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

Um Anomalien in industriellen Systemen zu detektieren, wollen wir eine günstige, einfache und performante Lösung finden. Dafür wurden seit Beginn der Masterarbeit die Vorbereitungen getroffen. Es wurden verschiedene Möglichkeiten zur Signalmessungen und -verarbeitung analysiert. Die Ergebnisse der Analyse werden im Folgenden vorgestellt.

Zuerst müssen wir die Signale der Sensoren abgreifen. Nach Recherche und Vergleich der Hardware zum Monitoring haben wir den Raspberry Pi 3 als zentrale Komponente ausgewählt. Wir ersetzen das DB15 Kabel zwischen den Buskoppler und dem Prozess mit 2 Kabeln und ein elektrisches Board. Auf das Board schließen wir die Kabel an so dass 2 ADC die Signale lesen, weil der Raspberry Pi nur numerischen Signalen lesen kann. Beide ADC sind MCP3008 Konverter die maximal 8 Signale abgreifen können. Das folgende Bild zeigt die finale Montage.

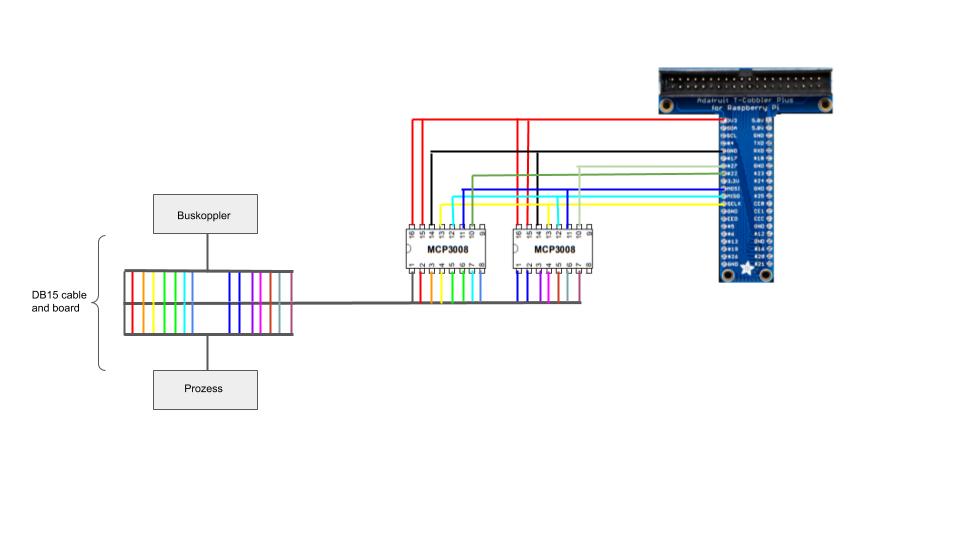


Abbildung 1: elektrische Montage um die Signale abzugreifen

Danach habe ich verschiedene in der Literatur vorgeschlagene Methoden zur Detektion von Anomalien analysiert. Wir wollen mehrere Methoden vergleichen und am Ende werden wir die beste Lösung für unsere Systeme empfehlen können.

Die erste Methode basiert auf das Convolutional Neural Networks (CNN). Das CNN lernt die Merkmale der Signale mit Faltungs-Layer. Drei Netzwerke werden aufgebaut. Das erste Netzwerk ist ein einfaches CNN (wie [1]) und der Output sind die vorhergesagten Signale. Das zweite Netzwerk benutzt Dimension Reduktion (wie [2]). Der Output ist die Entscheidung ob es eine Anomalie gibt oder nicht. Das letzte Netzwerk ist ein Autoencoder (wie [3]).

Die zweite Methode basiert auf Recurrent Neural Networks (RNN) (wie [4]). Wir wollen auch die Long Short-Time Memory (LSTM) (wie [5]) implementieren, weil sie meist bessere Ergebnisse liefern als RNNs.

Die letzte Methode basiert auf Support Vector Machines (SVM) (wie [6]). SVM kategorisiert die Signale in zwei Klassen. Eine Klasse besteht aus allen richtigen Werten der Signale und die andere besteht aus aller falschen Werter etwa den Anomalien.

Im nächsten Schritt, werde ich die Hardware installieren um die Signale abzugreifen und zu verarbeiten. Der Hardware darf nicht die Signale zwischen den Buskoppler und dem Prozess stören. Außerdem setze ich meine Literaturrecherche fort. Ich werde mit der Einarbeitung in die ICS Angriffe und den Machine Learning Frameworks beginnen.

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

[2] T. Ince, S. Kiranyaz, L. Eren, M. Askar, and M. Gabbouj, “Real-time motor fault detection by 1-d convolutional neural networks.” IEEE Trans. Ind. Electron., 63, 7067 (2016).

[3] 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).

[4] Xiang Li,Qian Ding, Jian-Qiao Sun, “Remaining Useful Life Estimation in Prognostics Using Deep Convolution Neural Networks.” Preprint submitted to Elsevier Science, June 2017

[5] YoudaoWang, Yifan Zhao, Sri Addepalli, “Remaining Useful Life Prediction using Deep Learning Approaches: A Review”, license (http://creativecommons.org/licenses/by-nc-nd/4.0/), 8th International Conference on Through-Life Engineering Service – TESConf 2019, October 27 – 29, 2019

[6] V. T. Tran, H. T. Pham, B. S. Yang, and T. T. Nguyen, “Machine performance degradation assessment and remaining useful life prediction using proportional hazard model and support vector machine.” Mechanical Syst. Signal Process., 32, 320 (2012).