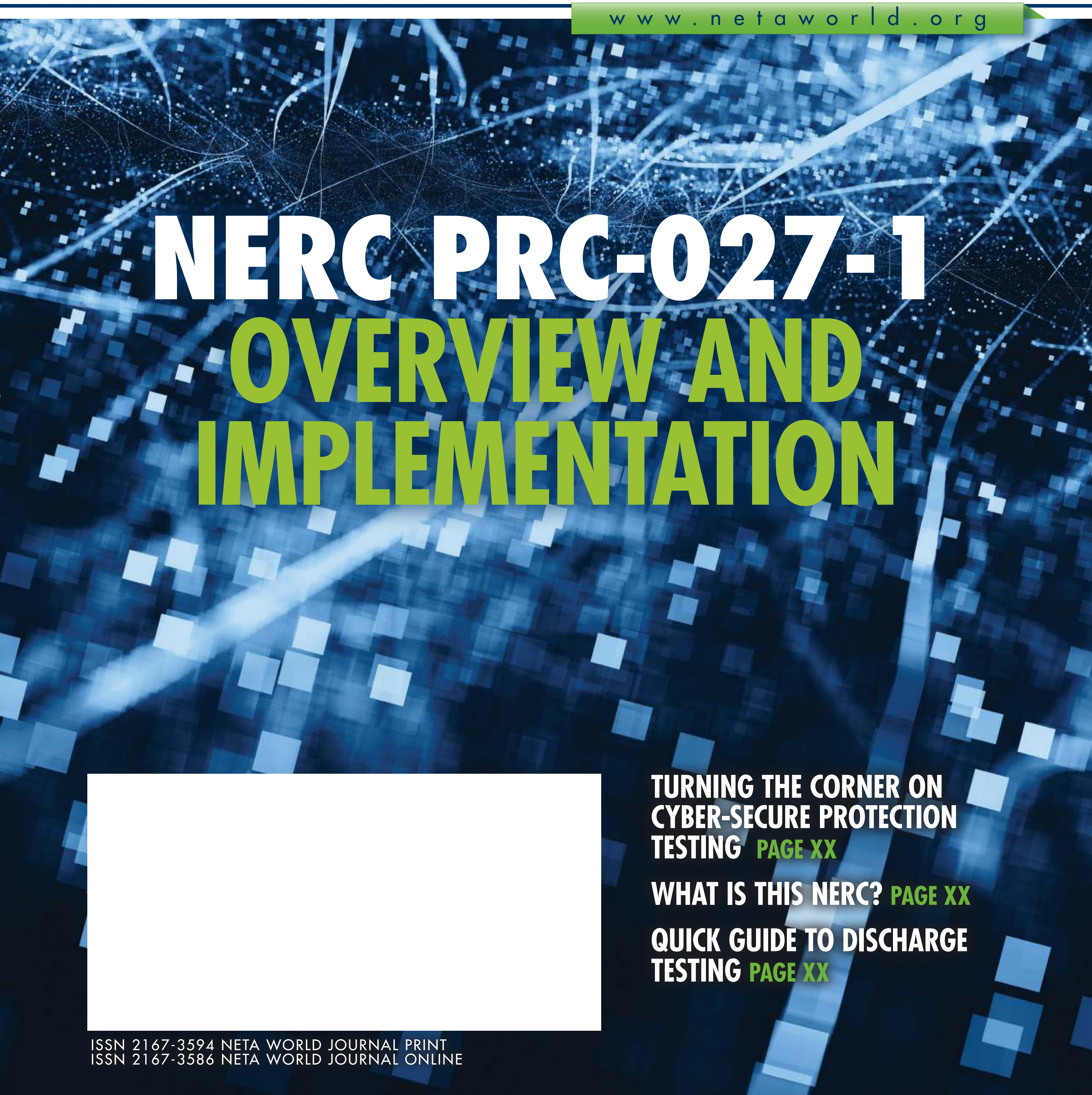
The InterNational Electrical Testing Association Journal

WINTER 2021

NETA WORLD™

www.netaworld.org



NERC PRC-027-1 OVERVIEW AND IMPLEMENTATION

TURNING THE CORNER ON CYBER-SECURE PROTECTION TESTING PAGE XX

WHAT IS THIS NERC? PAGE XX

QUICK GUIDE TO DISCHARGE TESTING PAGE XX

ISSN 2167-3594 NETA WORLD JOURNAL PRINT
ISSN 2167-3586 NETA WORLD JOURNAL ONLINE

FEATURE

TURNING THE CORNER ON CYBER-SECURE PROTECTION TESTING

BY BRYAN GWYN, SAGAR SINGAM, and JOE STEVENSON, *Doble Engineering Company*

Matters of NERC PRC and NERC CIP compliance intersect during protection system testing on substation networks. In the modern regulatory environment, the benefits of computer-based relaying are challenged by the costs of cyber security and disrupted or insufficient relay testing practices. The way forward demands interconnected data and the ability to track critical metrics automatically. Organizations can modernize while ensuring compliance readiness by implementing systems that integrate protection and cyber domains into scalable management platforms.

Electric power utilities that operate bulk electric system (BES) generation and transmission facilities confront more challenges than ever before. The stakes surrounding system reliability have never been higher, and the pressure on workers — especially protection and control (P&C) and information technology (IT) personnel — is tremendous.

Every turn in the modern utility work environment is seeing demands to modernize and deploy re-envisioned operations that

PHOTO: © ISTOCKPHOTO.COM/PORTFOLIO/DKOSIG

rely heavily on automation. Devising new philosophies and practices at a time when the grid is undergoing rapid power delivery transformations and cyber attacks are pervasive can significantly disrupt and overload the workforce.

Personnel in P&C and IT areas of utility operations perform work that directly affects system reliability. Despite evolving power system conditions and increased defenses against cyber threats, they must maintain stability with existing systems while plotting next steps to keep pace with advancing technologies. On top of it all, they face unique responsibilities concerning mandates that are enforced by the North American Electric Reliability Corporation (NERC).

COMPLIANCE

NERC Critical Infrastructure Protection (CIP) refers to a set of requirements that bind utilities to the protection, security, and maintenance of computer infrastructures that affect BES reliability. NERC CIP standards specify measures utilities must abide by to defend devices, software, and data against cyber threats. Twelve CIP standards are presently subject to enforcement, and some of them are being revised while new ones are being proposed for future enforcement.

NERC Protection and Control (PRC) standards require proof that elements affecting the reliability of protection and control systems among BES facilities are being addressed by utility engineering and maintenance processes. NERC PRC standards confront orthodoxy within P&C operations by expressly stating the metrics that are expected and the time that is allowed for attaining them. Some PRC standards allow alternatives to time limits if evidence can be presented that substantiates the necessary criteria. There are nineteen enforceable PRC standards, and as with CIP standards, there are PRC standards that are presently being revised and new ones that are being drafted.

NERC compliance means different things to IT and P&C teams, though cyber security and protection system reliability are interrelated subjects with evolving technical and regulatory responsibilities. CIP mandates affect PRC mandates and vice versa, and P&C teams and IT resources who support them are both affected by the complexities of dealing with various data from utility electronics and electrical equipment.

Personnel who engineer and test protection systems cannot do their work without company-issued computers installed with authorized software applications. It is not uncommon for P&C personnel to use dozens of software applications given the numerous device types and data formats in play. Consequently, security patches and software updates needed for P&C software applications can overwhelm IT support staff. Safeguards in place for CIP compliance can impede P&C workers who face PRC compliance deadlines. Regardless, NERC-mandated requirements must be completed on time, and thorough documentation must be kept that could be needed as evidence for compliance audits.

P&C PERSONNEL WHO PREVIOUSLY FACED LIMITED, IF ANY, COMPANY OVERSIGHT OF THEIR WORK COMPUTERS NOW OPERATE UNDER MUCH MORE SCRUTINY AND CONTROL.

RELAYS

A significant number of electromechanical relays are still used and usually have their own set of engineering and testing files, records warehousing, test materials, and maintenance practices. Electromechanical relays are single-function analog protective devices that require calibration during maintenance; they fall under NERC PRC-005, *Protection System, Automatic Reclosing, and Sudden Pressure Relaying Maintenance* if used on BES facilities.

Microprocessor-based relays are multi-function, networked devices that perform analog–digital/digital–analog signal conversions and algorithmic protection, automation, communication, and control processes. Microprocessor relays have software from their respective manufacturers that is used to program the devices. The files produced by the manufacturers' software contain settings data in different proprietary formats. Test technicians who commission microprocessor relays and those who perform periodic maintenance testing on them deal with hundreds or even thousands of settings not to mention logic parameters that must also be verified.

Purely digital relays — intelligent electronic devices (IEDs) — are multifunction, algorithmic, protection and control devices that have proprietary configuration software, though additional programming steps are necessary. IEDs must be set to respond properly to digital signals being emitted by other IEDs in substation network infrastructures. In protection and control systems based on the IEC 61850 standard, IEDs process digital signals containing power system quantities and inter-device communication streams in separate process bus (protection system) and station bus (control system) networks. IED programming involves not just the device itself, but also the configurations of other IEDs and even the process bus and station bus networks as a whole. The devices are nodes of substation networks.

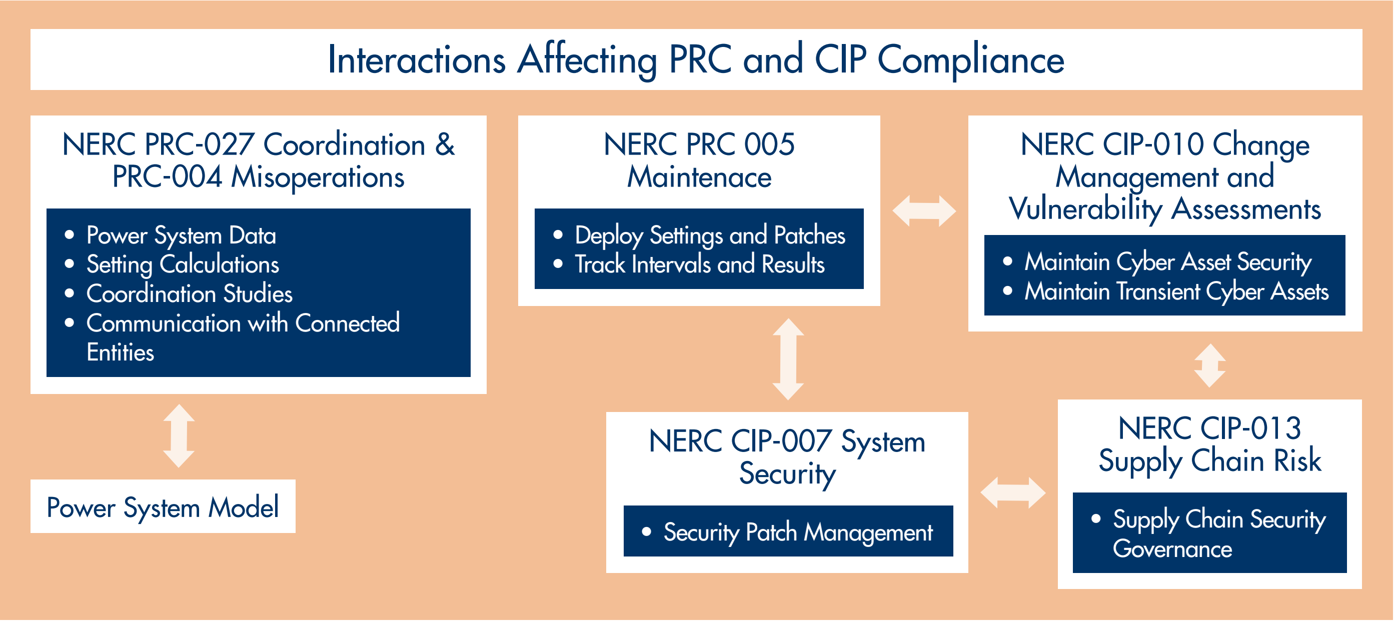

Interactions Affecting PRC and CIP Compliance
NERC PRC-027 Coordination & PRC-004 Misoperations
• Power System Data
• Setting Calculations
• Coordination Studies
• Communication with Connected Entities
Power System Model
NERC PRC 005 Maintenace
• Deploy Settings and Patches
• Track Intervals and Results
NERC CIP-010 Change Management and Vulnerability Assessments
• Maintain Cyber Asset Security
• Maintain Transient Cyber Assets
NERC CIP-007 System Security
• Security Patch Management
NERC CIP-013 Supply Chain Risk
• Supply Chain Security Governance

Figure 1: *Complying with NERC PRC and NERC CIP standards introduces complexities in utility operations.*

Microprocessor-based relays and IEDs used on BES facilities come under both PRC and CIP compliance mandates. As devices that affect the reliability of protection systems on BES facilities, they must be tested within required time intervals. As computers on BES facilities, they are considered cyber assets and added care must be taken during testing to prevent malware incursions into substation networks.

Protection system device testing requires specialized electrical equipment that usually is paired with control software provided by the respective test instrument manufacturer, although stand-alone protection test software also exists in the power industry marketplace. P&C departments might have designated personnel who specialize in testing certain relays, or they might have crews equally capable of testing across relay types. They might perform automated tests with certain relays and manual tests with others. They could outsource testing if in-house resources are too few or are inexperienced, or perhaps if they lack the necessary test instruments. In any event, they are responsible for compliance with NERC PRC and CIP standards as well as maintaining test records as evidence for compliance audits.

Protection system engineers use software tools that compute relay protection settings from configured power system models. Relay settings and configuration data are usually managed in various mediums from scanned documents to spreadsheets and databases to relay manufacturers' proprietary software files, although protection system asset management software is available commercially. The settings records of relays on BES facilities are subject to both PRC and CIP standards; BES relay settings must be verified on the actual devices, and settings data can only be applied to devices in secured computer-to-device exchanges.

Network topologies that are home to today's protection and control systems are managed by operational technology (OT) personnel in concert with IT departments that have enterprise cyber security top-of-mind. P&C personnel who previously faced limited, if any, company oversight of their work computers now operate under much more scrutiny and control. The systems and applications they use must be secured and maintained centrally through OT/IT, which invites challenges to ongoing support of older products and slows the adoption of the latest-and-greatest tools personnel might need.

COMPLIANCE

In essence, PRC compliance and CIP compliance are tightly integrated parts of overall NERC compliance programs. Although separately enforceable, they are mutually consequential. Utility compliance officers identify, track, and report on NERC-mandated elements within these standards but may not realize or plan for how the mandates impact workers. A best practice is proactive coordination between compliance officers and subject matter experts from OT/IT and P&C areas of the organization. Compliance program success is influenced greatly by the involvement of stakeholders who can reveal the complications endemic to cyber security when it comes to routine protection engineering and testing responsibilities.

Utility information systems can be separated by functional areas. For example, compliance management systems in the domain of compliance officers are separate from cyber security management systems that reside with IT. Protection system models and relay settings data are managed by protection engineers, whereas information about protection testing is found on field computers and shared drives or in filing cabinets.

For compliance program strategies to be effective, utilities need central data, information, and workflow management. OT/IT and P&C areas can become tasked with refining and expanding existing in-house systems. Where there are limits, workarounds are devised. Commercial software products that are used become integrated as far as possible, but varied data formats and diverse work processes within P&C cause gaps that in-house central management approaches don't overcome.

Many utilities use commercially available central management software that can consolidate, standardize, and integrate cyber security, protection engineering, protection testing, and compliance. Ultimately, these systems ensure cyber-secure transactions of critical data in mediums that do not hinder worker efficiency, even if workers have different needs and come from separate functional areas.

TRACKING AND REPORTING

With effective central management of cyber assets and P&C work details, compliance officers have visibility of numerous interconnections between processes and individual CIP and PRC standards. Having such visibility proves invaluable when plotting work steps for teams to follow. For instance, consolidated information about CIP and PRC mandates can enable compliance teams to focus on priorities (the mandates) and offload tracking and reporting functions to the software systems' automated management functions. Analytical tools can provide crucial insights about compliance-related activities and the effects they have on reliability.

For example, PRC-004, *Protection System Misoperation Identification and Correction* requires utilities to formalize procedures surrounding the identification and correction of unforeseen or unexpected protection system operations. Faulty test practices and incorrectly applied relay settings are two main causes of relay failures, and NERC mandates that utilities track how they investigate and resolve mistakes within their operations.

NERC PRC-004 tracking could expose one additional factor that leads to relay misoperations: overdue maintenance testing. Another standard, PRC-005, *Transmission and Generation Protection System Maintenance and Testing* requires utilities to provide evidence that relays and other protection system components are tested in regular maintenance intervals. Auditors want to see that utilities have viable protection system maintenance programs to the extent that they have the capacity to reach all BES protection system facilities and testing and calibration is accomplished by required deadlines.

MISOPERATIONS

But what if protection system misoperations result from relay settings that weren't correct in the first place? Another NERC PRC standard, PRC-027, *Coordination of Protection Systems for Performance During Faults* came into effect April 1, 2021, and addresses that issue by mandating periodic settings reviews and protection system coordination studies.

The new requirements affect protection engineers who must produce evidence of a formal process they adhere to when developing settings. Under PRC-027, protection engineers must also revisit system models, recalculate all protection settings values, and re-coordinate protection schemes.

WITH EFFECTIVE CENTRAL MANAGEMENT OF CYBER ASSETS AND P&C WORK DETAILS, COMPLIANCE OFFICERS HAVE VISIBILITY TO NUMEROUS INTERCONNECTIONS BETWEEN PROCESSES AND INDIVIDUAL CIP AND PRC STANDARDS.

PRC-027 brings into focus the accuracy of protection settings over time. Requirement 1 (R1) of the standard concerns the accuracy of the original power system models upon which protection settings are first calculated. The settings that go into service in protection schemes are only as good as the data in power system models. For this reason, PRC-027 R1 mandates that power system models are reviewed and updated.

Another part of R1 concerns review of protection system settings. Protection engineers must periodically revisit the settings for accuracy, but also to ensure that neighboring, electrically joined utilities have settings on record that coordinate with one another, such that protection systems operate in the intended sequence during faults. Settings verifications between affected utilities is a two-way street, and both share responsibilities under this PRC-027 requirement.

Why is this necessary? Because power systems change over time. With the PRC-027 standard, NERC addresses the likelihood that protection settings may become invalid as changes in fault currents occur. These changes may be due to changes in the power system such as changing power system characteristics as a result of significant additions of inverter-based renewables coming online that can affect protection system operability on the BES. NERC wants utilities to enact processes to proactively find incorrect relay settings, correct them, and communicate correct settings information to affected entities in a timely manner.

PRC-027 Requirement 2 (R2) concerns protection system coordination. Under R2, protection engineers must verify that coordination studies are performed on the affected protection systems any time there have been significant changes to the BES. Similar to R1, if any settings changes arise from coordination studies being performed, protection engineers must contact any affected electrically joined utilities and communicate the new settings information to ensure all protection systems in that area are coordinated properly for handling power system faults.

Concerning the communication to neighboring utilities of settings change information, R1 and R2 are not completed until there is documentation that the communication took place. Further, the matter of settings changes on electrically joined BES facilities isn't a one-and-done situation; both entities remain in consultation with one another back-and-forth until their respective peer-reviewed coordination studies can validate the settings are accurate within the given schemes involved. Both entities must agree and sign off to this effect, which is the documentation NERC auditors want to see provided with PRC-027 evidence.

DOCUMENTATION

NERC standards PRC-004, PRC-005, and PRC-027 are just three examples of standards that affect protection engineers and relay testing crews by requiring documented proof that activities are performed as mandated. The documentation these standards require can come from the same data source if a robust central management system is implemented that tracks lifecycle relay test details, maintenance intervals, relay settings and configuration changes, and associated work assignments. Many other NERC PRC standards impact protection engineers that also require evidence of compliance.

Protecting PRC compliance data and enabling automation while P&C teams do their work is possible with commercially available central management software. However, software automation depends on the human element. OT/IT teams need to be aware of processes and procedures P&C teams have in their compliance responsibilities. Conversely, P&C workers need to accept their roles and responsibilities in cyber security.

Implementing a central management system that supports PRC compliance reporting and office-to-field workflows takes a consultative process involving company stakeholders and the software vendor. A quality supplier will have a proven track record with many installed utility customers. The ideal supplier will offer configurable software and a detailed statement of work (SOW) that is clear and captures the full scope of the implementation project. The system must comply seamlessly with instituted cyber security measures and offer powerful administrative controls over user access privileges.

CYBER ATTACKS

Unrelenting cyber attacks on utility computer networks have increased concerns of adaptive measures cyber criminals will take to achieve their objectives. NERC CIP standards challenge utility cyber security programs to elevate their defenses by reducing their threat vectors.

NERC CIP-013, *Supply Chain Risk Management* in particular mandates that utilities have security controls concerning computer software and hardware products being procured. At issue are cyber threats that may be posed to the BES if the products are compromised coming from the vendor. CIP-013 requires proactive communication from vendors if cyber security risks are determined in products sold to utilities, and utilities must coordinate risk management plans in their supply chain procurement processes to prevent onboarding products that could pose cyber security risks.

NERC CIP-010, *Configuration Change Management and Vulnerability Assessments* exists to prevent unauthorized changes on BES cyber systems by external intruders. Utilities must determine and address vulnerabilities before hackers have the opportunity to exploit them for nefarious purposes.

CIP-010 requires vulnerability assessments every 36 months that look for gaps in and assess the effectiveness of preventive measures against malicious cyber attacks. One measure that can prevent hackers from accessing cyber systems is maintaining up-to-date security patches. Unpatched software allows hackers to run malicious code by using a known, unpatched security bug, and so cyber hackers always try to exploit unpatched systems.

As part of vulnerability assessments under CIP-010, utilities must produce evidence that they have reviewed installed patches, that they have a security patch review and mitigation process, and that they have processes for other cyber security vulnerability mitigations concerning software and software patches on cyber assets.

Requirement 4 (R4) of CIP-010 requires utilities to deploy transient cyber asset (TCA) computers for workers to use when connecting to cyber assets like microprocessor-based protective relays. Having secured TCAs prevents the possibility of malware being introduced onto cyber assets during maintenance.

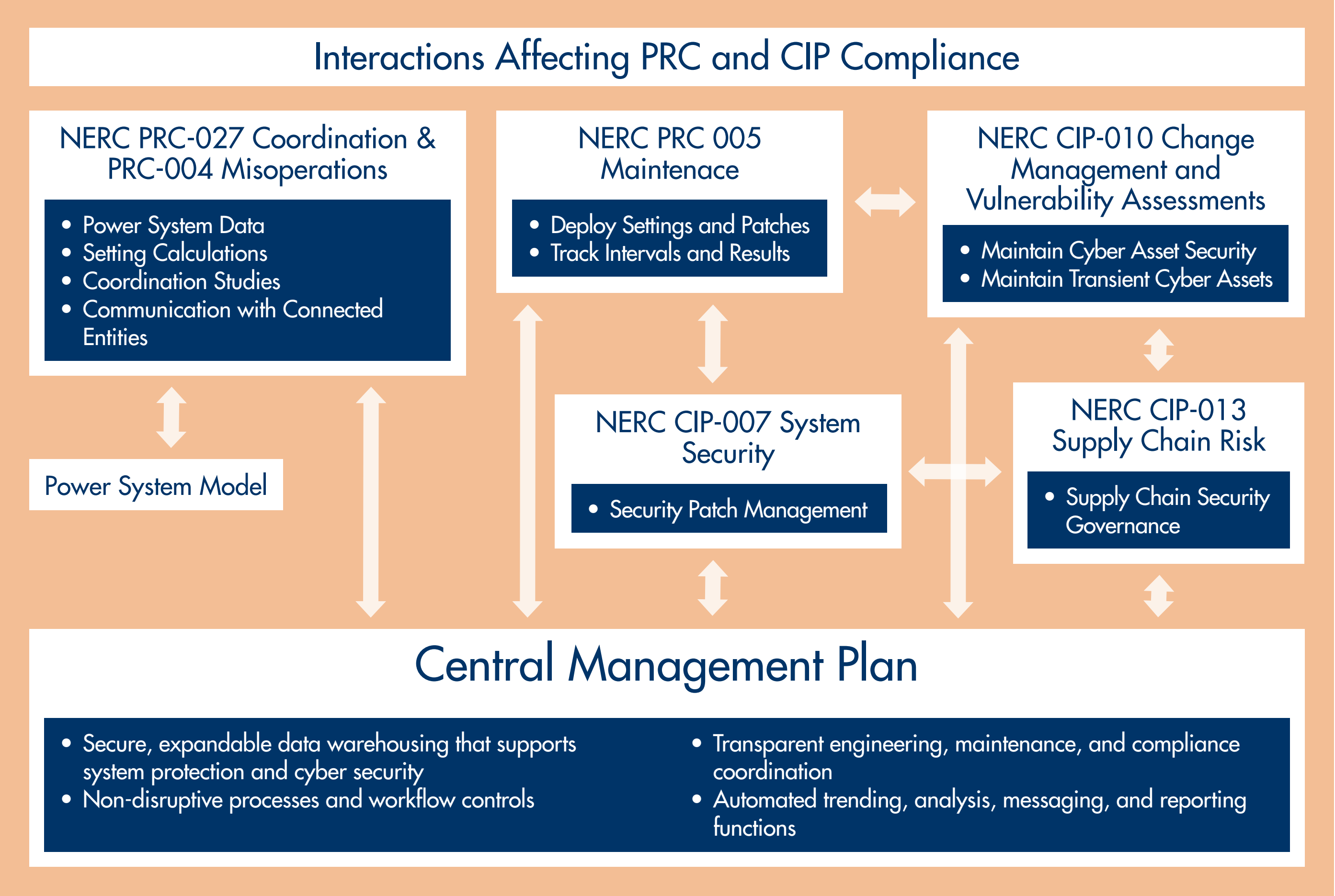

Interactions Affecting PRC and CIP Compliance
NERC PRC-027 Coordination & PRC-004 Misoperations
• Power System Data
• Setting Calculations
• Coordination Studies
• Communication with Connected Entities
NERC PRC 005 Maintenace
• Deploy Settings and Patches
• Track Intervals and Results
NERC CIP-010 Change Management and Vulnerability Assessments
• Maintain Cyber Asset Security
• Maintain Transient Cyber Assets
Power System Model
NERC CIP-007 System Security
• Security Patch Management
NERC CIP-013 Supply Chain Risk
• Supply Chain Security Governance
Central Management Plan
• Secure, expandable data warehousing that supports system protection and cyber security
• Non-disruptive processes and workflow controls
• Transparent engineering, maintenance, and compliance coordination
• Automated trending, analysis, messaging, and reporting functions

Figure 2: *Integrated data and workflow processes supported by a central management platform ensure efficient NERC PRC and NERC CIP compliance.*

Taken together, the requirements of CIP-010 impact OT/IT workers who must support security patching for a multitude of P&C software applications and manage those updates on TCAs across their organization. Baseline configurations of all cyber assets comprising cyber systems must be monitored and vulnerability assessments must be performed every 36 months to detect any means by which unauthorized changes to BES cyber assets could occur.

NERC CIP-007, *Systems Security Management* requires a process for assessing, tracking, and installing cyber security patches on BES cyber assets. Utilities must operate their patch management process every 35 days to avoid non-compliance penalties. Given the high volume of devices and applications this standard affects, efficient monitoring and control practices are critical. Commercial patch management that addresses CIP-007 requirements is available that provides a seven-day turnaround and can be a valuable solution for overwhelmed OT/IT resources.

Compliance with NERC PRC and NERC CIP requirements would benefit from some form of automation to offload burdens from personnel who already have heavy workloads. The optimal scenario is central management from an integrated platform of software systems that can track data from front-end testing and maintenance activities to protection system engineering to back-end compliance and cyber security processes.

Ultimately, PRC requirements come down to assurance that protection systems will operate as intended to maintain reliable power delivery on the BES. NERC mandates that utilities ensure their relay settings are reviewed and that they are properly coordinated across the grid.

Protection engineers must demonstrate consistency and thoroughness in all aspects of the settings development and deployment process. Personnel who test relays must maintain cyber secure measures while entering substations and performing work on substation networks. When they test relays — cyber assets — they have additional responsibilities to defend against cyber attacks while ensuring relays are properly set and correctly functioning.

NERC CIP requirements affect PRC compliance activities by requiring TCAs to be used by field crews. Additionally, the software P&C personnel need on their TCAs must be patched and monitored regularly, and the TCAs themselves must be tracked.

An integrated management platform must support the monitoring and patch management of testing software used in the field on TCAs. It must also handle power system model data and relay settings lifecycle changes generated by protection engineering teams. It should offer modules for connecting P&C data to enterprise asset management (EAM) systems, even offering specialized P&C work management components that augment EAM workflows. It must also provide straightforward, configurable reporting in all aspects for any stakeholder.

The platform must be supported by a relational database that can offer structured data for linking to external systems. Utilities working with a supplier to implement an automated central management system have the opportunity to look at existing processes and shed inefficient or unnecessary practices.

Through a consultative implementation process, utilities can harmonize different data from various sources and for different stakeholders into a modern way of working that benefits all parties:

- Field crews will operate with the applications they need and use TCAs seamlessly with test equipment and relays.
- Protection engineers will have templates that standardize settings development and will seamlessly flow settings data into power system models for efficient coordination studies.
- Compliance officers will have dashboards and simplified reporting.
- OT/IT personnel will have lower administrative burden.

CONCLUSION

Effective NERC compliance programs are those that enable utilities to achieve objectives. Right now, the benefits of substation automation and renewables are becoming tangible, but digital protection systems and the effects of inverter-based generation on the BES need workers' focus to overcome these complex issues. Compounding the complications they already face with inefficient compliance program operations can prevent modernization from happening. Utilities that work from a culture of NERC compliance and have the proper tools to do their jobs are in the best positions to avoid financial penalties from non-compliance and overcome the uncertainties of technological and regulatory changes over time.

__Bryan Gwyn, PhD, CEng__, is the senior director of solutions at Doble Engineering Company where he brings strategic leadership to engineering teams in protection system and cyber security subject areas that advance new product and service offerings for the global power delivery marketplace.

__Sagar Singam__ is a cyber security engineer with Doble Engineering Company where he performs consultative professional services in the delivery of Doble PatchAssure™ and Doble TCA Program™ cyber security solutions.

__Joe Stevenson__ is a product marketing manager with Doble Engineering Company where he develops marketing strategies and materials in support of Doble protection software including Doble PowerBase™, Doble Protection Suite™, and Doble RTS™.