# Using Engineering Access Roles and Credential Management to Secure Critical Infrastructure

David Prestwich
*Schweitzer Engineering Laboratories, Inc.*

Presented at the
9th South East Asia Protection, Automation, and Control Conference
Adelaide, Australia
September 2–4, 2025

# Using Engineering Access Roles and Credential Management to Secure Critical Infrastructure

David Prestwich, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—This paper explores the challenges and successes associated with implementing secure engineering access practices while minimizing disruptions to traditional organizational workflows. Key areas of focus include the rotation of passwords across a fleet of devices, management of access to resources, and addressing industry challenges related to role definitions. This paper also discusses strategies for leveraging existing workflows to handle traditional testing tasks without the need to distribute passwords. It highlights the importance of building comprehensive reports to facilitate audits and provide transparency regarding access at any given time. The findings aim to guide organizations in addressing potential reactions and concerns, ensuring a balanced approach to security and operational efficiency.**

**In conclusion, this paper provides a comprehensive analysis of secure engineering access practices, emphasizing the importance of balancing security measures with operational efficiency. By addressing key challenges and presenting practical solutions, it aims to equip organizations with the tools and strategies necessary to safeguard critical infrastructure while maintaining seamless workflows. Finally, this paper presents actionable information on where the industry is succeeding, as well as trends moving forward to solve the ever-evolving challenges of securing our critical infrastructure. The insights and recommendations offered are intended to foster a proactive approach to security, ensuring that organizations can effectively manage access and credentials in an increasingly complex technological landscape.**

***Keywords*—Engineering access control, Credential management, Operational technology (OT) security, Role-based access control, Critical infrastructure protection, Password vaults and privileged access management (PAM), Workflow integration, Auditability and compliance**

## I. Introduction

Securing critical infrastructure is not a new concept. For decades, the electrical industry has recognized the importance of protecting the systems that underpin our power grids, water supplies, transportation networks, and other essential services. Over the years, organizations have implemented a variety of security measures to safeguard these assets. However, as technology evolves and infrastructure ages, maintaining effective security practices has become increasingly complex.

This complexity is especially evident in the electrical industry, where one of the most pressing challenges is securing aging infrastructure against modern cybersecurity threats. Many critical infrastructure systems were designed and deployed long before today's cybersecurity threats emerged. As a result, these systems often lack the connectivity, processing power, or compatibility needed to support modern security protocols. In some cases, the infrastructure is so outdated that even basic connectivity is limited, making remote access and centralized management difficult. Compounding this issue is a growing shortage of skilled personnel, which places additional strain on organizations trying to maintain secure and efficient operations.

Despite these challenges, network connectivity to field devices has become a necessity. Engineers and technicians rely on remote access to perform diagnostics, apply updates, and manage configurations efficiently. However, this connectivity introduces new attack surfaces that adversaries can exploit. Every connection point becomes a potential vulnerability, especially when devices are not equipped with modern IT security features.

Many of the devices used in critical infrastructure environments do not support advanced authentication technologies such as Lightweight Directory Access Protocol (LDAP), multifactor authentication (MFA), or federated identity management. As a result, managing access credentials—particularly rotating passwords or adjusting access levels—remains a largely manual process. This not only increases the risk of human error but also makes it difficult to enforce consistent security policies across a diverse and distributed device fleet.

## II. Background and Industry Context

The transmission and distribution sectors of the electrical industry face unique cybersecurity challenges due to the nature of their infrastructure and operational requirements. Unlike traditional IT environments, these systems often include legacy devices that were never designed with cybersecurity in mind. As a result, implementing modern security controls, such as centralized identity management or automated credential rotation, can be difficult or even impossible without significant upgrades.

Credential management is a particularly pressing concern. In many utilities, access to field devices is still governed by shared credentials or static passwords that are rarely changed. This practice not only increases the risk of unauthorized access but also complicates auditing and accountability. According to the U.S. Department of Energy (DOE) cybersecurity baselines, utilities must prioritize access control and credential hygiene to protect against both external threats and insider risks [1].

The lack of support for modern authentication protocols in many operational technology (OT) devices further exacerbates the problem. Without integration into enterprise identity systems, utilities are forced to rely on manual processes to manage access—processes that are time-consuming, error-prone, and difficult to scale. As noted in the guidance from the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), these limitations create significant barriers

to implementing effective cybersecurity strategies across the grid [1].

Amid these challenges, the international electrical industry is coalescing around a growing body of recommendations and standards aimed at securing the grid. Coordinated strategies, shared best practices, and proactive credential management are essential to safeguarding the future of critical infrastructure.

## III. Challenges in Implementing Secure Engineering Access

One of the most persistent challenges in securing engineering access is the rotation of passwords across a diverse fleet of field devices. While password rotation is a foundational security practice, its implementation in OT environments is far from straightforward.

A major complication arises from inconsistency in interfaces and capabilities across vendors. Each manufacturer may provide a different method for changing credentials, ranging from web-based interfaces and proprietary software to legacy communication protocols or physical access via a local console. This lack of standardization not only increases the operational burden but also introduces opportunities for error, especially when technicians are unfamiliar with a specific device's interface or limitations.

Further complicating matters is the inconsistent implementation of user access models. Some devices support tiered access levels (e.g., operator, engineer, admin), while others rely on hardcoded user accounts with varying password complexity requirements. These inconsistencies make it difficult to apply uniform credential policies across an organization's infrastructure. In some cases, devices may not support password changes at all or may require a firmware update to enable such functionality—an impractical solution for many field-deployed assets.

Even when devices support secure protocols for credential management, the operational overhead remains high. Managing digital certificates, client application compatibility, and patching requirements adds layers of complexity. These tasks often require coordination across multiple teams and can introduce downtime or service interruptions if not carefully planned.

Adding to the confusion, vendors are continuously evolving their security capabilities. New firmware releases may introduce changes to password complexity rules, deprecate older authentication methods, or address vulnerabilities through security bulletins and common vulnerability disclosures. While these updates are necessary for improving security, they also create uncertainty about what a device currently supports and what changes may be required to maintain compliance.

From an operational standpoint, scheduled password rotations can disrupt critical workflows. If a password is rotated during a maintenance window or outage response, field technicians may find themselves locked out of essential systems, delaying restoration efforts. This risk contributes to a broader reluctance to adopt automated or frequent password rotation policies, especially in high-availability environments where uptime is paramount.

Ultimately, the challenge is not just technical—it is also cultural. Introducing new security controls can interfere with established engineering workflows, leading to resistance from field personnel and operational teams. Without careful planning and cross-functional collaboration, even well-intentioned security measures can become obstacles to productivity.

### *A. Managing Access Without Disrupting Workflows*

Implementing secure access controls in operational environments often introduces friction into well-established engineering workflows. While the intent is to enhance security, the reality is that these changes can slow down or complicate routine tasks, especially in time-sensitive scenarios.

A common example is the industry-wide practice of using known, shared passwords for field devices. This approach, while insecure by modern standards, has historically enabled quick and consistent updates during commissioning or outage response. Technicians could rely on a standard credential to access devices, apply changes, and document configurations without delay or confusion.

However, the rotation of passwords, either manually or through an automated policy, raises several questions:

- How does the field technician now access the device?
- What happens to SCADA systems or other applications that rely on that credential for communications?
- Should the new password be known to the technician, or should it remain hidden and accessed only through secure tools?
- Where is the password stored, and how is it securely retrieved?
- Do audit and reporting systems need to be expanded to track who accessed the password and when?

By leveraging existing workflows, such as the check-in and check-out process commonly used when working with large equipment, organizations can introduce new secure access practices in a familiar context. This approach allows technicians to associate credential management with tasks they already perform. For example, some access control applications now allow technicians to temporarily check out a device to access it without needing to know the actual password. During this period, the system replaces a complex, unknown password with a temporary one that enables the technician to complete their work. Once the task is finished, the technician can check in the device, prompting the system to revert the password back to a complex value. Alternatively, the system can automatically reset the password after a predefined timeout. This method enhances security while minimizing disruption to established workflows.

To address these challenges, many utilities are adopting password vaults or privileged access management (PAM) solutions. These tools securely store credentials, enforce access policies, and provide audit trails of who accessed what and when. Best practices include using long, unique passwords, rotating them regularly, and integrating vaults with identity management systems to streamline access [2].

However, even with these tools, the introduction of new security controls can interfere with established workflows. If vaults are not integrated into field tools or require additional steps to retrieve credentials, technicians may face delays or be tempted to bypass security protocols. This is especially problematic during critical outages when time is of the essence.

To reduce friction, organizations should:

- Design access controls that align with operational realities.
- Provide secure, streamlined methods for credential retrieval.
- Ensure that security tools are intuitive and field-ready.
- Offer training and support to build trust and adoption among engineering teams.

Ultimately, the success of any secure access initiative depends not just on the technology, but on how well it fits into the day-to-day work of those who rely on it.

### *B. Defining and Standardizing Engineering Roles*

A foundational element of secure engineering access is the clear definition and enforcement of user roles. However, in many organizations, especially those managing complex and distributed infrastructure, roles are inconsistently defined, informally assigned, or not mapped to access policies at all. This lack of standardization creates significant challenges for implementing secure, scalable access control.

One of the most common issues is inconsistent role definitions across teams or departments. Titles like “engineer,” “technician,” or “operator” may carry different meanings depending on the business unit or region. Without a shared understanding of what each role entails, it becomes difficult to assign appropriate access privileges. This inconsistency can lead to over-permissioning, where users have more access than necessary, or under-permissioning, which can hinder productivity and lead to workarounds that bypass security controls.

Compounding this issue is the absence of formal role hierarchies or access policies. In many cases, access decisions are made on an ad hoc basis, based on who needs do the work rather than on a structured policy. This approach may work in the short term but becomes unsustainable as organizations grow or face increased regulatory scrutiny.

Another challenge lies in mapping roles to device capabilities. Not all field devices support granular access levels. Some may only differentiate between basic and administrative access, while others may lack any role-based access control features entirely. This makes it difficult to enforce nuanced access policies, especially when trying to align them with organizational roles.

Onboarding and offboarding also become more complex without standardized roles. Provisioning access for new employees often requires manual configuration across multiple systems and devices. Similarly, when an employee leaves or changes roles, ensuring that all access is revoked or updated appropriately can be error-prone and time-consuming, introducing potential security gaps.

To address these issues, organizations must foster cross-functional alignment between engineering, IT, and security teams. Together, they can define roles that are both operationally practical and aligned with security best practices. This includes:

- Creating a standardized role catalog with clearly defined responsibilities and access levels.
- Mapping roles to device capabilities and identifying gaps in enforcement.
- Automating role-based provisioning and deprovisioning through identity and access management (IAM) systems.
- Regularly reviewing and updating roles to reflect changes in organizational structure or technology.

Thanks to new software applications being developed in the industry, organizations now have more tools to bridge the gap between IT and OT environments. These solutions allow for the integration of traditional IT authorization systems, such as Active Directory or LDAP, with secure OT applications. This enables organizations to define roles centrally and apply them consistently across both enterprise and field environments [3] [4].

For example, by aligning engineering access with existing IT-managed roles and responsibilities, utilities can implement a long-term strategy that ensures secure, role-based access to field devices. This approach supports both day-to-day operations and emergency response scenarios, reducing the risk of technicians being locked out during critical tasks. It also simplifies compliance with regulatory requirements by providing clear, auditable mappings of who has access to what and why [3].

### *C. Organizational Resistance and Cultural Barriers*

Even the most well-designed security solutions can fail if they are not embraced by the people who use them. In the context of engineering access, organizational resistance and cultural barriers often present some of the most difficult challenges to overcome. These barriers are not rooted in technology, but in perception, communication, and trust.

One of the most common issues is the perception of security as a productivity blocker. Engineers and field technicians often operate under tight deadlines and high-pressure conditions. When new security controls, such as password vaults, MFA, or session logging, are introduced, they may be seen as obstacles that slow down work rather than tools that protect it. This perception can lead to resistance, workarounds, or even outright non-compliance.

Another challenge is the lack of awareness or understanding of cyber risks. While IT and security teams are typically well-versed in the potential consequences of a breach, field personnel may not fully grasp how poor credential management can lead to system compromise, data loss, or regulatory violations. Without this context, security policies can feel arbitrary or excessive.

Change fatigue is also a significant factor. Many organizations are undergoing digital transformation, adopting new tools and updating procedures at a rapid pace. For teams

already stretched thin, the introduction of yet another system or policy can feel overwhelming. This fatigue can lead to disengagement or passive resistance, especially if the changes are not clearly communicated or supported [5].

A deeper issue lies in the trust and communication gaps between IT or security and engineering teams. When security solutions are developed in isolation, without input from the people who will use them, they often fail to account for real-world workflows and constraints. This misalignment can result in tools that are technically sound but operationally impractical.

To overcome these barriers, organizations must adopt strategies that empower end users and foster collaboration:

- Engage stakeholders early: Involve engineering and field teams in the design and evaluation of security solutions. Their insights can help shape tools that are both secure and usable.
- Provide targeted training: Educate users not just on how to use new tools but why they matter. Real-world examples of cyber incidents can help build understanding and buy-in.
- Empower users through workflow integration: Rather than forcing users to adapt to security tools, adapt the tools to fit existing workflows. This reduces friction and increases adoption.

Fortunately, a new generation of security strategies is emerging, designed not only to enhance protection but also to integrate seamlessly into existing engineering workflows. Empowering users to be part of the solution—not just the subjects of new policies—builds trust, improves adoption, and ultimately strengthens an organization's security posture.

### *D. Reporting and Auditability*

In any secure engineering access strategy, visibility is just as important as control. Without clear, reliable audit trails, organizations cannot verify compliance, investigate incidents, or continuously improve their security posture. Reporting and auditability are foundational to accountability, transparency, and operational resilience.

At its core, auditability ensures that every access event (who accessed what, when, from where, and what actions were taken) is captured and reviewable. This is essential not only for regulatory compliance but also for internal governance and incident response. In the event of a security breach or operational failure, audit logs provide the forensic data needed to perform root cause analysis and determine whether access policies were followed or circumvented.

However, building comprehensive audit trails in operational environments is not always straightforward. Many legacy devices lack native logging capabilities or use proprietary formats that are difficult to integrate with modern systems. Additionally, fragmented access methods, such as local console access, web interfaces, or vendor-specific tools, can result in inconsistent or incomplete logging.

To address these challenges, organizations are increasingly adopting centralized logging and reporting solutions. Technologies like Syslog are commonly used to collect logs from a wide range of devices and applications. These logs can then be processed by Security Information and Event Manager (SIEM) platforms or integrated with modern HTTPS-based application programming interfaces to feed data into enterprise analytics tools, such as Microsoft Power BI. This allows security and operations teams to visualize access patterns, detect anomalies, and generate compliance reports with minimal manual effort.

Beyond compliance, audit data can be used to drive operational improvements. For example, password rotation is often treated as a set-and-forget process. But in reality, rotating credentials, especially on field devices, requires careful coordination. Some devices may only support password changes during specific maintenance windows or require batch operations to avoid service disruptions. By generating reports that highlight upcoming risks or expiring credentials, organizations can proactively schedule work orders and assign tasks to the appropriate teams. This ensures that security actions are aligned with operational readiness.

As systems mature, these reports can be integrated into traditional workflows, such as outage planning, commissioning, or routine maintenance. When users see that security-related tasks are embedded into their existing processes, and that these changes are designed to support, not hinder, their work, they are more likely to adopt and support them. Over time, this integration helps shift the perception of security from a compliance burden to a shared responsibility that benefits the entire utility.

In summary, effective reporting and auditability:

- Provide transparency and accountability for all access events.
- Support compliance with internal and external standards.
- Enable root cause analysis and incident response.
- Inform proactive planning and task scheduling.
- Build trust by aligning security with operational workflows.

By investing in robust logging infrastructure and integrating audit data into everyday tools and processes, organizations can create a security culture that is both data-driven and user-aligned.

### *E. Industry Trends and Future Outlook*

As the cybersecurity landscape continues to evolve, utilities and critical infrastructure operators are adopting new technologies and strategies to secure engineering access while maintaining operational efficiency. The following trends highlight where the industry is heading and where opportunities for improvement remain.

#### *1) Emerging Technologies in Access Management*

One of the most significant shifts in access management is the adoption of jump host technologies deployed on virtual machines. These systems act as secure intermediaries between users and field devices, enforcing centralized authentication, session logging, and role-based access control. By funneling all access through a controlled environment, organizations can reduce the attack surface and gain greater visibility into user activity.

In parallel, web-based access platforms are replacing traditional thick-client applications. These modern interfaces eliminate the need to manage a fleet of field laptops and reduce the complexity of software updates. Web portals also support integration with identity providers, enabling seamless single sign-on and MFA across both IT and OT environments.

*2) Trends in Securing OT Environments*

Securing OT environments remains a top priority, especially as legacy systems are increasingly connected to enterprise networks. Key trends include:

- Zero-trust architecture (ZTA): OT networks are adopting ZTA principles, in which no user or device is inherently trusted. Access is granted based on continuous verification of identity, context, and device posture.
- PAM: Utilities are investing in PAM solutions tailored for OT, enabling secure credential storage, automated password rotation, and session recording.
- Microsegmentation: Network segmentation strategies are being refined to isolate critical assets and limit lateral movement in the event of a breach.

These approaches are helping utilities reduce risk while enabling secure remote operations—a necessity in today's distributed workforce.

## *F. Recommendations and Best Practices*

Securing engineering access in critical infrastructure environments requires more than just technical controls—it demands a holistic approach that balances security, usability, and organizational alignment. This section synthesizes the challenges discussed earlier and offers actionable guidance for organizations seeking to implement or enhance secure access strategies.

*1) Summary of Key Challenges*

Organizations face a range of obstacles when managing engineering access, including:

- Inconsistent password management across diverse device fleets, often due to vendor-specific limitations or lack of automation [1].
- Workflow disruption caused by security controls that are not aligned with operational realities, leading to resistance or workarounds [6].
- Unclear or inconsistent role definitions, which make it difficult to enforce access policies or scale security practices [4].
- Cultural resistance from engineering teams and technicians who may view security as a barrier to productivity rather than a shared responsibility [3].

*2) Actionable Strategies*

To address these challenges, organizations can adopt the following practical steps:

- Define standardized engineering roles with clearly mapped access privileges, supported by a centralized role catalog [4].
- Implement password vaults and PAM tools to securely store and rotate credentials [1].
- Automate provisioning and deprovisioning through IAM systems to reduce manual errors and improve auditability [3].
- Integrate audit tools, such as SIEM platforms and centralized logging, to provide visibility into access events and support compliance [7].

*3) Balancing Security and Operations*

Security initiatives must be designed with operational workflows in mind. This means:

- Ensuring that credential retrieval and access tools are intuitive and field-ready [3].
- Avoiding unnecessary friction that could lead to non-compliance or delays during critical operations [6].
- Embedding security tasks into existing processes, such as maintenance planning or outage response, to promote adoption [8].

*4) Building a Long-Term Roadmap*

A sustainable access strategy should be:

- Scalable: to accommodate organizational growth and evolving infrastructure [9].
- Adaptable: to support new technologies, regulatory changes, and emerging threats [7].
- Resilient: with contingency plans for emergency access and remote operations [6].

Organizations should regularly review and update their access policies, role definitions, and credential management practices to ensure continued effectiveness [1].

When designing scalable and adaptable access strategies, organizations should consider aligning their architecture with the Purdue Reference Model. This model provides a structured approach to segmenting industrial networks into hierarchical levels: from enterprise IT systems, Level 5, down to field devices, Level 0. By mapping access controls and role responsibilities to these levels, organizations can better enforce security boundaries, reduce lateral movement, and ensure that access policies are contextually appropriate for each layer of the infrastructure [10].

*5) Fostering a Security-First Culture*

Technology alone cannot solve access challenges. Success depends on:

- Cross-functional collaboration: between IT, security, and engineering teams [6].
- User empowerment: by involving field personnel in the design and rollout of security tools [3].
- Ongoing education and communication: to build awareness of cyber risks and the importance of secure practices [9].

By fostering a culture where security is seen as an enabler, not an obstacle, organizations can build trust, improve adoption, and strengthen their overall security posture.

*6) Building Strong IT Partnerships*

A critical enabler of successful implementation is a strong working relationship between engineering teams and IT departments. Many of the changes required to secure infrastructure, such as deploying new access tools, updating

firewall rules, or ensuring reliable network connectivity, depend on IT support and coordination. Challenges like slow connectivity, inconsistent uptime, and restrictive firewall configurations can delay or derail implementation efforts if not addressed collaboratively [6].

By fostering open communication and mutual understanding, engineering and IT teams can troubleshoot issues more effectively, streamline rollout processes, and even uncover opportunities for productivity gains. As both groups learn more about each other's systems and workflows, they can align their efforts to support shared goals—ultimately improving both security and operational efficiency [3].

*7) Staying Grounded in First Principles*

Organizations embarking on the journey to secure engineering access must be careful not to overcomplicate the process. While the challenges are real and the stakes are high, the path forward does not require perfection, it only requires progress. Security should be approached with a mindset rooted in first principles: protect what matters most, apply defense in depth, and build systems that are resilient, not just compliant [1].

In large, distributed environments, especially those that blend legacy and modern infrastructure, there will be exceptions. Not every device will support the latest protocols. Not every workflow will be easily automated. And not every policy will apply cleanly across all systems. That is okay.

The goal is not to solve everything at once, but to make steady, strategic improvements. Start with the most critical systems. Apply layered defenses. Use tools that enhance visibility and control. And most importantly, build a culture of collaboration where security is a shared responsibility, not a siloed function [6].

By taking a measured, principle-driven approach, organizations can make meaningful progress by improving security without sacrificing operational effectiveness and lay the foundation for a more secure, adaptable future.

## IV. Conclusion

Securing engineering access in critical infrastructure environments is a multifaceted challenge that demands both technical innovation and organizational alignment. This paper has explored the complexities of credential management, the importance of role standardization, and the cultural and operational barriers that often hinder the adoption of secure practices. It has also highlighted practical strategies, such as the use of password vaults, role-based access control, and audit-ready reporting systems, that help utilities strengthen their security posture without disrupting essential workflows.

A key insight is that successful security implementations are not solely about deploying new tools: they are about integrating those tools into the day-to-day realities of engineering teams. By aligning security controls with existing workflows, involving end users in the design process, and fostering collaboration between IT and OT teams, organizations can reduce resistance and improve adoption.

Looking ahead, the industry is making promising strides. The adoption of centralized jump host platforms, web-based access interfaces, and zero-trust principles reflects a growing maturity in how utilities approach access control. However, challenges remain, particularly around legacy systems, such as inconsistent role definitions and the need for scalable, adaptable solutions.

To foster a proactive and secure engineering environment, organizations must continue to invest in technologies that enhance visibility and control, while also cultivating a culture where security is seen as a shared responsibility. This means empowering users, building strong cross-functional partnerships, and staying grounded in first principles: protect what matters most, apply defense in depth, and prioritize resilience over perfection.

By taking a thoughtful, collaborative approach, utilities can not only meet today’s cybersecurity demands but also build a foundation for long-term operational and security success.

## V. References


[1] U.S. Department of Energy, “Cybersecurity Baselines for Electric Distribution Systems and DER,” 2025. Available: energy.gov/sites/default/files/2025-01/Cybersecurity%20Baselines%20for%20Electric%20Distribution%20System%20Interim%20Implementation%20Guidance.pdf.

[2] MAC Automation Inc., “SCADA Security Best Practices: How to Protect Your SCADA System,” 2025. Available: macautoinc.com/insights/scada-security-best-practices/.

[3] U.S. Department of Energy, “Operational Technology Cybersecurity for Energy Systems,” Federal Energy Management Program. Available: energy.gov/femp/operational-technology-cybersecurity-energy-systems.

[4] R. Chandramouli, D. Ferraoilo, and D. Kuhn, Role-Based Access Control, Second Edition, Artech House, 2007. Available: csrc.nist.gov/pubs/book/2007/01/rolebased-access-control/final.

[5] Safe Work Australia, “Guide for Managing the Risk of Fatigue at Work,” 2013. Available: https://www.safeworkaustralia.gov.au/system/files/documents/1702/managing-the-risk-of-fatigue.pdf.

[6] CESER, “Protecting Energy Infrastructure: CESER, Partners Publish Cybersecurity Guidance to Mitigate Cyber-Attacks,” 2025. Available: energy.gov/ceser/articles/protecting-energy-infrastructure-ceser-partners-publish-cybersecurity-guidance.

[7] ENISA, “Energy,” Cybersecurity of Critical Sectors. Available: enisa.europa.eu/topics/cybersecurity-of-critical-sectors/energy.

[8] D. Kilman and J. Stamp, “Framework for SCADA Security Policy,” 2005. Available: energy.gov/sites/prod/files/Framework%20for%20SCADA%20Security%20Policy.pdf.

[9] European Commission, “Critical Infrastructure and Cybersecurity,” Energy. Available: energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en.

[10] ISA, “ISA-95 Series of Standards: Enterprise-Control System Integration.” Available: isa.org/standards-and-publications/isa-standards/isa-95-standard.


Previously presented at the 9th South East Asia Protection, Automation and Control Conference (SEAPAC 25), Adelaide, Australia, September 2025.