Mérnöki Szimpózium a Bánkiban
(ESB 2025)

Feasibility of Digital Substations (Problem Statement)

[1]Máté Mórocz

[1]*Obuda University, Doctoral School on Safety and Security Sciences, Budapest, Hungary, morocz.mate@stud.uni-obuda.hu*

Abstract

The digitalization of power systems is fundamentally transforming substation operation and introducing new technical, regulatory, and safety challenges. Digital substations rely on optical communication, intelligent devices, and automated control, which can enhance reliability but remain sensitive to external disturbances. Ensuring the reliability of high-voltage optical measurement devices and the varying national implementations of the IEC 61850 standard create significant interoperability issues. This research applies HAZOP, FMEA, and risk-matrix methods to analyze the risks and safety aspects of digital substations. Its goal is to identify key obstacles in system integration, regulation, and occupational safety, and to support the secure and standardized digitalization of high-voltage secondary systems.

Keywords: digital substation, IEC 61850, high voltage, IED, interoperability

1 Introduction

The modernization processes of electric power supply systems are becoming increasingly visible worldwide, driven by changing consumer demands, the integration of renewables, and the growing expectation for grid flexibility [1]. A central element of this digitalization is the digital substation, which relies on network communication, data modeling, and the interaction of standardized devices instead of analog signals. The underlying IEC 61850 standard for digital substations provides a unified model and communication environment that theoretically allows for full interoperability [2]. However, numerous challenges arise during practical implementation, manifesting in the areas of technological maturity, real-time operation, cybersecurity, and organizational resistance [3].

2 Technological Feasibility Issues

The technological feasibility of digital substations is fundamentally determined by three main areas: interoperability challenges related to the interpretation of the IEC 61850 standard, the requirements for real-time network communication, and issues associated with the accuracy of time synchronization.

2.1 Interoperability

In terms of interoperability, the objective of the IEC 61850 standard is to ensure unified data modeling and communication; however, implementation differences between manufacturers remain significant. Practical experience shows that certain parts of the standard can be interpreted in multiple ways, leading to variations in the structure of Logical Nodes (LNs), the level of service support, or the handling of GOOSE/Sampled Values messages. This is confirmed by numerous case

studies and experimental systems: although conformance tests have evolved, they still do not cover all practical interoperability issues, particularly concerning the validation of complex SCL (Substation Configuration Language) files and the configuration alignment between different devices [4]. Another source of problems is that the evolution of the standard and manufacturer implementations do not always progress at the same pace: some devices are built on standard editions that are several years older, resulting in further integration difficulties [2]. All of this means that interoperability is not guaranteed by default, but rather requires dedicated project activities, manufacturer-independent testing environments, and validation procedures.

2.2 Requirements for Real-Time Network Communication

Questions of network architecture design and the feasibility of time-critical communication are likewise decisive for the overall performance of digital substations. Because many system functions—particularly protection functions—require deterministic communication, minimizing latency, jitter, and packet loss is critical. According to IEC 61850 requirements, GOOSE messages must reach their destination with less than 3 ms of end-to-end delay, even under faulty network conditions [3]. In practice, this can only be ensured through well-engineered architectures that typically rely on one of two main redundancy models: the Parallel Redundancy Protocol (PRP) or High-availability Seamless Redundancy (HSR). Although these protocols provide a high degree of availability, they also significantly increase network topology complexity, may result in 1.5–2× traffic growth, and require specialized diagnostic tools [5]. Load fluctuations, configuration errors, or improper QoS settings can easily lead to latency spikes that disrupt the operation of protection functions [6]. Moreover, the requirement for deterministic communication implies that conventional IP-based network hardware is not always suitable: several studies have shown that standard switches' internal scheduling and buffering algorithms do not guarantee priority handling or time-critical processing of protection messages [7]. Thus, the network infrastructure of digital substations is not merely a communication medium but an integral component of the protection system itself.

2.3 Time synchronization

Time synchronization is likewise a critical factor in assessing feasibility. The operation of measurement modules generating Sampled Values messages and of protection devices depends on a strict time base, typically provided by the IEEE 1588v2 (PTP) protocol. Achieving sub-microsecond accuracy, however, is non-trivial: fluctuations in network delay, insufficient PTP support in switches, or the loss of the Grandmaster Clock can lead to severe operational faults [8]. Research further indicates that the PTP protocol is highly vulnerable from a cybersecurity perspective: time-manipulation attacks — such as Delay Attacks or Spoofing — may lead to incorrect protection logic behavior, erroneous timestamps, or even complete system failure [9]. Adequate time-source redundancy, correct configuration of PTP profiles, and a time-synchronization strategy aligned with the network architecture are therefore essential elements of digital substation implementation. Moreover, inaccuracies in time synchronization affect not only protection but also the validity of measurement data, event reconstruction, and disturbance analysis—ultimately complicating operational optimization and fault diagnosis in the long term.

3 Cybersecurity Feasibility Considerations

3.1 Emerging Substation Threats

One of the most critical aspects of cybersecurity feasibility in digital substations is that, with the introduction of Ethernet-based communication and remote management functions, systems that were previously physically segregated and relied on analog signaling now exhibit a significantly

expanded attack surface. Manipulation of GOOSE and Sampled Values messages is particularly dangerous, as these carry the critical information required for protection logic operation. GOOSE spoofing, for example, enables an attacker to inject fraudulent protection commands or status indications, thereby disrupting protection functions and potentially triggering false trips. Because the GOOSE protocol is multicast-based and early versions of the standard did not include built-in authentication mechanisms, such attacks are technically feasible once an attacker obtains physical or logical access to the network [10]. Time-synchronization attacks pose a similarly severe threat: IEC 61850 Sampled Values messages and network event reconstruction rely on highly accurate timestamps, meaning that compromising the PTP (IEEE 1588) protocol—through delay manipulation or spoofing of Sync messages—can lead to a complete collapse of protection functionality, as measurement data become unintelligible under an incorrect time base [9]. Denial-of-Service (DoS) attacks impact the system by overloading the communication infrastructure: targeted traffic amplification can incapacitate network switches, resulting in delayed or lost protection messages and thereby directly jeopardizing system stability [5]. Firmware- and configuration-manipulation attacks are enabled by the complex embedded architectures of modern substation IEDs. A compromised firmware may remain undetected for extended periods while containing hidden functions, altered protection logic, or backdoors [11]. This makes firmware a particularly attractive target for attackers, as modifications at this level are difficult to detect even when other parts of the system employ robust security measures.

3.2 Cryptography

Protection-oriented communication—particularly GOOSE and Sampled Values—imposes real-time requirements, which severely constrain the applicability of security mechanisms. Digital signatures or encryption introduce processing delays that may jeopardize the guaranteed reaction times of protection functions. Ahmed and Baig (2019) demonstrated that even with optimized cryptographic algorithms, a non-negligible processing overhead is introduced, which in extreme cases may exceed the latency bounds permitted by IEC 61850 [12]. This implies that full encryption of real-time messages is currently not feasible without operational consequences. In practice, this has led to the adoption of hybrid models: the most critical messages are authenticated but not encrypted, whereas stronger cryptographic protection is applied to non-time-critical data exchanges. Researchers also emphasize that future post-quantum security requirements may further complicate system design, as quantum-resistant algorithms typically incur substantially higher computational costs [13].

3.3 Cybersecurity Frameworks and Regulatory Gaps

Cybersecurity frameworks and the associated regulatory landscape constitute another area where substantial gaps remain. Although the NERC CIP standards in North America and the ENTSO-E and IEC guidelines in Europe define baseline cybersecurity requirements for energy infrastructures, these regulations were primarily designed for general Industrial Control Systems (ICS) environments and do not fully cover the specific operational characteristics of digital substations. Knowles et al. (2015) highlighted that cybersecurity regulation for critical infrastructures in many countries is predominantly reactive—typically updated only in response to technological advancements or major cyber incidents [14]. Such an approach does not keep pace with the rapid technological innovations emerging from the deployment of IEC 61850. Moreover, the IEC 62351 standard series—intended to enhance the security of power system communications—cannot yet be considered fully mature or widely adopted across all domains. As a result, operators often must rely on internal guidelines, security policies, and bespoke solutions, leading to heterogeneous security levels across countries and organizations.

3.4 Training and Competency Gaps

The deployment of digital substations involves not only technological challenges but also significant organizational and human factors. In modern IEC 61850-based substation environments, operational and engineering competencies are shifting toward domains that require substantial knowledge expansion in information technology, industrial networking, cybersecurity, and software-driven configuration processes. Traditional protection engineers previously focused primarily on analog signals, physical wiring, and deterministic, hardware-based protection logic; in contrast, digital substations place emphasis on configuring IEDs, modeling logical relationships in SCL files, and understanding the operation of Ethernet networks. Research indicates that the industry faces a substantial skills gap, as the intersection of IT and power engineering constitutes a relatively new and not yet fully institutionalized knowledge domain [16]. Professionals must be familiar with communication protocols such as GOOSE and Sampled Values, understand switch QoS configurations, and apply core cybersecurity principles, including network segmentation, message authentication, and access-control mechanisms. In the absence of these competencies, the risk of configuration errors, flawed escalation processes, and cybersecurity incidents increases, collectively jeopardizing the operational reliability of digital substations.

These training gaps are further exacerbated by the fact that digital technologies evolve more rapidly than educational systems can adapt. Electrical engineering curricula worldwide continue to focus primarily on classical protection principles, while software-based configuration, network diagnostics, and cybersecurity receive only limited attention. As a result, newly graduated engineers often lack the skill set required to operate digital substations. Singh et al. [16] pointed out that more than 60% of engineers involved in substation operations would require formal training in IEC 61850 data modeling, network troubleshooting, and cybersecurity incident handling; however, the available training programs do not cover these topics with sufficient depth.

3.5 Organizational and Change Management

Organizational and change-management factors are equally decisive for the feasibility of digital substations. Digitalization is not merely a technological upgrade but requires the transformation of an entire organizational operating model. During the transition period, most companies must operate traditional and digital substations in parallel, resulting in substantial complexity across maintenance processes, troubleshooting workflows, and responsibility structures. Such heterogeneous technological environments frequently lead to the formation of competence silos: some teams are familiar only with legacy technologies, while others specialize in digital solutions, creating communication and coordination challenges. Cultural resistance can be particularly strong in organizations where traditional protection systems have functioned reliably and predictably for decades, and where engineers' professional identities are closely tied to those established operational paradigms. Hevner (2019) notes that the organizational introduction of technological innovation typically unfolds across three cycles—understanding, adaptation, and stabilization—and that most failures stem from organizations underestimating the time required for learning and transition [15]. In many cases, it is not the technology but the organization's operational processes that become the bottleneck: inadequate documentation, unclear responsibility assignments, outdated maintenance practices, and weak cybersecurity culture are all factors that may slow down or even jeopardize the digital transition.

Organizational maturity is another crucial factor that substantially determines whether a company can effectively implement and operate digital substation technologies. Mature organizations possess formalized processes such as incident-handling procedures, change-management protocols, configuration-management practices, and continuous auditing mechanisms. In their absence, the operation of digital substations may experience increased error rates, and overall

system resilience may be significantly reduced. Research indicates that most energy utilities remain in the early stages of digitalization, and in many cases, organizational structures, job roles, and operational processes are not yet aligned with the requirements of the digital operating model [15]. It can therefore be concluded that the technological feasibility of digital substations is sustainable only if an organization's human capacity, operational culture, and change-management capabilities evolve in parallel with the technology.

4 Conclusion

The feasibility of digital substations is a complex, multidimensional challenge situated at the intersection of technological innovation, cybersecurity threats, and organizational operation. Although the IEC 61850 standard family provides a unified framework for communication and data modeling that can serve as the foundation for future substation automation architectures, practical experience shows that interoperability issues, time-critical network requirements, and uncertainties surrounding time-synchronization accuracy demand substantial engineering effort. The growing number and complexity of cybersecurity threats further reinforce the recognition that protecting digital substations is not merely a technical concern but a strategic imperative—one that encompasses addressing vulnerabilities in real-time communication, ensuring firmware integrity, and continuously evolving the regulatory landscape. In addition, human and organizational factors play a decisive role: training deficiencies, change-management challenges, and operational gaps arising from heterogeneous technological environments can all hinder successful digitalization. The overall conclusion is that the long-term sustainability and security of digital substations can only be achieved if technological advancements are accompanied by increased organizational maturity, continuous development of engineering competencies, and a proactive, standards-based cybersecurity strategy.

5 References

[1] Farhangi, H. (2010). The path of the smart grid. IEEE Power and Energy Magazine, 8(1), 18–28. https://doi.org/10.1109/MPE.2009.934876

[2] Mackiewicz, R. (2006). Overview of IEC 61850 and benefits. Power Systems Conference, 376–383.

[3] Rietveld, G., & van der Meer, A. (2019). Impact of network performance on IEC 61850 Sampled Values. IEEE Transactions on Instrumentation and Measurement

[4] Behara, S., Ten, C.-W., & Manimaran, G. (2021). Interoperability assessment of IEC 61850-based substations. IEEE Transactions on Smart Grid, 12(3), 2418–2428.

[5] Hong, S., Lee, H., & Kim, H. (2018). Performance evaluation of PRP and HSR for mission-critical substation networks. IEEE Transactions on Industrial Informatics, 14(6), 2667–2677.

[6] Hossain, A., & Juris, F. (2020). Challenges in IEC 61850 communication networks for digital substations. International Journal of Electrical Power & Energy Systems, 117, 105646. https://doi.org/10.1016/j.ijepes.2019.105646

[7] Alcaraz, C., Lopez, J., & Wolthusen, S. (2017). Policy-based security for IEC 61850-based smart substations. International Journal of Information Security, 16(4), 419–434.

[8] Kostic, D., Prettico, G., & Lazaro, M. (2020). Achieving interoperability in IEC 61850 multi-vendor substations: A practical evaluation. Energies, 13(14), 3549.

https://doi.org/10.3390/en13143549

[9] Mizrahi, T. (2018). A secure and precise clock synchronization protocol for power systems. IEEE Transactions on Smart Grid, 9(5), 4725–4734.

[10] Jarmakiewicz, M., & Sobieraj, M. (2020). Cybersecurity vulnerabilities of IEC 61850 GOOSE communication in digital substations. Energies, 13(15), 3934. https://doi.org/10.3390/en13153934

[11] Cherepanov, A., & Mamedov, A. (2019). Security risks of firmware compromise in digital substations. International Journal of Critical Infrastructure Protection, 26, 100312. https://doi.org/10.1016/j.ijcip.2019.100312

[12] Ahmed, S., & Baig, Z. (2019). Performance evaluation of security mechanisms for IEC 61850 GOOSE messages. IET Generation, Transmission & Distribution, 13(11), 2112–2120.

[13] Naedele, M., Dzung, D., & Wang, X. (2016). Cryptographic techniques for substation automation security. IEEE Transactions on Industrial Electronics, 63(10), 6555–6565.

[14] Knowles, W., Prince, D., Hutchison, D., Jones, K., & Christianson, B. (2015). A survey of cyber security management in industrial control systems. International Journal of Critical Infrastructure Protection, 9, 52–80. https://doi.org/10.1016/j.ijcip.2015.02.002

[15] Hevner, A. (2019). A three-cycle view of design science research. *Scandinavian Journal of Information Systems, 31*(2), 3–17.

[16] Singh, R., Palensky, P., & van der Meijden, M. (2020). Skill requirements and training challenges for digital substation engineers. *Energies, 13*(5), 1231. https://doi.org/10.3390/en13051231