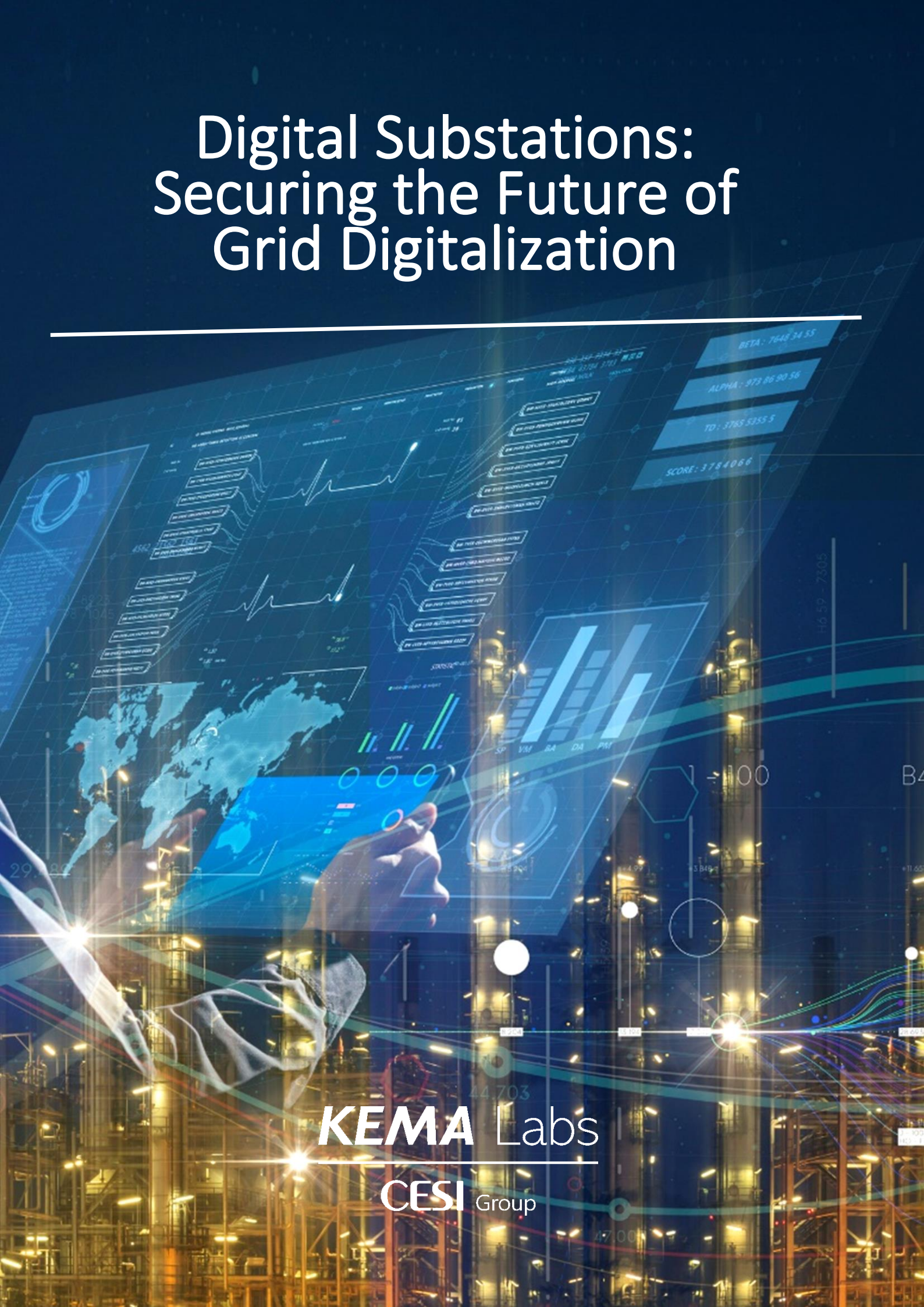
Digital Substations: Securing the Future of Grid Digitalization



KEMA Labs

CESI Group



IEC 61850: The Key Enabler

As the power sector accelerates its digital transformation, utilities and technology providers are increasingly adopting digital substations to improve efficiency, automation and operational visibility. Today, IEC 61850 has become the backbone of modern digital substation architectures, enabling seamless data exchange and interoperability between intelligent electronic devices (IEDs), protection systems and control centres. More than 80% of new substations worldwide are now being built using IEC 61850-compliant systems.

The benefits of this transition are significant. Digital substations enable real-time monitoring, smarter asset management, improved system reliability and more efficient grid operations. Technologies such as IoT, advanced analytics and predictive maintenance are helping utilities optimize performance while supporting the growing integration of renewable energy sources.

However, greater connectivity also brings new challenges. As operational technologies become increasingly interconnected, substations are exposed to a wider range of cybersecurity risks. Network vulnerabilities, unauthorized access, compromised devices, data manipulation and regulatory non-compliance can all threaten the reliability and security of critical infrastructure. Cyberattacks targeting energy systems have increased significantly in recent years, highlighting the need for more robust protection measures across the grid.

To address these challenges, the industry relies on a comprehensive cybersecurity framework. While regulations such as NIS2 define the obligations for operators of critical infrastructure and IEC 62443 establishes cybersecurity requirements for industrial automation systems, IEC 62351 provides a dedicated framework for securing communications within power system environments. It defines how security principles such as authentication, data integrity, confidentiality and access control should be applied to the communication protocols used throughout the energy sector.

IEC 62351 works alongside IEC 61850 rather than replacing it. While IEC 61850 enables interoperability and seamless communication between devices, IEC 62351 provides the security mechanisms needed to protect those communications from cyber threats. Together, the two standards create the foundation for digital substations that are not only efficient and interoperable, but also secure, resilient and compliant with evolving regulatory expectations.



IEC 62351: Securing Digital Substations

By integrating cybersecurity directly into operational communications, IEC 62351 helps utilities and manufacturers address growing concerns around data integrity, system availability and authorized access, ensuring that digitalization does not come at the expense of reliability.

Implementing a cybersecurity framework, however, is only part of the process. Utilities, manufacturers and system integrators must also demonstrate that products and systems meet the required standards and perform consistently in real operating environments. This is particularly important in digital substations, where interoperability between devices from different vendors and the secure exchange of data are critical to reliable operation.

As demand for secure and interoperable solutions continues to grow, conformity assessment has become an essential step in the development and deployment of substation automation systems, including SCADA platforms, RTUs and Intelligent Electronic Devices (IEDs). Independent third-party assessments help verify compliance with recognized standards, provide objective evidence of quality and security, and support confidence among network operators and other stakeholders.

The outcome of this process is a formal attestation of conformity, demonstrating that products and technical systems meet established requirements and contribute to a uniform, consistent and comparable level of quality across the industry.

For equipment manufacturers, implementing IEC 62351 demonstrates cybersecurity readiness and supports market acceptance. Secure products help improve interoperability, facilitate integration into utility environments and provide confidence that systems can operate safely within increasingly demanding regulatory frameworks. For utilities, adopting IEC 62351 contributes to stronger protection of critical assets, improved operational resilience and greater confidence in the long-term reliability of digital infrastructure.

Successfully applying these principles requires more than compliance alone. Cybersecurity must be considered from the earliest stages of product and system development through a security-by-design approach. Risk assessments, independent testing and conformance verification play a crucial role in validating that systems perform as intended and can withstand real-world operational challenges. Industry collaboration among utilities, manufacturers, system integrators and testing laboratories is essential to building a more secure and interoperable energy ecosystem.

As power systems continue their digital evolution, cybersecurity is becoming a fundamental enabler of grid modernization. IEC 62351 provides a practical and internationally recognized framework to secure critical communications, strengthen operational resilience and support regulatory compliance across the energy sector. To fully realize these benefits, organizations must combine robust standards with rigorous validation activities, including cybersecurity assessments, interoperability verification and independent testing. Together, these elements help utilities and manufacturers build trust in the next generation of digital substations and create a more secure, resilient and future-ready grid.