Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P7079-cd

Cyber-physical Studies for Smart Grid Sustainability and Resilience

Irina Oleinikova

Department of Electric Energy, Norwegian University of Science and Technology, Norway. E-mail: irina.oleinikova@ntnu.no

Denys Mishchenko

Department of Electric Energy, Norwegian University of Science and Technology, Norway. E-mail: denys.mischenko@ntnu.no

Cornelia Skaga

Department of Electric Energy, Norwegian University of Science and Technology, Norway. E-mail: cornelia.skaga@ntnu.no

Integrating renewables, power system infrastructure is becoming more digitally connected to ensure safer, more efficient, and decarbonized future. The challenge is that infrastructure is becoming increasingly vulnerable the more connected it becomes. A geopolitical tension with increased risks of cyber-attacks to critical infrastructure, and importance of security of energy supply shape power system this decade. To form and provide a solid foundation, to exploit the full range of system benefits from consumer engagement strategies to the use of flexible mechanisms in an efficient energy system, it is necessary to advance digitalization through an energy system integration strategy, including data exchange. From the perspective of control and stability of converter-dominated systems and the introduction of microgrids into the ever-expanding grid, the development of scalable and reliable control schemes is an urgent need. From the overall smart grid perspective, energy professionals are ready to offer different solutions, for different parts of the grid and voltage levels, to keep the lights on towards a reliable and resilient future of the society. Different aspects of cyber-physical mechanisms for flexible, reliable and resilient smart grid utilization are discussed in the paper. The key factors and barriers for critical infrastructure resilience and sustainability are summarised from the perspective of power system performance, behaviour and processes.

Keywords: cyber-security, power system, digitalization, critical infrastructure.

1. Introduction

To accelerate the dual mission of the green and digital transition, a transformation of energy industry, economy and society is needed to achieve climate neutrality in Europe by 2050. In the scope of this research, it focusses on moving towards greenhouse gas neutrality in the energy and transport no later than 2050, while enhancing their competitiveness, sustainability and value for citizens and society. The energy sector, as a key component of critical infrastructure, encompasses both IT and OT (Information and Operation Technology), making it a potential target for various threats. In 2024 cyber-security incident assessment, in the energy sector accounted for 4% of all reported incidents affecting targeted sectors [1], Fig. 1, proves the importance for cyber-physical studies.

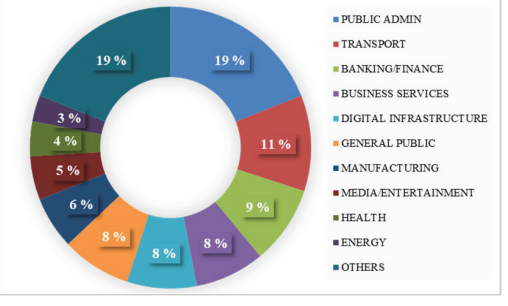

Fig. 1. Targeted sectors per number of cyber threats incidents

When developing and implementing new solutions, it is important to consider particularly critical aspects that affect the energy security of energy grid operation and management technologies. As energy security of the energy grid and safe storage of variable renewables is directly related to a cost-effective and sustainable energy system and therefore essential to European competitiveness, not only energy security aspects of the grid and storage technologies as such, but also those related to their respective value chains need to be addressed. [2]

This study presents the development of solutions for grid operation and management technologies that can significantly improve their sustainability, resilience and overall energy security performance in the long-term context.

This paper addresses the following key factors:

- High awareness of external threats, and a need to strengthen internal competence and training.
- Advanced methods, applications and frameworks addressing cyber-security risks at energy system transmission, distribution levels and operation technologies.

Europe is at the forefront of climate science and is committed to continuing to provide knowledge to ensure effective pathways and fair transitions to climate neutrality. Therefore, it is especially important to address these questions incorporating real-time grid monitoring, predictive analytics, and automated control systems, optimizing grid performance to improve efficiency, and ensure reliability and resilience.

2. Energy Sector Digitalization

In this context, energy sector digitalization is a key enabler for clean transition process; thus, the EU has published an EU Action Plan for digitalising the energy system as a substantial part of the investments foreseen for the European energy system. Through the EU Action for digitalising the energy system plan, several strategic targets, have been identified along with specific steps towards their achievement, where cyber-security enhancement is among them [2]. In this document, the Commission is targeting measures to increase the cyber resilience of the electricity system addressing cyber-security risks and ensuring an accessible and competitive market for new services and products. As well as, another document, The Network Code for Cyber-security [3] includes main rules on common (minimum) requirements addressing planning, monitoring, and reporting crisis management. The Commission has highlighted energy as a priority sector of critical infrastructure and provided guidelines [4] for the secure exchange of data and information, and enhanced capacity to anticipate, prepare, respond and recover from any disruption. From the research perspective, several research areas will require enhancing cyber-security and resilience, with a particular focus on ensuring the security of critical infrastructure, covering both cyber and physical assets, strengthening cyber-security and resilience of energy systems.

3. Cyber-security is an Important Consideration in Grid Operation

The reason why cyber-security should be addressed is that energy system infrastructure is becoming increasingly vulnerable the more connected it becomes. Unfortunately, the overall geopolitical situation and the increased risks of cyber-attacks on critical infrastructure that impact the security of the energy supply are shaping the energy system this decade. One of the several reasons why society has become so serious about cyber-security is the availability of reports of anomalies [5].

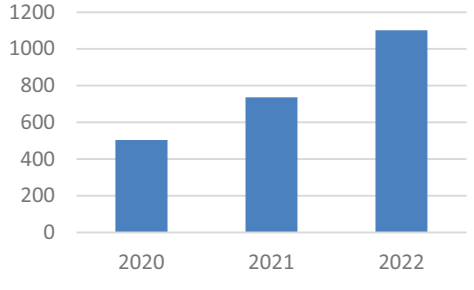

Fig. 2. Number of weekly cyberattacks [5].

In recent years, there has been an increase in reports of cyber-security in IT and OT in the energy sector, which is likely due not to a large increase in the anomalies themselves, but to more people taking responsibility for reporting and investigating these anomalies.

3. Power System Management

The massive growth of renewable energy sources (RES) and distributed energy resources (DER) has created significant opportunities for modern electric grid operation and management.

3.1. TSO-DSO Coordination and Data Interoperability

Improved coordination between transmission system operators (TSOs) and distribution system operators (DSOs) requires information exchange and integration of complexities such as grid congestion management, balancing and coordination between system and market operators, and all with application programming interfaces (APIs) to connect the platform(s) to various electricity consumers (prosumers and Electric Vehicle's-EV owners).

These strategies heavily rely on modern data interoperability and coordination supported by metering devices and sensing technologies, reproduced by simulating in real-time power system model, thus, providing information to all involved actors like TSOs and DSOs, market operators and aggregators. To this end, the idea of energy management and trading among various energy actors seems quite attractive, especially when it happens online. Thus, new security measures are needed combining the arsenals from both domains: IT and electric power engineering.

3.2. Implementing Flexibility for Resilience

It is already clear that a key element of future networks will be *flexibility solutions*, which is defined as the ability of the network to maintain a balance between generation and load under uncertainty [6]. The main sources of flexibility are controlled generation, storage technologies and consumer response to demand through their voluntary management of generation and consumption patterns and EV charging. Addressing the consumer flexibility, considering demand response methods and local energy management paradigm around individual end users/consumers and self-generated energy consumers – power producers, a new axis with different granularity has been added using SGAM[a] layers to achieve synergies across domains and covered areas including digital ecosystem, data and cyber-security principles, see Figure 3 [7]. To ensure integration of services that can optimize flexibility for the benefit of TSOs and DSOs, the ability to integrate multiple services, data platforms, and applications that enable automated transactions should also be considered [8].

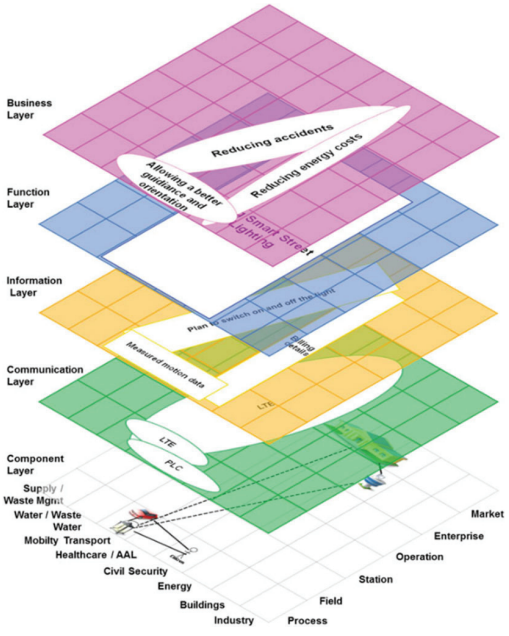

Fig. 3. Granularity of SGAM cube extended with different services and the end-user in focus.

Data platforms and its interoperability, data management from different sources relies on the availability and usability of meaningful data and tools, therefore, the design and performance of the proposed software application architectures become crucial [9]. ICT layer includes various closed-loop control systems to provide reliable and efficient electricity transmission, real-time protection and control functions of the grid. These control systems become attractive targets for cyber-attackers who aim at causing service outage and infrastructural damage. Therefore, considering power system complexity and many

[a] SGAM- Smart Grid Architecture Model

potentials ways of failure, systems like wide-area monitoring, protection, and control (WAMPAC) are expected to support the transmission system operators in maintaining stability and security of supply for modern power systems operation and control [10].

4. Power System Control

Implemented systems, such as supervisory control and data acquisition system (SCADA), were designed when cyber-security was not part of the technical specifications for the system design. In fact, cyber-attacks have become increasingly sophisticated, stealthy, targeted and multi-faceted, and incidents like power outages, failures and blackouts are happening, and they may affect the critical infrastructure of the utility and society. Therefore, the energy sector should further be enhanced implementing self-healing mechanisms in case of emergency, backup power, islanding and restoration concepts and solutions for modern power grids.

4.1. Test Infrastructure

The development of a robust testbed infrastructure is essential for conducting cyber-physical studies aimed at enhancing the sustainability and resilience of smart grids. To achieve this, a dedicated cyber-physical security (CPS) testbed was established within the National Smart Grid Laboratory (NSGL) at the Norwegian University of Science and Technology in Trondheim, Norway. The primary objective of this testbed is to explore and evaluate countermeasures against threats that commonly target power system components in the Nordic and Europe regions.

The NSGL is a facility that connects various infrastructure elements, including a control center, smart house, photovoltaic systems, and charging and energy storage units. These components are integrated through a network that enables simulations to be transmitted to the control center, creating a dynamic and realistic testing environment. A distinctive feature of the laboratory is its capability to combine real-time simulations with physical power system assets through hardware-in-the-loop configurations. The testbed supports ratings of up to 200 kVA, 400 V AC, or 700 V DC, allowing for the accurate replication of real-world conditions. The setup enables researchers to conduct comprehensive cyber-physical tests, systematically identifying vulnerabilities and evaluating security measures that contribute to the overall resilience of smart grid systems [11].

The CPS testbed was designed with adaptability in mind, allowing it to accommodate a wide range of industrial control systems across various domains, including generation, transmission, distribution, and consumption. Each structural level of the testbed consists of both physical and cyber components, providing flexibility and ensuring high fidelity in test results. The testbed's layered architecture, see Fig.4, allows interactions between different levels, simulating real operational conditions.

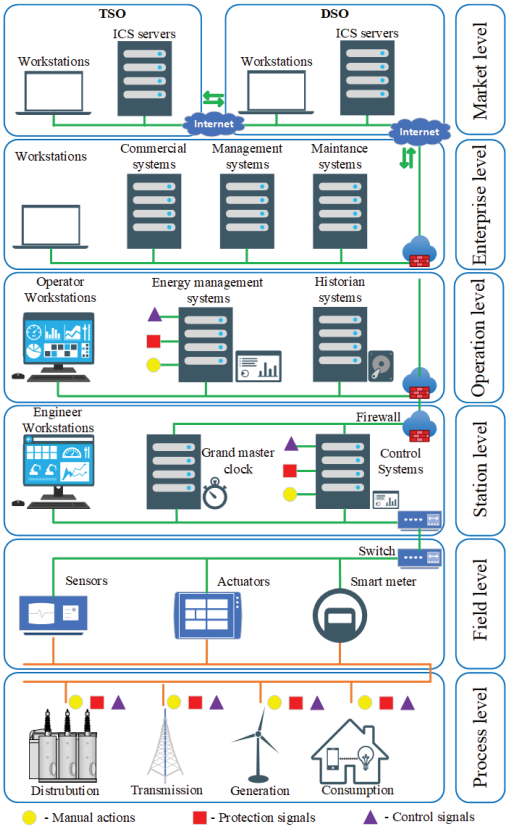

Fig. 4. Cyber-physical security testbed architecture

Alternatively, individual levels can be isolated to focus on specific threats, which is achieved through the configuration of network switches, routers, and firewalls. A demilitarized zone was

established within the testbed, offering a secure space for implementing threats without compromising the overall network integrity [12]. The communication layer of the testbed incorporates modern digital substation network protocols commonly used in monitoring, control, and protection systems. The testbed's integration with a physical devices and real-time digital simulator enables the testing of various case studies involving other widely used protocols, such as IEC61850, IEEE C37.118.2-2011, Modbus, IEC 60870-5-104, OPC UA, and more. This comprehensive communication framework allows for evaluating interoperability, resilience, and security across different layers of smart grid systems.

Case studies within the CPS testbed are constructed using an adversary setup specifically designed to simulate cyber-attacks. The adversary setup includes a suite of penetration testing tools and custom scripts developed in Python. These tools are employed to exploit security vulnerabilities and execute various cyber study scenarios. The process begins with a primary goal, such as compromising monitoring, protection, or control systems, or disrupting the power supply, and is further broken down into sub-goals and specific steps [13]. By strategically positioning the adversary setup within the testbed's layers, researchers can conduct thorough evaluations of cyber-physical vulnerabilities and test the effectiveness of protective measures.

A critical component of learning process involves creating realistic risk scenarios by considering system complexity, existing security measures, and the potential adversary position. These factors are essential for assessing the likelihood of achieved results and the corresponding impact on the power grid. The comprehensive approach provided by the CPS testbed allows for a deeper understanding of vulnerabilities within smart grid systems and facilitates the development of targeted solutions to enhance both security and resilience.

5. Implementing Micro Grid Control and Converter Dominated Systems

Increasing penetration of RES has driven the transformation into converter-dominated systems and smart microgrids. From a control perspective, developing scalable and robust control schemes are imperative to ensure stability in a continuously expanding grid. Consequently, distributed cooperative controllers have emerged as a promising secondary control strategy, enabling microgrids to maintain stability and scalability, while ensuring voltage regulation and proportional power sharing. Specifically, in [14, 15], a nonlinear distributed control framework is introduced for multi-agent DC microgrids (MGs), offering sufficient scalable stability guarantees. This framework incorporates digital communication links to achieve coordinated control, ensuring steady-state convergence with guaranteed voltage containment and proportional power sharing.

In recent years, these communication-based control strategies have transitioned from centralized to distributed cooperative configurations, bringing notable advantages such as enhanced scalability, reliability, flexibility, and operational efficiency [16]. Despite these benefits, a critical issue remains: their susceptibility to cyber threats that can compromise data integrity, sensor measurements, and control commands [17]. Adversarial actors aim to disrupt normal grid operations, posing risks of destabilization or even complete system failure, underscoring the need to strengthen the privacy, security, and resilience of DC MGs against potential cyber-attacks [18]. Given that MGs are integral to mission-critical applications, including military installations, hospitals, vehicles, spacecraft, and data centres there is a pressing demand for resilient control strategies capable of safeguarding these essential systems from adversarial threats [19-21].

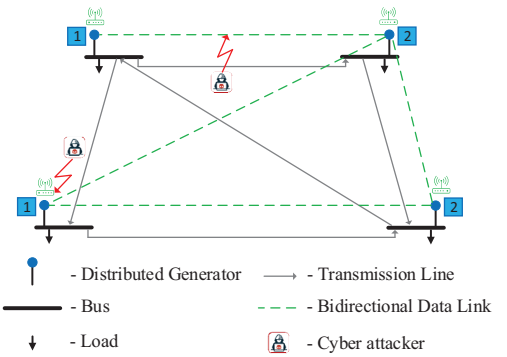

Fig. 5. Cyber-physical microgrid schematic

Figure 5. illustrates a simplified model of a cyber-physical microgrid with distributed, communication-based control, depicting how a potential attacker could infiltrate the system via communication links.

In the literature, *resilient control systems* are defined as an integrated framework that combines detection and mitigation strategies to comprehensively protect microgrids from cyber-attacks. Among the most utilized detection methods are observer-based techniques, commonly used to identify false data injection attacks (FDIA), and event-triggering approaches used for Denial-of-Service attacks. Once cyber-attacks are detected and the compromised units are identified, various event-driven approaches are typically applied to swiftly mitigate their impact.

One of the biggest concerns with these strategies is latency, as delays in detection and response can increase cyber security risks and impact the stability and performance of the MGs. Additionally, many existing methods rely on restrictive assumptions about the number of compromised units and require detailed knowledge of the nature or location of the attacks. These approaches also tend to impose a high computational burden for effective detection and mitigation. Given these challenges, integrating a cyber-attack resilience layer into the control framework becomes crucial for maintaining stability and reliable operation under adversarial conditions. Resilient controllers enhance robustness by ensuring that the system continues to function within acceptable limits, even in the presence of disturbances such as cyber-attacks. Specifically, resilient controllers are designed to minimize the *impact* of such attacks, enabling effective mitigation without requiring precise information about the number of compromised units or the immediate detection of the threat [17].

Despite their potential, most current resilient control strategies rely on *linear* controllers. For instance, references [16, 18, 22] employ small-signal stability analysis to establish *input-to-state stability* and derive carefully selected *design criteria* under which the system states remain uniformly bounded, guaranteeing asymptotic stability. These criteria are embedded into the resilient control design to ensure that, with sufficiently large control gains, the system asymptotically converges to an optimal steady state, achieving the desired control objectives despite cyber-attacks.

In reality, however, converters are often characterized by nonlinear dynamics. In addition, nonlinear controllers may provide more promising functionalities in terms of stability and performance; e.g., voltage containment as opposed to average voltage regulation [23]. Therefore, implementing resilient control in realistic nonlinear systems is essential, particularly as the demand for scalable solutions with large-signal stability guarantees continues to grow. Preliminary results in [24] leverage Lyapunov theory in a large-signal stability analysis of a linear DC MG, demonstrating ISS and deriving optimal design criteria for control gains to achieve resilient operations. Although this was applied to a linear system, applying this nonlinear theory may serve as a foundation for further studies. Employing nonlinear controllers, as in [14, 15], reconfigured according to the privacy-preserving resilient control design in [18], combined with potentially nonlinear observers for attack detection and fault differentiation, presents a promising approach to optimizing nonlinear secondary controllers for robustness against unknown bounded cyber-attacks.

6. Conclusions

Addressing power system sustainability and resilience, the overall goal is always to increase the critical infrastructure resilience and security of supply. It is important to provide a range set of tools and trainings to help energy companies address cyber-security issues.

Strong cyber-defence measures are required along with sophisticated strategies in the energy domain, where emerging solutions should guarantee cyber-security and resilience. By conducting relevant research, including previous lessons learned, researchers contribute to minimising the risk to society of being left without electricity.

When organizing personnel training, conducting research and developing scenarios, it is important to consider cyber-security risks to the power grid, considering a mix of different technologies such as hydropower, coal, nuclear, natural gas, hydrogen, solar and wind.

Protection of renewable energy integration from the risks of cyber-attacks and testing the resilience of the network(s) should also be included in the scope of the research addressing sustainability of the Smart Grids.

References

[1] C. European Union Agency for, ENISA Threat Landscape 2024, European Union Agency for Cybersecurity, 2024.

[2] C. European, Digitalising the energy system - EU action plan, European Commission, Brussels, 2022.

[3] E. Entso, "First Network Code on Cybersecurity for the electricity sector published today," 2024.

[4] M. Allen, "Guardians of the grid – protecting Europe's electricity supply from cyber-attacks," Horizon Magazine, 2024.

[5] A. International Energy, "Cybersecurity: Is the power system lagging behind?," 2020/02/14, 2020.

[6] I. Oleinikova, A. Iliceto, and E. Hillberg, Flexibility for Resilience: How can flexibility support power grids resilience?, 2022.

[7] T. Itu, Smart Sustainable Cities: An Analysis of Definitions, International Telecommunication Union — Focus Group on Smart Sustainable Cities, Geneva, Switzerland, 2014.

[8] D. Sieraszewsk, O. K. Olsen, D. Ivanko, I. Oleinikova, and H. Farahmand, "Multi-Period Hybrid AC/DC-OPF Model for Flexibility Market Clearing With Seamless TSO-DSO Coordination," IEEE Access, vol. 11, pp. 40093-40106, 2023.

[9] S. E. Melle, K. Bardal, D. Ivanko, I. Oleinikova, and H. Farahmand, "Framework and model for flexibility exchange between DSO and LECs." pp. 1-6.

[10] B. Elenga Baningobera, I. Oleinikova, K. Ulhen, and B. R. Pokhrel, "Challenges and solutions in low-inertia power systems with high wind penetration," IET Generation, Transmission & Distribution, vol. 18, no. 24, pp. 4221-4244, 2024.

[11] B. R. Pokhrel, I. Oleinikova, S. D'Arco, S. Sanchez, H. K. Hoidalen, A. Zeno, and K. O. Uhlen, "Advanced digital lab infrastructure for the development of smart power grid," in Proceedings of the 2024 UPEC Conference, Cardiff, Wales, U.K., 2024.

[12] D. Mishchenko, I. Oleinikova, L. Erdődi, and B. R. Pokhrel, "Multidomain Cyber-Physical Testbed for Power System Vulnerability Assessment," IEEE Access, 2024.

[13] D. Mishchenko, I. Oleinikova, L. Erdődi, and B. R. Pokhrel, "The Impact of Stealthy Data Integrity Attacks on Wide-Area Monitoring System Applications." pp. 1-5.

[14] C. Skaga, B. Abdolmaleki, and G. Bergna-Diaz, "Stability of a distributed controller for optimal current sharing and voltage containment in dc microgrids." pp. 356-361.

[15] C. Skaga, and G. Bergna-Diaz, "A Distributed Control Framework with Scalable Stability Guarantees for DC Current Sharing under Voltage Limits." pp. 1-6.

[16] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "Stability-oriented design of cyberattack-resilient controllers for cooperative DC microgrids," IEEE Transactions on Power Electronics, vol. 37, no. 2, pp. 1310-1321, 2021.

[17] M. S. Sadabadi, S. Sahoo, and F. Blaabjerg, "Resilient distributed control strategies in microgrids against cyber attacks," 2022.

[18] M. S. Sadabadi, "A resilient-by-design distributed control framework for cyber-physical DC microgrids," IEEE Transactions on Control Systems Technology, 2023.

[19] S. Sahoo, T. Dragičević, and F. Blaabjerg, "An event-driven resilient control strategy for DC microgrids," IEEE Transactions on Power Electronics, vol. 35, no. 12, pp. 13714-13724, 2020.

[20] S. Sahoo, T. Dragičević, and F. Blaabjerg, "Multilayer resilience paradigm against cyber attacks in DC microgrids," IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2522-2532, 2020.

[21] C. Papadimitriou, E. Zountouridou, and N. Hatziargyriou, "Review of hierarchical control in DC microgrids," Electric Power Systems Research, vol. 122, pp. 159-167, 2015.

[22] M. S. Sadabadi, M. W. S. Atman, A. Aynala, and A. Gusrialdi, "Resilient Design of Leader-Follower Consensus Against Cyber-Attacks," IEEE Transactions on Control of Network Systems, 2023.

[23] B. Abdolmaleki, and G. Bergna-Diaz, "A Nonlinear Control Framework for Optimal Load-Sharing and Voltage Containment in DC Networks," IEEE Transactions on Power Systems, vol. 38, no. 1, pp. 976-979, 2022.

[24] C. Skaga, and G. Bergna-Diaz, "Cyber-Attack Resilient DC Microgrids Under Distributed Control: An Energy Perspective." pp. 3319-3324.