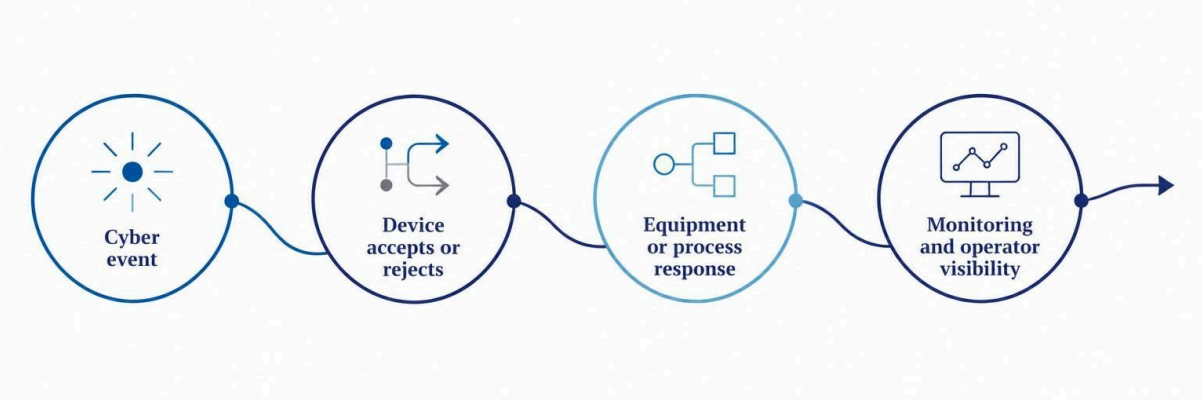
Beyond Attack Detection: Why Power Sector Cybersecurity Needs Cyber-Physical Testbeds

Cybersecurity Awareness Month | Research and Innovation in Critical Infrastructure Security

Author: Kiran TS
Designation: Lead Research Engineer
Organization: PGCOE



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

Is Detecting a Cyberattack Enough?

Suppose a cybersecurity monitoring system detects an unusual communication event in a power substation.

The event might involve an unexpected control command, modified process information or anomalous communication between automation devices.

The monitoring system raises an alert. From a conventional cybersecurity perspective, the detection mechanism appears successful.

However, several important questions remain unanswered.

Did the suspicious communication affect the physical process? Was the command accepted or rejected? Did an automation function change its behavior? Was the event visible to the operator? Could the system recover without compromising its operational requirements?

These questions reveal a fundamental challenge in operational technology (OT) cybersecurity:

> **Detecting a cyber event is not the same as understanding its operational consequences.**

For critical infrastructure such as electric power systems, cybersecurity assessments must establish the relationship between cyber events, equipment behavior, operational consequences and system resilience [1], [2].

Why Conventional Cybersecurity Testing Is Insufficient

Traditional cybersecurity testing frequently focuses on identifying vulnerabilities, evaluating network exposures and determining whether attacks can bypass security controls.

These are necessary activities, but they do not fully characterize cybersecurity risks in power automation environments.

Electric power systems combine computing infrastructure, communication networks, protection devices, controllers and physical processes.

A communication event that appears minor from a network-security perspective may have significant operational implications depending on the affected function and the prevailing system state.

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

Conversely, suspicious network traffic may be rejected by a receiving device without affecting the physical process.

Consequently, cybersecurity analysis must distinguish between an attempted cyber action, a successful cyber compromise and an observable operational consequence.

This distinction is central to meaningful risk assessment and is consistent with the broader system-level considerations described in NIST's OT security guidance [1].

The Role of Cyber-Physical Security Testbeds

Cyber-physical testbeds provide controlled environments in which cybersecurity scenarios can be evaluated alongside representative industrial equipment and automation functions.

A power automation testbed may integrate intelligent electronic devices, communication networks, supervisory systems, process interfaces, engineering workstations and monitoring infrastructure. Such environments create opportunities to investigate how cyber events propagate across multiple layers of a system. For example, an experiment involving a suspicious control command can examine:

1. Whether the communication reaches the intended device.
2. Whether the device accepts or rejects the command.
3. Whether authorization controls operate as intended.
4. Whether the command produces an observable equipment or process response.
5. Whether monitoring systems correctly identify the event.
6. Whether the operator receives adequate information to interpret the situation.

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

Each observation contributes evidence about a different aspect of system security. Importantly, a successful experiment does not necessarily require an attack to produce a physical disturbance. Demonstrating that controls prevent a dangerous consequence can be equally valuable. The NIST Framework for Cyber-Physical Systems provides a foundation for considering the interaction among system functions, physical processes and trustworthiness requirements [2].

From Network Packets to Operational Evidence

A significant challenge in cyber-physical experimentation is obtaining sufficient evidence to reconstruct what actually happened.

Network packet captures alone may show that a command was transmitted, but they may not establish whether a device accepted it or whether the physical process changed. Device logs may confirm an operation, but without reliable timestamps and contextual information, correlating the event with network activity can be difficult.

A defensible experimental record should therefore connect multiple sources of information:

- The initial scenario and system operating condition.
- The initiating cyber event.
- Relevant communication traces.
- Device and application responses.
- Available process-level observations.
- Security and operational alarms.
- Time references and synchronization quality.
- Recovery actions and final system state.

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

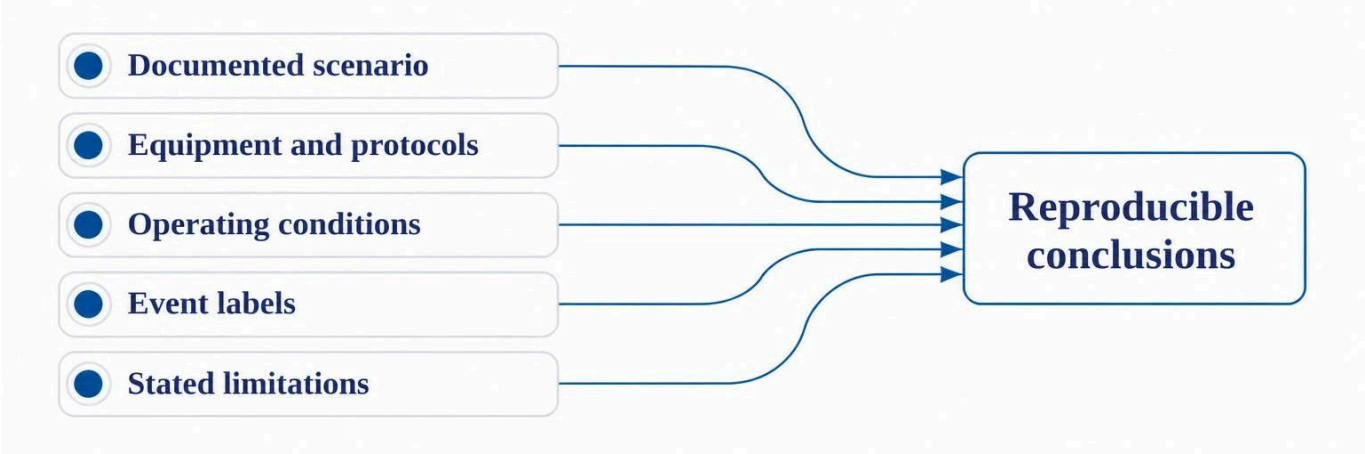
The objective is to create an evidence chain that supports reproducible technical conclusions. A crucial distinction must also be maintained between an observation and its interpretation. A dataset label such as "successful attack" should be supported by observable evidence rather than assigned solely because a particular scenario was executed. This evidence-oriented approach draws on the principles of systematic technical security assessment described in NIST SP 800-115 [3].

Why Reproducibility Matters

Cybersecurity research increasingly relies on datasets to develop detection algorithms, evaluate analytical techniques and compare security solutions.

However, the usefulness of a dataset depends on more than the number of captured events or attack categories represented.

Researchers should be able to determine how the data was generated, which equipment and protocols were involved, what operating conditions existed, how events were labeled and what limitations apply.



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

For example, the presence of time-synchronization traffic does not by itself prove that different observation systems maintained sufficiently accurate synchronization.

Likewise, an alert generated by one monitoring tool does not independently establish the ground truth of an experiment.

Reproducible cyber-physical research requires carefully documented scenarios, independent evidence where practical, and transparent treatment of uncertainties.

This approach helps prevent misleading conclusions about the effectiveness of security technologies.

From Research Infrastructure to Utility Readiness

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

Cyber-physical testbeds can support several objectives beyond conventional cybersecurity demonstrations.

They can enable validation of security mechanisms before deployment, examination of device interoperability, investigation of communication failures, evaluation of monitoring and detection systems, and training of engineers in controlled operational scenarios.

They also provide a means to examine security-induced failures without exposing production substations to unnecessary testing risks.

For utilities, these capabilities can help translate cybersecurity requirements into practical engineering questions and measurable acceptance criteria.

For researchers, they create opportunities to study problems that cannot be adequately represented using network traffic alone.

For technology developers, they offer realistic conditions under which security products can be evaluated before field implementation.

The NESCOR resources for electric utilities provide a relevant foundation for examining failure scenarios and developing security assessment activities for the electricity sector [4].

Experimental studies involving IEC 62351 deployment also illustrate why communication security must be evaluated in relation to system-level operational behavior [5].

The Next Step: Consequence-Driven Cybersecurity

A useful direction for power sector cybersecurity is to organize security evaluations around operational consequences rather than attack techniques alone.

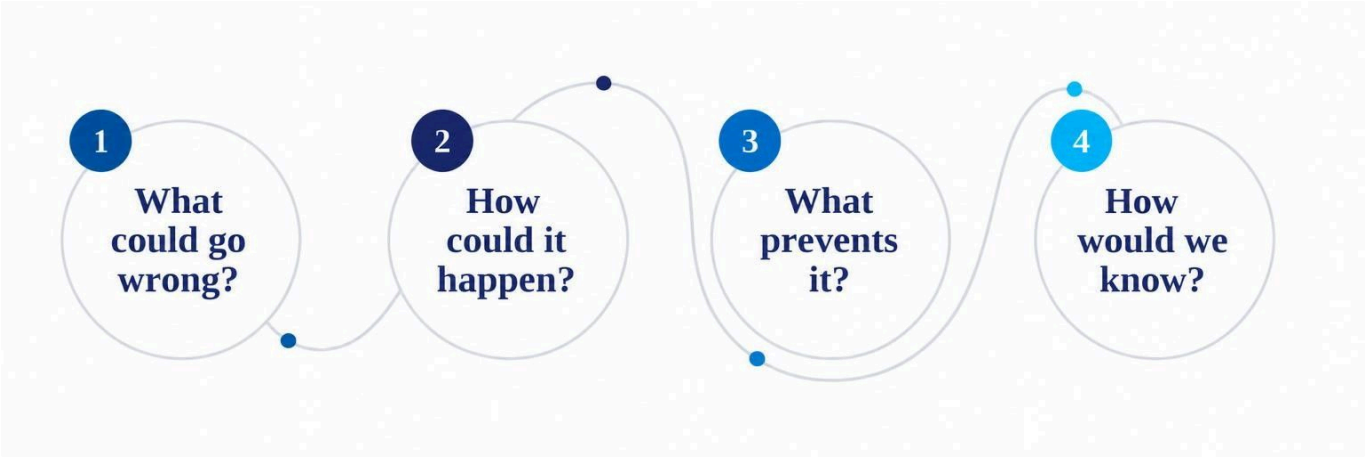
This requires asking four fundamental questions:

What could go wrong? Identify the undesirable operational outcome.

How could it happen? Examine credible cyber and system failure paths.

What prevents it? Identify and evaluate security and operational safeguards.

How would we know? Establish the evidence needed to determine whether the safeguards performed as intended.



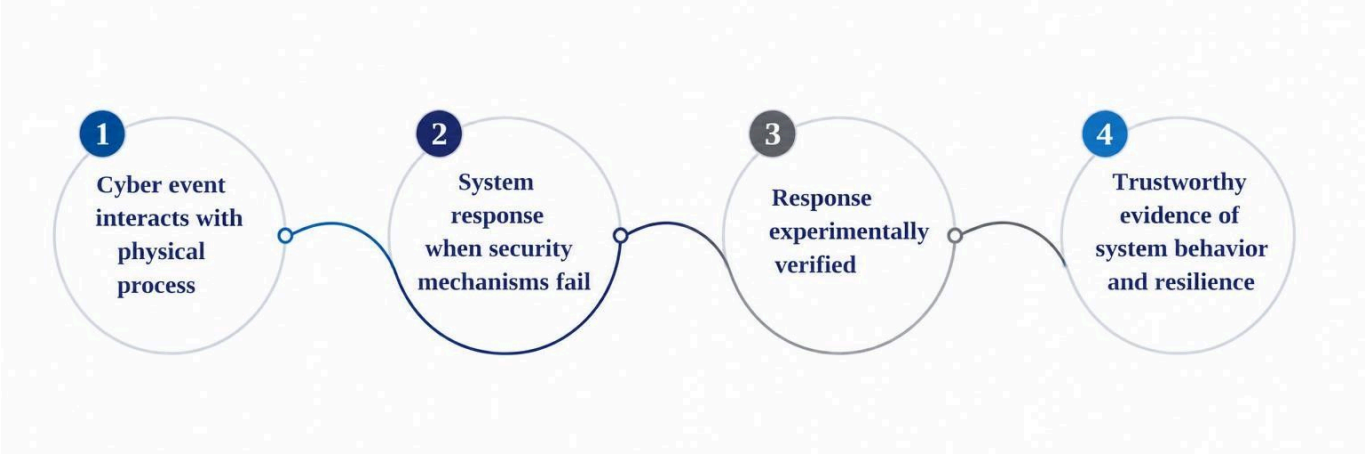
Conceptual illustration, not part of the author's technical claims. No measurements, test setup, real equipment or experimental validation implied.

This approach connects cybersecurity engineering with power system reliability, protection engineering and operational risk management.

The Key Takeaway

The future of power sector cybersecurity requires more than detecting suspicious traffic or demonstrating individual security controls.

It requires understanding how cyber events interact with physical processes, how systems respond when security mechanisms fail, and how those responses can be experimentally verified.



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

> **The ultimate value of a cyber-physical security testbed lies not in demonstrating that an attack is possible, but in producing trustworthy evidence about the system's behavior and resilience.**

Moving from isolated cybersecurity testing toward evidence-driven, consequence-aware evaluation can strengthen the reliability and security of critical power infrastructure.

References

[1] 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**

[2] E. R. Griffor, C. Greer, D. A. Wollman, and M. J. Burns, *Framework for Cyber-Physical Systems: Volume 1, Overview*, NIST Special Publication 1500-201, 2017. **https://doi.org/10.6028/NIST.SP.1500-201**

[3] K. Scarfone et al., *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115, September 2008. **https://doi.org/10.6028/NIST.SP.800-115**

[4] Electric Power Research Institute (EPRI), *National Electric Sector Cybersecurity Organization Resource (NESCOR): Failure Scenarios and Guide to Penetration Testing for Electric Utilities*. **https://smartgrid.epri.com/nescor.aspx**

[5] K. TS, S. Chaitanya, and G. Gurrala, *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**

Acknowledgment

The author acknowledges the contributions of colleagues and research collaborators involved in power automation, operational technology cybersecurity, cyber-physical testbed development and experimental security evaluation. The practical experience gained through laboratory investigations, communication analysis, evidence collection and technical validation has informed the engineering perspectives presented in this article.

The author also acknowledges the publicly available technical guidance provided by NIST, EPRI/NESCOR and the CIGRE research community.

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.