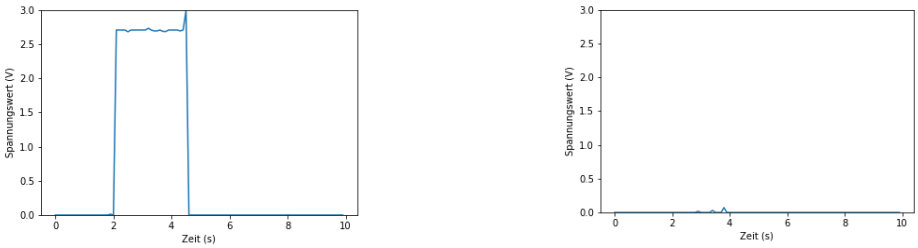
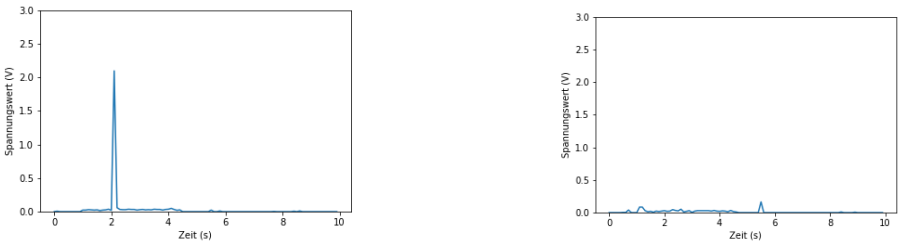
Machine-Learning-Based Electrical Signal Analysis for Intrusion Detection in Industrial Systems

In diesem Schritt, habe ich die Signale des Raspberry analysiert, einen Autoencoder und eine Support-Vector-Maschine (SVM) implementiert, den Zwischenvortrag vorbereitet und die Signale während verschiedener Angriffe aufgezeichnet.

Das System nutzt acht verschiedene Signale. Das Signal der Schranke zeigt, wenn die Schranke runter geht. Der induktive Sensor zeigt, wenn ein Silver Bucket detektiert wird. Das Funktionsprinzip wird in Abbildung 1 dargestellt.



a) Das Signal der Schranke zu einem Silver (links) und einem Black Bucket (rechts)



b) Signal des induktiven Sensors zu einem Silver (links) und einem Black Bucket (rechts)

Abbildung 1: Schranke Signale (a) und Induktiv Sensor Signale (Links)

Jedes der Signale im betrachteten Prozess repräsentiert einen logischen Wahrheitswert (wahr oder falsch). Die weiteren sechs Signale repräsentieren, ob das Laufband an ist, der Taster betätigt wurde, das Laufband nach links geht, die Leuchte eingeschaltet wird, der Schalter betätigt wurde und ob die Lichtschranke ausgelöst wurde.

Mit diesen Signalen, haben wir mit dem Autoencoder Ansatz aus [1] weitergemacht. Dieses Autoencoder hat 9 Fully Connected Layers. Die Dimensionsreduktion geht von 256 bis 14. Das Funktionsprinzip wird in Abbildung 2 dargestellt. Als Input übergibt man ein Array der letzten 40 Werte von jedem Sensor und als Output erhält man die nächsten 40 Werte.

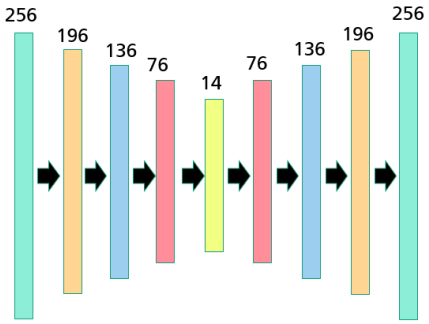


Abbildung 2: Autoencoder

In Abbildung 3, ist die Loss Evolution während des Lernens dargestellt. Das Lernen ist schneller als das Lernen für den 1D-CNN jedoch ist der Loss höher.

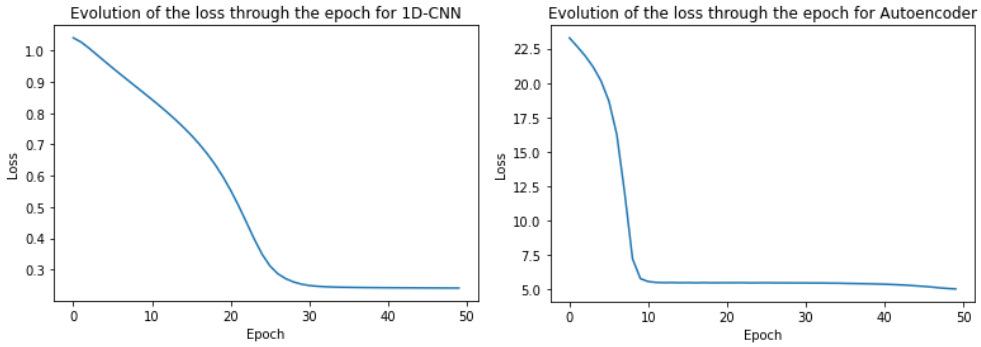


Abbildung 3: Loss Evolution der 1D-CNN (links) und der Autoencoder (rechts)

Wir haben auch die Signale von drei verschiedenen Angriffen abgegriffen. Der Rename-Angriff verändert den Gerätname des Buskopplers so dass die SPS nicht mehr mit dem Buskoppler kommunizieren kann. Der Relay-Angriff stoppt den Prozess und das Laufband geht nach links. Der letzte Angriff ist der Safety-Angriff der den Notaus Knopf verhindert.

Im nächsten Schritt, werde ich eine statistische Analyse der Signale machen. Ich werde die von mir ausgesuchten ML-Methoden und die im Zwischenvortrag vorgeschlagenen Methoden mit den Angriffen testen. Ich werde mit dem Schreiben der Masterarbeit beginnen.

[1] K. K. Reddy, S. Sarkar, V. Venugopalan, and M. Giering, “Anomaly Detection and Fault Disambiguation in Large Flight Data: A Multi-modal Deep Auto-encoder Approach.” in Annual Conf. Prognostics and Health Management Society (2016).