Industry, Production and Logistics

Machine Learning for Anomaly Detection in Time-Series Produced by Industrial Processes

Lorenz Rychener, J. Hennebert

HES-SO, HEIA-Fribourg, iCoSys – Institute of Complex Systems

Abstract

In the recent years, anomaly detection in time series has gained lots of attention. New paradigms like Industry 4.0 and Internet of Things are indeed pushing for digitalization of many industrial processes. Automating the detection of anomalies is a challenging problem due to the diversity of the processes that can produce them, due to the rarity of such events and due to the real-time nature of the problem. Machine Learning (ML) has the potential to offer solutions to these challenges by learning automatically from streamed data and avoiding the cumbersome work of handcrafting rule-based systems. This paper is written in the context of a PhD thesis focusing on this domain and supported by different applied research project. We present here a short survey of anomaly detection, a summary of the 3 main challenges and a taxonomy of ML systems applicable in industrial context.

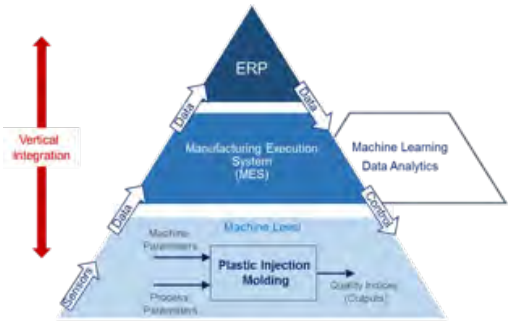
An anomaly in data is a measurement that deviated from the standard, the normal distribution or the expected behaviour [1]. Anomaly detection is an active field that has found many applications such as in telecommunications for network monitoring [2], in finance for detection of fraudulent use of credit cards [3], or in medicine for pathology detection [4]. A strong emerging field is in the supervision, optimisation and proactive maintenance of industrial processes where physical and software components are deeply intertwined forming cyber-physical systems [5][6]. In this field, we are usually facing 3 challenges.

Diversity. Industrial processes are diverse and the associated data can be stationary, cyclic, or including random variabilities. For each industrial process, multiple types of anomalies can also be observed such as drop, drift or time-related asynchronisation. Finally, values of a given sensor may be correlated to other sensors making the anomaly detection a multi-variate problem. By learning on exemplar data, ML is allowing adaptation to a multitude of processes and types of anomalies.

Rarity. Another difficulty is in the de-facto rarity of anomalies making it difficult to build a priori rules or models of such events. Again, machine learning allows to build robust models of normality where the data is abundant. The problem is then shifted to the detection of a deviation from the normality. When examples of anomalies are available, models of anomalies can also be built to discriminate against the model of normality.

Reactivity and density. The current trend for industrial machine is indeed to incorporate numerous sensors to observe the vital parameters of the machine and also, for production

	Type A	Type B	Type C
Examples of anomalies	None	Few	Many
ML category	Unsupervised	Semi-supervised / active learning	Supervised
Typical applications	Detect deviations from normality	Discriminate normal from abnormal	Classify types of anomalies



machines, to collect measurement related to the quality of the objects under production. The shift is going towards real-time anomaly detection in rather dense streaming of heterogeneous data. The top right Figure above illustrates this concept of *Vertical Integration* in the context of plastic injection where machines in a shop floor will be connected by Manufacturing Execution Systems themselves connected to ERP Systems, providing ML systems with large quantities of data [6]. Again, ML and more specifically Deep Learning can leverage on efficient GPU based hardware to cope with these challenges.

In the field of industrial processes, we can propose a taxonomy of three types of ML systems (see Table above). **Type A** – where there is no history of anomalies available. The ML approach is here unsupervised with the objective to model underlying data structures of normality and to compute a deviation from this model to detect anomalies. Potential methods include non-parametric distance based approaches such as K Nearest Neighbours, parametric probabilistic approaches such as Gaussian Mixture Models (GMMs) or deep learning systems to build prediction models. In this last case, an anomaly is detected when the actual value diverges too much from the predicted value [4][7]. **Type B** – where there are few examples of anomalies. Different strategies can be used to cope with the rarity of examples. A first one is to perform incremental learning from the normality model using for example MAP adaptation on top of GMMs. Other semi-supervised or active learning approaches can also be used to augment the quantity of anomaly examples and to improve the quality of the anomaly models [6]. **Type C** – where there are many examples of anomalies. In this situation, discriminant supervised classification systems can be used leading typically to the best performance of anomaly detection [7]. Ultimately, such systems could classify the types of anomalies, enabling automated control of machine settings to actively solve or avoid the anomaly.

References:

[1] V. Chandola et al, “Anomaly detection: A survey,” *ACM comp. surveys (CSUR)*, vol. 41 no. 3, p. 15, 2009.

[2] A. Lazarevic et al, “A comparative study of anomaly detection schemes in network intrusion detection,” in *Proc. SIAM Int. Conf. on Data Mining*. SIAM, pp. 25–36, 2003

[3] A. Srivastava et al. “Credit card fraud detection using hidden markov model,” *IEEE Transactions on dependable and secure computing*, vol. 5, no. 1, 2008, pp. 37–48, 2008

[4] S. Chauhan et al., “Anomaly detection in ECG time signals via deep long short-term memory networks,” in *Data Science and Adv. Analytics Int. Conf.* IEEE, 2015, pp. 1–7

[5] R. Anderl, “Industry 4.0–technological approaches, use cases, and implementation,” *at-Automatisierungstechnik*, vol. 63, no. 10, pp. 753– 765, 2015

[6] P. Morel et al., “Process 4 Plastics – Intelligence artificielle pour matériaux synthétiques”, Kunststoffxtra,Vol. 3, pp. 21-22, 2017

[7] N. Görnitz et al, “Toward supervised anomaly detection,” *Journal of Artificial Intelligence Research*, 2013.

[8] M. Wielgosz et al. “Using LSTM recurrent neural networks for detecting anomalous behavior of lhc superconducting magnets,” *arXiv preprint arXiv:1611.06241*, 2016