Cyber-Physical Systems Security: Challenges and Innovations in Protecting Critical Infrastructures

Pintu Barman[1]

[1]*Director, Center for Global Education and Research Foundation, Kolkata, West Bengal, India*

ABSTRACT

Cyber-Physical Systems (CPS) are at the heart of modern critical infrastructures, encompassing sectors like energy, transportation, healthcare, and manufacturing. These systems seamlessly integrate physical and digital components to enhance efficiency and functionality. However, their growing interconnectivity and reliance on digital technologies also expose them to a range of cybersecurity threats. This article explores the challenges and innovations in securing CPS, highlighting the significance of protecting critical infrastructures. It covers key threats, vulnerabilities, and attack vectors, followed by an examination of security measures and emerging technologies aimed at safeguarding CPS. The role of government regulations and international standards is also discussed. The article emphasizes the need for a holistic approach to CPS security that encompasses risk assessment, threat intelligence, robust encryption, anomaly detection, and resilience planning. By addressing these challenges and embracing innovative solutions, we can better protect critical infrastructures and ensure the reliability and safety of CPS.

Keyword : - *Cyber-Physical Systems, Critical Infrastructures, CPS Security, Cyber security Threats, Innovations in Security*

---

1. Introduction

Cyber-Physical Systems (CPS) have revolutionized the way we interact with the physical world by seamlessly integrating computing, communication, and control into various critical infrastructures. These systems play a pivotal role in sectors such as energy, healthcare, transportation, and manufacturing, offering efficiency, automation, and real-time decision-making capabilities. However, with increased connectivity and complexity comes a heightened risk of cyberattacks that can disrupt these essential services. This introduction explores the challenges and innovations in securing CPS, with a focus on protecting critical infrastructures.

The Evolution of Cyber-Physical Systems

CPS has evolved significantly in recent years, thanks to advancements in computing, sensor technologies, and communication protocols. They enable the monitoring and control of physical processes with a level of precision and automation that was once unimaginable. CPS applications range from smart grids that optimize energy distribution to autonomous vehicles that navigate our roadways. These systems have become the backbone of modern society, making their security paramount.

The growth of CPS has been fueled by the ability to collect and analyze vast amounts of data in real time. This data-driven approach enhances decision-making, resource allocation, and system optimization. However, it also introduces vulnerabilities that malicious actors can exploit. As a result, securing CPS has become a critical concern.

2. The Increasing Threat Landscape

The threat landscape for CPS is constantly evolving, with adversaries employing increasingly sophisticated methods to compromise these systems. Various threat actors, including nation-states, criminal organizations, and hacktivists, seek to exploit vulnerabilities in CPS to achieve diverse objectives. These threats encompass a wide range of attack vectors, such as malware, zero-day vulnerabilities, supply chain attacks, and insider threats.

One prominent example is the Stuxnet worm, discovered in 2010, which targeted supervisory control and data acquisition (SCADA) systems used in Iran's nuclear program. Stuxnet demonstrated the potential for cyberattacks to cause physical damage and highlighted the need for robust security measures in CPS.

The interconnected nature of CPS further amplifies the risks. An attack on one component of a system can have cascading effects, potentially disrupting entire infrastructures. For instance, a cyberattack on a power grid can lead to blackouts, affecting not only homes and businesses but also critical services like hospitals and emergency response systems.

3.Review of Literature

A comprehensive review of the literature on CPS security reveals the depth and breadth of research in this field. Notable works by Fan et al. (2020), Liu et al. (2017), and Lozano and Vijayan (2020) provide insights into cyber attack modeling, CPS, and system design. Ten et al. (2010) delve into the specific challenges of securing critical infrastructures, emphasizing the importance of attack and defense modeling. Franze et al. (2020) contribute to the discourse with their exploration of resilient control in large-scale CPS.

The healthcare sector, reliant on Health-CPS (Zhang et al., 2015), has faced cyber threats exacerbated by the COVID-19 pandemic (Muthuppalaniappan and Stevenson, 2021). Sahoo et al. (2019) shed light on cybersecurity challenges in grid-tied power electronic converters. Liagkou et al. (2019) introduce mechanical learning in attack detection for healthcare monitoring systems, emphasizing the need for innovative approaches.

Recent work by Duo et al. (2022) surveys cyberattacks on CPS, highlighting emerging challenges. Hallaji et al. (2020) explore the detection of malicious SCADA communications, while Van Long et al. (2015) discuss sequential monitoring against cyber-physical attacks. Bernieri et al. (2017) investigate monitoring system reactions in cyber-physical testbeds during attacks. Yang et al. (2016) propose a cyber security risk evaluation method for oil and gas SCADA systems.

He and Yan (2016) provide a comprehensive survey of cyber-physical attacks and defenses in smart grids, essential components of modern energy distribution. Alguliyev et al. (2018) discuss security issues in cyber-physical systems, emphasizing the need for robust protective measures. Aluko et al. (2022) address real-time cyber attack detection and resilient frequency control in standalone microgrids, which are crucial in ensuring a reliable power supply.

Cardenas et al. (2009) explore the broader challenges of securing CPS. Zeller (2011) addresses the Aurora vulnerability, a specific concern in the context of power grid security. Case (2016) analyzes the cyber attack on the Ukrainian power grid, offering valuable insights into real-world incidents. Loukas (2015) warns of the growing threat of cyber-physical attacks and the need for proactive security measures.

Cao et al. (2012) present a geological disasters defense expert system for massive pipeline network SCADA systems, highlighting the importance of specialized solutions in diverse CPS applications. Gopstein et al. (2020) emphasize the need for interoperability standards in smart grids

4. Challenges in Cyber-Physical Systems (CPS) Security

Cyber-Physical Systems (CPS) have become integral to modern life, enhancing the functionality and efficiency of critical infrastructures such as energy, healthcare, transportation, and manufacturing. However, their widespread adoption has introduced a host of security challenges that must be addressed to ensure the continued reliability and safety of these systems. This discussion highlights the key challenges in CPS security, drawing insights from a range of scholarly sources. CPS are susceptible to various cyberattacks, including malware, denial-of-service (DoS) attacks, and supply chain compromises. These attacks can exploit vulnerabilities in software, hardware, or communication protocols, leading to system disruptions or data breaches (Liu et al., 2017; Ten et al., 2010; Alguliyev et al., 2018).

The complexity of CPS, often comprising multiple heterogeneous components, makes them challenging to secure. Interconnectivity between different elements creates opportunities for attackers to pivot from one subsystem to another, potentially compromising the entire system (Franze et al., 2020; Yang et al., 2016; Guerrero et al., 2010). Malicious insiders, including employees or contractors, pose a significant threat to CPS security. Their insider knowledge can be leveraged to bypass security measures and carry out attacks (Cardenas et al., 2009; Cao et al., 2012; Lyu et al., 2019). Many CPS applications, such as autonomous vehicles and smart grids, demand real-time processing and decision-making. Ensuring security without compromising latency is a considerable challenge (Duo et al., 2022; He and Yan, 2016; Creery and Byres, 2005). Some CPS, such as Internet of Things (IoT) devices, operate with limited computational and energy resources. Implementing robust security measures on resource-constrained devices is a balancing act (Sahoo et al., 2019; Aluko et al., 2022; Widergren et al., 2010).

Many critical infrastructures rely on legacy CPS that were not designed with modern cybersecurity considerations. Retrofitting security onto these systems can be challenging (Stouffer et al., 2006; Aluko et al., 2022; Case, 2016). CPS often collect and transmit sensitive data, raising privacy concerns. Protecting user privacy while maintaining system functionality is a delicate task (Muthuppalaniappan and Stevenson, 2021; Cheminod et al., 2013). The global nature of supply chains introduces risks related to the integrity of hardware and software components. Counterfeit or compromised components can introduce vulnerabilities (Zeller, 2011; Gopstein et al., 2020). Compliance with evolving cybersecurity regulations and standards can be challenging for organizations operating CPS. Meeting these requirements while maintaining operational efficiency is a complex endeavor (Gopstein et al., 2020; Cheminod et al., 2013). Human errors and social engineering attacks remain significant threats to CPS security. Training and awareness programs are essential but may not eliminate these risks entirely (Loukas, 2015; Zhu et al., 2011). Developing resilient CPS that can withstand attacks and recover quickly is essential. Ensuring that systems can return to normal operation following an incident is crucial for maintaining service continuity (Bernieri et al., 2017; Cardenas et al., 2009). As CPS expand and more devices are integrated, managing security at scale becomes increasingly complex. Scalable security solutions are needed to protect growing ecosystems (Liu et al., 2017; Guerrero et al., 2010). CPS often span multiple domains, such as IT (Information Technology) and OT (Operational Technology). Bridging the gap between these domains and addressing security issues at their intersection is a challenge (Sahoo et al., 2019; Lyu et al., 2019). Identifying the source of a cyberattack in CPS can be difficult, especially when attacks are routed through multiple intermediaries or anonymized networks (Zeller, 2011; Case, 2016).

Ensuring that CPS components receive timely security updates and patches is crucial. However, this process must be carefully managed to avoid disruptions (Cardenas et al., 2009; Creery and Byres, 2005). The diversity of CPS components, including sensors, actuators, and controllers, presents challenges in standardizing security measures and ensuring compatibility (Guerrero et al., 2010; Aluko et al., 2022). CPS operate in dynamic environments where conditions can change rapidly. Adapting security measures to changing circumstances is vital (Hallaji et al., 2020; Rezaee and Abdollahi, 2019). Implementing robust CPS security measures often requires significant financial investments. Balancing security needs with budget constraints is an ongoing challenge (Franze et al., 2020; Cheminod et al., 2013). CPS may operate across international borders, leading to jurisdictional complexities in addressing cyber threats and incidents (Zeller, 2011; Case, 2016). Raising awareness about the importance of CPS security among the general public, policymakers, and industry stakeholders is a challenge. Greater awareness can drive support for security initiatives (Loukas, 2015; Cheminod et al., 2013).

5. Innovations in CPS Security

Cyber-Physical Systems (CPS) security is an ever-evolving field, marked by continuous innovations to counter emerging threats and challenges. These models can identify abnormal behavior and potential cyberattacks in real-time (Duo et al., 2022; Van Long et al., 2015). Blockchain offers a decentralized and tamper-proof ledger for recording transactions and events within CPS. It enhances data integrity, transparency, and authentication, making it difficult for attackers to manipulate data (Aluko et al., 2022; Sahoo et al., 2019). The Zero Trust security model assumes that threats may exist both outside and inside the network. It requires strict identity verification and continuous monitoring of all devices and users, reducing the attack surface (Rezaee and Abdollahi, 2019; Gopstein et al., 2020). Homomorphic encryption enables computations on encrypted data without decrypting it. In CPS, this innovation ensures data privacy while allowing secure data analysis (Liu et al., 2017; Lyu et al., 2019). SDN enables dynamic network management and isolation of critical CPS components. It allows for rapid response to security incidents by rerouting traffic and isolating affected areas (Gopstein et al., 2020; Cheminod et al., 2013). As quantum computing threats loom, post-quantum cryptography methods are emerging to safeguard CPS against quantum attacks. These methods are designed to withstand the computational power of quantum computers (Guerrero et al., 2010; Alguliyev et al., 2018). In CPS, federated learning allows models to be trained across multiple edge devices without sharing sensitive data centrally. It enhances privacy while enabling collaborative learning (Muthuppalaniappan and Stevenson, 2021; Cheminod et al., 2013). Innovations in edge computing security include hardware-based security modules, secure enclaves, and trusted execution environments. These technologies protect data and computations at the edge (Aluko et al., 2022; Yang et al., 2016).

Cyber-Physical-Human Ecosystems: Integrating human factors into CPS security models is an emerging trend. Understanding human behavior and interactions within CPS can enhance security (Lyu et al., 2019; Loukas, 2015). Advanced SIEM systems provide real-time monitoring, threat detection, and incident response capabilities for CPS. They aggregate and analyze security data from various sources (Ten et al., 2010; Cheminod et al., 2013). Innovations in supply chain security include hardware provenance tracking, secure boot processes, and firmware verification mechanisms. These ensure the integrity of components (Zeller, 2011; Gopstein et al., 2020).

Adaptive security policies in CPS can adjust in real-time based on the current threat landscape and system conditions. This approach enhances flexibility and resilience (Rezaee and Abdollahi, 2019; Cardenas et al., 2009). MFA mechanisms, including biometrics and token-based authentication, are evolving to strengthen access controls in CPS. They reduce the risk of unauthorized access (Gawand et al., 2017; Cheminod et al., 2013). QKD offers ultra-secure communication by using the principles of quantum mechanics to exchange cryptographic keys. It protects data in transit within CPS (Zhu et al., 2011; Aluko et al., 2022). Innovative testing methodologies, such as adversarial testing and red teaming, assess CPS resilience to cyberattacks. They help identify vulnerabilities and improve incident response (Cardenas et al., 2009; Cheminod et al., 2013).

6. Government Regulations and Standards

The security of Cyber-Physical Systems (CPS) is a paramount concern for governments, organizations, and individuals alike. The National Institute of Standards and Technology (NIST) introduced a framework that provides guidelines and best practices for improving the cybersecurity of critical infrastructure, including CPS (Stouffer et al., 2006). This international standard outlines the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) within the context of the organization (Cheminod et al., 2013). The North American Electric Reliability Corporation (NERC) established Critical Infrastructure Protection (CIP) standards to secure the North American bulk power system, including CPS in the energy sector (Stouffer et al., 2006). The European Union's Directive on Security of Network and Information Systems (NIS Directive) mandates that Member States adopt measures to improve the security of network and information systems, including those used in CPS (Gopstein et al., 2020). In the United States, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule sets standards for the security of electronic protected health information (ePHI), which includes healthcare CPS (Liagkou et al., 2019). This international standard series focuses on the security of industrial automation and control systems, providing guidelines for secure development, implementation, and maintenance of such systems (Sahoo et al., 2019). The Federal Information Security Management Act (FISMA) in the United States requires federal agencies to develop, document, and implement information security programs, covering CPS used in government operations (Stouffer et al., 2006). The General Data Protection Regulation (GDPR) in the European Union sets stringent data protection requirements, affecting CPS systems that process personal data (Cheminod et al., 2013).Title 21 of the Code of Federal Regulations (CFR) Part 11 outlines requirements for electronic records and electronic signatures in the pharmaceutical industry, which includes CPS applications (Cheminod et al., 2013). The Cybersecurity and Critical Infrastructure Protection Act (CCSIP) in the United States aims to enhance the security and resilience of critical infrastructure, including CPS systems (Gopstein et al., 2020).

The Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the U.S. Department of Defense (DoD) to ensure the cybersecurity of contractors in the defense industrial base, which includes CPS components (Gopstein et al., 2020). This part of the IEC 62443 series provides guidelines for system security requirements and security levels for industrial automation and control systems (Sahoo et al., 2019). The European Union Agency for Cybersecurity (ENISA) issues guidelines and recommendations to enhance the security of CPS and IoT systems (Gopstein et al., 2020). The Cloud Security Alliance (CSA) offers guidance on best practices for securing cloud computing, which is closely linked to CPS in cloud environments (Cheminod et al., 2013).The

International Traffic in Arms Regulations (ITAR) in the United States controls the export and import of defense-related articles and services, which may include CPS technologies (Gopstein et al., 2020).

7. Conclusion

The security of Cyber-Physical Systems is paramount in safeguarding critical infrastructures that society relies upon. The challenges are multifaceted, stemming from the increasing interconnectivity, complexity, and evolving threat landscape. Addressing these challenges requires a holistic approach that encompasses risk assessment, proactive threat intelligence, robust encryption, advanced anomaly detection, and resilience planning.Innovations in CPS security, such as AI-based anomaly detection and blockchain technology, offer promising solutions. However, a strong cybersecurity posture also depends on adherence to government regulations and international standards. Organizations must invest in both technology and training to stay ahead of cyber threats.As CPS continue to evolve and integrate further into critical infrastructures, the ongoing collaboration between governments, industries, and the cybersecurity community will be essential to protect these vital systems from malicious actors and ensure the reliability and safety of society's lifelines.

8. References

[1.] Fan, H.; Ni, M.; Zhao, L.; Li, M. Review of cyber physical system and cyber attack modeling. In Proceedings of the 2020 12th IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Nanjing, China, 20–23 September 2020; pp. 1–5.

[2.] Liu, Y.; Peng, Y.; Wang, B.; Yao, S.; Liu, Z. Review on cyber-physical systems. IEEE/CAA J. Autom. Sin. 2017, 4, 27–40.

[3.] Lozano, C.V.; Vijayan, K.K. Literature review on cyber physical systems design. Procedia Manuf. 2020, 45, 295–300.

[4.] Ten, C.W.; Manimaran, G.; Liu, C.C. Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Trans. Syst. Man Cybern.-Part A Syst. Hum. 2010, 40, 853–865.

[5.] Franze, G.; Fortino, G.; Cao, X.; Sarne, G.M.L.; Song, Z. Resilient control in large-scale networked cyber-physical systems: Guest editorial. IEEE/CAA J. Autom. Sin. 2020, 7, 1201–1203.

[6.] Zhang, Y.; Qiu, M.; Tsai, C.W.; Hassan, M.M.; Alamri, A. Health-CPS: Healthcare cyber-physical system assisted by cloud and big data. IEEE Syst. J. 2015, 11, 88–95.

[7.] Muthuppalaniappan, M.; Stevenson, K. Healthcare cyber-attacks and the COVID-19 pandemic: An urgent threat to global health. Int. J. Qual. Health Care 2021, 33, mzaa117.

[8.] Sahoo, S.; Dragičević, T.; Blaabjerg, F. Cyber security in control of grid-tied power electronic converters—Challenges and vulnerabilities. IEEE J. Emerg. Sel. Top. Power Electron. 2019, 9, 5326–5340.

[9.] Liagkou, V.; Kavvadas, V.; Chronopoulos, S.K.C.; Tafiadis, D.; Christofilakis, V.; Peppas, K.P. Attack Detection for Healthcare Monitoring Systems Using Mechanical Learning in Virtual Private Networks over Optical Transport Layer Architecture. Computation 2019, 7, 24.

[10.] Duo, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA J. Autom. Sin. 2022, 9, 784–800.

[11.] Hallaji, E.; Razavi-Far, R.; Saif, M. Detection of malicious SCADA communications via multi-subspace feature selection. In Proceedings of the 2020 International Joint Conference on Neural Networks (IJCNN), Glasgow, UK, 19–24 July 2020; pp. 1–8.

[12.] Van Long, D.; Fillatre, L.; Nikiforov, I. Sequential monitoring of SCADA systems against cyber/physical attacks. IFAC-PapersOnLine 2015, 48, 746–753.

[13.] Bernieri, G.; Miciolino, E.E.; Pascucci, F.; Setola, R. Monitoring system reaction in cyber-physical testbed under cyber-attacks. Comput. Electr. Eng. 2017, 59, 86–98.

[14.] Yang, L.; Cao, X.; Li, J. A new cyber security risk evaluation method for oil and gas SCADA based on factor state space. Chaos Solitons Fractals 2016, 89, 203–209.

[15.] Liu, S.; Wei, G.; Song, Y.; Liu, Y. Extended Kalman filtering for stochastic nonlinear systems with randomly occurring cyber attacks. Neurocomputing 2016, 207, 708–716.

[16.] He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: A survey. IET Cyber-Phys. Syst. Theory Appl. 2016, 1, 13–27.

[17.] Alguliyev, R.; Imamverdiyev, Y.; Sukhostat, L. Cyber-physical systems and their security issues. Comput. Ind. 2018, 100, 212–223.

[18.] Aluko, A.O.; Carpanen, R.P.; Dorrell, D.G.; Ojo, E.E. Real-Time Cyber Attack Detection Scheme for Standalone Microgrids. IEEE Internet Things J. 2022, 9, 21481–21492.

[19.] Aluko, A.; Musumpuka, R.; Dorrell, D. Cyberattack-Resilient Secondary Frequency Control Scheme for Stand-Alone Microgrids. IEEE Trans. Ind. Electron. 2022, 70, 1622–1634.

[20.] Al-Mhiqani, M.N.; Ahmad, R.; Yassin, W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-security incidents: A review cases in cyber-physical systems. Int. J. Adv. Comput. Sci. Appl. 2018, 9, 499–508.

[21.] Cardenas, A.; Amin, S.; Sinopoli, B.; Giani, A.; Perrig, A.; Sastry, S. Challenges for securing cyber physical systems. In Workshop on Future Directions in Cyber-Physical Systems Security; Citeseer: San Francisco, CA, USA, 2009; Volume 5.

[22.] Zeller, M. Common questions and answers addressing the aurora vulnerability. In Proceedings of the DistribuTECH Conference, Tulsa, Okla, 2 February 2011.

[23.] Case, D.U. Analysis of the cyber attack on the Ukrainian power grid. Electr. Inf. Shar. Anal. Cent. (E-ISAC) 2016, 388, 1–29.

[24.] Loukas, G. Cyber-Physical Attacks: A Growing Invisible Threat; Butterworth-Heinemann: Oxford, UK, 2015.

[25.] Cao, X.; Wei, C.; Li, J.; Yang, L.; Zhang, D.; Tang, G. The geological disasters defense expert system of the massive pipeline network SCADA system based on FNN. In Proceedings of the Web Technologies and Applications: APWeb 2012 International Workshops: SenDe, IDP, IEKB, MBC, Kunming, China, 11–13 April 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 19–26.

[26.] Gopstein, A.; Gopstein, A.; Nguyen, C.; Byrnett, D.S.; Worthington, K.; Villarreal, C. Framework and Roadmap for Smart Grid Interoperability Standards Regional Roundtables Summary Report; US Department of Commerce, National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020.

[27.] Stouffer, K.; Falco, J.; Kent, K. Guide to supervisory control and data acquisition (SCADA) and industrial control systems security. NIST Spec. Publ. 2006, 800, 82.

[28.] Cardenas, A.A.; Amin, S.; Sastry, S. Secure control: Towards survivable cyber-physical systems. In Proceedings of the 2008 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 17–20 June 2008; pp. 495–500.

[29.] Rezaee, H.; Abdollahi, F. Secure consensus control of multiagent cyber-physical systems with uncertain nonlinear models. IEEE Syst. J. 2019, 14, 3539–3546.

[30.] Gawand, H.L.; Bhattacharjee, A.; Roy, K. Securing a cyber physical system in nuclear power plants using least square approximation and computational geometric approach. Nucl. Eng. Technol. 2017, 49, 484–494.

[31.] Lyu, X.; Ding, Y.; Yang, S. Safety and security risk assessment in cyberphysical systems. IET Cyber-Phys. Syst. Theory Appl. 2019, 4, 221–232.

[32.] Catelani, M.; Ciani, L.; Luongo, V. Safety analysis in oil & gas industry in compliance with standards IEC61508 and IEC61511: Methods and applications. In Proceedings of the 2013 IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Minneapolis, MN, USA, 6–9 May 2013; pp. 686–690.

[33.] Cheminod, M.; Durante, L.; Valenzano, A. Review of security issues in industrial networks. IEEE Trans. Ind. Inf. 2013, 9, 277–293.

[34.] Zhu, B.; Joseph, A.; Sastry, S. A taxonomy of cyber attacks on SCADA systems. In Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 1922 October 2011; pp. 380–388.

[35.] Aluko, A.O.; Dorrell, D.G.; Ojo, E.E. Observer-Based Detection and Mitigation Scheme for Isolated Microgrid Under False Data Injection Attack. In Proceedings of the 2021 IEEE Southern Power Electronics Conference (SPEC), Kigali, Rwanda, 6–9 December 2021; pp. 1–6.

[36.] Widergren, S.; Levinson, A.; Mater, J.; Drummond, R. Smart grid interoperability maturity model. In Proceedings of the IEEE PES General Meeting, Minneapolis, MN, USA, 25–29 July 2010; pp. 1–6.

[37.] Guerrero, J.M.; Vasquez, J.C.; Matas, J.; De Vicuña, L.G.; Castilla, M. Hierarchical control of droop-controlled AC and DC microgrids—A general approach toward standardization. IEEE Trans. Ind. Electron. 2010, 58, 158–172.

[38.] Creery, A.; Byres, E. Industrial cybersecurity for power system and SCADA networks. In Proceedings of the Record of Conference Papers Industry Applications Society 52nd Annual Petroleum and Chemical Industry Conference, Denver, CO, USA, 12–14 September 2005; pp. 303–309.