Advantages of anomaly detection between a controlling unit and its process devices for Industrial Control Systems

Rick Lahaye
Anouk Boukema

supervisor:
Dima van de Wouw
Deloitte

The Problem

ICS is usually old

- Security not main focus
- Meant to last for 20-30 years
- Continuously available

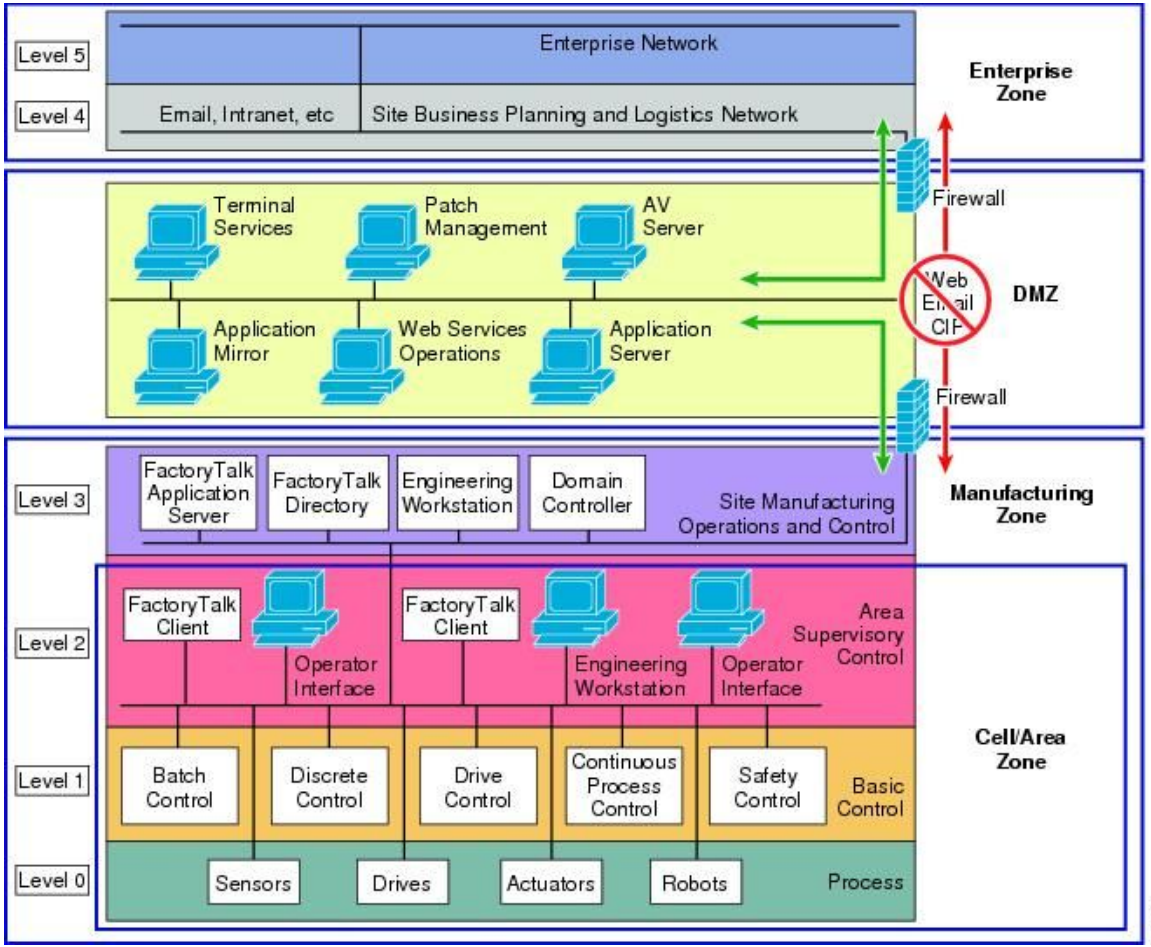
Wrong production

- Destroy centrifuge
- Power outage

Problem Analysis

- Initial infection coming from within company
- Overwrites PLC
- Fools every device above PLC

Hack is found only when damage is noticeable



Purdue Model for Control Hierarchy

Research Question & Methodology

Research Question

"What are the advantages of anomaly detection between the controlling unit and its process devices?"

Methodology

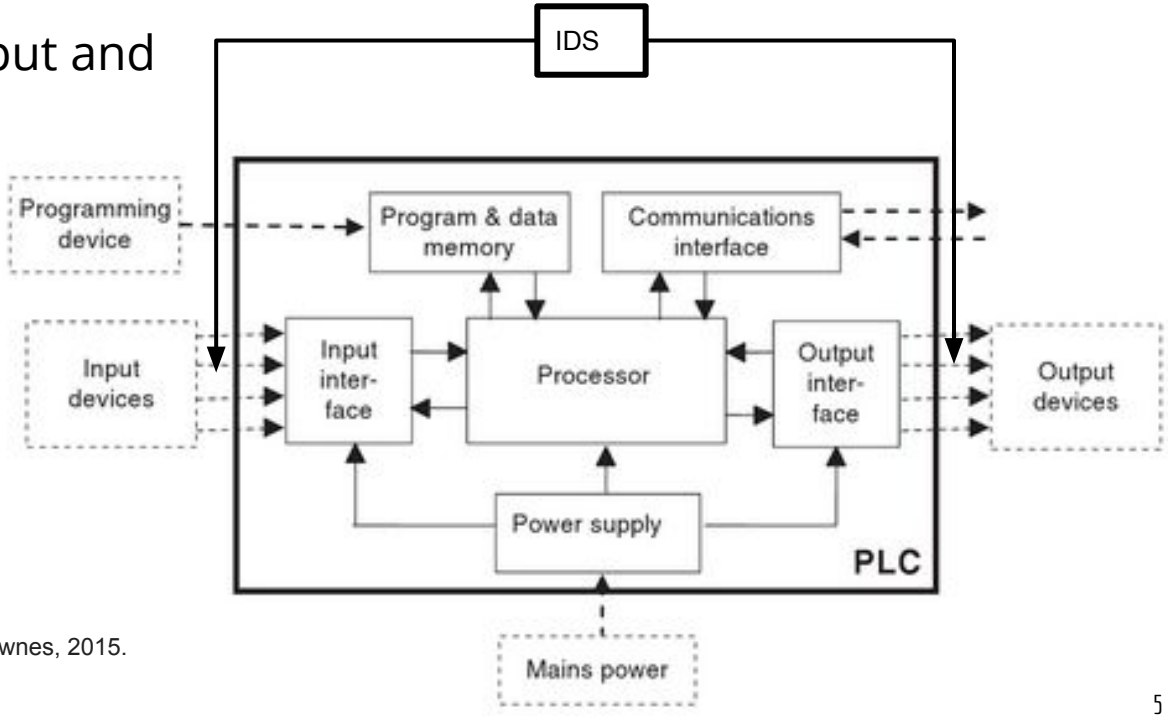
1. Related Work
2. Literature Study
3. Proof of Concept
    a. data experiments

Solution to Minimize Damage

Detection along with Prevention

Anomaly detection at the input and output devices of PLC

- raw data
- Integer data
- Just before PLC



Source: Bolton, William. *Programmable logic controllers*. Newnes, 2015.

Related Work

Detection between level 1 and 0 already provided by security companies?

- Do not give much info
- Not in the white papers

Why so little info?

- Competitive reasons
- Confidentiality (security)

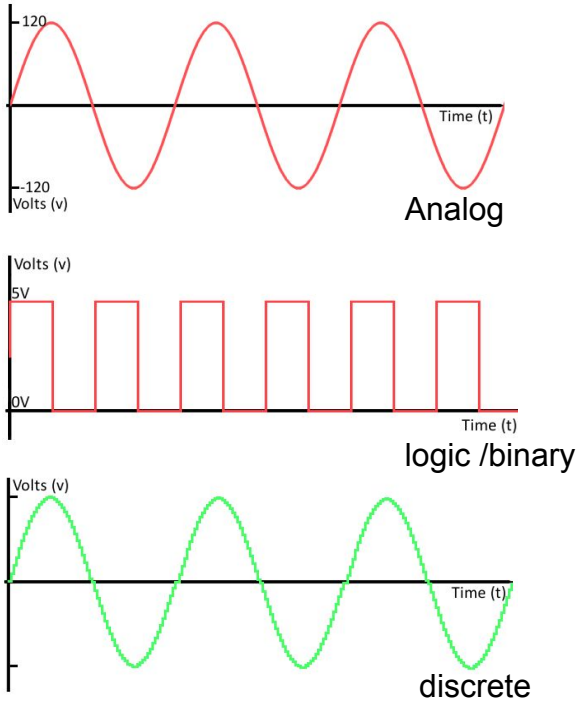
Source: http://www.icscybersecurityconference.com/

Anomaly Detection on Raw Data

3 types of in- and output signals of level 0 devices

Conform to a pattern of the production process

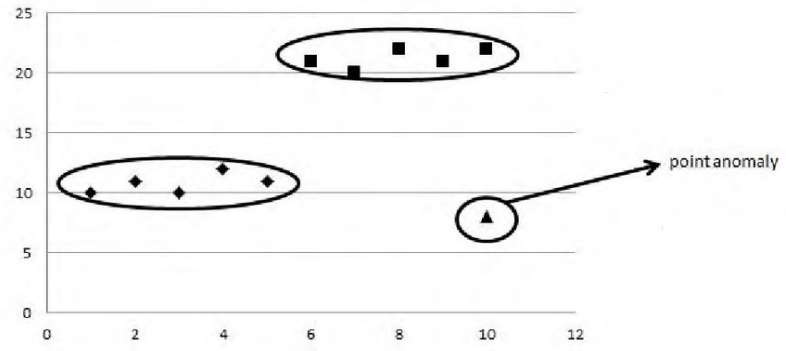
- Keeping right temperature



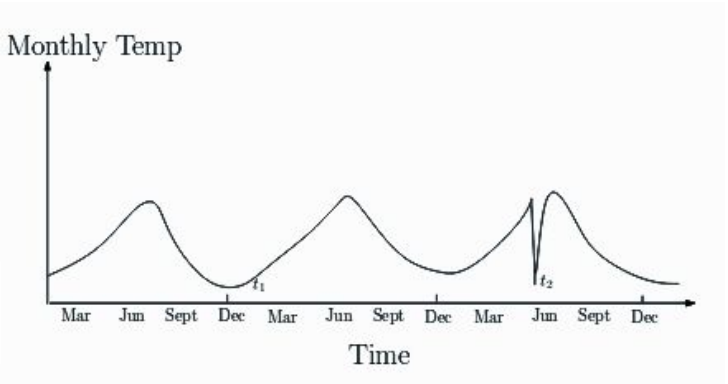
Source: https://learn.sparkfun.com/tutorials/analog-vs-digital

Anomaly Types

- Point Anomalies
- Contextual Anomalies



ICS specific what is of high importance



source : http://cucis.ece.northwestern.edu/projects/DMS/publications/AnomalyDetection.pdf

Proof of Concept

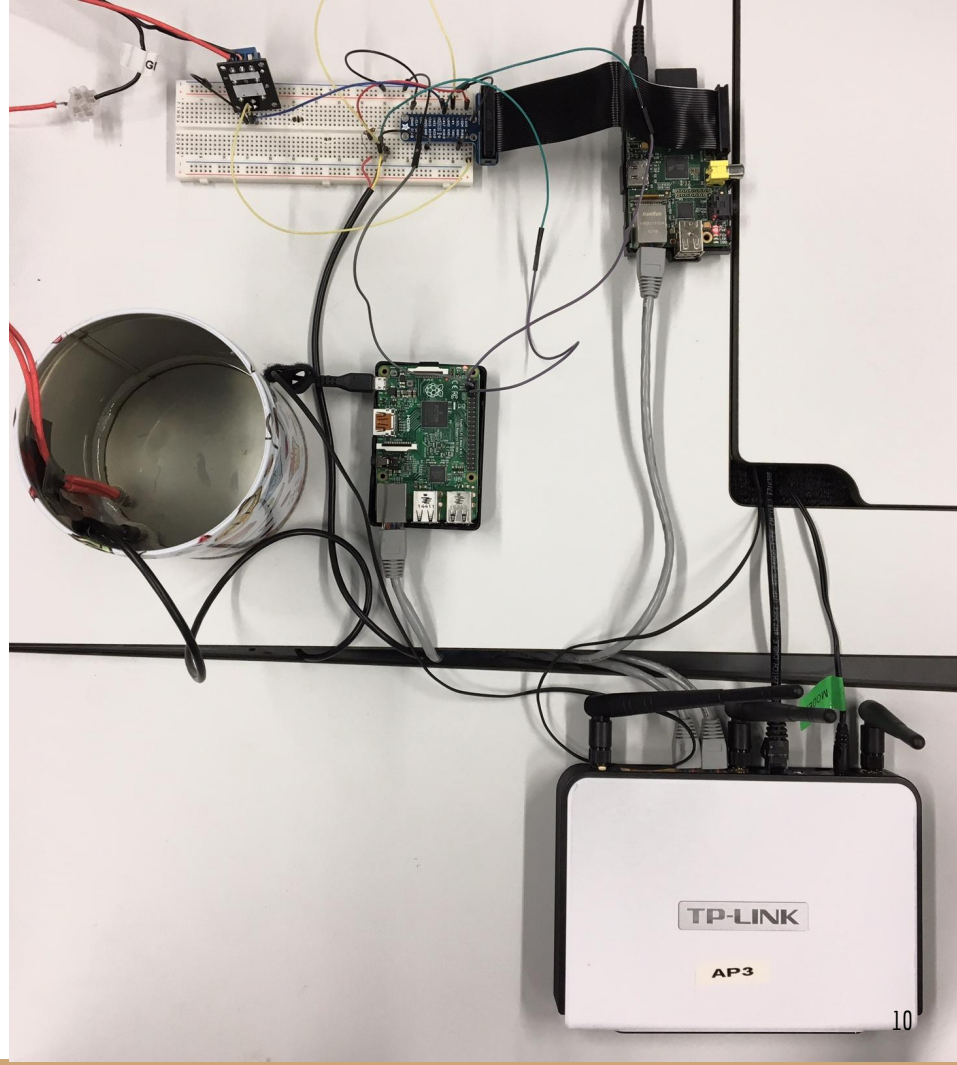
Requirements

- Point and Contextual Anomaly Detection
- Realistic comparison to ICS
- Available components for setup
- Simple setup to proof possibility to our research question

Closed Thermostatic Environment

Components

- Heater (digital logic signal)
- Sensor (digital discrete signal)
- Raspberry Pi - PLC
- Raspberry Pi 2 - IDS



Anomaly Detection Techniques for PoC

Requirements of ADT	Knowledge Based	ML SVM	ML LSTM
Real-Time	✓	✓	✓
Point detection	✓	✓	✓
Contextual detection	✓	✗	✓
Generic setup	✗	✓	✓

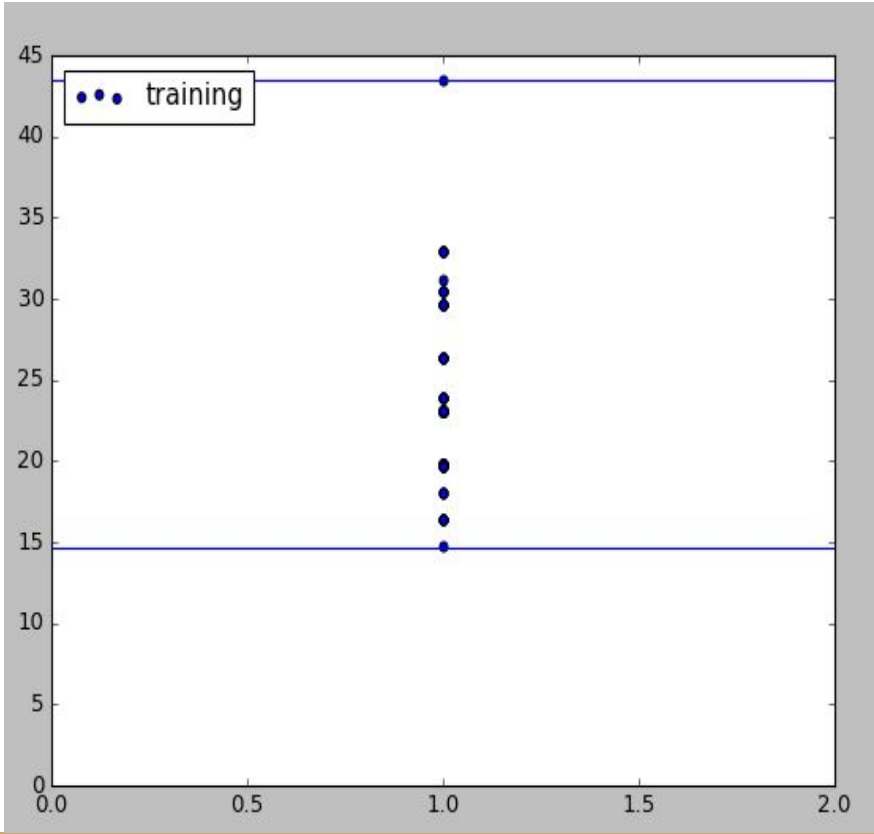
ML-based One Class Support Vector Machine

Implementation

- Unsupervised learning (unlabeled)
- On training data
- Classification

Proof of Concept

- Real time classification every second



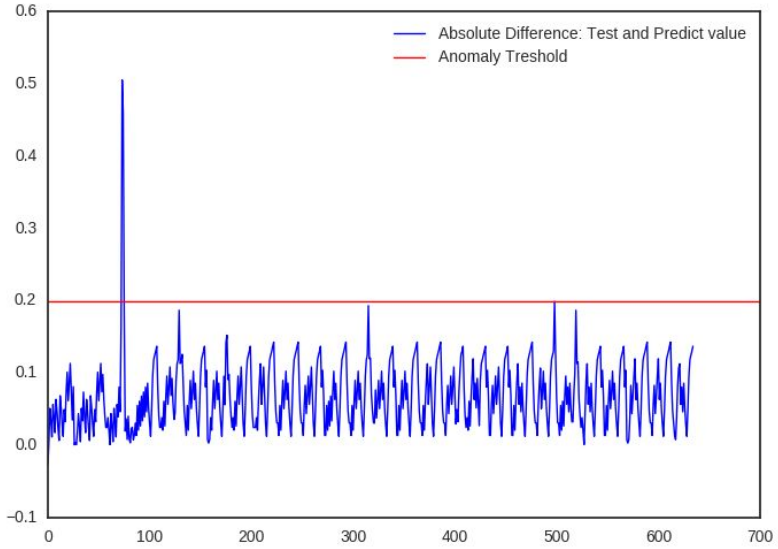
ML-based Long Short-Term Memory

Prediction by LSTM network

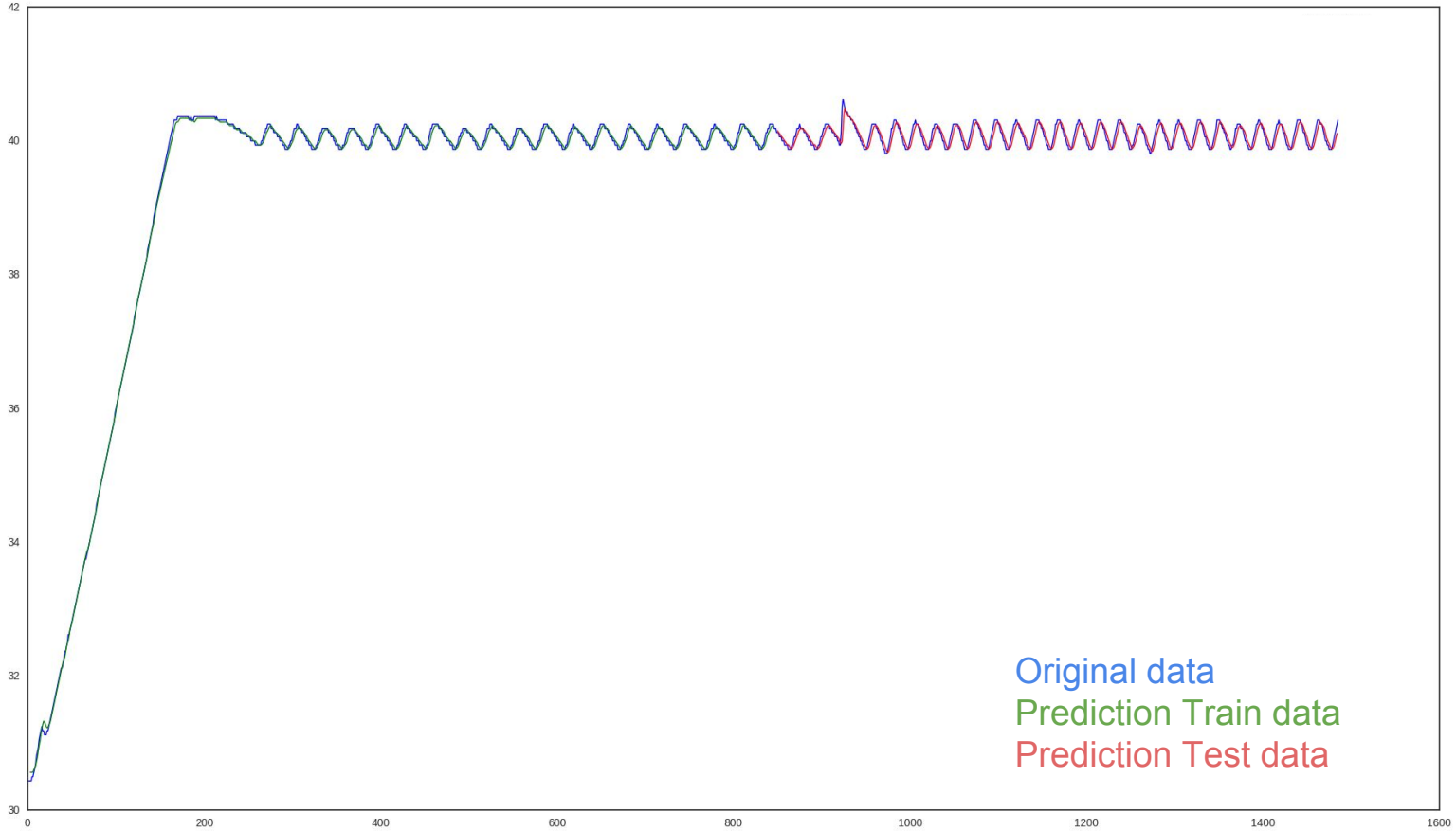
- Recurrent Neural Network
- Windowsize 3

Anomaly Detections

- Norm = |Real value - Predicted value|
- Threshold = Max($Norm_{Train}$)
- Anomaly = {x | $Norm_{Test}$ (x) > Threshold}



Source: Jason Brownlee.Time Series Prediction with LSTM Recurrent Neural Networks in Python with Keras.
Source: Pankaj Malhotra et al. “Long short term memory networks for anomalydetection in time series


42
40
38
36
34
32
30
0
200
400
600
800
1000
1200
1400
1600
Original data
Prediction Train data
Prediction Test data

The Data

IDS.py script

- Writes train and test files
- Uses multithreading to run SVM and LSTM concurrently both use train data
- SVM is real-time
- LSTM on test data file

30.0	0	1485959229.51
30.0	0	1485959230.34
30.0	0	1485959231.17
30.0	0	1485959232.0
29.937	0	1485959232.83
30.0	0	1485959233.66
29.937	1	1485959234.49
29.937	1	1485959235.32
29.937	1	1485959236.15
29.937	1	1485959236.97
29.937	1	1485959237.79
29.937	1	1485959238.61
29.937	1	1485959239.43
29.937	1	1485959240.25
29.937	1	1485959241.07
29.937	1	1485959241.89
29.937	1	1485959242.71
29.937	1	1485959243.53
29.937	1	1485959244.35
30.0	1	1485959245.17
30.0	1	1485959245.99
30.0	1	1485959246.81
30.062	0	1485959247.63

30.062

Results IDS

new test session starts for 10.0 minutes 2017-02-06 17:18:52
SVM: Anomaly detected - heater was on for 1.639986038
Train length: 1091
Test length: 308
the train data is 0.77% of total
Threshold: 0.129699897766
LSTM: Anomaly has magnitude of 18% above norm

new test session starts for 10.0 minutes 2017-02-06 17:28:54
Train length: 1091
Test length: 305
the train data is 0.78% of total
Threshold: 0.129699897766

new test session starts for 10.0 minutes 2017-02-06 17:38:57
2017-02-06 17:33:16.160318

Experiments & Results

Trainset = 50 min. **Testset = 10 min.**	Knowledge based	SVM	LSTM
0. Nothing	✓	✓	✓
1. Remove sensor at min 2 and heater at 6 min for 10 sec	✓	✓	✓
2. Activate heater 5 sec longer after min 2	2/5	3/5	✓
3. Add Icecube at min 2	✓	✓	✓
4. Slowly remove 16% of water at min 2	✓	✓	✓

Conclusion

"What are the advantages of anomaly detection between the controlling unit its process devices?"

- Requirements are met by combining SVM and LSTM
- Anomaly detection to find:
  - 1. Malfunction of components
  - 2. Hacks
  - 3. Vandalism/Stupidity
- Cost Efficient
- ICS owner has to make the trade-off
  - Implementation and equipment cost VS prevented high damage costs
- Further development and research is needed to develop into a business use case

Discussion & Future Work

- Used a Pi instead of real PLC
- Not tested on other ICS environments
- Combine sensor and actuator data and compare for better Detection
- Setup warning system

Questions