

Enhancing the Dependability of Cyber-physical Systems with AI-enabled Digital Twin

Qinghua Xu, Shaukat Ali, Tao Yue

Simula Research Laboratory, Kristian Augusts gate 23, Oslo and 0164, Norway

Keywords: *Cyber-physical Systems; Dependability; Uncertainty; Digital Twin, Artificial Intelligence*

Cyber-physical Systems (CPS) have played an essential role in Industry 4.0 [1]. Since then, CPS are evolving to be increasingly heterogeneous, integrated, intelligent, operating in dynamic and ever-changing environment. This exposes CPS to broader threats, which cannot be sufficiently tackled with traditional techniques. Our work focuses on exploring the potential of applying Digital Twin (DT) to improve dependability of CPS. The key idea is to build a DT as a virtual representation of a CPS, and develop DT functionalities with ML/AI algorithms to ensure the dependability of CPS operating in dynamic, uncertain and constantly-evolving environment.

This research topic started in 2020 in the Engineering Complex Software Systems Department at Simula. As the first step, we chose *Anomaly Detection* as our main targeted research area, which is a sub-domain of the CPS dependability. Our current work consists of three phases: 1) designing and building a **DT-based model**, 2) enhancing it with **Curriculum Learning (CL)** [2], and 3) improving it with **Transfer Learning** [3].

- First, we have proposed a general DT-based model for anomaly detection. In this work, we built a Timed Automaton Machine (TAM) as the digital representation of the CPS, and implemented a Generative Adversarial Network (GAN) to detect anomalies. We evaluated this method (named ATTAIN) with three public datasets and achieved state-of-art results.
- Second, we proposed LATTICE by extending ATTAIN by introducing CL to optimize its learning paradigm. CL is inspired by human learning process, which indicates that deep learning methods can benefit from a easy-to-difficult curriculum. We evaluated LATTICE with five public datasets and results show improvements over ATTAIN.
- Currently, we are exploring to use transfer learning to further improve LATTICE. This is motivated because we found that most existing methods (including ours) are CPS-agnostic and become obsolete when new scenarios emerge. Therefore, we plan to improve predictive performance and reduce prediction uncertainty by transferring knowledge from these obsolete models to new models. We will evaluate this work on real elevator data from Orona—world leader in building industrial elevators.

References

- [1] Kagermann, Wahlster W, Helbig J (2013) "Recommendations for implementing the strategic initiative INDUSTRIE 4.0" . *Final Rep Ind 40 WG*.
- [2] Soviany P, Ionescu RT, Rota P, Sebe N (2021) "Curriculum Learning: A Survey" . **14**, 1–29.
- [3] Weiss K, Khoshgoftaar TM, Wang DD (2016) "*A survey of transfer learning*" , Springer International Publishing.



Please mark your interests of contribution during the conference (choose multiple options that you are interested):

√	<i>I like to give an oral presentation</i>
	<i>I like to submit original unpublished scientific work in Nordic Machine Intelligence Journal</i>
	<i>I like to present a poster / demo</i>