Cybersecurity Assessment of Digital Twin in Smart Grids

Mulualem Bitew Anley[1,4], Otuekong Ekpo[2,4] and T. Milinda H. Gedara[3,4]

[1]Università degli Studi di Milano, Milano, Italy
[2]Università degli Studi di Napoli, Napoli, Italy
[3]Università degli Studi di Salerno, Salerno, Italy
[4]IMT School for Advanced Studies Lucca, Italy

Abstract

The advent of the digital twin paradigm marks a technological revolution, particularly within smart grid systems enhanced by the Internet of Things (IoT). This study investigates the application of the PILAR tool for assessing the potential cyber risk in a smart grid, leveraging digital twins for improved data management and system performance. Our methodology, informed by standards such as ISO/IEC 27002:2022, the cybersecurity framework, and GDPR, evaluates the security measures necessary for protecting these infrastructures. The effectiveness of PILAR in risk and security control identification is underscored through a comparative analysis with current literature, establishing a proactive risk management approach vital for the cyber-resilience of a smart grid.

Keywords

Cybersecurity, Digital Twin, Risk Assessment, Smart Grid

1. Introduction

Smart grids are a key part of today's energy systems. They bring together efficiency, sustainability, smart management, and energy distribution. Central to this innovation is the integration of Cyber-Physical Systems (CPS) and the Internet of Things (IoT), with the Digital Twin (DT) concept significantly enhancing the performance and operational intelligence of these systems. These virtual counterparts of the physical grids play a crucial role in mirroring and managing the complexities of energy networks. However, this advancement increases cybersecurity risks, as interconnected digital infrastructures become more prevalent and critical in smart grids, making them targets for sophisticated cyber-attacks with potentially wide-reaching implications [1].

Cyber-attacks on smart energy grids are a serious worldwide issue, as these grids are vital for powering our homes, businesses, and critical services. These advanced and connected grids are at risk of cyber threats, which could lead to large-scale power cuts, financial damage, and threats to national safety. For instance, the cyber-attacks in Ukraine during 2015 and 2016 [2], [3], [4]. These attacks caused extensive blackouts, affecting hundreds of thousands of people and exposing the fragility of national power systems [5]. These attacks disrupt the power supply, pose risks to data privacy, and undermine public trust in safeguarding essential services. Moreover, they threaten personal and national security by exposing sensitive information, diminishing confidence in energy providers [6]. The use of DTs in smart grids is widespread because it allows the application and testing of new experiments without affecting mission-critical physical systems with the aid of Industry 4.0 and IoT. Simulation and emulation of physical system components play a vital role in DT of smart grid [7]. However, it also adds additional cyber risk to the smart grids.

In response to cyber risk, a detailed cybersecurity risk analysis of the DT of the smart grid needs to be performed[8]. In the absence of such safeguards, cyber-criminals may compromise the integrity, confidentiality, and availability of this system. It motivates the introduction of a comprehensive risk assessment method specific to DT in smart grid using PILAR [9], a distinguished commercial tool known for its adeptness in modeling complex grid infrastructures and evaluating various security risk

ITASEC 2024: The Italian Conference on CyberSecurity
mulualem.anley@unimi.it (Mulualem Bitew Anley); otuekong.ekpo@imtlucca.it (Otuekong Ekpo); thewadaundagedara@unisa.it (T. M. H. Gedara)

scenarios [10]. By enabling a proactive approach, PILAR allows grid operators to anticipate, prepare for, and mitigate potential cyber threats effectively, thus reinforcing the security posture of smart grids. The tool's advanced algorithms are instrumental in assessing the likelihood and impact of different cyber-attack types, aiding in prioritizing and implementing critical security measures. The analysis highlights the vulnerabilities and potential threats looming over these sophisticated energy networks. By leveraging the capabilities of DT in testing, monitoring, and standardizing security protocols within smart grid environments, the study seeks to highlight the practical implications and challenges, thereby emphasizing the imperative of fortifying the security framework of smart grids against the ever-evolving landscape of cyber risks.

This paper's primary focus is to thoroughly examine the smart grid infrastructure digital twin, with particular emphasis on identifying potential threats and vulnerabilities. Subsequently, the study aims to provide a comprehensive set of recommendations aimed at strengthening the security posture of the smart grid digital twin systems. This is achieved through a critical assessment of the assets, identifying the potential cyber threats, vulnerabilities, and security controls actioned to safeguard these critical infrastructures. The remainder of the paper is structured as follows: section 2 provides related studies on risk assessment in the implementation of the smart grid digital twin; section 3 presents our methodology for risk assessment using PILAR. Section 4 presents the results of our findings from the risk assessment and strategic recommendations for strengthening the cyber resilience of the smart grids in the face of sophisticated cyber threats. Finally, section 5 concludes the paper and outlines the possible directions for future research.

2. Related Works

The current body of research on cybersecurity risk assessment in smart grids is presented in this section. A range of approaches and tools have been proposed to investigate the threats in smart grid infrastructure.

In [11], the authors investigate the cyber-physical security aspects of a microgrid (the building block of the smart grid) concerning their vulnerabilities and threat landscape. This is achieved through a risk assessment exercise to evaluate the impact of risk on microgrid operations. In their findings, they identify possible threats to the microgrid, which include physical attacks, eavesdropping and interception attacks, and nefarious activities. Organizations, cyber criminals, insider threats, hacktivists, nation-state actors, terrorists, and cyber-fighters were also identified as possible threat agents. However, their study only offers theoretical insights into the threat landscape of the microgrid.

The authors in [12] address the challenges associated with the integration of ICT and its standards in a smart grid. They offer a risk management framework based on the CAN/CSA Q-634-91 standard to address both security and health risks associated with smart meters in a smart grid. The framework follows a nine-step process that includes: risk identification, risk analysis, risk planning, risk prioritization, risk treatment, risk monitoring, risk evaluation, risk communication, and documentation. They suggest that further studies are still required to efficiently guide resource allocations and optimize practices at all levels of the smart grid platform to identify, measure, and minimize associated risks. In another study, [13]carried out a cybersecurity risk assessment to methodically examine the impact and likelihood of cyberattacks. They leverage the smart grid Information Security (SGIS) toolbox and apply it to a voltage control and power flow optimization smart grid use case. To determine the security level of an information asset, the toolbox uses a six-step procedure to arrive at its findings. In their results, they assert that a smart grid's operational behavior and related infrastructure may be affected by compromising the integrity of information assets that are essential for voltage control. Also, they assert that the impact of the availability of information assets is limited because grid protection measures account for possible sensor failures. Importantly, they find that compromising the confidentiality of essential assets, such as metering data, could have a significant impact on the Distribution System Operator (DSO) under consideration, thereby impacting the population as a whole and resulting in reputational damage for the operator. In [14], they investigate the applicability of tool-assisted threat

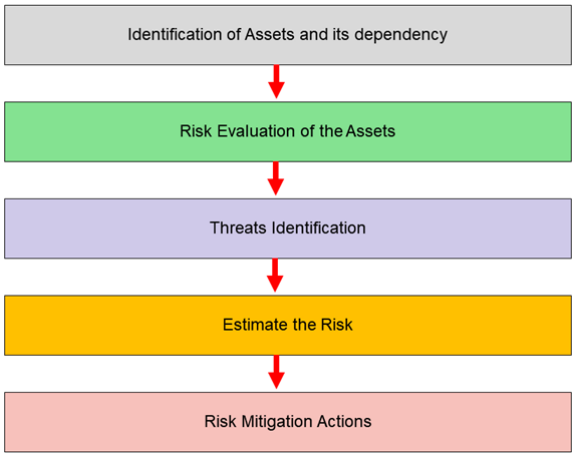


Figure 1: Proposed methodology

modeling to the smart grid. In their study, they employ the Microsoft Threat Modeling Tool (MTMT) to present a template that enables tool support for threat modeling of cyber security in the smart grid. This template is characterized by four threat properties which include priority, loss of power, difficulties in implementing mitigation, and affected systems. The strength of their study lies in the possibility of using the template to reduce the problem of threat explosion that is often encountered during threat modeling.
Similarly, [15] describes a framework for scenario-based risk assessment methodologies that employs a multi-directed graph model to depict the asset-dependency model of smart grids. They achieve this by first categorizing the assets and then developing a web-based tool for visualizing a graph-based model of the assets and their dependencies.
A smart grid ontology with adversarial models and vulnerabilities is presented in [16]. They offer an automated method for integrating the ontology with relevant entries from the Common Vulnerabilities and Exposures (CVE) database, which is the industry-standard vulnerability knowledge base. This leads to a deeper understanding that informs the establishment of security policies and vulnerability assessments for smart grid systems.

Our work distinctively uses the PILAR risk assessment tool to assess the risk in a smart grid, leveraging digital twins for improved data management and system performance. We follow a well-laid-out methodology to examine risks across multiple dimensions, including confidentiality, integrity, availability, authenticity, and traceability (accountability). Our approach is highly parameterizable, allowing customization based on assets, asset dependencies, threat profiles, and security controls. It also supports quantitative and qualitative analysis, impact analysis, and business continuity. This approach, leveraging PILAR with specific capabilities, provides a general yet practical and domain-dependent methodology, distinguishing our work from the existing literature in the field.

3. Proposed Methodology

In this section, the step-by-step methodology followed in assessing the cyber risk of the smart grid using PILAR software as a tool is presented. In state-of-the-art, the DT smart grid risk assessment is identified as an interesting research area. As a use case scenario, the DT of Smart Microgrid Polygeneration (SPM) in Savona Campus, Genoa [7, 17], has been selected to perform the risk assessment. However, the study is conducted in a more general method covering the basic components of DT of the smart grid. The proposed methodology consists of five steps, as shown in Fig 1 followed by the PILAR software. Evaluation and identify critical areas of risk mitigation action needed. The following paragraph details describe each step in the evaluation process.

3.1. Identification of Assets and its Dependencies

In this phase of the risk assessment, forty-four (44) key assets were identified of SMP in Savona Campus [7]. These assets comprise physical components (solar panels, batteries, turbines, etc.), software components (SCADA data systems and energy management applications, etc.), as well as people (operators, administrators, and technical staff). We also categorized and identified the roles that these assets play, especially those that are mission-critical. For example, the data generated from the SCADA is considered critical for real-time monitoring and control, whereas storage equipment for energy is considered pivotal in maintaining an energy balance. Other critical assets identified were remote access control devices, the main controlling system, and various internal services and communication protocols. Additionally, the interdependence of the assets was also identified. For instance, the SCADA system functions through a reliance on various interconnected components like servers, firewalls, and communication lines. This holistic approach puts forward the complex nature of the network of dependencies that characterize a typical smart grid. This can range from advanced control systems to human resources to software, each contributing to the overall efficiency of this critical infrastructure.

3.2. Risk Evaluation of the Assets

In this phase, the dependencies of the assets were evaluated and earlier identified to evaluate them. This valuation is necessary in providing an understanding of risk factors for each asset as well as that of the entire system. Each asset is assessed based on five criteria: availability, integrity, confidentiality, authenticity, and accountability as provided by the tool.

Due to their interconnected nature, we observe that the evaluation of one asset can have an impact on other assets that depend on it. We consider this a butterfly effect as a threat to one asset can have an impact on others dependent on it or otherwise, it depends. Similarly, this evaluation also takes into cognizance factors such as recovery time, compliance with legal and regulatory obligations, security measures, protection of commercial interests, potential activity disruption, maintenance of public order, alignment with operational missions, management considerations, preservation of goodwill, and support in crime prosecution efforts. The severity of the risk impact on the assets is categorized using a numerical range of one (1) to ten (10). A rating of 10 indicates the highest potential impact, while a rating of 1 suggests a negligible impact. This allows for a structured approach to assessing risk, minimizing bias, and achieving consistent evaluation across asset categories. The tool also provides for automated categories of assets such as essential assets, internal services, equipment, subcontracted services, facilities, and personnel which is useful in this phase.

3.3. Threats Identification

After identifying potential risks, the threats posed to the system were evaluated by using the PILAR tool to identify security threats with a particular focus on privacy, errors, unintentional failures, and industrial risks which are typical of such systems. The threats identified are rated on a scale of zero (0) to ten (10) as performed during the risk evaluation phase. Here, a rating of 10 represents a catastrophic system failure, while 0 indicates the absence of a threat. This rating is however adjustable, allowing for modification based on the evaluator's insights.

In the study, the focus is on cybersecurity risk which results in the exclusion of potential threats due to natural phenomena (such as earthquakes and volcanoes, etc.) The PILAR tool is invaluable in providing insights into the likelihood (frequency) of each threat and its impact on the security objectives of each asset. The security objectives include availability, integrity, confidentiality, privacy, user and information authenticity, and accountability of service and data.

In this phase, threats have been identified which include, for instance, threats to the SCADA Data, Such as software failure, hardware failure, malware diffusion, data misuse, and external attacks, each with its frequency of occurrence. These threats significantly affect aspects like asset accessibility and accountability. From the digital twin point of view, we identified threats related to remote access control.

These threats include unauthorized access, identity masquerading, and abuse of access privileges, each affecting integrity and availability to varying degrees.

Other risks, like system failures due to resource exhaustion or administrative errors, and the deliberate or accidental alteration of information, are also noted for their high frequency and impact. By systematically evaluating these threats and their potential impacts, the PILAR tool facilitates an extensive understanding of the risks associated with different assets. This understanding is crucial for making informed decisions and developing effective mitigation strategies.

3.4. Risk Assessment

In this phase, the risk was assessed by using the PILAR tool to again categorize the risk into ten distinct levels (0 - 9). It is also used to automatically generate other potential risks to the system, which can be manually refined and adjusted based on the accumulated knowledge and prior evaluations. This target level is informed by the ISO/IEC 27002:2022 Information Security Controls and Cybersecurity framework/ The security risk of the system, an essential step following the comprehensive threat analysis. Pilar plays a pivotal role in this phase by categorizing risks into ten distinct levels. These levels range from 0, indicating negligible risk, to 9, denoting catastrophic failure. PILAR's role extends beyond mere risk categorization; it automatically generates potential risks, which can be manually refined and adjusted based on accumulated knowledge and prior evaluations. This target level is informed by the ISO/IEC 27002:2022 Information Security Controls and cybersecurity framework.

3.5. Risk Mitigation

Following the evaluation of risks associated with the digital twin, it is evident that most critical points require targeted mitigation actions. To effectively address these, we adhere to the guidelines set forth by ISO/IEC 27002:2022, the Cybersecurity Framework, and GDPR. These standards are crucial in guiding our approach to cyber risk mitigation and mainly focus on a proactive approach to cybersecurity risk management and protecting critical information from unauthorized access and loss instead of a common standard for process control systems ISO/IEC 27019:2017. In this process, the PILAR tool plays a significant role, providing essential recommendations for establishing a robust and resilient security framework. These measures, as advised by PILAR, are not just suggestions but form the backbone of our strategy to reinforce the security of the digital twin's critical components.

4. Findings from the Risk Assessment

In this section, we present the results of the risk assessment methodology followed in using the PILAR tool. We acknowledge the subjectivity of most risk assessment efforts which we recognize is mostly dependent on the experience and knowledge of the analyst. However, in our experience, we are a group of five (5) security specialists (evaluators) actively involved in this kind of exercise, therefore, biases are reduced to the barest minimum.

4.1. Evaluating our Approach

All evaluators concur on the identification of 44 essential assets that constitute a comprehensive representation of the smart grid's digital twin. These assets span from physical components such as solar panels, sensors, and turbines—represented in the digital environment through simulations. Software elements like SCADA data systems and energy management applications, are emulated within the digital twin framework. Additionally, 'pass-through' assets that encompass the human element, including operators, administrators, and technical staff, were considered crucial to the operation. A pivotal part of this analysis was the categorization and assessment of each asset's significance and role within the system. For instance, SCADA data is critical for real-time monitoring and control, while storage energy plays a pivotal role in energy balance. Other significant assets included remote access

control and the main controlling system, along with various internal services and communication protocols. The analysis also highlighted 62 interdependencies among these assets, with the SCADA system's functionality being particularly dependent on interconnected components such as servers, firewalls, and communication lines.
Given the subjective nature of risk evaluation, especially concerning human factors, the assessments were quantified based on each evaluator's viewpoint. The consensus was that the SCADA system data is critically vital, warranting the highest criticality rating and priority in the evaluation. Conversely, the data associated with the turbine on and off functions were assigned the lowest values, as depicted in Table 1. This critical asset evaluation is an essential part of the overall risk assessment, spotlighting the data as highly vulnerable to attacks and instrumental in the operation of the digital twin of the smart grid. This structured and professional approach to risk assessment ensures a balanced and comprehensive evaluation, crucial for the strategic management and protection of the digital twin's key assets.

Asset	**[C]**	**[I]**	**[A]**	**[Auth]**
SCADA data	5	9	9	9
Storage energy	3	5	7	4
Remote access control	6	5	7	6
Main controlling system	9	7	9	7
Data about power Usage	6	5	7	5
Storage discharge	3	5	7	7
Turbine start	4	7	7	3
Turbine stop	4	7	7	3

Table 1
Risk assessment of assets based on different security categories.

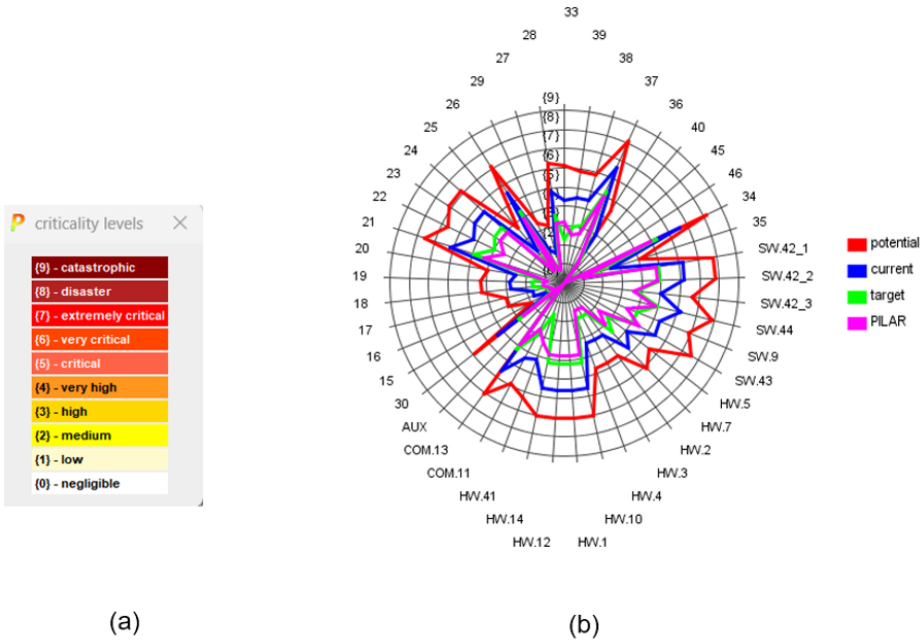
After evaluating potential risks, threats to each asset are evaluated in the next stage. However, here, we only consider cyber security threats and their frequency of occurrence. Table 2 shows the most critical threat identified and the probable frequent attacks or threats that can occur. Table 2 presents the most significant threats, with masquerading of identity (52%), unauthorized access (51%), and deliberate alteration of information (52%) ranking as the most frequently occurring. Other considerable threats include abuse of access privileges (40%), manipulation of configuration files (31%), and denial of service attacks (20%). Conversely, malware diffusion, software manipulation, defects in software maintenance/updating, resource exhaustion-induced system failure, equipment loss or damage, hardware failure, and third-party software information leaks are deemed to pose a less significant risk, each with less than 15% likelihood of occurrence.

Threat	**Frequency of happen (%)**
Unauthorized access	51
Masquerading of identity	42
Abuse of access privileges	40
Denial of service	20
Deliberate alteration of information	52
Manipulation of the configuration files	31
Defects in software maintenance/updating	17
Malware diffusion	15

Table 2
Critical threats and frequency of occurrence .

Based on the potential threat to each asset, the risk estimation is calculated as described in the methodology. The systematic risk evaluation is done on each asset, as shown in Fig 2: the radar chart. The outer layer represents each asset, which is a total of 53, and each level of the inner layer represents the critical levels, indicating each asset's risk level. The critical level description is shown in

Fig2(a), which varies from catastrophic level(9) to negligible level(0). Moreover, the chart delineates four distinct levels: the potential risk inherent to each asset, the current actual risk level, the target risk level as determined by evaluators, and the recommended risk level as suggested by the PILAR tool. Our assessment's alignment with PILAR's guidelines underscores the accuracy of our evaluation, aligning closely with the standardized levels established by the tool's framework.



(a) (b)

Figure 2: Overall asset risk analysis: (a) Level of criticality defined by PILAR; (b) based on input, final risk analysis of assets, current risk, potential risk target, and suggestion level from PILAR.

4.2. Security Controls for Risk Mitigation

In the experimental findings of the study on the PILAR tool's capabilities in mitigating information security risks, several critical areas of focus are identified, aligning with established standards such as ISO/IEC 27002:2022, the Cybersecurity Framework, and the General Data Protection Regulation (GDPR) 2016.

1. **Access control:** The first critical area identified is access control. The experiments show that effective risk mitigation involves comprehensive management of identities and credentials for all authorized entities, including devices, users, and processes. Implementing principles such as least privilege and separation of duties in access permissions management is emphasized. Additionally, the authentication processes for users, devices, and assets are tailored to match the associated risk levels.
2. **Data and information security:** The study highlights the importance of implementing robust protections against data leaks in the realm of data security. This finding underscores the necessity of safeguarding sensitive data from unauthorized access and potential breaches. The study also points out the significance of information security, suggesting that organizations should formulate and regularly review comprehensive information security policies. Effective management of information security roles and responsibilities in the internal organization is deemed essential. Moreover, segregating duties and properly handling information security incidents are crucial elements.
3. **Remote access and online services:** For security control measures in remote access and online services, the findings stressed adherence to business requirements for access control and provisioning. The management of privileged access rights and the secure handling of secret

authentication information are highlighted. Secure log-on procedures and controlled access to program source code are also recommended.

4. **Cryptography:** In the field of cryptography, the implementation of cryptographic controls and effective key management emerged as a key finding. This approach is essential for ensuring the confidentiality and integrity of sensitive data.
5. **Operational security:** The Operations Security section of the study reveals the necessity for well-documented operational procedures, encompassing change management and capacity management. Additionally, protection against malware, backup strategies, and information logging and monitoring are pivotal elements.
6. **Communication security:** Communications security is another crucial area, with the study emphasizing network security management and ensuring network services' security. Policies and procedures for information transfer and electronic messaging are also considered essential. The communication protocol needs to always be encrypted.
7. **System acquisition, development and maintenance of digital twins:** Lastly, in system acquisition, development, and maintenance, ensuring security requirements in information systems and secure development policies are vital. Policies include adhering to secure system engineering principles and conducting thorough system security testing. By integrating these comprehensive security control measures and adhering to the guidelines provided, organizations can significantly enhance their information security posture. This approach effectively mitigates risks and ensures a robust security framework in compliance with recognized industry standards and regulations.

4.3. Comparison with the State of the Art

Proposed Method	Rekik et.al [11]	Lars et. al [14]	Tefek et.al [16]
Access Control	Physical threats	Spoofing	Malicious command injection
Data Security	Unintentional data damage	Tampering	Malicious firmware or configuration
Information Security	Unintentional data damage	Repudiation	False data injection
Remote Access and Online Services	Interception, Hijacking	Information Disclosure	Remote Attack via VPN
Cryptography	Nefarious Activities	Denial of Service	Attacks via User Interface
Operations Security	-	Elevation of Privilege	-
Communications Security	-	-	-
System Acquisition, Development, and Maintenance	-	-	-

Table 3
Identified risks in digital twin smart grid.

Our findings not only show an intersection with some findings in the existing literature but also expand upon it as given in Table 3. To the best of our knowledge, while studies into the cyber risk assessment of the smart grid, leveraging digital twins for improved data management and system performance was lacking in the literature, our work has now filled this gap by eliciting more domain-dependent threats as well security controls to mitigate them. We provide a detailed comparative analysis below.

Access control is universally acknowledged, with the literature citing physical threats, spoofing, and malicious command injection as risks. The proposed approach more clearly details identified vulnerabilities and intensely emphasizes managing identities and credentials, along with robust authentication procedures, which directly mitigates these threats by preventing unauthorized physical and digital access.

Data and information security are also covered and identified by other studies as a concern due to unintentional data damage, tampering, and the potential for malicious firmware or configuration changes. The study's recommendation for robust data leak protections corresponds with the need for preventative measures against such tampering and unauthorized modifications.

Remote access and online services risks, such as interception, hijacking, and remote attacks via VPN, are met with the study's control measures that include adherence to strict access control standards and management of authentication information, thereby safeguarding against such interceptions and unauthorized access. Communications security partially addresses issues such as eavesdropping in the literature.

Even though other studies did not identify cryptography, our studies have now proposed this as a direct response to nefarious activities, with the implementation of cryptographic controls and key management providing a robust defense against threats to confidentiality and integrity. Also, our findings on operations security offer an in-depth approach to mitigating the risk posed by malicious actors. Documented procedures and malware protection are essential to safeguarding the integrity of operational systems.

Finally, our findings on system acquisition, development, and maintenance provide a thorough defense against the information disclosure, denial of service, and elevation of privilege risks identified in the literature. Secure development policies and system security testing are crucial to prevent such vulnerabilities. In summary, the study supports and extends the existing literature by offering specific control measures to address the identified risks in smart grid systems. By implementing these control measures, organizations can effectively mitigate the risks highlighted in this study.

5. Conclusion and Future Work

In this paper, we have systematically analyzed the security risk mitigation strategies proposed by the PILAR tool within the context of digital twin smart grids, comparing our findings against existing findings in the literature. Our findings reveal a significant correlation between the proposed methods and the literature, with additional depth provided by PILAR's adherence to updated international standards. Moving forward, the focus for future work lies in addressing the emerging security risks associated with digital twins, including the incorporation of predictive analytics and artificial intelligence to anticipate and counteract potential cyber threats. This proactive stance is imperative as the complexity and sophistication of digital twin systems evolve, demanding equally dynamic and resilient security measures.

Acknowledgments

We extend our heartfelt gratitude to Prof. Paolo Prinetto, Prof. Stefania Tomasiello, and Prof. Pierangela Samarati for their expert guidance and unwavering support throughout this study. We are also grateful to the CINI Cybersecurity National Lab of Italy for providing essential information, and to the National Ph.D. program in Cybersecurity at the IMT School for Advanced Studies Lucca for the opportunity to undertake this research. Their collective expertise and encouragement have been instrumental to our work.

References

[1] N. Tzanis, N. Andriopoulos, A. Magklaras, E. Mylonas, M. Birbas, A. Birbas, A hybrid cyber physical digital twin approach for smart grid fault prediction, in: 2020 IEEE conference on industrial cyberphysical systems (ICPS), volume 1, IEEE, 2020, pp. 393–397.

[2] J. E. Sullivan, D. Kamensky, How cyber-attacks in Ukraine show the vulnerability of the U.S. power grid, The Electricity Journal 30 (2017) 30–35.

[3] A. Bindra, Securing the Power Grid: Protecting Smart Grids and Connected Power Systems from Cyberattacks, IEEE Power Electronics Magazine 4 (2017) 20–27.
[4] D. E. Whitehead, K. Owens, D. Gammel, J. Smith, Ukraine cyber-induced power outage: Analysis and practical mitigation strategies, in: 2017 70th Annual Conference for Protective Relay Engineers (CPRE), IEEE, 2017.
[5] M. Lehto, Cyber-attacks against critical infrastructure, in: Cyber Security: Critical Infrastructure Protection, Springer, 2022, pp. 3–42.
[6] L. S. Gajanan, M. Kirar, M. Raju, Cyber-Attacks on Smart Grid System: A Review, in: 2022 IEEE 10th Power India International Conference (PIICON), IEEE, 2022.
[7] E. Russo, G. Costa, G. Longo, A. Armando, A. Merlo, Lidite: a full-fledged and featherweight digital twin framework, IEEE Transactions on Dependable and Secure Computing (2023) 1–14. doi:10.1109/TDSC.2023.3236798.
[8] T. Krause, R. Ernst, B. Klaer, I. Hacker, M. Henze, Cybersecurity in power grids: Challenges and opportunities, Sensors 21 (2021) 6225.
[9] S. N. S. Agency, Ear/pilar- environment for the analysis of risk, 2004. URL: https://www.pilar-tools.com/en/.
[10] H. Mokalled, C. Pragliola, D. Debertol, E. Meda, R. Zunino, A Comprehensive Framework for the Security Risk Management of Cyber-Physical Systems, Springer International Publishing, Cham, 2019, pp. 49–68. URL: https://doi.org/10.1007/978-3-319-95597-1_3. doi:10.1007/978-3-319-95597-1_3.
[11] M. Rekik, Z. Chtourou, C. Gransart, A. Atieh, A cyber-physical threat analysis for microgrids, in: 2018 15th International Multi-Conference on Systems, Signals & Devices (SSD), IEEE, 2018, pp. 731–737.
[12] R. W. Habash, V. Groza, D. Krewski, G. Paoli, A risk assessment framework for the smart grid, in: 2013 IEEE Electrical Power & Energy Conference, IEEE, 2013, pp. 1–6.
[13] L. Langer, P. Smith, M. Hutle, Smart grid cybersecurity risk assessment, in: 2015 International Symposium on Smart Electric Distribution Systems and Technologies (EDST), IEEE, 2015, pp. 475–482.
[14] L. H. Flå, R. Borgaonkar, I. A. Tøndel, M. G. Jaatun, Tool-assisted threat modeling for smart grid cyber security, in: 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), IEEE, 2021, pp. 1–8.
[15] A. Priyanka, A. Monti, Towards risk assessment of smart grids with heterogeneous assets, in: 2022 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), IEEE, 2022, pp. 1–6.
[16] U. Tefek, E. Esiner, C. Cheh, D. Mashima, A smart grid ontology: Vulnerabilities, attacks, and security policies, in: 2023 IEEE Conference on Communications and Network Security (CNS), IEEE, 2023, pp. 1–6.
[17] S. Bracco, M. Brignone, F. Delfino, R. Procopio, An energy management system for the savona campus smart polygeneration microgrid, IEEE Systems Journal 11 (2017) 1799–1809. doi:10.1109/JSYST.2015.2419273.