# Machine-Learning-Based Electrical Signal Analysis for Intrusion Detection in Industrial Systems

In diesem Schritt, haben wir die Installation der Hardware beendet und die Implementation der Software begonnen. Wir haben die insgesamt 16 Signale abgreifen und abspeichern können.

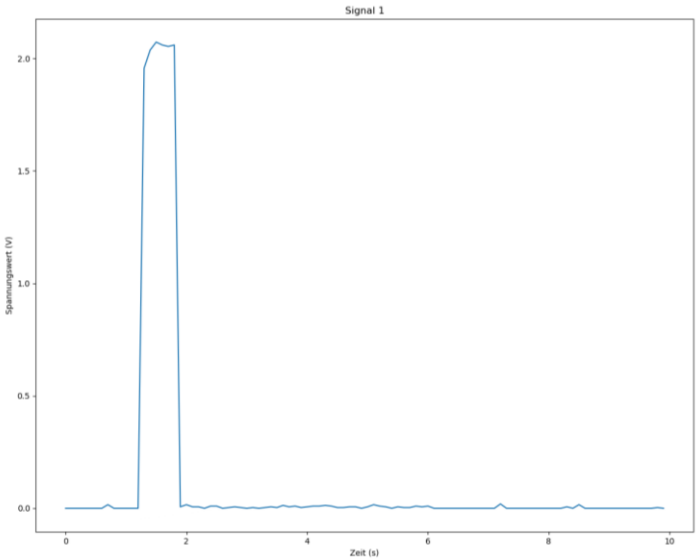


Abbildung 1: Signale 1, Objekt Erkennung

Zum Beispiel stellt Abbildung 1 eines der abgegriffenen Signale dar. Dieses Signal zeigt, wenn ein Objekt die Lichtschranke passiert. Die Lichtschranke ist links in Abbildung 2. Die Akquisition wird mit einem 10 Sekunden Zeitfenster und einer 10 Hz Frequenzabtastung durchgeführt.

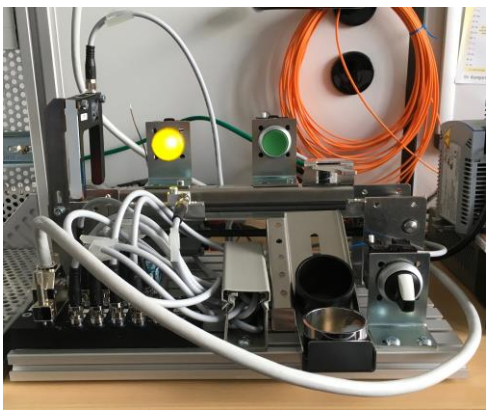

Abbildung 2: Komplete Prozess

Mit den Eingabesignalen können wir die maschinellen Lernverfahren trainieren. Wir haben mit dem 1D-CNN Ansatz aus [1] weitergemacht. Dieses CNN hat 6 Convolution Layers und 3 Concatenate Layers. Das Funktionsprinzip wird in Abbildung 3 dargestellt. Als Input übergebe man ein Array der letzten 30 Werte und als Output erhält man die nächsten 30 Werte. Wir vergleichen den Output mit den nächsten abgegriffenen Werten und mit einem Grenzwert können wir eine Anomalie erkennen.

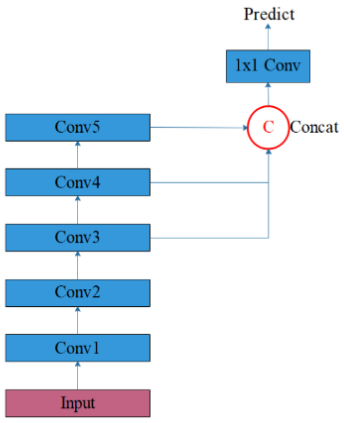


Abbildung 3: 1D-CNN

Um die Trainierzeit zu verbessern, benutzt man Dilation Convolution. Es lässt jede 2, oder mehr Werte aus um die Convolution zu berechnen. Die Abbildung 4 stellt dar wie die Dilation mit verschiedener Werter funktioniert.

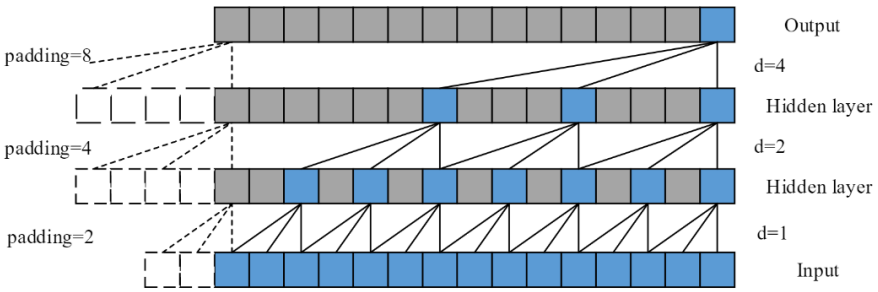


Abbildung 4: Dilation Convolution

Im nächsten Schritt, werde ich die nächsten ML-Methoden (Autoencoder, SVM, LSTM, RNN) fortfahren zu implementieren. Ich werde die Signale mit verschiedenen Frequenzabtastung abgreifen. Damit kann ich die ML-Methoden vergleichen und die beste Frequenzabtastung, welche die beste Lösung ergibt, auswählen.

[1] Yangdong He and Jiabao Zhao, “Temporal Convolutional Networks for Anomaly Detection in Time Series”, 2019 J. Phys.: Conf. Ser. 1213 042050