

# Smart Critical Infrastructures Security management and governance: Implementation of Cyber Resilience KPIs for Decentralized Energy Asset

Ali AGHAZADEH ARDEBILI<sup>1,2,\*</sup>, Cristian MARTELLA<sup>1,†</sup>, Angelo MARTELLA<sup>1,†</sup>,  
Alessandro LAZARI<sup>1,†</sup>, Antonella LONGO<sup>1,\*</sup> and Antonio FICARELLA<sup>1,†</sup>

<sup>1</sup>Dept. of Engineering for innovation, University of Salento, Lecce, Italy

<sup>2</sup>Dept. of Research and Development, HSPI Consulenti di Direzione, Rome, Italy

## Abstract

In the wake of terrorist attacks in Europe, the European Union has increasingly prioritized collaborative efforts to bolster the protection, resilience, and cybersecurity of critical infrastructures and essential services. Nevertheless, a significant gap persists in accurately quantifying the resilience of these systems, particularly regarding the integration of Artificial Intelligence, which remains underdeveloped. This article endeavors to bridge this gap by developing a robust data-driven framework for Resilience Key Performance Indicators. This study focuses on identifying effective data-driven methodologies to assess the response of cyber-physical critical infrastructures to cyber attacks. A case study is also deployed to replicate cyber attack scenarios on cyber-physical assets and provide a meticulous evaluation of the resilience performance of an energy cyber-physical framework, comprising a Smart PV Station, Data Infrastructure, and Digital Twin for essential services. Notably, the anomaly detection algorithm successfully identifies anomalous behavior induced by simulated cyber attacks, thereby averting the system from reacting to falsely imposed conditions. Furthermore, the assessment inspects the functionality and features of the framework, thus enriching our comprehension and quantification of cyber-physical infrastructure resilience through Resilience Key Performance Indicators.

## Keywords

Cyber resilience, Resilience KPIs, Resilience Quantification, Critical infrastructure security, Anomaly detection, Early warning, Incident response

## 1. Introduction

Immediately after 9/11 and the attacks in Madrid and London of 2004 and 2005, the Member States of the European Union have shown an increasing political will in establishing a joint framework aimed at enhancing the protection, resilience and cybersecurity of critical infrastructures, entities and operators of essential services. It can be affirmed, in fact, that despite the initial difficulties in

---

*ITASEC24: Italian Conference on Cybersecurity, April 8-12, 2024, Salerno, Italy*

\*Corresponding author.

†The authors contributed equally in Conceptualization, background review, methodology, implementation, and writing draft.

✉ ali.a.ardebili@unisalento.it (A. A. ARDEBILI); cristian.martella@unisalento.it (C. MARTELLA);

angelo.martella@unisalento.it (A. MARTELLA); alessandro.lazari@unisalento.it (A. LAZARI);

antonella.longo@unisalento.it (A. LONGO); antonio.ficarella@unisalento.it (A. FICARELLA)

🆔 0000-0002-3557-9986 (A. A. ARDEBILI); 0000-0001-9751-9367 (C. MARTELLA); 0000-0002-1082-7293

(A. MARTELLA)



© 2022 Copyright for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0).

overcoming the metabolization of key principles and the fulfilment of minimum harmonization thresholds, the EU and its Member States have adopted overtime a very comprehensive, effective and up-to-date framework that nowadays stands as reference also for neighboring countries and allied of the EU.

In the era of rapid technological advancement, the integration of cutting-edge technologies like Digital Twins (DTs), big data analysis, and the Internet of Things (IoT) with Critical Infrastructures (CIs) has transformed the critical entities into smart cyber-physical complex systems. However, traditional risk assessment methods are proving inefficient for the evaluation of future AI-integrated CIs. There exists a significant gap in the quantification of resilience for these complex systems due to the lack of standardization, particularly concerning AI integration, which is not yet industrialized in CIs operations and control systems. As we move closer to an era where data-driven cyber resilience indicators are imperative, this article aims to fill this gap by developing a robust Resilience Key Performance Indicator (R-KPI) implementation framework. This involves employing highly cited methods to quantify resilience of a smart PV panel which is developed in Data Lab, University of Salento (see Section 4.1), draw multiple resilience curves and associated R-KPIs, comparing the results to discern the most comprehensive understanding of system behavior under varied disturbances. The disturbance in current study is a cyber attack scenario which is detailed in Section 4.3. The central question addressed in this study is the best data-driven practice for presenting the behavior of Cyber-Physical (CP) CIs in response to a cyber attack, utilizing a case study methodology involving the repetition of a cyber attack scenario on CP assets. The article's main contribution lies in providing a framework to employ approved R-KPIs for evaluating the cyber resilience of smart infrastructures, opening research lines for data-driven anomaly detection and early warning systems. Furthermore, the article bridges existing gaps by offering a universal framework for employing R-KPIs in smart infrastructures, enhancing the understanding of cyber resilience and enabling improved resilience quantification for AI-integrated CIs.

The remainder of the article is structured as follows: Methodology, Case Study, Results and Discussion, Conclusion and Future Work. Next Section 2 will delve into the state of the art of resilience quantification in CP CIs.

## **2. Background Review**

Resilience engineering is pivotal for safeguarding the uninterrupted operation of CIs, ensuring the delivery of vital services [1, 2]. The trend of digitalization is molding an ecosystem that seamlessly integrates the physical and digital realms, imbuing systems with inherent intelligence through the utilization of cutting-edge technologies [3]. The resilience of smart CIs, particularly CP power systems, is a key concern [4]. Inter-dependencies between cyber, physical, and social elements in water, transportation, and cyber infrastructures must be considered to enhance resilience [5]. A multi-disciplinary approach is crucial for addressing the challenges faced by future cities in developing secure and resilient Cyber-Physical Systems (CPSs) [6]. However, quantifying resilience remains a crucial challenge, marked by an absence of an efficiently addressed standard approach in the existing literature in knowledge and practice [7, 8].

Existing technologies do not address the disparate time and spatial scales across the many

system domains [9, 10]. New methods for managing system resilience, including computing, sensing, machine learning, artificial intelligence, and advanced analytics, are needed to ensure CPSs can withstand adverse events. The Society of Risk Analysis Workshop in December 2021, attended by over fifty scientists and engineers, aimed to identify key technologies and techniques for designing resilience in infrastructures. Four promising themes for research include resilient topologies of sensors and hardware [11, 12, 13], state-of-the-art modeling and the DT [14, 15, 16], machine learning and AI [17, 18, 19], and energy networks and the System of Systems [20]. Cyber-attacks and system complexity pose challenges to risk assessment and management. Resilience, utilizing flexible response, distributed decision making, modularity, and redundancy, helps absorb and recover from adverse events when technical objectives, schedule, or cost are insufficient. Resilience is crucial for CPSs, as it allows for quick and effective recovery from threats. While mitigating risks is important, adverse events will still occur, and a system hardened to avoid risks is not inherently robust enough to recover. International standardization bodies and agencies have developed several cybersecurity standards, including ISO 27000 [21], NIST SP 800-82 [22], NIST SP 800-53 [23], and NIST SP 800-72 [24]. The Department of Homeland Security has also published standards for Common Cybersecurity Vulnerabilities in Industrial Control Systems (ICSs). Some standards have been published to address specific CPSs for smart grids IEC 62351 [25], and specific CPS functions like interoperability and communication. These standards provide best practices for cybersecurity or technical guidelines for its implementation in specific sectors.

As anticipated in the introduction, the EU has adopted overtime a series of directives and regulations that contributed to the establishment of a very comprehensive and advanced framework aimed at enhancing the cyber/physical security and resilience of critical entities and essential services. With the launch of the European Programme for Critical Infrastructure Protection (EPCIP) in 2006, the EU has created the condition for the establishment of an EU-wide forum in which risk assessment methodologies, mitigation activities, incident response, crisis management and cooperation mechanism could be discussed, analysed and improved. The so-called NIS 2 and CER directives, promulgated on the 16th of December 2022, and currently being adopted by the Member States, are the last mile of a 20 years journey that has now a strong focus on resilience. Past legislation, in fact, initially focused on the protection from all-hazards and included initial activities aimed at introducing prevention, preparedness and response. In the current context, given the obligations respectively introduced by the NIS and CER directives, embracing resilience at strategic and tactical levels is of utmost importance. This is also confirmed by the 2016 NATO's baseline requirements for resilience that include the following priorities: 1) assured continuity of government and critical government services; 2) resilient energy supplies; 3) ability to deal effectively with uncontrolled movement of people; 4) resilient food and water resources; 5) ability to deal with mass casualties; 6) resilient civil communications systems; 7) resilient civil transportation systems.

With "resilient energy supplies" ranking second in the order of highest priorities, it goes per se that research has to dig deep in this lifeline sector, to ensure that all measures are taken to prevent, absorb and recover from attacks aimed at disrupting the continuity of vital systems in the "energy supply chain". Since it is time consuming and expensive to commit the human resources in continuously monitoring infrastructures and the systems and networks they rely upon, it is fundamental to study and introduce tools and mechanisms that can be automatically

triggered to prevent or mitigate a potential attack or anomaly. Such mechanisms should be characterised by a high degree of learning up to the point in which they can deal with the anomaly or attack in a completely autonomous way.

In the Italian context, the importance of the energy sector is further reaffirmed by the "Perimetro Nazionale di Sicurezza Cibernetica" which is an additional measure that has "national security" as final goal and introduces further obligations for the operators of essential services, including some safeguard mechanism on the procurement of digital devices, equipment and tools.

One promising approach provides to implement resilience by design throughout the lifecycle of systems development. Currently, resilience efforts are primarily focused on single-domain networks like energy, water, and freight [20, 26, 27, 28, 29]. However, initiatives have been developed to assess multi-domain resilience using qualitative expert judgment. The Argonne National Lab developed an infrastructure survey tool to collect information on protection and resilience from 16 CI domains [30]. DTs of individual buildings can integrate data from all domains, allowing for examination of correlations and causal relationships. Data must be gathered from individual domains, a data warehouse constructed, and key resilience indicators developed. System operators must identify correlations and causal relationships using ML and causal inference techniques. Addressing this challenge requires a focus on R-KPIs in metric development[31].

The smart grid, as a complex CPS, faces significant security challenges, and a comprehensive understanding of attack threats and defense strategies is essential [32]. A full group of physical impact scenarios on an infrastructure can be calculated [33]. A resilience metric is desirable for smart grids [34]. The detection of security threats in CPSs is becoming increasingly critical due to the increasing interconnection of CIs with public networks. Further research is needed to advance academic research and develop preventative solutions for safe and secure implementation of these systems. Typical cyber-attacks targeted to CPSs include Input Fuzzing, Man-in-the-Middle, distributed Denial of Service, False Data Injection, and more [35]. Resilience can be ensured by implementing a process for anomaly detection or early warning. Anomaly detection, also known as outlier detection, is a real-time monitoring process that aims to identify patterns in a data set that do not align with normal behavior, typically referring to infrequent events [36]. Tightly linked to anomaly detection is the concept of early warning system. Even such a system implements a real-time monitoring process that is capable of detecting adverse trends and making reliable predictions. An early warning process collects, analyzes, interprets, and communicates data, enabling early decision-making to protect public health and the environment [37]. So, anomaly detection can be considered as part of the early warning process. Both threat/anomaly detection and early warning are commonly used in various fields, including cyber-attack threats. While threat detection and prevention in enterprise networks is mature, CPS currently lacks equivalent capabilities [35]. For the aim of this paper, we implement a specific cyber-attack scenario in which we simulate the anomaly detection to increase the system resilience. As future work, we aim to develop an early warning system based on a comprehensive anomaly detection algorithm for the resilience enhancement of CIs.

In [38], a CPS resilience assessment framework is proposed, which consists of three phases called (1) System Description (SD), (2) Disruption Scenario (DS), and (3) Resilience Strategy (RS), each corresponding to the typical steps of the resilience cycle. Both the hazard and the resilience

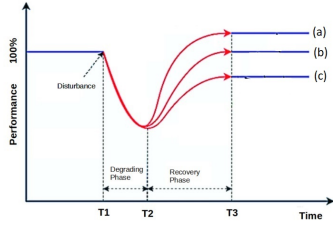
strategy contribute to determining the damage to the system. The damage scenario and the CPS model are used to assess resilience, but not all three phases are necessary. In the SD phase, data and knowledge about the system structure and processes are gathered to build the model for the CPS. A Measure of Performance (MoP) is defined according to the resilience objectives of the CPS, which is computed over time to represent the evolution of the CPS's structure and processes. In the DS phase, data and knowledge about possible hazards that may disrupt the CPS and the resulting damages are gathered or created. Deductive methods estimate the damage caused by a known hazard, while deductive methods identify hazards that may cause a given damage. Finally, RS provides to gather data and knowledge about available resilience strategies, either reactive or proactive, which aim to mitigate or prevent damages, with reactive strategies restoring system performance and minimizing losses after damage has occurred. Resilience can be assessed based on the analysis of system attributes and performance during normal operating conditions. Critical components and processes can be identified, and resilience can be preemptively assessed. A disruption scenario can be added for an accurate assessment of system behavior during disrupted conditions. The resulting damage can be mitigated with the implementation of resilience strategies. However, in some real-world scenarios, systems may not be restored by the aid of resilience strategies and may collapse or recover as the disruption elapses. The CPS model and the damage scenario created through these phases are used for the resilience assessment, with defined resilience metrics provided as input and a resilience report with quantified metrics obtained as output. In [38], for each phase of the proposed framework a list of the most common disruption scenarios and the corresponding resilience strategies is provided.

The first step for resilience evaluation is resilience quantification, which employs a scenario-based approach, with methods tailored to the nature of the studied risk [39, 40, 41]. While much literature concentrates on analytical frameworks for disaster resilience [42, 43, 44, 45], the surge in studies evaluating the resilience of CIs under CP attacks is evident [46, 47, 48, 5]. In this article, we explore the resilience of a smart PV power station under a cyber attack scenario.

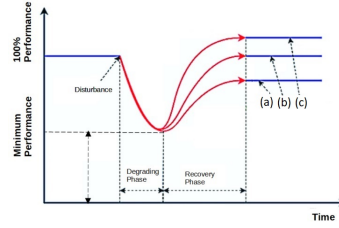
Various metrics have been proposed for Engineering Resilience Quantification, yet in the CI domain, prioritizing service continuity and maintaining a minimum service level is crucial for societal well-being during risks, including extreme events and CP attacks [49, 50, 51, 52]. Therefore, this article focuses on indicators linked to system recovery time [51, 53, 54] and functionality loss.

### 3. Methodology

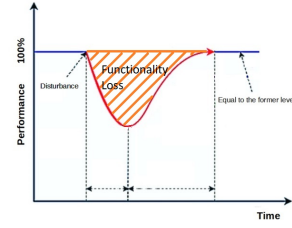
The primary aim of resilience-enhancing metrics is to elevate the three core capacities of resilience, namely absorption, adaptation, and restoration. To evaluate the behaviour of the system after a disturbance, three Resilience KPIs are selected. The recovery time (Figure 1) is the most important indicator of the resilience of CI. Particularly in sectors like energy, due to its direct impact on the overall operational resilience recovery time is the most important Resilience KPI. Recovery time is the period during which a system experiences a decline in functionality or performance, measured from the occurrence of the disturbance until the system returns to a state of stable performance. As Figure 1 shows, the new performance level after



**Figure 1:** Recovery time



**Figure 2:** Min. performance



**Figure 3:** Functionality loss

stabilization can be a) Lower than the prior disturbance level of performance, b) Equal to the former level, or c) Higher than the prior disturbance.

The determination of the minimum performance level (Figure 2) in CI is contingent upon the inherent design features of the system and the severity of the encountered disturbance. Monitoring this minimum performance level holds crucial significance as it ensures the preservation of essential services vital for the system's proper functioning. The minimum performance level is intricately defined by the indispensable thresholds associated with the societal needs for that particular service.

Resilience curves are applied across the CI literature shows two kind of curve: typical representation with a semi-linear degradation and semi-linear recovery phase, or non-idealized system behavior(Figure 3). The research employs a resilience assessment framework adapted from [51], which is an Integral-based metric that incorporate both time and performance. This framework evaluates the impact of disturbances on infrastructure by estimating the degradation in service quality ( $Q(t)$ ). The process involves assessing the degradation from the disturbance ( $t_0$ ) until full recovery ( $t_1$ ), representing the recovery phase.

Regarding Loss of Functionality ( $LF$ ), it quantifies service quality degradation during the recovery period, irrespective of the system's behavior. The calculation is expressed as:

$$LF = \int_{t_0}^{t_1} [100 - Q(t)] dt$$

For better demonstrate the usefulness of the three aforementioned Resilience KPIs as means to evaluate the behaviour of the system in a realistic cyber-attack scenario, a case study is proposed in the following section. This case study is intended to use these KPIs for the efficacy assessment of the anomaly detection algorithm in bolstering the system's resilience.

## 4. Case Study

The case study aims to assess the proposed energy CP framework, which includes three main building blocks: Physical Asset, Data Infrastructure, and DT. The Physical Asset is constituted by a Smart PV Station (SPVS), that is portable power-generating infrastructure featuring a PV panel with sensors and actuators for orientation. The Data Infrastructure focuses on data streaming and persistence, deployed using a fog node on a Raspberry PI 4B. The DT is a virtual world interactive model of the SPVS, containing four fundamental services: Dynamic Environment, Operation, Ideal State, and Demand. These services are deployed on a workstation,

representing the cloud backend of the framework, but with limited processing and storage capabilities. The case study serves as an experiment to evaluate the framework’s functionality and features. For the sake of clarity, the case study corresponds to a simplified scenario, eliciting additional complex, interconnected and dependent events and factors that come into play and significantly impact in a real-world context. Finally, a more comprehensive and exhaustive evaluation test is planned to be accomplished for assessing the proposed R-KPIs also on larger scale implementations, such as smart grids and smart cities scenarios.

#### 4.1. Physical Asset

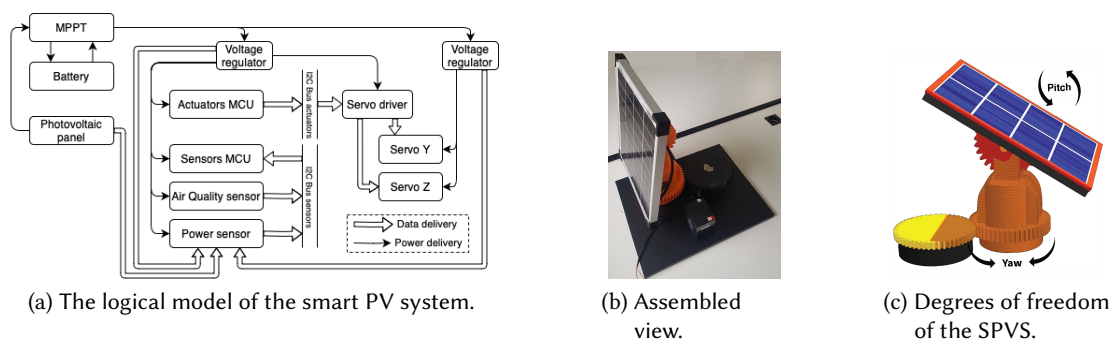
The models discussed in this case study are applied in the PV power generation system called SPVS. Such a system is part of the real testbed implemented in [55, 56] and which is detailed in the present section. The list of components that are presented in Table 1 was used for assembling the CP infrastructure (Figure 4b) and for evaluating our experimental setup. The logical model of the SPVS is shown in Figure 4a, where the physical components and the connections between them are represented. In particular, it includes two types of physical connections: power delivery and data delivery. The former is used to highlight the electric circuit to power the SPVS components, whilst the latter maps the data streams between the components.

A 20W monocrystalline solar module, is chosen for the implementation of the portable SPVS testbed. The module uses high-efficiency monocrystalline solar cells, costing over 18%, and is suitable for 12V systems.

The SPVS uses sensors and actuators to monitor and interact with its environment. It assesses air quality and collects data on the PV panel’s live power production, battery power, and system operations. The station can track specific orientations using onboard actuators, including servo motors that control the panel’s pitch and yaw angles (as shown in Figure 4c).

The SPVS physical asset’s brain uses ESP32 microcontroller units due to their good performance, low cost, and compact size. The boards also features an antenna module for wireless communication on the 2.4GHz band.

The device is powered by the energy generated by the PV panel and stored in a battery. To this end, a Maximum Power Point Tracker (MPPT) monitors the PV panel’s output to regulate voltage and current to keep the system at maximum power at all times. However, the MPPT’s



**Figure 4:** SPVS physical asset implementation.

**Table 1**

List of Sensors, Actuators, and Other Components

Category	Component	Specification
Sensors	Air quality	Bosch BME280
	Power	INA3221
Actuators	Servo Motors	2x (0°-180°)
Other Components	MCU	2x ESP32
	Voltage converter	2x
	MPPT	
	Battery	LiFePo4 12V 6Ah
	PV panel	20W monocrystalline

output is too high to power the logical components, which require 5 volts. Thus, separate power sources are used for low power (sensors and control devices) and high power (servo motors). In particular, two step-down voltage converters are installed between the battery and downstream modules, ensuring constant 5 volts output and avoiding power decreases during power-intensive operations.

## 4.2. System Architecture and Software Components

The Data Streaming service facilitates interaction between the SPVS and its DT virtual services using MQTT protocol. A MQTT message broker is instantiated to process message queues between publishers and subscribers. Client services must include MQTT client implementations to secure and publish sensor data payloads, ensuring timely data reception. Inbound messages are deserialized to transform payloads into JSON objects ready for data processing. The service manages the communication between the physical SPVS and its DT services, and forwards data messages to the Data Persistence service.

The Data Persistence service consists of two microservices that maintain historical data records between the SPVS and Energy DT's services, including sensor readings and action commands. MongoDB was chosen for the case study due to its document-based structure, which allows high-performance IoT data querying and fast insert queries [57]. MongoDB outperforms relational DBMSs like MySQL in terms of resource utilization and latency [58, 59]. It supports efficient local data storage on edge devices, reducing the need for data transmission to remote servers or cloud infrastructures. In this case study, a Python script implements the interface microservice for the DBMS. In particular, the script acts as a middleman, providing subscriptions for MQTT topics and preparing data for storage through MongoDB microservice interaction.

The Anomaly Detection Service (ADS) is responsible for detecting anomalous behaviours of the SPVS to enhance system efficiency and ensure service continuity. It predicts optimal production parameters for real-time variables like temperature, solar irradiation, and energy consumption using mathematical models [60] or machine learning models. The ADS compares estimated current, voltage, and power values to the provided measured set of related parameters, and if the difference exceeds predetermined tolerance levels, an anomaly is recognized. For developing the present case study, the aforementioned ADS was adopted to identify induced electrical production anomalies and then to mitigate the corresponding effects, as detailed in Section 5.

### 4.3. Attack Scenario

For the purpose of this research, the assumption is that in the current geopolitical scenario, there could be a number of state and non-state actors willing to create minor disturbances or severe disruptions to energy infrastructures as part of a single or more complex and coordinated attack aiming at making interconnected infrastructures and their supply chains cripple. For this reason, the attack scenarios considered for this research and the tests that have been performed on the PV system, is that the attacker would use a "man-in-the-middle" technique. Such a technique is used to interfere with the correct functioning of the generation infrastructure by modifying (tampering with) the part of the setup that allows the synchronization of the clock which controls the correct orientation of the PV, by tracking the most efficient irradiation position throughout the daily lifecycle. Furthermore, in this context, it is assumed that if an attacker would intervene on the synchronization of the system's clock by providing a wrong value, the system would work outside of the established and more performing ranges, up to the point in which the system would position the PV in "sleep mode" in all of the cases in which the wrong value falls before dawn or after dusk. In these cases, the energy production can be significantly reduced with all the corresponding consequences on the missing generation and its inevitable impacts on the expected demand from both the transmission and distribution infrastructures.

### 4.4. Test Condition

January 24, 2023 was the date selected for the tests<sup>1</sup> because during that day the weather remained mostly clear with occasional partial cloud cover. Overall, the weather conditions were relatively stable(see Figure 5), with no significant variations in temperature (see Figure 6) or visibility. The day featured mostly clear skies, transitioning to partly cloudy in the early afternoon(see Figure 7), and the wind speed remained moderate throughout the observed period. These conditions were favorable for conducting tests and collecting data as part of the system implementation. More specifically, the detailed environmental data related to the weather conditions of the selected day have been collected from *Weather Spark*<sup>2</sup>. In the present scenario, stable conditions were chosen to reduce the complexity and minimize the sources of disturbance attributable to third-party factors. The goal of this work is to provide a first evaluation of the proposed R-KPIs in a simplistic scenario, highlighting the contribution of rogue alterations of the physical asset parameters. The effects of further external disturbance factors and the way they can impact on the system behaviour and on the proposed R-KPIs is out of the scope of this paper and can be better analyzed in future works.

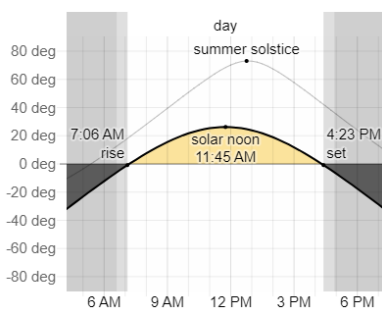
## 5. Results and Discussion

The collected data on the day of the test is depicted in Figure 8. The simulation of a CP attack initiates at 10:10 in the morning. Disturbances caused by the CP attacks are illustrated in

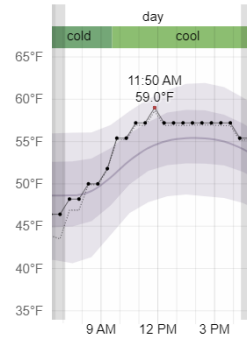
---

<sup>1</sup>The portable smart PV power station testbed is situated within the Ecotekne complex, located in Lecce, Italy. The geographical coordinates are 40°19'59.2"N latitude and 18°06'51.3"E longitude.

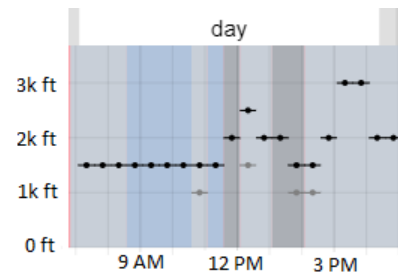
<sup>2</sup><https://weatherspark.com/>



**Figure 5:** Solar Elevation.

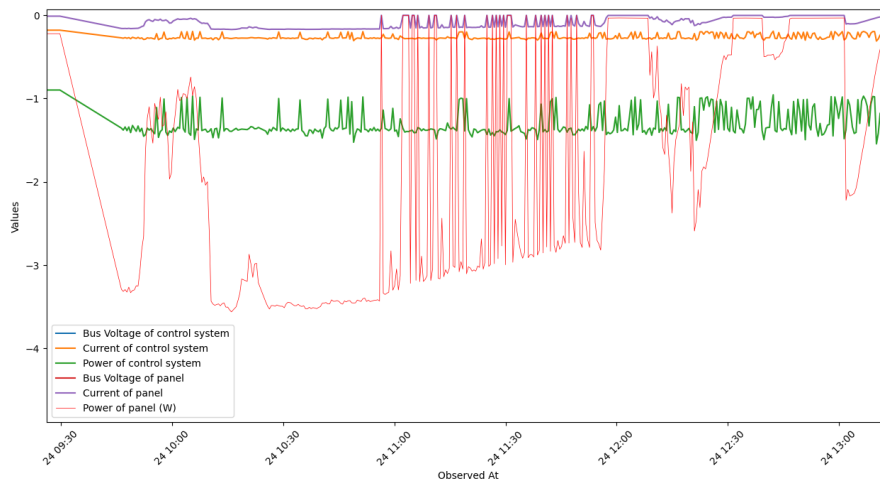


**Figure 6:** Temperature.



**Figure 7:** Cloud Cover.

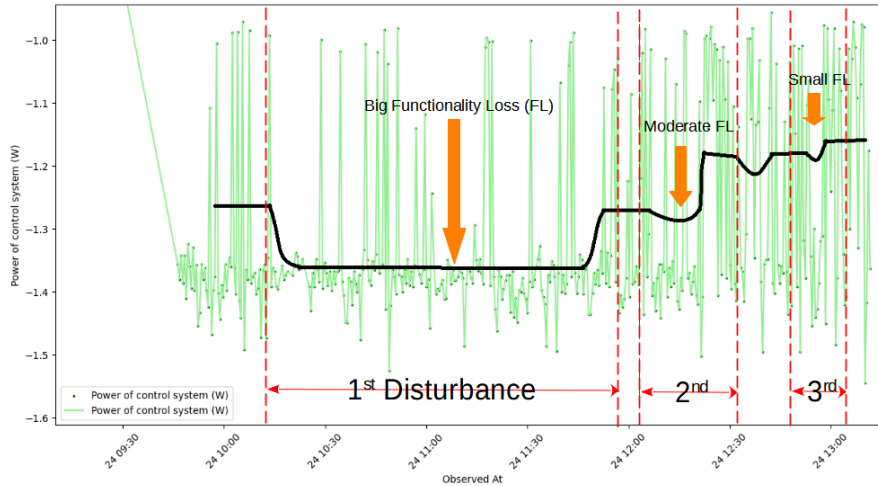
Figure 9. The red line in the figure represents the power consumption induced by the CP attack, forcing the PV panel to return to the rest position. This return to the rest position has a significant impact on power generation, as indicated by the green line.



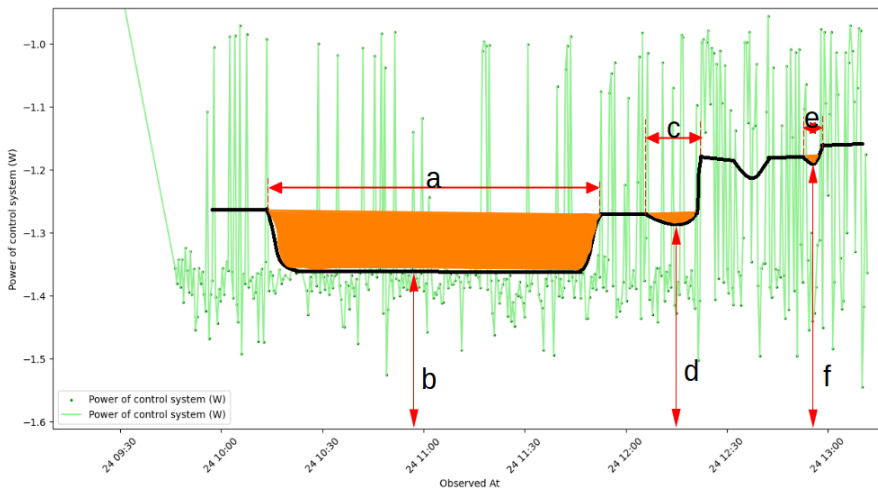
**Figure 8:** Collected data on the day of the test. Power is measured in Watts (W), Voltage is measured in Volts (V), and Current is measured in Amperes (A).

Despite the system being forced into the rest position, the DT's ideal state service attempts to adjust the orientation of the PV panel to follow the sun's trajectory based on time and position. However, the continuous disruption from the CP attack disturbs the system's normal functioning. Around 12 o'clock, the anomaly detection algorithm identifies the anomalous behavior caused by the cyber attack, preventing the system from responding to false imposed conditions.

The second attack simulation occurs at 12:05, and with the anomaly detection trained from the previous behavior and attack features, the system identifies the attack quickly, resulting in minimal functionality loss. After the second attack, the system rapidly returns to the ideal position. In the last attack at 12:35, the functionality loss is negligible, showcasing an improvement in resilience and service continuity. Metrics such as functionality loss, minimum



**Figure 9:** Resilience curve and the disturbance from cyber-physical attacks



**Figure 10:** Resilience curve and the Resilience KPIs (shown by letters from a-j).

performance level, and recovery time demonstrate improvement in response to this attack scenario.

Figure 10 illustrates the R-KPIs for the system during the mentioned attack scenario, as introduced in Sections 3 and 4.3, respectively. The R-KPI values presented in Table 2<sup>3</sup> are derived from the scenario outlined in Figure 10. These findings highlight the efficacy of the anomaly detection algorithm in bolstering the system's resilience.

**Initial Attack Analysis** An examination of the Key Performance Indicators (KPIs) reveals a significant loss of functionality during the first attack. This aligns with the high impact rating

<sup>3</sup>calculated by <https://www.sketchandcalc.com/>

**Table 2**

R-KPIs for the simulated attack scenario

	<b>First Attack</b>	<b>Second Attack</b>	<b>Third Attack</b>
Functionality Loss (FL)	1.8168	0.0657	0.0069
Disturbance Starts	10:10	12:05	12:45
Disturbance Ends	11:55	12:35	13:05
Recovery Time (RT)	01:45	00:30	00:20
Min Performance (Pmin)	1.36	1.29	1.19

assigned within the risk assessment matrix. The scenario poses a greater threat compared to natural disasters, based on a quantity of relevant literature on intentional disruptions versus natural events in literature. Consequently, employing an anomaly detection system is recommended to effectively identify and respond to such attacks. Post-Attack Performance and Recovery: The system's performance exhibits a precipitous decline following the initial attack, reaching a critically low point of 1.36. A comprehensive investigation into this minimum performance level is crucial in the critical infrastructures of the society with real users of the service. This analysis should determine the energy infrastructure's capacity to meet the essential service needs of users during an attack. Furthermore, assessing the recovery time is equally critical in real-world critical infrastructure scenarios. This evaluation entails determining the timeframe for which energy users reliant on this source can sustain operations with the minimum energy level to deliver essential services.

**Impact of Anomaly Detection** The implementation of an anomaly detection system demonstrably improves performance across all Key Performance Indicators (KPIs) during the second and third attacks. This significant improvement suggests a sharp reduction in risk impact when employing such an algorithm. While the attack probability might remain constant, the risk scenario's position within the risk-probability matrix shifts towards a zone characterized by low impact and high probability. Consequently, these risks can be classified as moderate, implying the system's ability to absorb and recover from such disturbances. Nevertheless, further efforts to mitigate the likelihood of occurrence are needed. A comprehensive study is recommended in such a scenario to identify potential modifications within the cyber-physical infrastructures that could enhance overall security and diminish the probability of this specific attack scenario.

## 6. Conclusion and Future Work

This research has allowed the team to fine tune the understanding of the dynamics behind a possible attack to a PV generation infrastructure. Thanks to the use of a testbed, the research has provided very solid premises and insights that will allow the extension to real cases and full scale infrastructures. Even though further analyses are required, the team is motivated to look for partners in the domain of electricity distribution, transmission and generation to allow the execution of a full scale test in a more complex data management infrastructure such as a data space, fostering the cabling of early warning and response policies in DTs of smart grids and CIs. In this regard, the long term goal is to understand the self-healing capabilities of systems and

networks enabling the continuous and undisturbed delivery of essential services, leveraging novel data-driven approaches to digital services that use real-time field data.

The case study presented is validated using a small scale portable testbed that includes a single PV panel, as discussed in section 4.1. Although the current setup provided valuable insights as discussed in this paper, it is limited and poses significant challenges with respect to large scale scenarios. Future studies will also address the scalability of the proposed approach to full-scale infrastructures, also involving key role players in the power distribution sector.

## References

- [1] A. I. H. A. Ramadan, A. A. Ardebili, A. Longo, A. Ficarella, Advancing resilience in green energy systems: Comprehensive review of ai-based data-driven solutions for security and safety, in: *2023 IEEE International Conference on Big Data (BigData)*, 2023, pp. 4002–4010. doi:10.1109/BigData59044.2023.10386721.
- [2] Y. Lim, J. Ninan, S. Nooteboom, M. Hertogh, Organizing resilient infrastructure initiatives: A study on conceptualization, motivation, and operation of ten initiatives in the netherlands, *Resilient Cities and Structures 2 (2023)* 120–128. doi:10.1016/j.rcns.2023.10.001.
- [3] E. Evangelopoulos, Smart counties: technologies, considerations, characteristics, challenges, policies, and theoretical concerns, Elsevier, 2022, p. 49–78. doi:10.1016/b978-0-12-819130-9.00039-5.
- [4] S. Paul, F. Ding, K. Utkarsh, W. Liu, M. J. O'Malley, J. Barnett, On vulnerability and resilience of cyber-physical power systems: A review, *IEEE Systems Journal* 16 (2022) 2367–2378. doi:10.1109/jsyst.2021.3123904.
- [5] S. Mohebbi, Q. Zhang, E. Christian Wells, T. Zhao, H. Nguyen, M. Li, N. Abdel-Mottaleb, S. Uddin, Q. Lu, M. J. Wakhungu, Z. Wu, Y. Zhang, A. Tuladhar, X. Ou, Cyber-physical-social interdependencies and organizational resilience: A review of water, transportation, and cyber infrastructure systems and processes, *Sustainable Cities and Society* 62 (2020) 102327. doi:10.1016/j.scs.2020.102327.
- [6] H. Boyes, R. Isbell, T. Watson, *Critical Infrastructure in the Future City*, Springer International Publishing, 2016, p. 13–23. doi:10.1007/978-3-319-31664-2\_2.
- [7] J. Ingrisch, M. Bahn, Towards a comparable quantification of resilience, *Trends in Ecology & Evolution* 33 (2018) 251–259. doi:10.1016/j.tree.2018.01.013.
- [8] P. Tamvakis, Y. Xenidis, Comparative evaluation of resilience quantification methods for infrastructure systems, *Procedia - Social and Behavioral Sciences* 74 (2013) 339–348. doi:10.1016/j.sbspro.2013.03.030.
- [9] A. S. Jin, L. Hogewood, S. Fries, J. H. Lambert, L. Fiondella, A. Strelzoff, J. Boone, K. Fleckner, I. Linkov, Resilience of cyber-physical systems: Role of ai, digital twins, and edge computing, *IEEE Engineering Management Review* 50 (2022) 195–203. doi:10.1109/emr.2022.3172649.
- [10] B. Cassottana, M. M. Roomi, D. Mashima, G. Sansavini, Resilience analysis of cyber-physical systems: A review of models and methods, *Risk Analysis* 43 (2023) 2359–2379. doi:10.1111/risa.14089.

- [11] D. E. Culler, H. Mulder, Smart sensors to network the world, *Scientific American* 290 (2004) 84–91.
- [12] S. N. Vecherin, D. K. Wilson, C. L. Pettit, Optimal sensor placement with signal propagation effects and inhomogeneous coverage preferences, *International Journal of Sensor Networks* 9 (2011) 107–120.
- [13] S. Slijepcevic, M. Potkonjak, Power efficient organization of wireless sensor networks, in: *ICC 2001. IEEE international conference on communications. Conference record (Cat. No. 01CH37240)*, volume 2, IEEE, 2001, pp. 472–476.
- [14] M. O. Ahmad, M. A. Ahad, M. A. Alam, F. Siddiqui, G. Casalino, Cyber-physical systems and smart cities in india: Opportunities, issues, and challenges, *Sensors* 21 (2021) 7714.
- [15] A. El Saddik, Digital twins: The convergence of multimedia technologies, *IEEE multimedia* 25 (2018) 87–92.
- [16] F. Tao, H. Zhang, A. Liu, A. Y. Nee, Digital twin in industry: State-of-the-art, *IEEE Transactions on industrial informatics* 15 (2018) 2405–2415.
- [17] T. Wang, Y. Liang, W. Jia, M. Arif, A. Liu, M. Xie, Coupling resource management based on fog computing in smart city systems, *Journal of Network and Computer Applications* 135 (2019) 11–19.
- [18] T. Wang, Y. Liang, Y. Yang, G. Xu, H. Peng, A. Liu, W. Jia, An intelligent edge-computing-based method to counter coupling problems in cyber-physical systems, *IEEE Network* 34 (2020) 16–22.
- [19] D. Martínez, W. Brewer, A. Strelzoff, A. Wilson, D. Wade, Rotorcraft virtual sensors via deep regression, *Journal of Parallel and Distributed Computing* 135 (2020) 114–126.
- [20] P. E. Roege, Z. A. Collier, J. Mancillas, J. A. McDonagh, I. Linkov, Metrics for energy resilience, *Energy Policy* 72 (2014) 249–256.
- [21] J. Brenner, Iso 27001 risk management and compliance, *Risk management* 54 (2007) 24–29.
- [22] K. Stouffer, J. Falco, K. Scarfone, et al., Guide to industrial control systems (ics) security, NIST special publication 800 (2011) 16–16.
- [23] J. T. Force, Security and privacy controls for information systems and organizations, Technical Report, National Institute of Standards and Technology, 2017.
- [24] C. I. Cybersecurity, Framework for improving critical infrastructure cybersecurity, URL: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.4162018> (2018).
- [25] F. Cleveland, Iec tc57 wg15: Iec 62351 security standards for the power system information infrastructure, White Paper (2012).
- [26] A. Al-Mutairi, S. AlKheder, S. Alzwayid, D. Talib, M. B. Heji, J. H. Lambert, Scenario-based preferences modeling to investigate port initiatives resilience, *Technological Forecasting and Social Change* 176 (2022) 121498.
- [27] A. Hasandka, J. Rivera, J. Van Natta, NREL’s Cyber-Energy Emulation Platform for Research and System Visualization, Technical Report, National Renewable Energy Lab.(NREL), Golden, CO (United States), 2020.
- [28] T. M. Aljohani, M. J. Beshir, Matlab code to assess the reliability of the smart power distribution system using monte carlo simulation, *Journal of Power and Energy Engineering* 5 (2017) 30–44.
- [29] S. Chanda, A. K. Srivastava, Defining and enabling resiliency of electric distribution systems with multiple microgrids, *IEEE Transactions on Smart Grid* 7 (2016) 2859–2868.

- [30] D. T. Ton, W. P. Wang, A more resilient grid: The us department of energy joins with stakeholders in an r&d plan, *IEEE Power and Energy Magazine* 13 (2015) 26–34.
- [31] N. Yodo, P. Wang, Engineering resilience quantification and system design implications: A literature survey, *Journal of Mechanical Design* 138 (2016). doi:10.1115/1.4034223.
- [32] H. He, J. Yan, Cyber-physical attacks and defences in the smart grid: a survey, *IET Cyber-Physical Systems: Theory & Applications* 1 (2016) 13–27. doi:10.1049/iet-cps.2016.0019.
- [33] S. A. Timashev, Cyber reliability, resilience, and safety of physical infrastructures, *IOP Conference Series: Materials Science and Engineering* 481 (2019) 012009. doi:10.1088/1757-899x/481/1/012009.
- [34] L. Das, S. Munikoti, B. Natarajan, B. Srinivasan, Measuring smart grid resilience: Methods, challenges and opportunities, *Renewable and Sustainable Energy Reviews* 130 (2020) 109918. doi:10.1016/j.rser.2020.109918.
- [35] N. Jeffrey, Q. Tan, J. R. Villar, A review of anomaly detection strategies to detect threats to cyber-physical systems, *Electronics* 12 (2023) 3283.
- [36] V. Chandola, A. Banerjee, V. Kumar, Anomaly detection: A survey, *ACM computing surveys (CSUR)* 41 (2009) 1–58.
- [37] J. E. Quansah, B. Engel, G. L. Rochon, Early warning systems: a review, *Journal of Terrestrial Observation* 2 (2010) 5.
- [38] B. Cassottana, M. M. Roomi, D. Mashima, G. Sansavini, Resilience analysis of cyber-physical systems: A review of models and methods, *Risk Analysis* (2023).
- [39] A. Shafieezadeh, L. Ivey Burden, Scenario-based resilience assessment framework for critical infrastructure systems: Case study for seismic resilience of seaports, *Reliability Engineering & System Safety* 132 (2014) 207–219. doi:10.1016/j.res.2014.07.021.
- [40] T. Davies, S. Beaven, D. Conradson, A. Densmore, J. Gaillard, D. Johnston, D. Milledge, K. Oven, D. Petley, J. Rigg, T. Robinson, N. Rosser, T. Wilson, Towards disaster resilience: A scenario-based approach to co-producing and integrating hazard and risk knowledge, *International Journal of Disaster Risk Reduction* 13 (2015) 242–247. doi:10.1016/j.ijdr.2015.05.009.
- [41] A. Al-Mutairi, S. AlKheder, S. Alzwayid, D. Talib, M. B. Heji, J. H. Lambert, Scenario-based preferences modeling to investigate port initiatives resilience, *Technological Forecasting and Social Change* 176 (2022) 121498. doi:10.1016/j.techfore.2022.121498.
- [42] G. P. Cimellaro, A. M. Reinhorn, M. Bruneau, Framework for analytical quantification of disaster resilience, *Engineering Structures* 32 (2010) 3639–3649. doi:10.1016/j.engstruct.2010.08.008.
- [43] S. L. Cutter, C. G. Burton, C. T. Emrich, Disaster resilience indicators for benchmarking baseline conditions, *Journal of Homeland Security and Emergency Management* 7 (2010). doi:10.2202/1547-7355.1732.
- [44] J. C. Matthews, Disaster resilience of critical water infrastructure systems, *Journal of Structural Engineering* 142 (2016). doi:10.1061/(asce)st.1943-541x.0001341.
- [45] A. Fekete, Critical infrastructure cascading effects. disaster resilience assessment for floods affecting city of cologne and rhein-erft-kreis, *Journal of Flood Risk Management* 13 (2020). doi:10.1111/jfr3.12600.
- [46] A. Salvi, P. Spagnoletti, N. S. Noori, Cyber-resilience of critical cyber infrastructures:

- Integrating digital twins in the electric power ecosystem, *Computers & Security* 112 (2022) 102507. doi:10.1016/j.cose.2021.102507.
- [47] K. Hausken, Cyber resilience in firms, organizations and societies, *Internet of Things* 11 (2020) 100204. doi:10.1016/j.iot.2020.100204.
- [48] M. Malatji, A. L. Marnewick, S. Von Solms, Cybersecurity capabilities for critical infrastructure resilience, *Information & Computer Security* 30 (2021) 255–279. doi:10.1108/ics-06-2021-0091.
- [49] A. Mottahedi, F. Sereshki, M. Ataei, A. N. Qarahasanlou, A. Barabadi, Resilience estimation of critical infrastructure systems: Application of expert judgment, *Reliability Engineering & System Safety* 215 (2021) 107849. doi:10.1016/j.res.2021.107849.
- [50] W. Sun, P. Bocchini, B. D. Davison, Resilience metrics and measurement methods for transportation infrastructure: the state of the art, *Sustainable and Resilient Infrastructure* 5 (2018) 168–199. doi:10.1080/23789689.2018.1448663.
- [51] C. Poulin, M. B. Kane, Infrastructure resilience curves: Performance measures and summary metrics, *Reliability Engineering & System Safety* 216 (2021) 107926. doi:10.1016/j.res.2021.107926.
- [52] W. Liu, Z. Song, Review of studies on the resilience of urban critical infrastructure networks, *Reliability Engineering & System Safety* 193 (2020) 106617. doi:10.1016/j.res.2019.106617.
- [53] L. Iannacone, N. Sharma, A. Tabandeh, P. Gardoni, Modeling time-varying reliability and resilience of deteriorating infrastructure, *Reliability Engineering & System Safety* 217 (2022) 108074. doi:10.1016/j.res.2021.108074.
- [54] B. A. Alkhaleel, H. Liao, K. M. Sullivan, Risk and resilience-based optimal post-disruption restoration for critical infrastructures under uncertainty, *European Journal of Operational Research* 296 (2022) 174–202. doi:10.1016/j.ejor.2021.04.025.
- [55] C. Martella, A. Longo, M. Zappatore, A. Ficarella, Dataspace in urban digital twins: a case study in the photovoltaics, volume 3478, 2023.
- [56] A. Somma, A. D. Benedictis, M. Zappatore, C. Martella, A. Martella, A. Longo, Digital twin space: The integration of digital twins and data spaces, *IEEE*, 2023, pp. 4017–4025.
- [57] N. Yilmaz, O. Alatlı, B. Çiloğlugil, R. C. Erdur, Evaluation of storage and query performance of sensor based internet of things data with mongodb, in: 2018 International Conference on Artificial Intelligence and Data Processing (IDAP), *IEEE*, 2018, pp. 1–6.
- [58] T. Mladenova, I. Valova, Performance study of mysql and mongodb for iot data processing and storage, in: 2022 International Conference Automatics and Informatics (ICAI), *IEEE*, 2022, pp. 60–63.
- [59] M. M. Eyada, W. Saber, M. M. El Genidy, F. Amer, Performance evaluation of iot data management using mongodb versus mysql databases in different cloud environments, *IEEE access* 8 (2020) 110656–110668.
- [60] A. A. Ardebili, A. Longo, A. Ficarella, Digital twinning of pv modules for smart systems - a comparison between commercial and open-source simulation models, in: 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCCom/CyberSciTech), 2023, pp. 1045–1050. doi:10.1109/DASC/PiCom/CBDCCom/Cy59711.2023.10361505.