A Digital Twin-based Framework for Cyber-Physical Ecosystem Monitoring and Defense

Nicolò Picchi
Dept. of Information Engineering
University of Pisa
Pisa, Italy
nicolo.picchi@ing.unipi.it

Antonio Virdis
Dept. of Information Engineering
University of Pisa
Pisa, Italy
antonio.virdis@unipi.it

Gianluca Dini
Dept. of Information Engineering
University of Pisa
Pisa, Italy
gianluca.dini@unipi.it

Enzo Mingozzi
Dept. of Information Engineering
University of Pisa
Pisa, Italy
enzo.mingozzi@unipi.it

Cinzia Bernardeschi
Dept. of Information Engineering
University of Pisa
Pisa, Italy
cinzia.bernardeschi@unipi.it

***Abstract*—We present a framework to secure Cyber-Physical Ecosystems (CPES) by combining Digital Twins (DT) with Machine Learning (ML). Cyber-attacks are detected and classified by analyzing runtime data in relation to a real-time Digital Twin that continuously mirrors nominal system behavior. When a threat is identified, DT-based simulations predict consequences and trigger reconfiguration commands to ensure system safety. A proof-of-concept is implemented in the autonomous driving domain, demonstrating real-time monitoring, attack detection, and mitigation. The approach is generalizable to other CPES contexts.**

***Index Terms*—Cyber-Physical Systems, Digital Twin, Anomaly Detection, Machine Learning, Cybersecurity, Attack Mitigation, Co-simulation**

I. Introduction

Cyber-Physical Ecosystems (CPES) consist of interconnected Cyber-Physical Systems (CPSs) interacting with their environment through distributed sensing, actuation, and control. Their complexity and interdependence expose them to cyber-attacks, potentially compromising physical processes, communication, and control integrity [1]. Digital Twin (DT) technology has emerged as a promising tool for enhancing CPS security by enabling real-time system mirroring and predictive analytics [2]. In particular, DT-based frameworks have proven effective in smart manufacturing and autonomous systems, facilitating anomaly detection and proactive response to cyber threats [3].

To address these risks, we propose a security framework combining DT simulation with Machine Learning. DT continuously mirrors the nominal behavior of the physical system in real time, enabling anomaly detection through state comparison. Detected attacks are further classified, and DT-based simulations predict system evolution and guide appropriate mitigation strategies. This work demonstrates a proof-of-concept in the domain of autonomous driving [4]. Beyond enabling real-time monitoring, threat detection, and adaptive response to cyber-attacks, the framework's modular design allows it to be applied to diverse configurations within this domain and extended to other CPES scenarios.

II. Proposed Framework

The framework implements a modular architecture developed in Python using the Flask web framework. Fig. 1 shows the framework architecture, which supports secure, bidirectional communication via RabbitMQ using a publish-subscribe pattern. Core components include: (i) a data acquisition module; (ii) a runtime Digital Twin module for continuous state comparison; (iii) an ML-based detection and classification unit; (iv) a DT simulation engine that, upon attack classification, runs targeted simulations from the current system state to predict its impact and detect critical conditions; and (v) a reconfiguration module that issues control commands when required. Co-simulation is orchestrated through the INTO-CPS platform using Functional Mockup Units (FMUs) compliant with the FMI standard to represent physical dynamics, control software, and adversarial behavior via an Attack FMU that injects malicious data during runtime. Three formal models guide system behavior: the DT models define simulation logic, the adversary model encodes attack patterns and mitigation rules, and the configuration model describes system topology and interfaces. A Platform Manager coordinates runtime execution and module interactions. Upon detection and classification of an attack, the framework triggers a Digital Twin simulation initialized from the current physical system state, incorporating the identified attack parameters. If a critical condition is anticipated, the reconfiguration module enforces corrective actions, such as switching to a safe mode. The framework is extensible, supporting multiple detection units and customizable mitigation logic for different CPES domains.

III. Case Study and Experiment Results

To validate the framework, we consider a Cyber-Physical Ecosystem (CPES) consisting of two vehicles: a Lead car

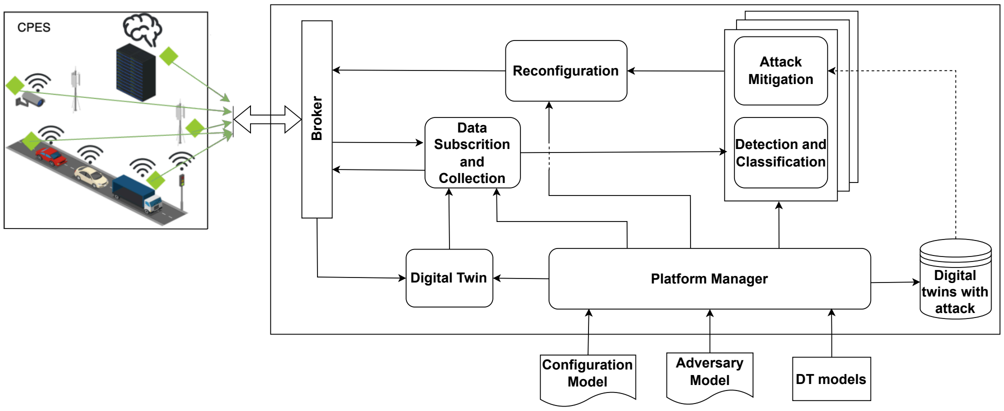

Fig. 1. Framework architectural design.

and an Ego car. The Ego car is equipped with a Cooperative Adaptive Cruise Control (CACC) system designed to maintain a safe following distance from the Lead car, which operates independently. To evaluate resilience, we simulate a data alteration attack targeting inter-vehicle communication. The attack is modeled as a Man-in-the-Middle scenario using an Attack FMU. The latter manipulates the original input signal $I(t)$ after a configurable delay T_a, replacing it with a constant spoofed value A_v. In the experiment, the Lead car's speed is spoofed with a constant value of $A_v = 8\,\text{m/s}$ after $T_a = 6\,\text{s}$, causing the Ego car to accelerate unnecessarily. The ML-based detection module, a Multilayer Perceptron (MLP), identified the anomaly after 8 s and triggered mitigation at second 8.2. The system responded by switching the Ego car to a deceleration mode governed by a proportional controller. This prevented a collision by bringing the vehicle to a controlled stop. As shown in Fig. 2, the DT simulation forecasts a critical state shortly after detection (leading to a crash at 15 s), which prompts the mitigation procedure. Fig. 3 illustrates how the Ego car's speed decreases to zero following the reconfiguration command. The results confirm that the proposed approach enables timely detection and response to cyber threats through DT simulation and ML inference, ensuring operational safety.

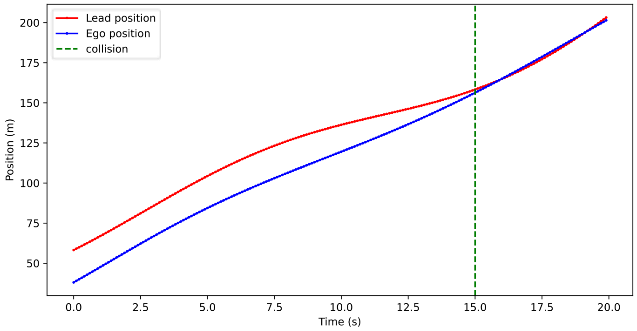

Fig. 2. Digital twin prediction.

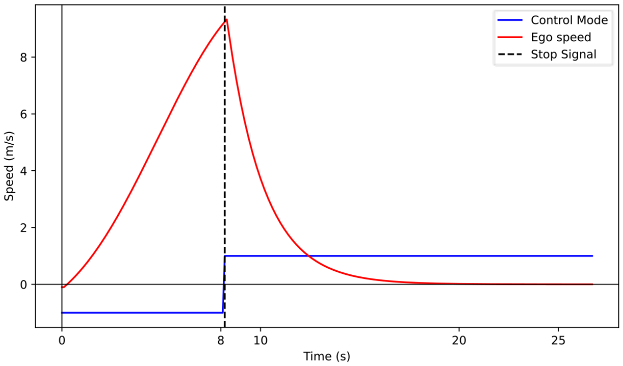

Fig. 3. Ego speed after the reconfiguration command.

IV. Conclusions

This work presented a DT and ML-based framework for CPES that effectively responds to real-time cyber threats to ensure safety.

Acknowledgment

This work was partially supported by the European Union - Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP J33C22002810001, partnership on "SEcurity and RIghts In the CyberSpace" (PE00000014 - program "SERICS").

References

[1] S. A. Varghese, A. Dehlaghi Ghadim, A. Balador, Z. Alimadadi, and P. Papadimitratos, "Digital twin-based intrusion detection for industrial control systems," in *Proc. IEEE PerCom Workshops*, 2022, pp. 611–617.

[2] F. Tao, H. Zhang, A. Liu, and A. Y. C. Nee, "Digital twin in industry: State-of-the-art," *IEEE Trans. Ind. Informatics*, vol. 15, no. 4, pp. 2405–2415, Apr. 2019.

[3] J. Friederich, D. P. Francis, S. Lazarova-Molnar, and N. Mohamed, "A framework for data-driven digital twins for smart manufacturing," *Comput. Ind.*, vol. 136, Art. no. 103586, 2022.

[4] M. Ali, G. Kaddoum, W. T. Li, C. Yuen, M. Tariq, and H. V. Poor, "A smart digital twin enabled security framework for vehicle-to-grid cyber-physical systems," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 5258–5271, 2023.