University of Kalisz

Kalisz, 23–24.10.2025

Innovations and Industrial Technologies 2025

Cybersecurity of Control Systems in Transformer Stations of the Polish Energy Group, Mining and Conventional Energy, Bełchatów Power Plant Branch

Jacek Klatka

Kalisz University, Faculty of Social Sciences, Institute of Security and Defense – PhD student

ABSTRACT

The aim of the paper is to provide a synthetic assessment of the maturity and development directions of cybersecurity for control systems in transformer stations of the Polish Energy Group, Mining and Conventional Energy, Bełchatów Power Plant Branch, in both normative and research perspectives. The OT infrastructure in the power industry is characterized by high functional safety requirements, which determine the specificity of protective measures compared to IT. The reference framework includes NIST guidelines for OT and the sector-specific ISO/IEC 27019 standard, which adjusts the selection of controls for process environments. The architecture and protective mechanisms of communication in substations (IEC 61850/MMS, GOOSE, SV) are defined by the IEC 62351 standards, while the security capability requirements of IED devices are specified in IEEE 1686. The literature indicates that vulnerabilities in the cyber-physical chain may result in the loss of controllability of power supply systems and disturbances in grid operation. Real-world incidents in the power sector, including attacks on distribution systems in Ukraine, emphasize the importance of operational resilience and recovery procedures. Research on IEC 61850 security reveals GOOSE/SV vulnerabilities to spoofing and timing manipulation and proposes countermeasures such as R-GOOSE, NSM monitoring in accordance with IEC 62351-7, and anomaly detection using ML methods. For environments with critical availability, the recommended measures include substation-process segmentation, identity and key management, IED/RTU hardening, as well as penetration testing and security validation based on cyber-physical risk models. The proposed program for transformer stations of the Bełchatów Power Plant integrates: a) zone and conduit architecture, b) a cryptographic policy compliant with IEC 62351, c) NSM security telemetry, d) scenarios for restoring substation functions after an incident.Such an approach strengthens compliance with best practices (NIST/IEC/ISO) and measurably enhances resilience against attack scenarios at the protocol and device layers.

OBJECTIVES

To assess the maturity of cybersecurity systems applied in transformer stations of the Polish Energy Group, with particular emphasis on the Bełchatów Power Plant Branch. To identify key vulnerabilities and threats in communication between control devices (GOOSE, SV, MMS) and within the cyber-physical chain of OT infrastructure. To analyze the compliance of existing solutions with industry standards and guidelines, including IEC 62351, IEEE 1686, ISO/IEC 27019, and NIST, and to determine their impact on the level of operational security. To develop a model of an integrated cybersecurity program for transformer stations, encompassing OT zone segmentation, a cryptographic policy, NSM security telemetry, and recovery procedures. To evaluate the impact of the proposed program on the resilience of control systems against contemporary cyber threats and its significance for advancing cybersecurity maturity in the power industry.

CONCLUSIONS

The analysis has shown that effective cybersecurity of control systems in transformer stations requires an integrated approach based on industry standards (IEC 62351, IEEE 1686, ISO/IEC 27019) and NIST guidelines for OT systems. The maturity of security measures in the power sector depends on their implementation and continuous improvement. The main challenges concern vulnerabilities in communication (GOOSE, SV, MMS) and threats within the cyber-physical chain, which may lead to loss of controllability and disruptions in grid operation. Experiences, including attacks on distribution systems in Ukraine, confirm the need to strengthen operational resilience and enhance security monitoring. At the Bełchatów Power Plant, a protection program has been proposed based on: segmentation of OT zones and conduits, an IEC 62351-compliant cryptographic policy, NSM security telemetry, recovery procedures following an incident. This model increases compliance with NIST/IEC/ISO best practices, strengthens resilience against attacks at the protocol and device layers, and brings the power infrastructure closer to achieving full cybersecurity maturity.

REFERENCES

[1] K. Stouffer, V. Pillitteri, et al., Guide to Operational Technology (OT) Security, NIST Special Publication 800-82 Rev.3, Gaithersburg, 2023.[2] ISO/IEC 27019:2017, Information technology — Security techniques — Information security controls for the energy industry, Geneva, 2017.[3] F. Cleveland, IEC TC57 WG15: IEC 62351 Security Standards for the Power System Information Infrastructure, White Paper, 2010.[4] IEEE Std 1686-2013, IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities, New York, 2014.[5] S. Sridhar, A. Hahn, M. Govindarasu, “Cyber–Physical System Security for the Electric Power Grid,” Proceedings of the IEEE, 100(1), 2012, pp. 210–224.[6] W. Knowles, D. Prince, D. Hutchison, J. Disso, K. Jones, “A Survey of Cyber Security Management in Industrial Control Systems,” International Journal of Critical Infrastructure Protection, 9, 2015, pp. 52–80.[7] A. Humayed, J. Lin, F. Li, B. Luo, “Cyber-Physical Systems Security—A Survey,” IEEE Internet of Things Journal, 4(6), 2017, pp. 1802–1831.[8] E-ISAC, SANS, Analysis of the Cyber Attack on the Ukrainian Power Grid, 2016.[9] A. Aydeger et al., “Vulnerability and Impact Analysis of the IEC 61850 GOOSE Protocol in the Smart Grid,” Sensors, 21(4), 2021, art. 1554.[10] H. Bindra et al., “A Novel Hybrid Methodology to Secure GOOSE Messages…,” Scientific Reports, 12, 2022, art. 22434.[11] E. O. Schweitzer III et al., “IEC 61850 Network Cybersecurity: Mitigating GOOSE Message Threats,” SEL Technical Paper, 2019.[12] T. Koh et al., “A Flexible OT Testbed for Evaluating On-Device Implementations of Cybersecurity Mechanisms,” International Journal of Critical Infrastructure Protection, 2023.[13] C. Vellaithurai, S. Biswas, A. Srivastava, S. Zonouz, “CPINDEX: Cyber-Physical Vulnerability Assessment for Power-Grid Control Networks,” 2014.[14] M. Ndiaye et al., “Implementing Secure Routable GOOSE and SV Messages Based on IEC 61850-90-5,” IEEE Access, 2020.[15] L. Yang et al., “A New Methodology for Anomaly Detection of Attacks in IEC 61850 Substations,” Sustainable Energy, Grids and Networks, 31, 2022.[16] C. Robillard, J. Bélanger, “Network and System Management Using IEC 62351-7 in a Digital Substation,” 2018.[17] R. Zhu et al., “Cyber System Recovery for IEC 61850 Substations,” 2021.[18] S. M. Hussain, S. Taha, “A Review of IEC 62351 Security Mechanisms for IEC 61850 Message Exchanges,” 2019.[19] C.-W. Ten, C.-C. Liu, G. Manimaran, “Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees,” IEEE PES General Meeting, 2007.[20] Q. Su et al., “Vulnerability Analysis of Cyber–Physical Power Systems Based on Failure Propagation Probability,” International Journal of Electrical Power & Energy Systems, 158, 2024.[21] A. F. Taha et al., “GOOSE Secure: A Comprehensive Dataset for In-Depth Analysis of GOOSE Spoofing Attacks,” Energies, 17(23), 2024, art. 6098.[22] J. T. Moyne, E. A. White, “Security Evaluation of IEC 62351,” 2016.

ACKNOWLEDGEMENTS

The author wishes to thank the Bełchatów Power Plant for providing technical data and assistance.

CONTACT

Contact: phone +48 504 217 244,
e-mail: jacekklatka@interia.pl

University of Kalisz

The project is co-financed from the state budget,

allocated by the Minister of Science under „Doskonała Nauka II” programme.

Ministerstwo Nauki i Szkolnictwa Wyższego