

From Compliance to Evidence: Rethinking Cybersecurity Conformance Testing for Power Automation

Cybersecurity Awareness Month | Technical Perspectives on Critical Infrastructure Security

Author: Kiran TS

Designation: Lead Research Engineer

Organization: PGCoe



Declared capability



Verified evidence

Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Is Compliance Enough to Establish Cybersecurity?

Consider an intelligent electronic device (IED) deployed in a digital substation. Its technical documentation indicates support for secure communication, role-based access control, event logging and user authentication.

The device appears to satisfy several cybersecurity requirements. But what does that actually establish?

Does the device reject an unauthorized control command? Does it correctly validate an expired certificate? Are security-related events recorded with sufficient information for investigation? What happens when security configurations change during operation?

More importantly, how can these capabilities be demonstrated independently?

This highlights an important distinction in power sector cybersecurity:

A declared security capability is not the same as a verified security capability.

As electric utilities increasingly adopt digitally interconnected protection, control and automation systems, cybersecurity evaluation must move beyond feature declarations and checklist-based assessments toward technically reproducible evidence.

Why Traditional Compliance Assessments Have Limitations

Cybersecurity standards establish requirements for systems, products and operational processes.

IEC 62443 addresses security within industrial automation and control systems, including system-level and component-level technical requirements. IEC 62351 addresses security mechanisms for power system communications, while IEEE 1686 specifies cybersecurity capabilities associated with intelligent electronic devices [1]–[4].

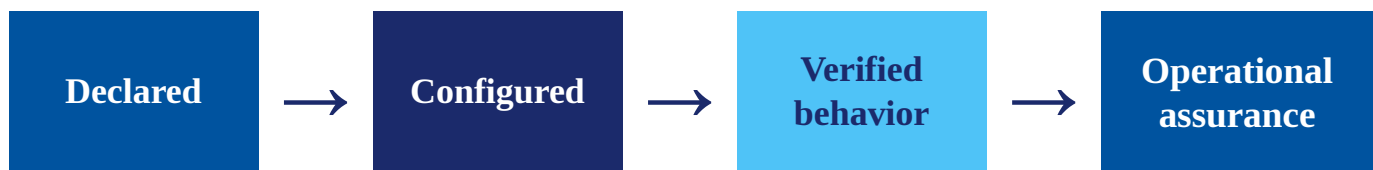
These standards serve different purposes, and their requirements should not be treated as interchangeable.

However, translating their requirements into an assessment process introduces a common engineering challenge.

A statement such as "the device supports access control" does not, by itself, establish whether access restrictions operate correctly under different user roles, communication interfaces or operating conditions.

A complete evaluation should distinguish between four levels of evidence:

1. **Declared capability:** The manufacturer or developer states that the feature is supported.
2. **Configured capability:** The relevant feature is demonstrably enabled and appropriately configured.
3. **Verified behavior:** A controlled test demonstrates the expected outcome, including rejection of unauthorized operations.
4. **Operational assurance:** Additional system-level testing examines whether the feature continues to behave acceptably under representative operating conditions.



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

These are progressively stronger forms of evidence, but they are not universally prescribed certification levels.

The distinction helps clarify what has actually been demonstrated during a security assessment.

Turning Security Requirements into Executable Tests

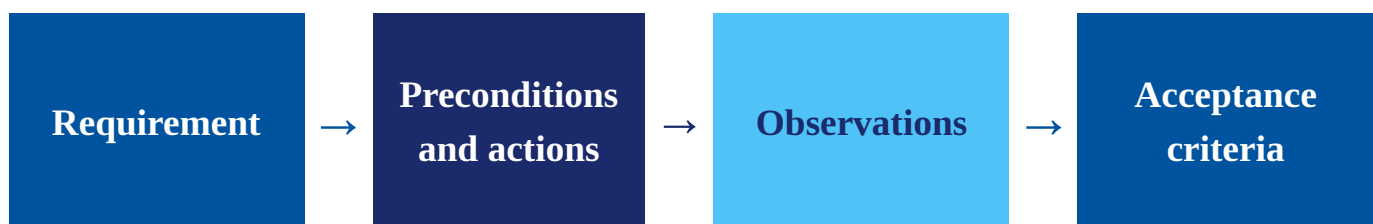
One of the most important tasks in cybersecurity assessment is translating a written requirement into an objective test.

Consider a simplified access-control requirement:

"Only an authorized user shall be permitted to modify protection configuration parameters."

This statement expresses a security objective, but it is insufficient as a standalone test procedure. An executable assessment must identify:

- The device and firmware version under test.
- The relevant communication or management interface.
- The configured users, roles and permissions.
- The initial operating and security conditions.
- The operation to be attempted.
- The expected behavior for authorized and unauthorized users.
- The evidence required to establish the result.
- The criteria for pass, fail or an inconclusive outcome.



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

For example, an authorized engineering user may be permitted to modify a configuration parameter, while an operator assigned read-only permissions must be prevented from making the same modification. The assessment should verify both outcomes.

A successful authorized operation demonstrates availability of the intended functionality, while successful rejection of an unauthorized operation demonstrates enforcement of the access restriction for the tested condition. This distinction is important because a device that rejects every operation is not necessarily implementing access control correctly.

Cybersecurity testing must verify correct acceptance as well as correct rejection.

The Importance of Negative Testing

Security functions are frequently designed to prevent undesirable behavior. As a result, testing only successful operations provides limited assurance.

Consider a secure communication service based on certificates.

An evaluation may first establish that a client and server can communicate using valid credentials.

However, additional negative tests are needed to determine how the implementation behaves when presented with unacceptable security conditions.

Representative test scenarios may include:

- A certificate that has expired.
- A certificate issued by an untrusted authority.
- A revoked certificate, where revocation checking is applicable and configured.
- Incompatible security parameters.
- An unauthorized request to access a protected function.

The expected response depends on the applicable standard, security profile, configuration and operating context [2], [5].

Testing must therefore avoid assuming that every rejected connection represents correct security behavior.

For example, a connection that fails because of a network outage cannot establish that certificate validation is functioning correctly.

The tester must distinguish between rejection by the intended security mechanism and failure caused by unrelated conditions.

This is why cybersecurity conformance testing requires controlled preconditions, observable responses and explicit acceptance criteria.

Positive testing

Valid credentials → expected communication

Negative testing

Unacceptable security conditions → evaluate the intended security response

Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Evidence Is More Than a Pass/Fail Result

A security assessment commonly produces an outcome such as PASS, FAIL or INCONCLUSIVE.

These outcomes are useful, but the result alone is insufficient for independent technical review.

A defensible assessment record should explain how the conclusion was reached.

Relevant evidence may include:

- Identification of the device and tested software version.
- The applicable requirement and test procedure.
- The security configuration and test preconditions.
- Executed operations and their observed responses.
- Relevant network communication records.
- Device-generated security events.
- Time references and known synchronization limitations.

- Any deviations from the approved test procedure. A network capture may establish that a request was transmitted and that a response was observed. However, it may not independently prove that a configuration change was rejected or that an internal security event was recorded.

Likewise, an application log may report an access denial without proving that the protected state remained unchanged.

Where practical, important test conclusions should therefore be supported by complementary sources of evidence.

For instance, an unauthorized configuration-write test can combine communication traces, application responses and readback of the protected configuration parameter.

This creates a more defensible connection between the test action, the observed behavior and the final verdict.



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Why Automation Alone Is Not the Solution

Automation can significantly improve cybersecurity assessment by supporting repeatability, consistent test execution and systematic evidence collection.

However, automating an incomplete or ambiguous test does not necessarily improve its validity.

If the expected outcome is incorrectly specified, the automated tool may repeatedly produce a misleading result.

Similarly, a test engine that classifies a communication timeout as a security rejection may report a successful test even when the intended security mechanism was never exercised.

A technically sound assessment framework should therefore separate the following functions:

Requirement interpretation: Establish what the applicable standard actually requires.

Test specification: Define preconditions, actions, observations and acceptance criteria.

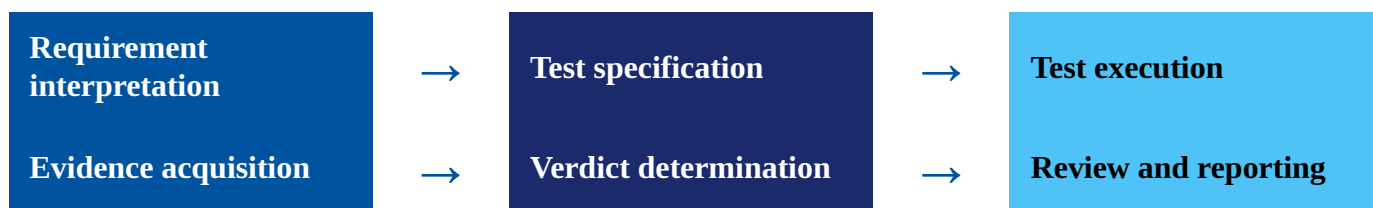
Test execution: Interact with the device or system through the relevant interface.

Evidence acquisition: Collect the data needed to support technical conclusions.

Verdict determination: Evaluate evidence against defined acceptance criteria.

Review and reporting: Preserve traceability and identify limitations requiring engineering judgment.

Automating these functions can improve consistency, but expert review remains important, particularly for ambiguous responses, vendor-specific behavior and system-level operational consequences.



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

Conformance, Security Effectiveness and Operational Resilience

Cybersecurity assessments must also distinguish among three related but different questions.

Conformance: Does the implementation satisfy the specified requirements within the defined assessment scope?

Security effectiveness: Does the implemented control provide meaningful protection against the threats and misuse conditions being considered?

Operational resilience: Does the system preserve required functions, or recover acceptably, when security-related disturbances occur?



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

A device may pass an applicable conformance test while the larger system still contains weaknesses caused by integration errors, configuration dependencies or inadequate operational procedures.

For example, an IED may correctly reject unauthorized communication, while the supervisory system provides insufficient diagnostic information for an operator to distinguish a security rejection from a network fault.

The IED's behavior and the system's operational response must be evaluated separately.

The reverse is also important: an observed successful operation does not establish that the device satisfies every requirement of a cybersecurity standard.

Therefore, conformance results should always identify the standards, clauses, configurations, product versions and test boundaries to which they apply.

A Practical Assessment Model for Power Automation

A structured cybersecurity assessment of power automation equipment can follow a traceable workflow:

Step 1: Establish the assessment boundary. Identify the device, product version, interfaces, applicable standards and selected requirements.

Step 2: Define the testable security behavior. Translate each applicable requirement into observable actions and acceptance criteria.

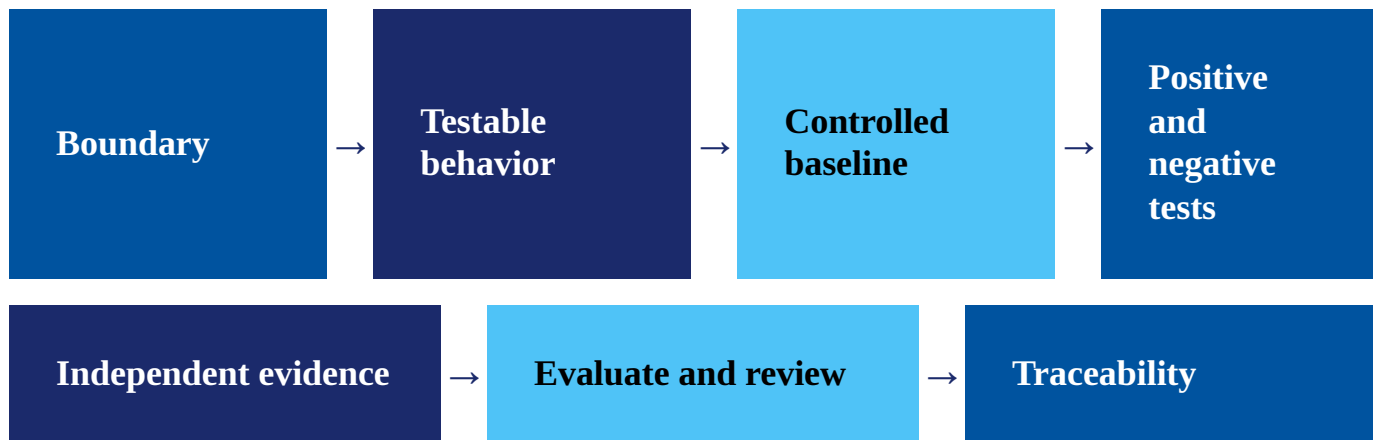
Step 3: Establish a controlled baseline. Record device settings, security configuration, network conditions and relevant operating states.

Step 4: Execute positive and negative tests. Verify both permitted operations and the rejection of prohibited or invalid operations.

Step 5: Collect independent evidence where feasible. Correlate communication records, device responses, configuration state and audit events.

Step 6: Evaluate and review findings. Distinguish conformance failures, execution failures, environmental problems and inconclusive results.

Step 7: Preserve traceability. Maintain the relationship between the requirement, test procedure, observed evidence, verdict and final report.



Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

This model is consistent with the broader principles of systematic technical security assessment described in NIST SP 800-115 [6].

It does not replace an official certification scheme or guarantee that an implementation conforms to an entire standard. Rather, it provides an engineering framework for producing transparent and reviewable assessment evidence.

The Opportunity for the Power Sector

As substations and control systems adopt increasingly interconnected digital technologies, utilities need greater confidence in the cybersecurity properties of the equipment they procure and deploy.

Evidence-driven assessments can help utilities evaluate security claims, support procurement acceptance, identify implementation weaknesses and investigate interoperability problems.

For technology developers, repeatable test procedures can reveal defects earlier in the product development lifecycle.

For testing laboratories, structured evidence improves the consistency and defensibility of technical assessments.

And for researchers, testability opens opportunities to develop automated assessment techniques, reusable test specifications and better methods for validating security controls under representative operating conditions.

The long-term opportunity is not merely to automate cybersecurity checklists, but to establish repeatable methods for linking **security requirements, observed implementation behavior and operational consequences.**

The Key Takeaway

Cybersecurity standards provide essential requirements for securing electric power automation systems.

However, the presence of a security feature, a compliant configuration or a successful communication session is not, on its own, sufficient evidence of comprehensive cybersecurity assurance.

A credible assessment must establish what was tested, how it was tested, what was observed and what conclusions the evidence supports.

The value of cybersecurity conformance testing lies not simply in declaring that a system is secure, but in demonstrating precisely which security requirements have been satisfied and under what conditions.

For the power sector, moving from compliance-oriented documentation toward transparent, reproducible and evidence-driven testing is an important step toward building trustworthy and resilient digital infrastructure.

References

- [1] IEC 62443-4-2:2019, *Security for Industrial Automation and Control Systems, Part 4-2: Technical Security Requirements for IACS Components*. International Electrotechnical Commission. <https://webstore.iec.ch/en/publication/34421>
- [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] IEEE Std 1686-2022, *IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities*. IEEE Standards Association. <https://standards.ieee.org/ieee/1686/7207/>
- [4] IEC 62443-3-3:2013, *Industrial Communication Networks, Network and System Security , Part 3-3: System Security Requirements and Security Levels*. International Electrotechnical Commission. <https://webstore.iec.ch/en/publication/7033>
- [5] 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>
- [6] K. Scarfone, M. Souppaya, A. Cody, and A. Orebaugh, *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115, September 2008. <https://doi.org/10.6028/NIST.SP.800-115>

Acknowledgment

The author acknowledges the collaborative contributions and technical discussions associated with cybersecurity assessment of power automation systems, intelligent electronic devices and industrial communication protocols.

Engineering experience in standards-based security evaluation, test procedure development and evidence-driven analysis has informed the perspectives presented in this article.

The author also acknowledges the IEC, IEEE and NIST standards and technical guidance that provide the foundation for the discussion.

About the Author

Kiran TS is a Lead Research Engineer at PGCOE, working in operational technology cybersecurity and power system automation. His technical interests include IEC 62351 and IEC 62443 security assessment, IEEE 1686 intelligent electronic device cybersecurity, automated security testing, conformance assessment methodologies and evidence-based validation of critical power infrastructure.