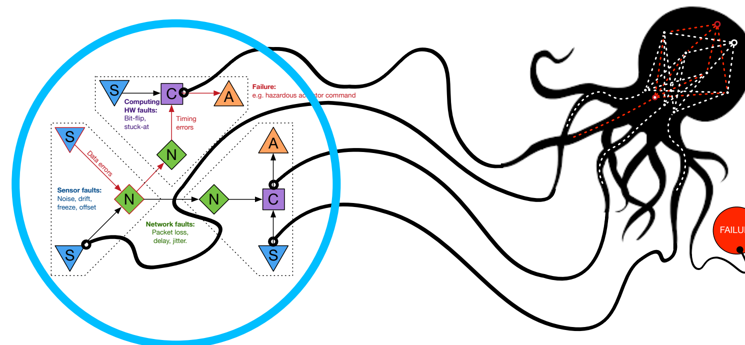


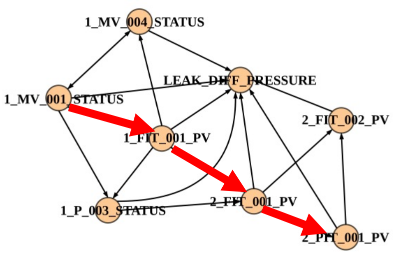
Challenges

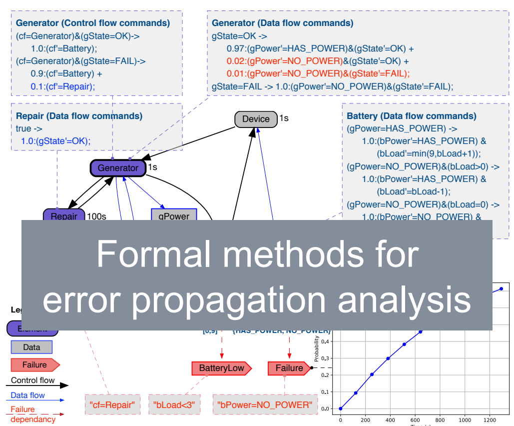
How to select a suitable access points?

Context-aware anomaly detector:

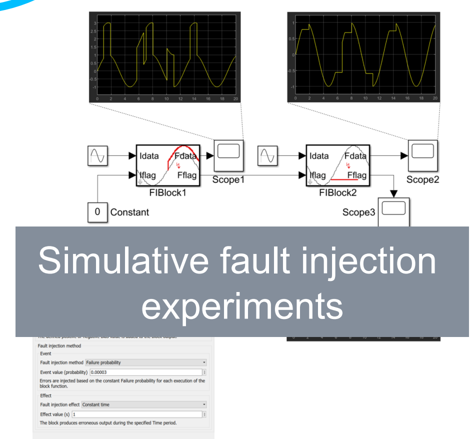
- System-level control flow, data flow, and error propagation analysis
- Dynamic switch according to the attention mechanism







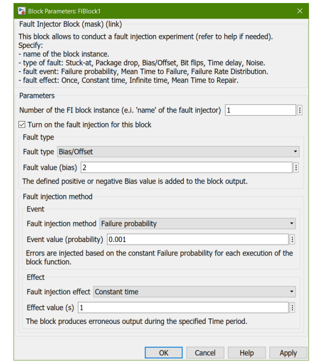
Formal methods for error propagation analysis

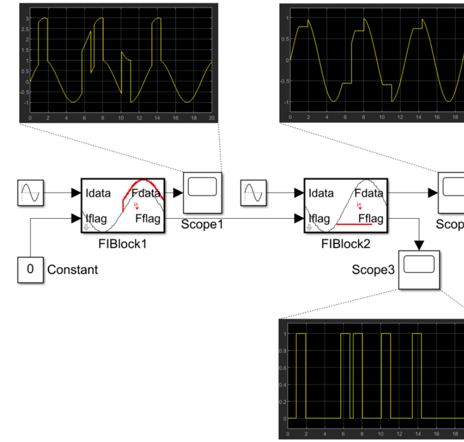


Simulative fault injection experiments

Challenges

How to generate training and testing data?



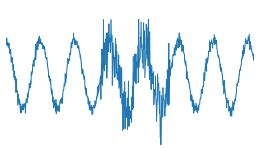
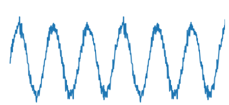
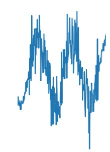


Fault Injection Tool FIBlock for Simulink

The user can specify:

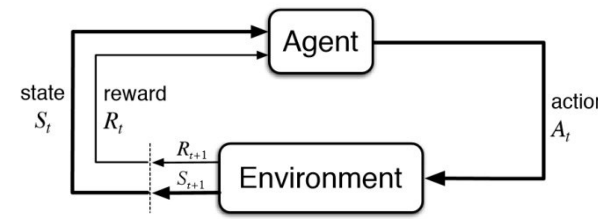
- Fault type: Stuck-at, Package drop, Bias/Offset, Bit flips, Time delay, Noise.
- Fault event: Failure probability, Mean Time to Failure, Failure Rate Distribution.
- Fault effect: Once, Constant time, Infinite time, Mean Time to Repair.

Augmented data = Normal data (real data) + Fault samples (from a database)

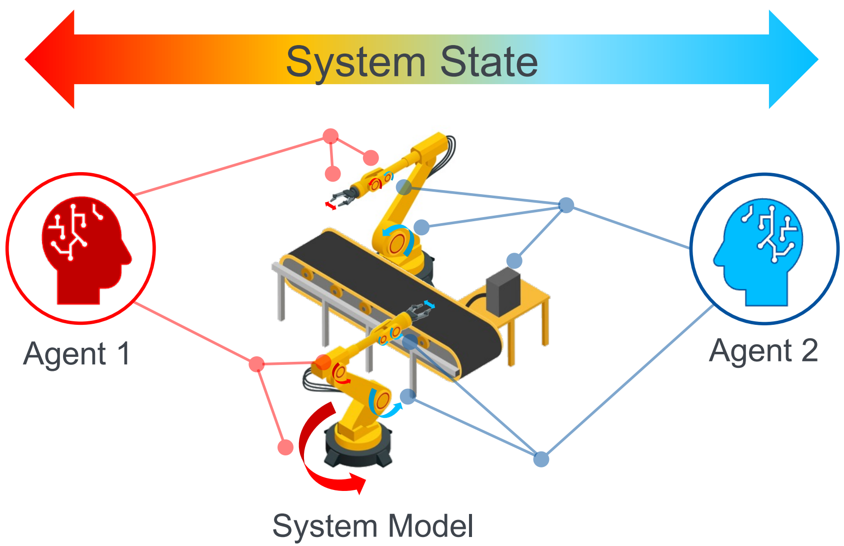




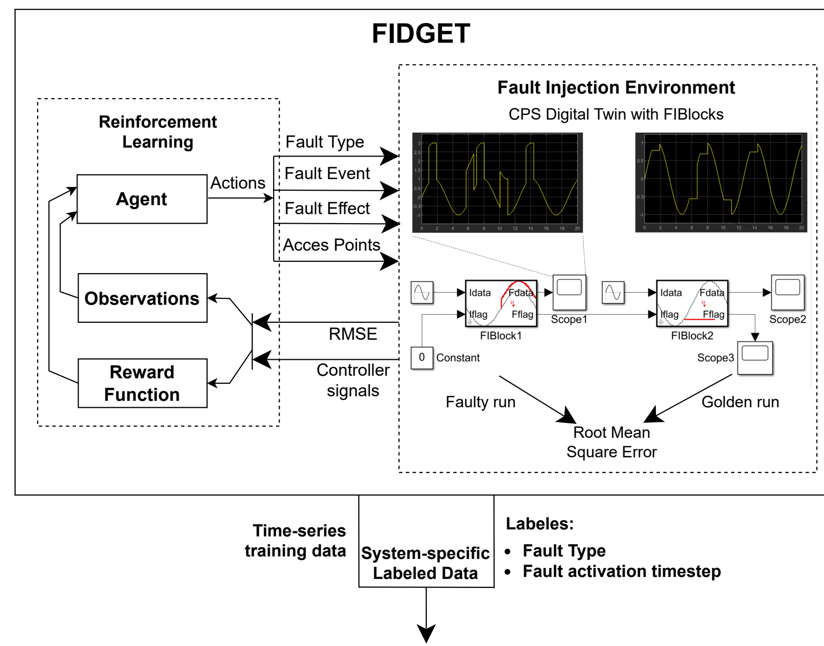
Challenges

How to generate training and testing data?



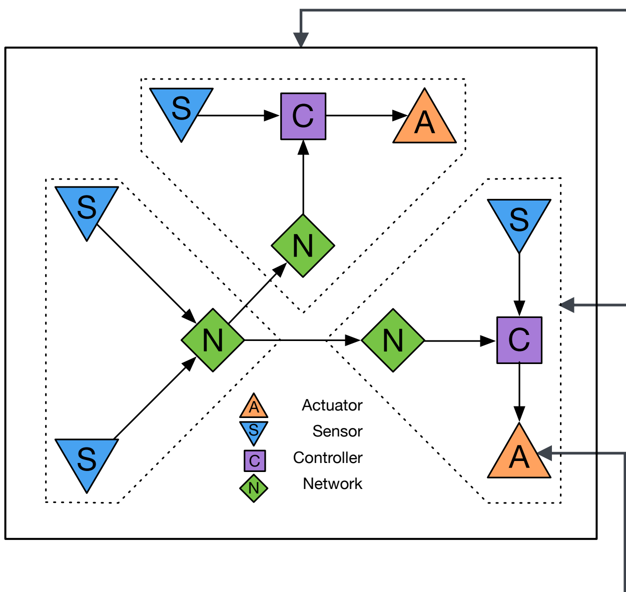
Reinforcement Learning-based Fault Injection

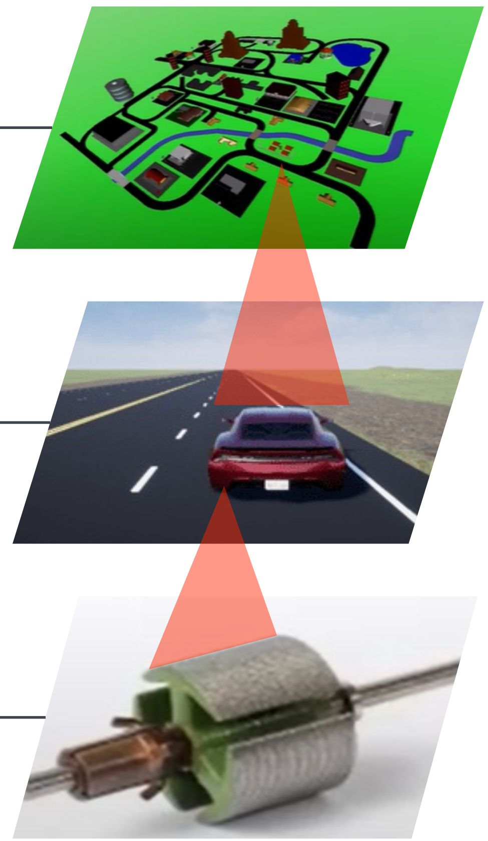




Challenges

Three levels of anomaly detection



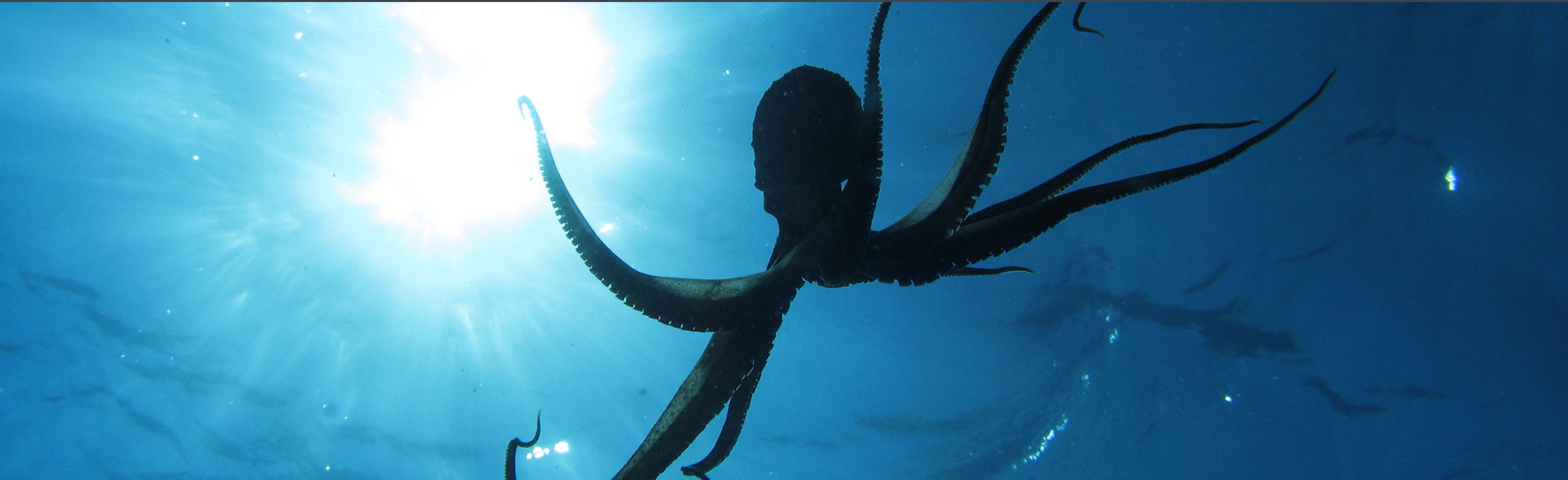


System-of-Systems-Level
- Attention switching
- Scaling
- Edge-Fog-Cloud

System-Level
- System analysis
- Dynamic switching access points
- Multivariate time series

Component-Level
- Selection, combination, tuning of DNNs
- Dynamic switching of DNNs
- Univariate time series

Thank you



Vielen Dank!

Jun.-Prof. Dr.-Ing. Andrey Morozov

e-mail andrey.morozov@ias.uni-stuttgart.de
phone +49 (0) 711 685-67312
www.ias.uni-stuttgart.de/en/institute/team/Morozov/

University of Stuttgart
Institute of Industrial Automation and Software Engineering
Networked Automation Systems