

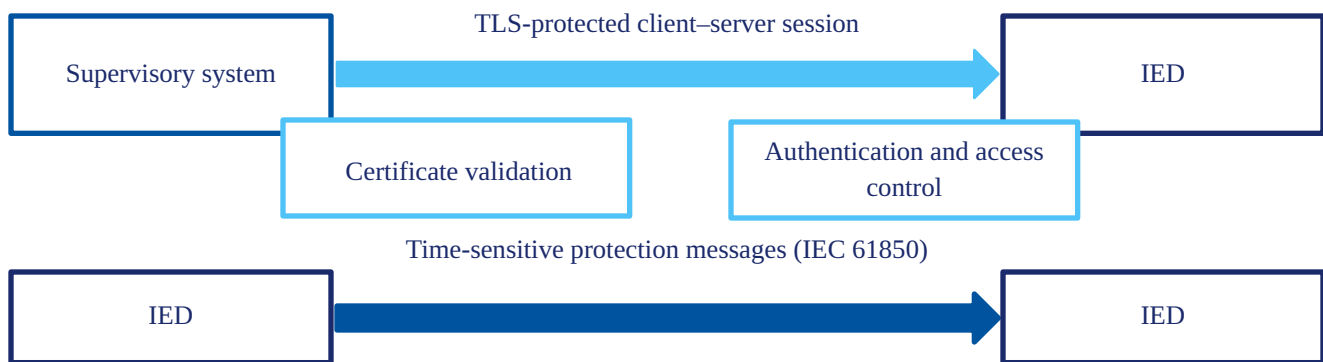
When Cybersecurity Becomes an Operational Challenge: Securing IEC 61850-Based Substations

Cybersecurity Awareness Month | Technical Perspectives on Power System Security

Author: Kiran TS

Designation: Lead Research Engineer

Organization: PGCOE



Conceptual illustration, not part of the author's technical claims. Security mechanisms such as certificate validation and authentication sit on the communication paths between a supervisory system and an IED, alongside time-sensitive protection messages. No measurements, test setup or real equipment.

The Security–Reliability Question

In conventional IT environments, cybersecurity is often discussed in terms of preventing unauthorized access, protecting information and detecting attacks. However, in electric power systems, cybersecurity has an additional responsibility: ensuring that security mechanisms do not unintentionally compromise the operational functions they are intended to protect.

Consider a digital substation in which intelligent electronic devices (IEDs) exchange information using IEC 61850 communication protocols. Some messages support monitoring and supervisory control, while others are involved in time-sensitive protection and automation functions.

Introducing cybersecurity mechanisms into these communication paths raises an important engineering question:

Can a system remain secure without compromising the timely, dependable and predictable operation of its critical functions?

The answer cannot be established through cryptographic strength or protocol compliance alone. It also requires understanding how security controls behave under normal operating conditions, communication disturbances, configuration errors and equipment failures.

Research into the practical implementation of IEC 62351 security mechanisms in IEC 61850 environments has examined these challenges, highlighting the importance of considering operational behavior alongside communication security [1].

Security Changes the Behavior of Communication Systems

IEC 62351 provides security mechanisms applicable to power system communications, including TLS-based protection, message authentication, access control and key management [2]–[4].

These mechanisms strengthen security properties, but their deployment introduces additional operational dependencies.

For example, enabling TLS for client–server communication requires compatible protocol configurations, trusted credentials and certificate validation. A certificate-related failure may prevent a communication session from being established even when the underlying network is functioning correctly.



Similarly, protecting time-sensitive messages introduces considerations related to authentication processing, message acceptance and rejection, and security association management.

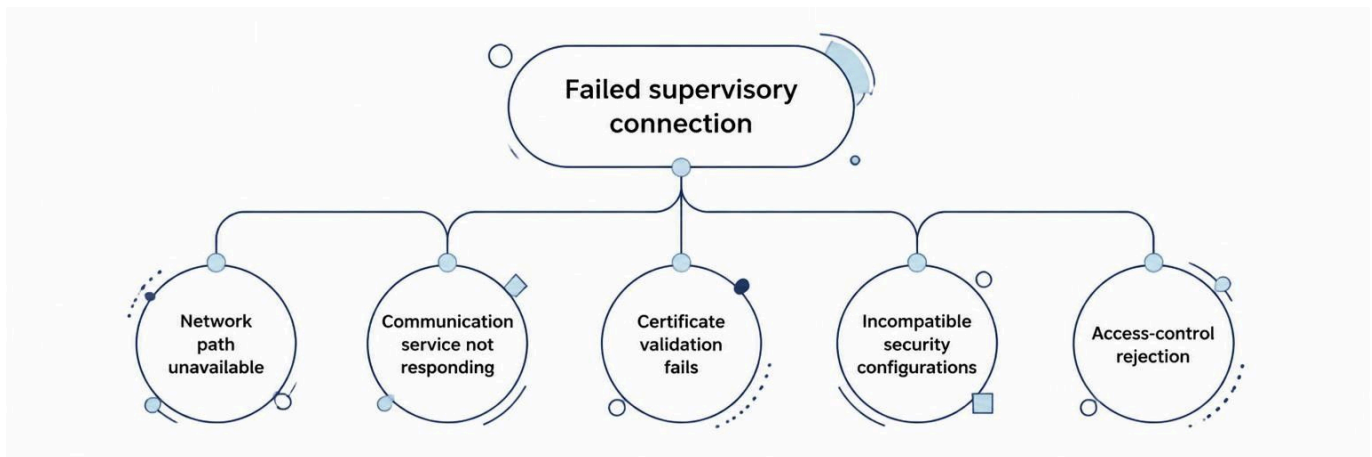
Such behavior is not necessarily a weakness in the security mechanism. Rejecting unauthorized or invalid communication may be exactly what the mechanism is designed to do. The operational challenge is ensuring that the system responds safely and predictably when such rejection occurs.

When a Security Failure Looks Like a Network Failure

Consider a hypothetical situation in which a supervisory system cannot establish communication with an IED.

The apparent symptom may resemble an ordinary network connectivity problem. However, several underlying conditions are possible:

- The network path is unavailable.
- The communication service is not responding.
- Certificate validation fails.
- The devices have incompatible security configurations.
- Access-control policies reject the requested operation.



Conceptual illustrations. No measurements, test setup or real equipment.

These conditions can produce similar symptoms while requiring fundamentally different corrective actions.

Without appropriate diagnostic information, engineers may spend considerable time investigating network connectivity when the actual issue lies in security configuration or credential management.

This highlights an important requirement for secure power automation: **security controls must provide sufficient diagnostic evidence to distinguish security-related failures from conventional communication faults.**

The importance of diagnosing security-related communication failures is also reflected in the engineering challenges examined in IEC 62351 implementation research [1] and in broader OT cybersecurity guidance [5].

Redundancy Does Not Automatically Guarantee Security Resilience

Modern substations may use redundant network architectures, including Parallel Redundancy Protocol (PRP), to improve communication availability.

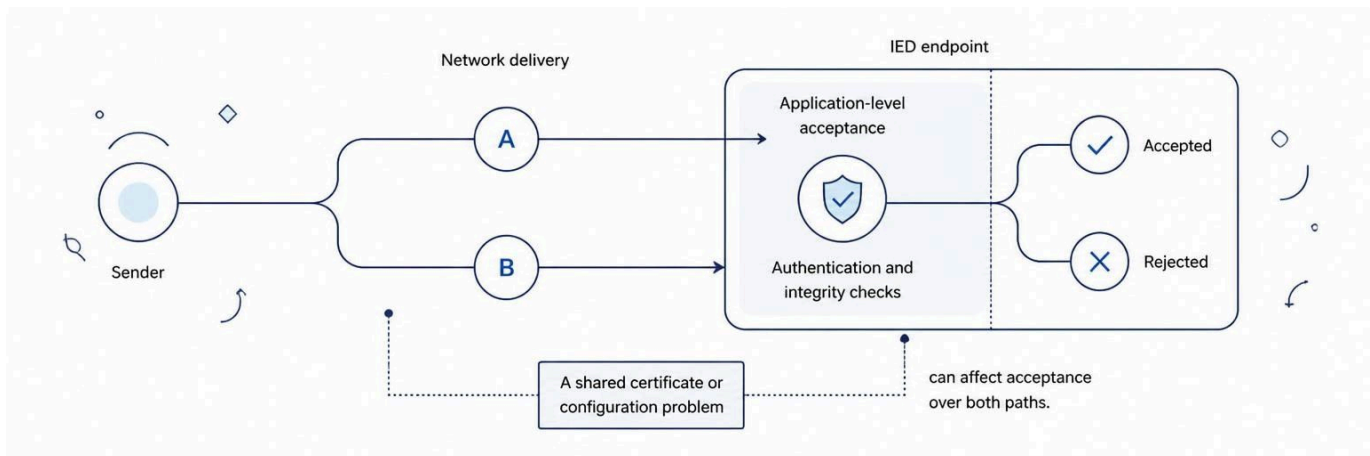
However, communication-path redundancy and security-related fault tolerance are different properties.

A redundant network may continue transporting packets while an endpoint rejects them because of authentication or integrity failures. Similarly, a shared certificate or configuration problem may affect communications over both redundant paths.

This creates a distinction between network availability and application-level communication acceptance.

A comprehensive security evaluation should therefore examine not only whether messages reach their destination, but also whether valid messages are accepted, invalid messages are rejected, and critical functions maintain their required behavior during disturbances.

This distinction is particularly relevant when assessing cybersecurity mechanisms in redundant power automation communication architectures [1], [5].



Conceptual illustration. No measurements, test setup or real equipment.

Moving Beyond Security Compliance

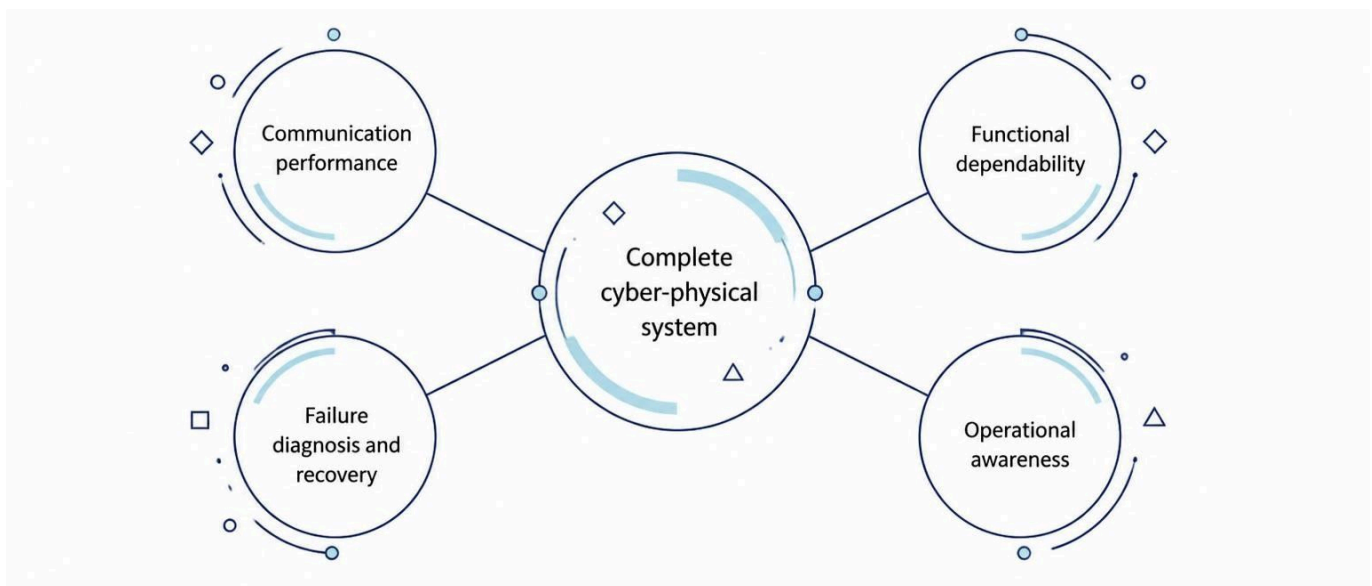
A meaningful assessment of secure IEC 61850 communication should address at least four engineering dimensions:

1. Communication performance: How do security mechanisms affect latency, processing demands and time-sensitive message delivery?

2. Functional dependability: Do protection, automation and supervisory functions continue to behave according to their specified requirements?

3. Failure diagnosis and recovery: Can engineers identify and recover from certificate failures, authentication errors or misconfigurations without introducing additional operational risks?

4. Operational awareness: Can operators distinguish between equipment failures, communication disturbances and security-induced service restrictions?



Standards conformance remains essential. However, successful implementation also requires system-level integration testing under representative operating conditions.

These engineering considerations are consistent with the operational performance and reliability concerns emphasized in NIST's guidance for securing operational technology [5].

An Engineering Approach to Secure Deployment

A practical deployment process should begin with identifying critical communication services and their operational requirements.

Security configurations should then be introduced and validated in a controlled environment before deployment.

Tests should include both expected successful operations and negative conditions such as expired credentials, unauthorized requests, mismatched security configurations and communication disturbances.

The evaluation should capture protocol behavior, security events, application responses and recovery actions.

Most importantly, acceptance criteria should be defined before testing, so that security improvements are assessed against measurable operational expectations rather than assumed benefits.

Such evaluations can complement the technical security mechanisms specified in IEC 62351 and the broader operational considerations identified in OT security guidance [2]–[5].

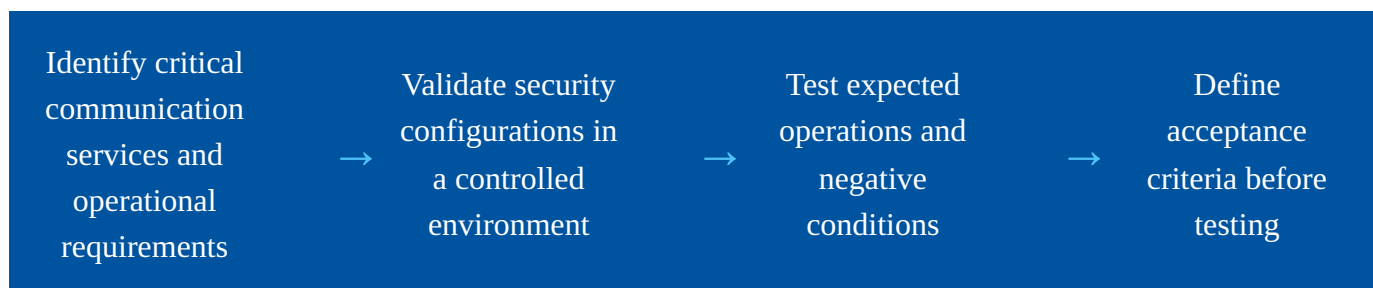
The Key Takeaway

The success of cybersecurity in power automation should not be measured solely by whether security mechanisms have been enabled.

It should be measured by whether the system can **enforce security requirements, preserve required operational behavior, identify failures and recover predictably.**

As substations become increasingly digital and interconnected, cybersecurity engineering must evolve from implementing individual controls to validating the behavior of the complete cyber-physical system.

A secure power system is not simply one that rejects unauthorized communication. It is one that responds to security events without creating unacceptable operational consequences.



Conceptual illustration of the process described above; not part of the author's technical claims. No measurements, test setup or real equipment.

References

- [1] K. TS, S. Chaitanya, and G. Gurralla, *Study of Cybersecurity in Power Automation: Implementation Challenges of IEC 62351 for IEC 61850 Systems*, CIGRE Paris Session 2026, Study Committee D2, Preferential Subject D2-PS2, Paper 10665, 2026. <https://www.e-cigre.org/publications/detail/session-2026-d2-session-2026-sc-d2-package.html>
 - [2] IEC 62351-3:2023, *Power Systems Management and Associated Information Exchange, Data and Communications Security, Part 3: Communication Network and System Security, Profiles Including TCP/IP*. International Electrotechnical Commission. <https://webstore.iec.ch/en/publication/68410>
 - [3] IEC 62351-6:2020, *Power Systems Management and Associated Information Exchange, Data and Communications Security, Part 6: Security for IEC 61850*. International Electrotechnical Commission. <https://webstore.iec.ch/en/publication/63742>
 - [4] IEC 62351-9:2023, *Power Systems Management and Associated Information Exchange, Data and Communications Security, Part 9: Cyber Security Key Management for Power System Equipment*. International Electrotechnical Commission. <https://webstore.iec.ch/en/publication/66864>
 - [5] K. Stouffer et al., *Guide to Operational Technology (OT) Security*, NIST Special Publication 800-82, Revision 3, September 2023. <https://doi.org/10.6028/NIST.SP.800-82r3>
-

Acknowledgment

The author acknowledges the contributions of colleagues and research collaborators involved in the investigation of IEC 62351 implementation challenges for IEC 61850-based power automation systems, including the research presented at CIGRE Paris Session 2026. The technical investigations and engineering discussions concerning communication security, network redundancy, fault diagnosis and operational recovery have informed the perspectives presented in this article.

The author also acknowledges the relevant IEC standards and NIST publications that provide technical guidance for securing power automation systems.

About the Author

Kiran TS is a Lead Research Engineer at PGCOE, working in operational technology cybersecurity and power system automation. His areas of work include cyber-physical security testbeds, industrial communication security, cybersecurity experimentation, evidence-based assessment and security validation for critical power infrastructure.