Digital Twins of Cyber Physical Systems in Smart Manufacturing for Threat Simulation and Detection with Deep Learning for Time Series Classification

Carol Lo[1], Thu Yein Win[2], Zeinab Rezaeifar[1], Zaheer Khan[1], Phil Legg[1]
[1]University of the West of England, UK
[2]University of Sunderland, UK
Carol.Lo@uwe.ac.uk

***Abstract*—With increasing reliance on Cyber Physical Systems (CPS) for automation and control in Industry 4.0 and 5.0, ensuring their security against cyber threats has become paramount. Traditional security mechanisms, constrained by operational continuity and safety requirements, offer limited proactive threat detection capabilities against sophisticated Advanced Persistent Threats (APT). This research introduces the use of a Digital Twin testbed for repeatable simulation of diverse threat scenarios, generation of rich and varied datasets that depict a cyber incident, along with the ability to train time-series classification models for attack recognition. Our research aims to overcome the limitations of physical testbeds and challenges of data scarcity for Machine Learning (ML) or Deep Learning (DL) model development. By leveraging Digital Twins for data-driven analysis, this study proposes the use of supervised DL for accurate threat detection and classification in CPS within smart manufacturing. This paper demonstrates that Digital Twins testbed provides a cost-effective option for generating datasets to train and test supervised deep learning-based time series classification model for threat detection in CPS. It also discusses the benefits and limitations of the proposed testbed and suggests future research areas.**

***Index Terms*—digital twin, testbed, cyber security, threat simulation and detection, cyber physical systems**

I. Introduction

A. Challenges in Securing Cyber-Physical Systems (CPS)

In the realms of Industry 4.0 and 5.0, smart manufacturing often uses computerized and Internet-connected CPS to automate industrial processes, boosting productivity and fostering enhanced human-machine collaboration [1]. However, securing these systems present unique challenges, as they may have been designed historically without connectivity in mind, and they require continual uptime and so can be difficult to update. Therefore, strategies such as security through obscurity or isolation have been traditionally employed to protect these systems [2].

Cyber attacks targeting CPS can have severe consequences [3], as seen in the Maroochy water treatment plant attack in 2000, where a cyber incident led to the spillage of 800,000 liters of untreated sewage, affecting the local community. Similarly, the cyber attack on Ukraine's electric grid demonstrated the APT attack groups have the capabilities to cause extensive power outage. These examples highlight the urgent need for robust threat detection system.

B. Use of Testbeds for Security Experimentation

Testbeds provide a scaled-down, controlled replica environment of a complex industrial system, and are typically developed for high-risk industries where failures could have severe implications for public health, safety, and the environment [4], such as safety-critical manufacturing [5] and railway infrastructure [6]. These testbeds allow researchers to examine potential threats, test security measures, collect data, and train personnel in a risk-free and controlled environment.

While physical testbeds provide a realistic environment for experimentation, using physical testbeds come with significant drawbacks, including high setup and maintenance costs [7], confidentiality issues with real production data [8], [9], and the impracticality of replicating full-scale production environments. These inherent limitations often lead to difficulty in reproducing or verifying the work of others across the research community. Recognising these challenges, virtual testbeds, often based on simulation software such as Simulink [10], have emerged as a viable option for a more flexible and cost-effective approach as shown by [11] and [12].

Building on this notion, our research explores the potential of Digital Twins, which are virtual replicas of real-world processes, systems, or objects, as a testbed for simulating various threats in CPS and leveraging deep learning-based time series classification for advanced detection. This paper introduces a Digital Twin testbed that integrates Factory I/O [13], a simulation software with virtual sensors and actuators, and OpenPLC [14], an open-source programmable logic controller (PLC) platform, to create a virtual representation of physical manufacturing processes.

Our approach is novel in its focus on using supervised models for classifying both normal and advanced threat scenarios in CPS, providing actionable insights for enhanced situational awareness and rapid incident response. Our testbed enables a cost-effective, risk-free platform that facilitates realistic and repeatable threat simulation, data collection, model development, and evaluation. Furthermore, it addresses the limitations of traditional security mechanisms, and offers deeper insights into CPS dynamics for predictive security analytics.

C. Research Questions and Contributions

To overcome the challenges in industrial cyber security research and explore alternatives to physical testbeds, this paper aims to address the following two research questions:

1) To what extent can Digital Twins simulate varied threat scenarios in CPS to create robust datasets for enabling a proactive data-driven threat detection mechanism?
2) Can threat detection models trained on data from Digital Twins accurately classify threats in smart manufacturing CPS using time series classification with deep learning?

To answer the above questions, we leverage existing simulation technology to conduct threat simulation and data collection. The curated dataset is then used to train and test various time series classification models with deep learning for benchmarking their capabilities on accurately detecting and classifying simulated threats. This research make the following contributions to the field of CPS security:

- We demonstrate that a Digital Twin testbed can provide a cost-efficient and risk-free option for simulating various threat scenarios on CPS in smart manufacturing, and efficiently collecting and labeling data for training and testing threat detection models.
- We present the use of a Digital Twin to gather data for training and testing different supervised deep learning-based time series classification models, providing a novel approach to benchmark and enhance threat detection.

The remainder of this paper is organized as follows: Section II discusses related work and identifies gaps in current research practices. Section III details the design and implementation of the Digital Twins testbed, outlines the simulated threat scenarios, and describes the data collection, feature extraction, and labeling processes. The methodology and results of applying time series classification models for threat detection are presented in Section IIIE, and followed by a discussion of findings and limitations in Section IV. The paper concludes with future research directions in Section V.

II. Related Works

This section outlines the existing research literature and practices on using testbeds for research, the issues of insufficient security datasets and the use of Digital Twins for cyber security research are also discussed.

A. Use of Testbeds for Cyber Security Research

The implementation of physical testbeds ([15], [16], [17], [18], [19], [20], [5]), integrating real Industrial Control System (ICS) hardware and software, provides a highly realistic environment but significant financial investment and resources for development and maintenance [7]. Given the large scale and investment, it is not typically feasible to replicate such testbeds for the purpose of reproducible academic research.

In contrast, virtual testbeds usually leverage simulation software such as Simulink [10] for process simulation and MiniNet [21] for networking simulation. Although cost-effective and scalable, virtual testbeds may be criticised due to authenticity or fidelity of the real-world processes being modelled. For instance, GRFICS [22] relies on simulation software to emulate industrial components, such as SCADASim [23] for simulating SCADA system and MiniCPS [24] for simulating Programmable Logic Controllers (PLC). Despite criticisms, several studies [25], [11], [26], [27] demonstrated the use of virtual testbeds can successfully enable cyber security research.

Striking a balance, hybrid testbeds such as [12], [6], incorporating less ICS hardware components compared to physical testbeds, and use software to simulate part of the industrial processes. Hybrid testbeds offer a cost-effective setup, encompassing some physical aspects of the process, however the challenge of testbed sharing remains.

B. Datasets related to Advanced Persistent Threat (APT)

The scarcity of robust datasets for Advanced Persistent Threat (APT) research significantly hampers the ability to detect sophisticated cyber threats. Such issue have been outstanding for years, surveys conducted by [28], [29], [8], [9] and [30] all found that datasets used by researchers have been outdated, non-representative, lack of diversity and unreliable.

For the development, evaluation, and benchmarking of intrusion and anomaly detection systems to be effective, access to quality datasets is essential. However, dataset creation for the purposes of scientific empirical-based study is not straightforward. In some cases, datasets are constrained by operational and confidentiality concerns, leading to difficulties in sharing these datasets to the wider community. This contributes to the inability to reproduce research findings and subjects the work to potential criticism or rejection from academic publishers [31]. The absence of a systematic approach to develop, refresh, and maintain a repository of comprehensive, reliable datasets continues to be a significant barrier in APT research. Overcoming this gap is imperative for advancing threat detection.

C. Leveraging Digital Twin for Cyber Security Research

The adoption of Digital Twins within cyber security research has seen a notable increase in recent years. Digital Twins have been applied in various contexts, including cyber range exercise [32], security compliance assessment [33], incident detection [34] and enhancing anomaly-based intrusion detection system with data collected from Digital Twins [35].

While our research aligns with these innovative approaches, particularly with the use of Digital Twins for dataset generation as proposed by [36] for weakly supervised machine learning for anomaly detection, our work differ and focus on training and testing supervised deep learning-based time series classifiers, aiming on classifying both normal and advanced threat scenarios related to CPS in smart manufacturing. Our novel research work further refines the existing threat detection mechanism by investigating the use of supervised model for providing clear, actionable insights into various threat scenarios. This approach aims to enable operators relevant information for situational awareness, such that they could respond to incidents quickly and appropriately.

III. Design and Proof of Concept

This section outlines the methods for designing and implementing Digital Twins of Cyber-Physical Systems (CPS) as a testbed for threat simulation, dataset creation and detection model development, for which a conceptual design is illustrated in Figure 1 and explained in the sub-sections.

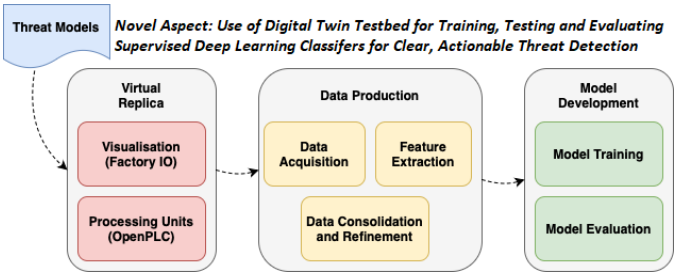

Fig. 1. Conceptual Design of Digital Twins Testbed

A. Design and Implementation of Digital Twins Testbed

In addressing the challenges of building physical testbeds for security research, we prioritised two critical factors when designing Digital Twins testbed for threat simulation.

1) Ease of Testbed Setup: the testbed shall be cost-effective to create, operate, dismantle, replicate and modify as needed.

2) Ease of Data Collection: to enable data-driven security research, the data generated by the testbed shall be easily obtainable and shareable, facilitating reproducible, verifiable and collaborative research efforts.

With this practical reason, our Digital Twins testbed is implemented using Factory I/O [13] and OpenPLC [14].

- Factory I/O - it is a simulation software with sensors and actuators commonly used in smart manufacturing. It allows risk-free simulation and data collection for studying the physics dynamics of CPS and intuitively visualise the impacts to non-technical audiences under different unsafe threat conditions.
- OpenPLC - it is an open-source Programmable Logic Controllers (PLC) software benchmark with IEC 61131-3 standard to enable trustful simulation of control logic on sensors and actuators that are relevant and applicable to real-world industrial systems. Currently, the OpenPLC Runtime managing the Factory I/O simulation is hosted on a Raspberry Pi 4 Model B [37].

For the purpose of exploring the effectiveness of time series classification in accurately detecting and classifying multiple simulated threats, this testbed can generate a diverse and comprehensive dataset that encompasses a broad spectrum of threat scenarios. With the total investment under £100 (including cost of Raspberry Pi and the monthly licence fee for Factory I/O), this affordable testbed provides an ideal platform for dataset creation and model evaluation.

B. Threat Simulation: Case study

A risk-based approach is adopted when determining the factory scenes and threat scenarios, ensuring the case study is relevant to real-world industrial settings. In particular, we focus on disruptions to the quality checking process, as quality control is a crucial operation in manufacturing which significantly impacts product integrity. Failures or disruptions in these processes can lead to substantial financial losses due to product recalls and legal actions, as well as a loss of customer trust and reputational damage due to substandard products.

Our Digital Twin testbed simulates an automated quality check process on a conveyor belt system, a common setup in industrial environment. Generally, automation tasks such as sorting, picking, and assembling are typically interconnected via conveyor belts, which facilitate the movement of workpieces across different automation stations along the production line. Thus, any malfunction or manipulation of a conveyor belt can significantly disrupt the entire assembly line operation. From a cyber security perspective, threat actors, such as Advanced Persistent Threat (APT) groups, could employ stealthy techniques to subtly decelerate, accelerate, halt, or reverse the direction of the conveyor belts. Their aim is to undermine production efficiency, damage products, or allow suboptimal products to pass the quality check. While subtle alterations may appear trivial initially, their cumulative effect can lead to long-term productivity or financial losses.

To prepare for threat simulation in Factory I/O, a simple scene is set up as shown in Figure 2. The scene involves quality checks on boxes of random sizes using a sensor situated next to a pusher. When the quality check sensor detects larger boxes (goods regarded unqualified), the pusher pushes away the box. In contrast, the pusher will not react when smaller boxes (goods regarded qualified) pass along the conveyor belt.

Akin to typical CPS, users can control actuators with sensors in Factory I/O, where the speed and direction of conveyor belt can be adjusted with the potentiometer, as shown in Figure 3. Reflecting typical manufacturing conditions, Factory I/O's potentiometer has an Analog input range from -5 volts to +5 volts, the input value is displayed on the LED display on the switchboard. Positive input values denote forward movement, negative input values denote backward movement. With the forced tag feature in Factory I/O, control over actuators can be overridden manually to enable threat simulation such as fault or failure injection. Such forced actuation can force the conveyor belt to move at a range from -10 volts to +10 volts, simulating unexpected conveying speed.

With the current scene setup, 10 threat scenarios related to the manipulation of the conveyor belt speed and direction are created, as shown in Table I.

The above list entails a wide range of potential threats on the quality check process, and as shown in Figure 4, our Digital Twins testbed enable intuitive visualisation to understand the impacts of threat scenario.

C. Data Collection and Preprocessing

To create a dataset that facilitate training and testing of supervised classifier for threat detection, 10 simulation runs are conducted for each of the 10 scenarios described in Table I, creating 100 instances in the dataset. The data are methodically

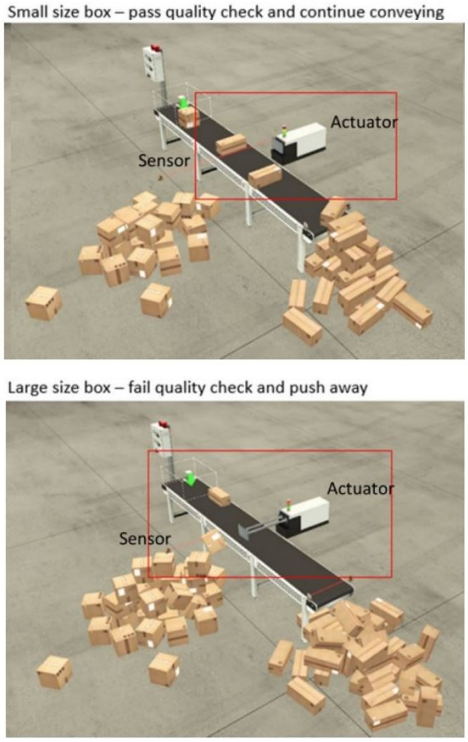

Fig. 2. Quality Checking Scene in Factory I/O

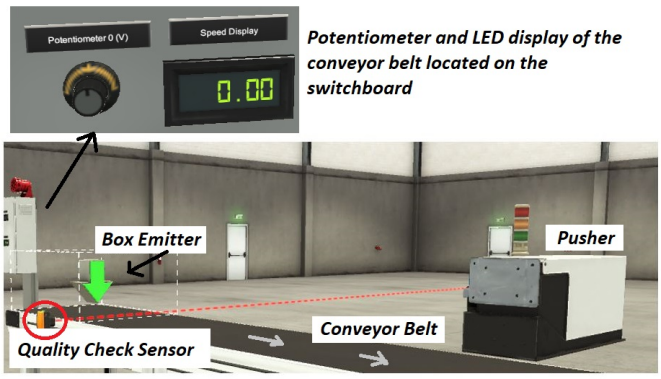

Fig. 3. Overview of the Key Elements in the Simulated Factory

TABLE I
10 SCENARIOS FOR THREAT SIMULATION - SPEED WAS BASED ON AVAILABLE SETTINGS IN FACTORY I/O ASSETS

Label	Trigger Point	Speed Status	Conveyor Speed
1	Sensor	Normal speed	$2.31 < \text{speed} \leq 5.00$
2	Sensor	Too slow or halt	$0 \leq \text{speed} \leq 2.30$
3	Sensor	Oscillate	Subtle speed change at any value
4	Sensor	Wrong direction	$-5 < \text{speed} < 0$
5	Forced Actuator	Normal speed	$2.31 < \text{speed} \leq 5.00$
6	Forced Actuator	Too slow or halt	$0 \leq \text{speed} \leq 2.30$
7	Forced Actuator	Too fast	$5.01 < \text{speed} \leq 7.00$
8	Forced Actuator	Extremely fast	$7.01 < \text{speed} \leq 10.00$
9	Forced Actuator	Oscillate	Subtle speed change at any value
10	Forced Actuator	Wrong direction	$-10 < \text{speed} < 0$

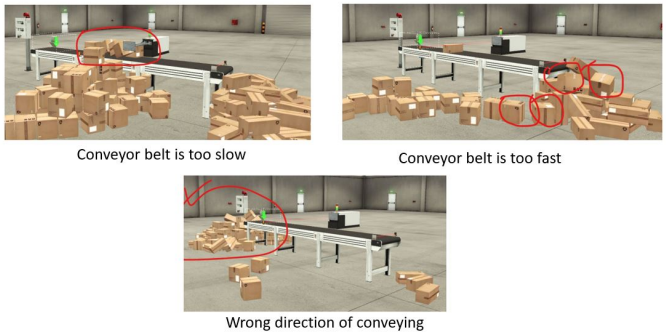

Fig. 4. Impact of Speed Manipulation on Conveyor Belt System

collected from the Factory I/O and processed before model training via several Python scripts.

1) Step 1: Data Acquisition: For comprehensive and efficient data collection from Factory I/O, a custom Python script (data_collector_enhanced.py) was executed alongside each simulation run. The script fetched data via Factory I/O's Web API at half-second intervals during the 1-minute simulation run, creating 119 timepoints per simulation instance.

2) Step 2: Feature Extraction and Labelling: specific features were extracted to capture the dynamics of the conveyor belt system with the aforesaid python script, aiming to provide insights on the CPS state changes over time, including

- Trigger point: Identification of whether movements were triggered by sensor inputs or direct actuator manipulation.
- Speed change and acceleration indicator: Analysis of speed variations and acceleration patterns to discover any abnormal behaviours.
- Actual conveyor status: Assessment of conveyor operations based on actuator outputs.

Each instance was labelled by the aforesaid Python script to assist analysis on different threat scenarios.

3) Step 3: Data Consolidation and Refinement: All 100 instances in separate .csv files were merged into one dataset using a second Python script (combineCSV.py), resulting in a comprehensive .csv file. To refine our dataset for model training, a subsequent filtering process was employed with Python script (combined_dataset_filtered.py), retaining only six essential variables that were deemed most indicative of conveyor belt performance. Specifically, 'var_0' captures the potentiometer input affecting conveyor's speed.'var_1' and 'var_2' track actual speed and its display. 'var_3' indicates speed changes. 'var_4' and 'var_5' distinguish acceleration and operational status. This resulting dataset (factoryiodata.csv), with 11,900 timepoints, are used for training the threat detector.

D. Threat Detection using Time Series Classification

Leveraging the Digital Twins testbed, we have been able to gather a rich, diverse dataset that accurately reflects the dynamics and interactions between sensors and actuators in CPS in Factory I/O. This approach addresses the persistent challenge of obtaining high-quality data for training supervised machine learning models for precise threat detection.

With the goal of achieving high accuracy in threat detection and classification while minimizing false positives and negatives, which are critical for manufacturing, we explore the effectiveness of Time Series Classification (TSC) algorithms, that are typically used in domains such as speech or motion recognition in smart healthcare systems, to assign labels to time series data based on learned data patterns over time.

For the purpose of benchmarking, several deep learning-based TSC models were selected to evaluate their performance on our dataset. To ensure simplicity in the sharing and reproduction of our research findings, we utilized the sktime Python library—a comprehensive time series analysis toolkit developed by The Alan Turing Institute [38], and the implementation of deep learning model training and evaluation was conducted within a Google Colab [39]. The dataset comprising 100 instances was divided into training and testing subsets in a 70:30 ratio, employing stratification and a predefined random seed to ensure reproducibility and fairness in model performance assessment.

E. Benchmarking the Results of Threat Detection

Several architectures are used for evaluation: Convolutional Neural Networks (CNN), Fully Convolutional Networks (FCN), InceptionTime, Long Short-Term Memory Fully Convolutional Networks (LSTM-FCN), Multi-Channel Deep Convolutional Neural Networks (MCDCNN), and Residual Neural Networks (ResNet). Each model was evaluated based on accuracy, precision, recall, and F1-score, as shown in Table II, providing a comprehensive measure of their performance in accurately classifying different threat scenarios.

TABLE II
COMPARATIVE ANALYSIS OF DEEP LEARNING TIME SERIES CLASSIFICATION MODELS

Model	Accuracy	Precision	Recall	F1-Score
CNN	90.0%	93.0%	90.0%	89.0%
FCN	93.0%	95.0%	93.0%	93.0%
InceptionTime	90.0%	93.0%	90.0%	89.0%
LSTM-FCN	93.0%	94.0%	93.0%	93.0%
MCDCNN	90.0%	93.0%	90.0%	89.0%
ResNet	87.0%	90.0%	87.0%	85.0%

From the comparative analysis, the deep learning based TSC models such as FCN and LSTM-FCN demonstrated excellent performance, achieving an accuracy of 93% on the test set. This high level of accuracy indicates the model's effectiveness in distinguishing between different operational states and identifying specific threat scenarios based on the temporal patterns in the conveyor belt's speed.

Furthermore, although feature about oscillation (i.e. illogical acceleration and deceleration) were extracted during data preprocessing stage by assessing if there are five or more notable abnormal speed changes within a 15-second window, the analysis of the model's performance indicated that most of the TSC models have misclassified this type of threat, highlighting areas for further refinement on feature extraction.

IV. DISCUSSION

This study has demonstrated the use of Digital Twins of CPS as an effective testbed for repeatable simulations of a wide range of threat scenarios within a risk-free environment. This approach provides a cost-effective and efficient alternative to physical testbeds, traditionally employed for security research.

The Digital Twins testbed not only facilitated the efficient generation of a diverse dataset for exploring the applicability of Time Series Classification (TSC) in accurately detecting and classifying threats, but also signifies a potential paradigm shift from traditional reliance on anomaly-based detection methods, which merely indicate the presence of anomalies as 'normal' or 'abnormal,' towards adopting supervised machine learning and deep learning models, which efficiently classify specific threats, thereby providing operators with clear and explainable insights into the nature of the encountered threat for more efficient incident analysis and response.

The Digital Twins testbed, developed using Factory I/O [13], showcased an efficient methodology for simulating diverse threat scenarios. However, the current version of Factory I/O restricts the import of customized assets. Consequently, our current threat datasets include abnormal behaviors of conveyor speed but do not cover other possible threats, such as tampering goods' weight and quantity. This limitation underscores the potential benefits of leveraging other simulation-capable software, such as the Unity game engine [40], to gain greater flexibility in the development of Digital Twins testbeds.

Although our comparative analysis highlighted the high accuracy achieved on detecting most of the threat scenarios, there are still challenge associated with detecting subtle oscillatory patterns within time series data - a typical low and slow Advanced Persistent Threats (APTs) attack behaviour. Future research endeavors will focus on increasing sample size and enhancing feature extraction techniques to better identify these nuanced patterns that subtly undermine manufacturing processes. Moreover, as Roopak [41] achieved 99% accuracy using LSTM for attack classification in IoT networks, we could explore their techniques to enhance model accuracy.

V. CONCLUSION AND FUTURE WORK

This paper introduced a Digital Twin testbed utilizing Factory I/O, designed to enhance threat detection within Cyber-Physical Systems (CPS) in smart manufacturing. Our methodology enables the safe simulation of sophisticated threats against CPS and supports the creation of extensive datasets essential for developing and validating time series classification models via deep learning. Such classification models not only facilitate accurate threat detection but also expedite the process of understanding and responding to identified threats.

As our research progresses beyond the simulation of CPS components, we envision the integration of our Digital Twin testbed with common industrial networks such as OPC UA and Modbus, as well as other systems typically used in the smart manufacturing, such as Human-Machine Interface (HMI), Supervisory Control and Data Acquisition (SCADA) system. This enhancement aims to simulate more complex scenarios,

broadening the testbed's relevance and application to real-world industrial settings, and expanding scope of datasets.

Furthermore, exploring the potential of early time series classifiers based on our datasets represents a compelling research opportunity. Such investigations could illuminate the feasibility of early threat detection with supervised Machine Learning or Deep Learning, which is paramount for the prompt response to and mitigation of incidents, ensuring robust and trustable cyber security measures in smart manufacturing environments in Industry 4.0 and 5.0.

VI. Dataset and Code

This research is conducted as part of the UWE Bristol's Fully Funded PhD programme. The code and the dataset are available at: https://github.com/carolsworld/FactoryIO_TSC.

References

[1] ISA, "What's the difference between industry 4.0 and industry 5.0?" https://blog.isa.org/whats-the-difference-between-industry-40-industry-50.

[2] CISA, "Improving industrial control system cybersecurity with defense-in-depth strategies," CISA, www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

[3] MITRE, "MITRE ATT&CK," mitre.org, https://attack.mitre.org/.

[4] M. Conti, D. Donadel, and F. Turrin, "A survey on industrial control system testbeds and datasets for security research," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 4, pp. 2248–2294, 2021.

[5] Rolls-Royce, "Testbed facilities," Rolls-Royce, https://www.rolls-royce.com/innovation/testbed-facilities.aspx#/.

[6] H. Neema, X. Koutsoukos, B. Potteiger, C. Tang, and K. Stouffer, "Simulation testbed for railway infrastructure security and resilience evaluation," in *Proceedings of the 7th Symposium on hot topics in the science of security*, ser. HotSoS '20. ACM, 2020, pp. 1–8.

[7] B. Green, A. Le, R. Antrobus, U. Roedig, D. Hutchison, and A. Rashid, "Pains, gains and plcs: Ten lessons from building an industrial control systems testbed for security research," in *10th USENIX Workshop on Cyber Security Experimentation and Test, CSET 2017, Vancouver, BC, Canada, August 14, 2017.*, Aug. 2017.

[8] B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. Secur.*, vol. 92, p. 101734, 2020.

[9] Z. Chen, J. Liu, Y. Shen, M. Simsek, B. Kantarci, H. T. Mouftah, and P. Djukic, "Machine learning-enabled IoT security: Open issues and challenges under advanced persistent threats," *ACM Comput. Surv.*, vol. 55, no. 5, Dec 2022.

[10] MathWorks, "Matlab," MathWorks www.mathworks.com.

[11] V. S. Koganti, M. Ashrafuzzaman, A. A. Jillepalli, and F. T. Sheldon, "A virtual testbed for security management of industrial control systems," in *2017 12th International Conference on Malicious and Unwanted Software (MALWARE)*, 2017, pp. 85–90.

[12] A. Dehlaghi-Ghadim, A. Balador, M. H. Moghadam, H. Hansson, and M. Conti, "ICSSIM - a framework for building industrial control systems security testbeds," *Computers in Industry*, vol. 148, p. 103906, 2023.

[13] Real Games Unipessoal Lda, "Factory I/O," Real Games Unipessoal Lda, https://realgames.co/company/.

[14] Autonomy Logic, "OpenPLC," https://autonomylogic.com/.

[15] I. MacKinnon, "The biggest offshore wind 'living lab' in the world to be developed in the humber," catapult, https://ore.catapult.org.uk/press-releases/the-biggest-offshore-wind-living-lab-in-the-world-to-be-developed-in-the-humber/.

[16] O. Mohammed, "Smart grid testbed," Florida Intl. Uni., https://energy.fiu.edu/smart-grid-test-bed-laboratory/.

[17] Gov.UK, "5G Testbeds and Trials Programme," Gov.UK, www.gov.uk/guidance/5g-testbeds-and-trials-programme#about-the-programme.

[18] A. P. Mathur and N. O. Tippenhauer, "SWaT: a water treatment testbed for research and training on ics security," in *2016 International Workshop on Cyber-physical Systems for Smart Water Networks (CySWater)*. IEEE, 2016, pp. 31–36.

[19] C. Ahmed, V. Palleti, and A. Mathur, "WADI: a water distribution testbed for research in the design of secure cyber physical systems," in *Proceedings - 2017 3rd International Workshop on Cyber-Physical Systems for Smart Water Networks, CySWATER 2017*, ser. CySWATER '17. ACM, 2017, pp. 25–28.

[20] T. U. A. E. Authority, "Connected autonomous vehicle testbed," RACE, https://race.ukaea.uk/test-facilities/cav/.

[21] Mininet, "Mininet: Rapid prototyping for software defined networks," https://github.com/mininet/mininet.

[22] D. Formby, M. Rad, and R. Beyah, "Lowering the barriers to industrial control system security with grfics," in *USENIX Workshop on Advances in Security Education*, 2018.

[23] Carnegie Mellon University, "SCADA simulator," Carnegie Mellony, https://github.com/cmu-sei/SCADASim.

[24] Singapore University of Design and Technology, "MiniCPS: a framework for cyber-physical systems real-time simulation," Singapore University of Design and Technology, https://github.com/scy-phy/minicps.

[25] T. Alves, R. Das, and T. Morris, "Virtualization of industrial control system testbeds for cybersecurity," in *ACM International Conference Proceeding Series*, ser. ICSS '16. ACM, 2016, pp. 10–14.

[26] M. Khan, O. Rehman, I. M. H. Rahman, and S. Ali, "Lightweight testbed for cybersecurity experiments in scada-based systems," in *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, 2020, pp. 1–5.

[27] D. L. Marino, C. S. Wickramasinghe, V. K. Singh, J. Gentle, C. Rieger, and M. Manic, "The virtualized cyber-physical testbed for machine learning anomaly detection: A wind powered grid case study," *IEEE Access*, vol. 9, pp. 159 475–159 494, 2021.

[28] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," in *International Conference on Information Systems Security and Privacy*, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:4707749

[29] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, "Survey of intrusion detection systems: techniques, datasets and challenges," *Cybersecurity*, vol. 2, 2019. [Online]. Available: https://api.semanticscholar.org/CorpusID:197645932

[30] M. Zipperle, F. Gottwalt, E. Chang, and T. Dillon, "Provenance-based intrusion detection systems: A survey," *ACM Comput. Surv.*, vol. 55, no. 7, dec 2022. [Online]. Available: https://doi.org/10.1145/3539605

[31] S. McElwee, "How to decide on a dataset for detecting cyber intrusions," towards Data Science, https://towardsdatascience.com/how-to-decide-on-a-dataset-for-detecting-cyber-attacks-c92e4f78e7a7.

[32] A. Bécue, Y. Fourastier, I. Praça, A. Savarit, C. Baron, B. Gradussofs, E. Pouille, and C. Thomas, "Cyberfactory#1 — securing the industry 4.0 with cyber-ranges and digital twins," in *2018 14th IEEE International Workshop on Factory Communication Systems (WFCS)*, 2018, pp. 1–4.

[33] M. Atalay and P. Angin, "A digital twins approach to smart grid security testing and standardization," in *2020 IEEE International Workshop on Metrology for Industry 4.0 and IoT*, 2020, pp. 435–440.

[34] M. Dietz, M. Vielberth, and G. Pernul, "Integrating digital twin security simulations in the security operations center," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, ser. ARES '20. New York, NY, USA: Association for Computing Machinery, 2020. [Online]. Available: https://doi.org/10.1145/3407023.3407039

[35] E. C. Balta, M. Pease, J. Moyne, K. Barton, and D. M. Tilbury, "Digital twin-based cyber-attack detection framework for cyber-physical manufacturing systems," *IEEE Transactions on Automation Science and Engineering*, pp. 1–18, 2023.

[36] A. Castellani, S. Schmitt, and S. Squartini, "Real-world anomaly detection by using digital twin systems and weakly supervised learning," *IEEE Transactions on Industrial Informatics*, vol. 17, pp. 4733–4742, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:226306873

[37] RaspberryPi, https://www.raspberrypi.com//.

[38] M. Löning, A. Bagnall, S. Ganesh, V. Kazakov, J. Lines, and F. J. Király, "sktime: A unified interface for machine learning with time series," *arXiv preprint arXiv:1909.07872*, 2019.

[39] E. Bisong, *Google Colab*. Berkeley, CA: Apress, 2019, pp. 59–64.

[40] J. K. Haas, "A history of the unity game engine," 2014.

[41] M. Roopak, G. Y. Tian, and J. Chambers, "An intrusion detection system against ddos attacks in iot networks," in *2020 10th Annual Computing and Communication Workshop and Conference*, 2020, pp. 0562–0567.