A resilience Component for a Digital Twin*

Valeria Valdés Ríos[1 [0009−0000−6632−396X]], Fatiha Zaidi[2 [0000−0003−3414−8815]], Ana Rosa Cavalli[1,3 [0000−0003−2586−9071]], and Wissam Mallouli[1 [0000−0003−2548−6628]]

[1] Montimage EURL, Paris, France {firstname.lastname}@montimage.com
[2] Université Paris-Saclay, CNRS, ENS Paris-Saclay, Laboratoire Méthodes Formelles, 91190, Gif-sur-Yvette, France
fatiha.zaidi@universite-paris-saclay.fr
[3] Institut Politechnique, Telecom SudParis, France

Abstract. Industry 4.0 has popularized Cyber-Physical Systems (CPSs), engineered systems integrating physical components with computerized controls for process management. Despite efforts by academia and industry to address CPSs challenges, security remains a key concern. This involves identifying vulnerabilities, weaknesses, and threats. The primary objectives of security are the evaluation of CPSs' security status, uncovering flaws, and suggesting risk mitigation. Nevertheless, besides lists of several CPSs security improvement techniques and methodologies for detecting CPSs security issues, little emphasis is paid to their resolution. This paper analyzes existing techniques to enhance resilience in CPSs, encompassing both design and operational phases to mitigate identified risks. Additionally, we introduce the integration of a resilience component into a Digital Twin (DT) framework. This component utilizes the capabilities of the DT to oversee resilience mechanisms within the system, monitor system activity, and respond effectively to security events.

Keywords: Cyber Physical Systems · Resilience · Digital Twin · Security · Mitigation.

1 Introduction

Cyber Physical Systems (CPSs) refers to systems where the physical components are interconnected through communication technologies to create efficient control systems [18]. Comprising physical and cyber layers, CPSs use sensors to collect data, controllers manage system behavior. The cyber layer, a network of connected components, facilitates message transmission for tasks like controller configuration. This integration supports coordination in complex systems, enabling constant monitoring, control, and adaptation of CPSs.

CPSs find applications in domains like smart grids, transportation, healthcare, smart cities, and homes [5]. However, they face heightened security risks

* This work is partially supported by the European Union's Horizon Europe research and innovation program under grant agreement No 101070455 (DYNABIC)

due to their critical roles. Resilience, defined as the ability to resist, absorb, recover or adapt to adversity or a changing conditions [7], plays a crucial role in CPSs. This involves proactive and reactive measures. While cyber security and resilience share overlapping concepts, resilience is primarily concerned with ensuring the continuity of system operations during adverse conditions or disruptions. In this context cyber security is closely related, focusing on protecting and defending systems against cyber attacks [19].

A Digital Twin (DT) is a virtual replica of a system, widely used in CPSs and networks [21]. DTs incorporate real-time data from the physical system, enabling bidirectional data exchange [16] and enhancing CPS resilience through real-time adaptation. Despite their potential to enhance CPS resilience, challenges remain in scalability, performance, and system impact. Scalability involves managing larger systems efficiently, while performance may be affected by changes, potentially causing cascading effects. The DT's simulation capability allows comprehensive analysis before implementing changes, reducing risks and consequences.

The main contribution of this paper is described as below:

- Introduction of a novel resilience component tailored for Digital Twin technology, enhancing its capability to effectively respond to security events in CPSs. This component serves as a critical addition to improve resilience of CPSs.
- Integration of the resilience component developed within a DT architecture. This integration showcases the adaptability of our approach, allowing existing DT systems to easily incorporate security measures.
- Experimental validation using a model of a Electrical Vehicle Charging Station, allowing the resilience component to monitor and react to flood attacks against the central system of the architecture using a moving target defense approach.

The remainder of this paper is organized as follows. Section 2 presents the related work. Section 3 presents various resilience mechanisms and techniques. Section 4 presents the proposal of a DT extension with a resilience component. Section 5 presents the application and evaluation. The discussion is presented in Section 6, and final remarks and conclusions in Section 7.

2 Related Work

DTs are an emerging and powerful tool for understanding and controlling complex systems, researchers are applying them in different domains and research about them has increased since its first proposed approach in 2006 by Hellen Gil [14]. This section provides an overview of recent research studies that focus on enhancing resilience in CPSs by leveraging the capabilities of DTs and the use of alternative methodologies and strategies.

The academic community extensively explores methodologies for securing and enhancing resilience in CPSs, particularly in smart grids and power systems [13, 20, 22]. Studies address security controls, attack detection, resilience in

industrial CPSs [8] and proposing resilience frameworks [4]. However, none of these studies consider the use of DT to enhance CPS resilience.

Various studies delve into the utilization of DTs for enhancing resilience in CPSs.. Brucherseifer *et al.* [2] propose a DT framework covering analysis, optimization, and automated low-level decisions. Becue *et al.* [3] view DTs as tools for root cause analysis. Saad *et al.* [15] employ IoT-based energy CPSs to detect attacked components through agent consensus. Lektauers *et al.* [12] utilize DTs for simulation and data sharing. Faleiro *et al.* [9] focus on healthcare DT applications, discussing security layers. Hussaini *et al.* [11] propose a DT defense mechanisms taxonomy, introducing a Secured DT Development Life Cycle based on layer architecture.

The research studies reviewed highlight the role of DT in enhancing CPS resilience. However, a common limitation is absence of specific strategies for incident response due to the need for event and domain specific approaches.

Resilience metrics quantify a system's vulnerability and offer a comprehensive understanding of its response to diverse challenges and changes. They aid in understanding system behavior during events, enabling post-event analysis and evaluating resilience strategies. Various studies discuss and define generic resilience metrics. Haque *et al.* [10] consider asset criticality, risk, and network topology, while Colibianchi *et al.* [6] include path redundancy, device status, and quality of service. Barbeau *et al.* [1] introduces two novel control-theoretic concepts, k-steerability and l-monitorability for determining CPS resilience. Segovia *et al.* [17] propose a resilience metric for a single system variable extended to an overall stability metric assessing attack impact across the entire system. These metrics quantify post-event resilience. In a real-time data-driven context like a DT, the performance metric stands out for real-time monitoring, comparing model and actual data in the DT interface. When an attack is detected, and the system fully recovers its desired performance, an analysis can measure resilience, utilizing factors such as absorb and recovery time as mentioned in previous studies.

3 Resilience mechanisms and techniques

3.1 Proactive techniques

Proactive mechanisms are strategies applied before detecting an attack or unusual events, enhancing system resilience by design. Intrusion Detection Systems (IDS) monitor CPSs using policies, historical data, and attack signatures. Advanced monitoring integrates machine learning for early detection, optimizing models and reconstructing data. Proactive strategies include risk assessment to identify critical CPS components and allocate resources for protection.

Diversification techniques are proactive strategies that hide specific segments of the system to disrupt the adversary understanding and dynamically alter the attack surface. Redundancy is a form of diversity, it involves creating varied versions of the same component, reducing vulnerability attacks focused on specific

weaknesses. In this context, Moving Target Defense (MTD) seamlessly switch to alternative components with different designs. Moreover, diversification techniques also include the dynamic change of components positions, resources, and pathways. These constant adjustments decrease system predictability, establishing a barrier that requires adversaries to invest more resources and time to deduce the internal behavior of the system.

Isolation and segmentation are techniques employed in the design of CPSs. Isolation creates separate environments for independent components, preventing an adversary with control of one component from accessing others. Even if the components are independent, being in the same environment makes it easier for an adversary to get access from one to the another. Similarly, segmentation divides the CPS into components or subsystems that interact with each other. The goal is to limit the adversary from getting access from one component to another.

To achieve resilience by design, several classical guidelines can be followed, such as the use of secure communication protocols, authentication control, user privilege restrictions, secure software usage, firewalls, and security best practices to ensure confidentiality, integrity, and availability.

3.2 Reactive techniques

Reactive mechanisms respond to detected unusual events, aiming to restore normal CPS operation and functionality. As part of reactive techniques, adaptive response dynamically alters the system's behavior and configuration upon event detection to mitigate damage, maintain the system operations and integrity. It employs strategies like incident response plans, where the system selects a specific defense strategy based on the characteristics of the detected event. CPSs may adopt dynamic code changes to reduce their attack surface. However, debugging challenges can arise due to the nature of the code.

Once an incident is detected and addressed, it's crucial to analyze the event to identify the vulnerability that led to its occurrence. Post-event analysis provides insights into the root cause, allowing long-term actions for preventing similar events in the future and improving CPS resilience and security.

To prevent similar events in other CPSs, the use of incident sharing platforms facilitate the exchange of security information, threat, attack details, and security techniques among multiple CPSs, promoting collective defense against potential security events, though sharing sensitive data requires careful consideration. This collaborative approach serves as a collective defense to protect CPSs and mitigate potential security events.

As CPS face a variety of attack types, relying solely on a single defense technique often proves inadequate to protect the system. Given that certain defense techniques are attack-specific, it is a common practice to employ a multi-layered defense to elevate the overall security and resilience of CPS. Combining security by design with reactive mechanisms enhances the system's adaptability to various attacks, ensuring comprehensive protection against a broad spectrum of security events.

4 Resilience component

This research proposes integrating a built-in resilient component into a DT architecture, managing both existing and new resilience mechanisms within the system. The resilience component takes advantage of the DT's feedback capability to control resilience mechanisms in the system. Since the DT allows to collect information of a system in real time and collect information from a model, such as a predictive models, these two sources of information can be compared to obtain real-time resilience metrics representing the current state of the system that can be visualized and monitored through the DT.

As outlined in Section 3, resilience mechanisms fall into proactive or reactive categories. Proactive mechanisms run continuously, with their execution controllable by the resilience component. Reactive mechanisms, respond to specific events, triggered by the resilience component when necessary, updating DT models is essential whenever system changes occur.

The reactive mechanism workflow is illustrated in Figure 1, involves the resilience component responding to event detection by taking appropriate actions and updating the system model. Proactive mechanisms follow a similar workflow, where the resilience component continuously updates the system and model without relying on event detection.

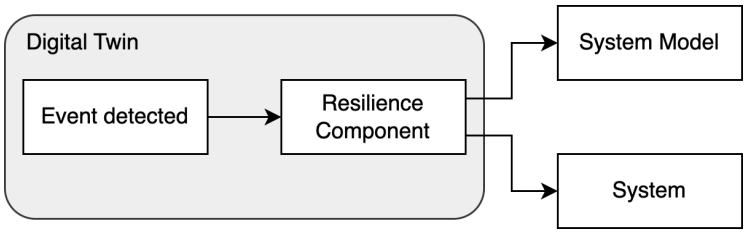


Fig. 1: Workflow of the Resilience Component for reactive mechanisms

As an example of a resilience mechanism, the resilience component employs Moving Target Defense (MTD). To implement MTD, it is necessary to have beforehand a set of equivalents components for the same functionality, exhibiting the same behavior but with different implementations, making them less vulnerable to the same attacks. The resilience component instruct the system to replace a component with an equivalent one, and updates the system model accordingly.

In addition to the MTD mechanism, the resilience component has the capability to integrate various other mechanisms, both existing within the system and newly introduced ones. This integration aims to leverage the strengths of theses mechanisms to enhance system resilience. For new mechanisms, they can be implemented as new services within the resilience component. As for the existing mechanisms, the resilience component can manage and control them by

establishing connections or utilizing available APIs. This allows the resilience component to effectively oversee and enhance the system's resilience by leveraging the capabilities of these integrated mechanisms.

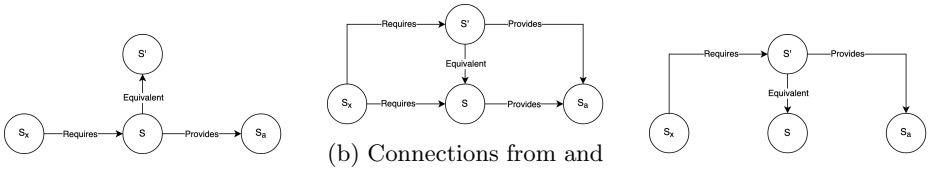
5 Application of Resilience Component in a DT

MADT4B [4] (Multi-Aspect DT for Business Continuity) is an ongoing real-time DT platform that provides system insights. It connects and synchronizes a CPS in real time, offering contextual information and extending DT capabilities for business continuity. It uses a Knowledge Graph (KG) to represent system and features a NeoDash dashboard linked to a Neo4j database backend.

The resilience component is integrated as a new service to the DT's backend, including resilience mechanisms. Functioning centrally, the resilience component controls these mechanisms. Management is through the DT's GUI, with a new "Mechanism" node in the KG meta-model. The MTD mechanism replaces a vulnerable asset with an equivalent, which refers to a new component that provides identical services as the original but with a distinct implementation.

To maintain isolation between the original component and its equivalents, the connection between them is present only in the knowledge graph presented by the DT, indicating their equivalence. However, these connections do not exist in the physical system itself. It is responsibility of the MTD mechanism to rearrange the connections once a component is replaced with its equivalent.

The MTD mechanism, depicted in Figure 2, begins with a component denoted as S in Figure 2a. Represented as S', the equivalent component replaces the original one. S_a represent the component or set providing functionality, while S_x represents those required for S to operate. Subsequently, connection are duplicated to ensure service availability in Figure 2b. After establishing connections, the old component is safely disconnected in Figure 2c, ensuring uninterrupted service during the transition.



(a) Connections before MTD starts

(b) Connections from and to node S are duplicated in node S'

(c) Node S is disconnected

Fig. 2: Simple MTD replacement

For component replacement, we initially opt for random selection. However, a prioritization strategy based on factors such as component status, performance

[4] https://github.com/SINTEF-9012/madt-neodash

metrics, costs, and other criteria can enhance the selection process for optimal system replacement.

5.1 Modeled system

The resilience component is tested using an electric vehicle charging station (EVCS) scenario, representing a CPS. The EVCS includes physical components like charging stations and virtual components, such as the charging station management system (CSMS). Multiple charging stations (CS) are connected to a network switch for Ethernet connectivity to the CSMS. The CSMS, hosted on a private cloud, remotely maintains and monitors the CSs using the Open Charge Point Protocol (OCPP) over the Internet. A router and WiFi access points enhance Internet connectivity. For grid-related protection, a Feeder Protection Relay (FPR) is synchronized with a GPS clock. Figure 3 depicts the high-level architecture.

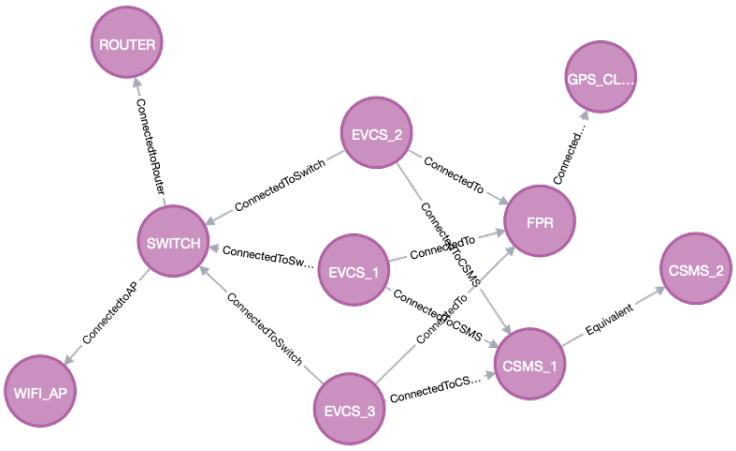


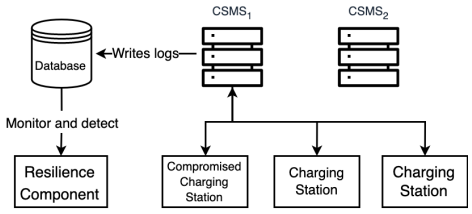
Fig. 3: Knowledge Graph for EVCS

5.2 Adversary Model: Flood attack to CSMS, detection and reaction

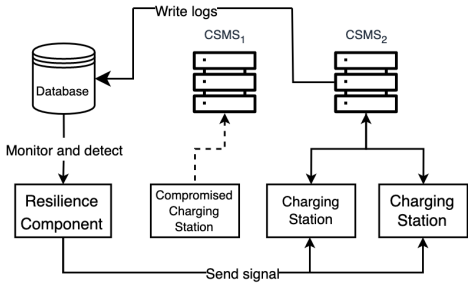
We considered a Heartbeat flood attack from a CS to the CSMS, aiming to saturate the communication channel and CSMS resources. The Heartbeat message serves the purpose of indicating that a charging point is currently connected and operational. The initial entry point of the adversary is the charging point. The adversary can gain control over this component of the system using various spoofing techniques, including eavesdropping on communication or executing

man-in-the-middle attacks. Additionally, the adversary could steal identification details from the charging point device, such as TLS certificates to gain access.

The resilience component, monitoring the CSMS logs, as depicted in Figure 4a, includes a monitor system fetching connection details from the KG. This system connects to the InfluxDB database, focusing on Heartbeat logs for rule-based flood attack detection.



(a) System under Flood Attack



(b) Reaction of resilience component

Fig. 4: Detection and reaction of flood attack to CSMS

Under normal conditions, heartbeat messages are sent every 8 minutes, but during flooding attack, the frequency increases to about 0.1 seconds. The detection system uses a tolerance attribute for rule-based detection.

Upon detecting an attack, the affected CS is flagged in the DT's KG, triggering a MTD strategy as depicted in Figure 4b. Two CSMS implementations were used: a python application [5] with the ocpp library, and a second extension[6].

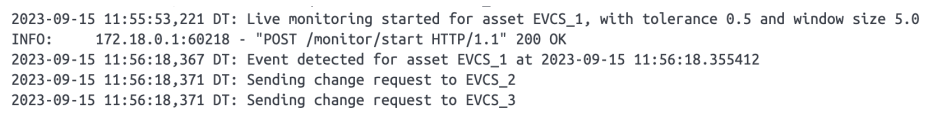
We conducted 10 flooding attacks, messages were randomly sent from a charging station at intervals d seconds, $d \in (0, 1]$. Table 1 compares system behavior with and without the resilience component. The system, with the resilience component, showed a lower average response time during attacks. Recovery is not recorded without the resilience component since a single charging station's attack isn't sufficient to bring down the system. However, with the resilience component, recovery is considered as the transition time in one charging station when

[5] https://github.com/mobilityhouse/ocpp
[6] https://github.com/villekr/ocpp-asgi

switching to a new CSMS. In both scenarios, the services remains available, resulting in no downtime. Figure 5 displays logs in the resilience component and one charging station when an event is detected, and MTD is triggered.

Metric	Without resilience component	With resilience component
Response time	0.47 [s]	0.38 [s]
Recover time	-	0.005 [s]
Downtime	0 [s]	0 [s]

Table 1: System behaviour without resilience component and with it.



(a) Log in resilience component, send an update to charging stations.

(b) Log in charging station upon receiving update and reconnect to the new CSMS.

Fig. 5: Logs when an event is detected and MTD is triggered

6 Discussion

DTs provide diverse services to CPSs, and security is a crucial aspect. Despites its capabilities in real-time information collection, the MADT4BC DT platform lacks an inherent resilience component. The bidirectional communication allows the DT to detect anomalies, while a resilience component offers protection and feedback for mitigation.

To assess the resilience component's response effectiveness, several aspects should be considered. This includes scalability in terms of the number of adversaries and the system's complexity. It is important to test the system in complex and realistic scenarios for ensure its reliability, evaluate its performance in both normal conditions as well as during attacks. For MTD, when replacing components with equivalents, connected elements need reestablishment. If the equivalent has existing connections, no need for this step. In hybrid cases, renew remaining connections for seamless integration. Moreover, for subscription services, updating all subscribers is vital. This informs them of changes and allows adjustments to their setup and interactions.

Additionally, when selecting a resilience mechanism, it's crucial to weigh the cost of implementation and execution within the system. Some mechanisms

might promise better performance but implementations costs can be significant. In such cases, lower performance options that meet systems constraints could be necessary.

Lastly, the goal is to achieve self-healing systems that autonomously recover from attacks and security events. However, the operator involvement in the feedback loop remains vital. The DT can suggest responses based on event complexity. For common security scenarios, the DT can trigger automatic responses, forming a hybrid resilient component. This balances automated and manual strengths, ensuring effective response to diverse incidents. MTD empowers self-healing, removing the need for manual operator responses.

7 Conclusion

In this study, we presented the integration of a resilience component into the DT architecture, aiming to improve resilience in a critical infrastructure by responding to detected events in the CPS. The response of the component varies according on the nature of the event. Our focus was on implementing a reactive MTD mechanism within the resilience component, requiring the implementation of equivalent components with identical functionality beforehand. To facilitate the MTD implementation while preserving the generic DT meta-model architecture, an additional attribute indicating the current status of a component is added to the DT. This attribute enables differentiation between healthy and attacked components following incident detection. Furthermore, this attribute also denotes whether the component is active in the system, enabling the MTD to trigger a component switch using an equivalent counterpart.

As part of our future work, we intend to delve into further research on reactive strategies. This exploration aims to enable the resilience component to prioritize among these strategies and provide the most appropriate response for events based on relevant metrics.

References

1. Barbeau, M., Cuppens, F., Cuppens, N., Dagnas, R., Garcia-Alfaro, J.: Metrics to enhance the resilience of cyber-physical systems. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 1167–1172 (2020). https://doi.org/10.1109/TrustCom50675.2020.00156
2. Brucherseifer, E., Winter, H., Mentges, A., Mühlhäuser, M., Hellmann, M.: Digital twin conceptual framework for improving critical infrastructure resilience. at - Automatisierungstechnik **69**(12), 1062–1080 (2021). https://doi.org/doi:10.1515/auto-2021-0104, https://doi.org/10.1515/auto-2021-0104
3. Bécue, A., Maia, E., Feeken, L., Borchers, P., Praça, I.: A new concept of digital twin supporting optimization and resilience of factories of the future. Applied Sciences **10**(13) (2020). https://doi.org/10.3390/app10134482, https://www.mdpi.com/2076-3417/10/13/4482

4. Cassottana, B., Roomi, M.M., Mashima, D., Sansavini, G.: Resilience analysis of cyber-physical systems: A review of models and methods. Risk Analysis (Jan 2023). https://doi.org/10.1111/risa.14089, https://doi.org/10.1111/risa.14089
5. Chen, H.: Applications of cyber-physical system: A literature review. Journal of Industrial Integration and Management **02**(03), 1750012 (2017). https://doi.org/10.1142/S2424862217500129, https://doi.org/10.1142/S2424862217500129
6. Colabianchi, S., Costantino, F., Di Gravio, G., Nonino, F., Patriarca, R.: Discussing resilience in the context of cyber physical systems. Computers & Industrial Engineering **160**, 107534 (2021). https://doi.org/https://doi.org/10.1016/j.cie.2021.107534, https://www.sciencedirect.com/science/article/pii/S0360835221004381
7. Committee, D.R.S., et al.: Dhs risk lexicon. Department of Homeland Security Tech. Rep (2008)
8. Ding, D., Han, Q.L., Xiang, Y., Ge, X., Zhang, X.M.: A survey on security control and attack detection for industrial cyber-physical systems. Neurocomputing **275**, 1674–1683 (2018). https://doi.org/https://doi.org/10.1016/j.neucom.2017.10.009, https://www.sciencedirect.com/science/article/pii/S0925231217316351
9. Faleiro, R., Pan, L., Pokhrel, S.R., Doss, R.: Digital twin for cybersecurity: Towards enhancing cyber resilience. In: Xiang, W., Han, F., Phan, T.K. (eds.) Broadband Communications, Networks, and Systems. pp. 57–76. Springer International Publishing, Cham (2022)
10. Haque, M.A., Shetty, S., Krishnappa, B.: Cyber-Physical Systems Resilience: Frameworks, Metrics, Complexities, Challenges, and Future Directions, p. Chapter 12 (12 2019)
11. Hussaini, A., Qian, C., Liao, W., Yu, W.: A taxonomy of security and defense mechanisms in digital twins-based cyber-physical systems. In: 2022 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics). pp. 597–604 (2022). https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics55523.2022.00112
12. Lektauers, A., Pecerska, J., Bolsakovs, V., Romanovs, A., Grabis, J., Teilans, A.: A multi-model approach for simulation-based digital twin in resilient services. WSEAS TRANSACTIONS ON SYSTEMS AND CONTROL **16**, 133–145 (Jan 2021). https://doi.org/10.37394/23203.2021.16.10, https://doi.org/10.37394/23203.2021.16.10
13. Paul, S., Ding, F., Utkarsh, K., Liu, W., O'Malley, M.J., Barnett, J.: On vulnerability and resilience of cyber-physical power systems: A review. IEEE Systems Journal **16**(2), 2367–2378 (2022). https://doi.org/10.1109/JSYST.2021.3123904
14. Pivoto, D.G., de Almeida, L.F., da Rosa Righi, R., Rodrigues, J.J., Lugli, A.B., Alberti, A.M.: Cyber-physical systems architectures for industrial internet of things applications in industry 4.0: A literature review. Journal of Manufacturing Systems **58**, 176–192 (2021). https://doi.org/https://doi.org/10.1016/j.jmsy.2020.11.017, https://www.sciencedirect.com/science/article/pii/S0278612520302119
15. Saad, A., Faddel, S., Youssef, T., Mohammed, O.A.: On the implementation of iot-based digital twin for networked microgrids resiliency against cyber attacks. IEEE Transactions on Smart Grid **11**(6), 5138–5150 (2020). https://doi.org/10.1109/TSG.2020.3000958

16. Segovia, M., Garcia-Alfaro, J.: Design, modeling and implementation of digital twins. Sensors **22**(14) (2022). https://doi.org/10.3390/s22145396, https://www.mdpi.com/1424-8220/22/14/5396
17. Segovia, M., Rubio-Hernan, J., Cavalli, A.R., Garcia-Alfaro, J.: Cyber-resilience evaluation of cyber-physical systems. In: 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). pp. 1–8 (2020). https://doi.org/10.1109/NCA51143.2020.9306741
18. Segovia., M., Rubio-Hernan., J., Cavalli., A.R., Garcia-Alfaro., J.: Switched-based control testbed to assure cyber-physical resilience by design. In: Proceedings of the 19th International Conference on Security and Cryptography - SECRYPT. pp. 681–686. INSTICC, SciTePress (2022). https://doi.org/10.5220/0011327300003283
19. of Standards, N.I., Technology: Guide for conducting risk assessments. Tech. rep. (2012). https://doi.org/10.6028/nist.sp.800-30r1, https://doi.org/10.6028/nist.sp.800-30r1
20. Tahar, B.M., Amine, S.M., Hachana, O.: Machine learning-based techniques for false data injection attacks detection in smart grid: A review. In: Hatti, M. (ed.) Advanced Computational Techniques for Renewable Energy Systems. pp. 368–376. Springer International Publishing, Cham (2023)
21. Wagg, D., Worden, K., Barthorpe, R., Gardner, P.: Digital twins: State-of-the-art future directions for modelling and simulation in engineering dynamics applications. ASCE-ASME J Risk and Uncert in Engrg Sys Part B Mech Engrg **6** (03 2020). https://doi.org/10.1115/1.4046739
22. Zhang, D., Li, C., Goh, H.H., Ahmad, T., Zhu, H., Liu, H., Wu, T.: A comprehensive overview of modeling approaches and optimal control strategies for cyber-physical resilience in power systems. Renewable Energy **189**, 1383–1406 (2022). https://doi.org/https://doi.org/10.1016/j.renene.2022.03.096, https://www.sciencedirect.com/science/article/pii/S0960148122003809