



Automating NERC Compliance with Tripwire Enterprise



The North American Electric Reliability Corporation (NERC) is a nonprofit corporation chartered to ensure that the bulk electric system in North America is reliable, adequate and secure. As the federally designated Electric Reliability Organization (ERO) in North America, NERC enforces comprehensive reliability standards for planning and operating the collective bulk power system. Among these are the Critical Infrastructure Protection Cyber Security Standards, commonly referred to as the NERC-CIP Standards 002-009, which are designed to ensure the protection of the “Critical Cyber Assets” (the computers, servers, networks and devices etc.) that control or affect the reliability of North America’s bulk electricity systems. How to routinely and economically meet these requirements has become a pressing issue for IT organizations working in every sector of the North American energy industry.

“NERC has taken an important step toward delivering on the promise of maintaining full grid reliability. We are counting on active NERC compliance audits to assure these standards are vigorously implemented.”

— Pat Wood, III
Chairman, Federal Energy
Regulatory Commission

In 2006, the Federal Energy Regulatory Commission (FERC) approved the Security and Reliability Standards proposed by NERC, making the CIP Cyber Security Standards mandatory and enforceable across all users, owners and operators of the bulk-power system.

COMPLIANCE TIMELINE

NERC CIP standards and guidelines apply to all entities within the bulk-power system. The timeline for the implementation of NERC critical infrastructure protection controls follows a phased approach designed to structure the implementation and ensure compliance. The timeline is broken into four phases:

- Phase One (also called “BW” or “Begin Work”). In this phase, the entity must

have developed and approved plans, scoped resources and must have begun implementation of plans.

- Phase Two (also called “SC” or “Substantially Compliant”). In this phase, the entity must be well along in its implementation plan but not necessarily fully compliant. Most bulk electricity entities were required to be substantially compliant by Q2 of 2008.
- Phase Three (also called “C” or “Compliant”). In this phase, the entity controls must have met the full intent of the requirements and is beginning to maintain required audit artifacts. Most bulk electricity entities must be compliant by July 1, 2009.

SOLUTION BRIEF

“Tripwire is very reliable at detecting changes made to our production systems; therefore we can audit our Change Management process, provide accurate reports for compliance, ensure all end users are following standards and procedures, as well as back out any changes that caused a detrimental effect to our environment!”

— Jennifer Ackley
Senior Systems Administrator, Georgia System Operations Corp.

- Phase Four (also called “AC” or “Auditably Compliant”). In this phase, the controls in place within the entity must meet the full intent of the requirements and can demonstrate this to an external auditor, including a minimum of twelve months of audit artifacts. Most bulk electricity entities must be Auditably compliant by July 1, 2010.

Compliance milestones depend primarily on the type of responsible entity; some entities were required to complete the first phase of NERC implementation by June 2008; others have until June 2009 or June 2010. The rollout timeline also is specific to the CIPs themselves. Although some organizations may not yet require a NERC audit, if a breach is discovered daily fines can be levied—including retroactively. Also, organizations are expected to notify NERC if there is a compliance breach, even if they have not yet reached the date for regular NERC audits.

FINANCIAL PENALTIES

Due to the importance of securing the North American power supply, financial penalties for

NERC non-compliance are hefty—entities can be fined up to \$1 million per day until they have brought themselves back into a compliant state. Although NERC audits are regularly scheduled, additional NERC audits can result if there is a power outage or other incident. Therefore, many entities are taking a proactive approach to NERC compliance, ensuring compliance not just for isolated audits, but also file integrity monitoring with change detection to ensure continuous and uninterrupted NERC compliance.

SCADA SYSTEMS AND THE CHALLENGES OF NERC COMPLIANCE

The NERC CIPs are very detailed and prescriptive configurations. If implemented manually, energy organizations would have to spend countless man-hours bringing their systems—including mission-critical SCADA systems—into compliance. Even if compliance is achieved through manual efforts, configurations have a tendency to “drift” over time, causing the same systems that once passed an audit with flying colors to slip back into a

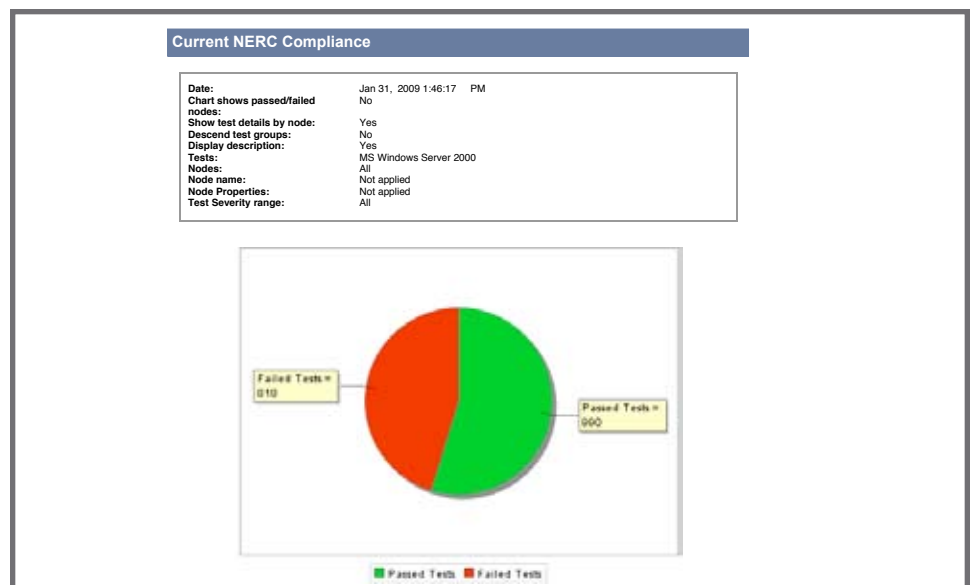


Fig. 1 Tripwire Enterprise gives you a clear graphical representation of the state of your NERC compliance efforts, plus all the details you need to remediate “drifted” or out-of-bounds configurations.

SOLUTION BRIEF

“With compliance issues driving our IT structure, Tripwire assists us in our transition to compliance with reliable reporting and auditing.”

— Jennifer Ackley
Senior Systems Administrator, Georgia System Operations Corp.

non-compliant state. Worse, the systems are then left wide open to malicious and potentially devastating attacks.

To complicate this situation many SCADA vendors are reticent to allow monitoring software to be installed on their devices in the field, citing potential conflicts and threatening cancelation of warranties and support contracts if the software is installed. This unfortunate no-win situation is often the starting point for discussions aimed at getting operational systems into alignment with the NERC CIPs.

Tripwire believes that every player in the game brings their own expertise. Tripwire’s is security, an area in which SCADA systems have been consistently flagged. A report by Sandia National Laboratories titled “Sustainable Security for Infrastructure SCADA” outlined some of the difficulties inherent in making SCADA systems adhere with NERC CIPs when it stated, “Security for SCADA is typically five to ten years behind typical information technology (IT) systems because of its historically isolated stovepipe

organization.”¹ But Tripwire believes these challenges can be met by combining our deep experience in file integrity monitoring with the domain expertise of SCADA vendors. This may in fact be the only way to deliver a win-win in which these systems become fully integrated into enterprise ecosystems.

AUTOMATING NERC COMPLIANCE WITH TRIPWIRE ENTERPRISE

Tripwire helps ensure that configurations continuously meet CIP Cyber Security requirements, while providing the required audit trail for changes. In fact, only Tripwire® Enterprise software combines powerful configuration assessment against NERC policies with the continuous compliance of change auditing. These two powerful technologies work together to ensure that your organization remains secure and NERC-compliant at all times—regardless of when your next audit might be.

The Tripwire Enterprise solution helps automate the requirements and sub-requirements in CIP 005, CIP 007, and CIP 003-6. The enterprise-class features of Tripwire

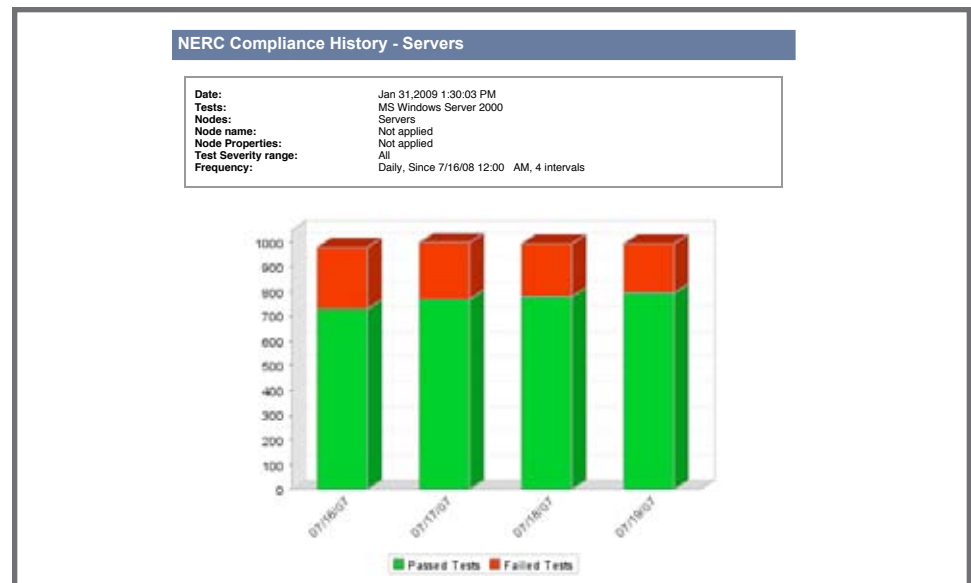


Fig. 2 “You can’t manage what you can’t measure.” Tripwire Enterprise enables historical comparisons of compliance by servers, nodes, or device groups, tracking your ongoing efforts to achieve and maintain NERC compliance.

include centralized management, drill-down reports, and the ongoing and automatic generation of audit artifacts. Tripwire provides powerful change management, patch management, and configuration management auditing to detect all changes, making sure your systems stay in known and trusted configurations. It continuously monitors the security status of your infrastructure, automatically correlating security events and providing meaningful reports. Tripwire minimizes human error, automates repetitive tasks requiring minimal manual effort, and gives you continuous confidence in the security and compliance of your critical systems.

Tripwire's NERC solution helps you:

- Automate NERC compliance. Tripwire rapidly assesses your environment, matching your configurations against the configurations mandated by NERC's CIP Security Standards.
- Maintain continuous NERC compliance. Tripwire continuously monitors the state of your configurations, alerts you if any non-compliant change is made, and generates NERC-specific audit artifacts.
- Mitigate cyber security risks. Tripwire Enterprise monitors and reports on every change made across the data center regardless of source, detecting unauthorized change and non-conforming configurations to proactively discover and manage cyber security and NERC compliance risks.

HOW TRIPWIRE ENTERPRISE WORKS

Tripwire is a leader in providing configuration assessment and change auditing in order for

organizations to meet a broad range of security and compliance requirements. Leveraging an extensive background in policy mapping for dozens of industry and governmental regulations (including CIS benchmarks, DISA STIGs, and FISMA compliance), Tripwire's policy development team continuously builds and updates policies for the testing of IT configurations against the specifications required by industry and government regulations.

Tripwire Enterprise assesses critical systems against over 60 NERC CIP requirements. Through its built in remediation guidance an IT organization can quickly and easily bring their critical systems back into a secure and compliant state. From that point forward, Tripwire's change auditing continuously monitors your configurations, alerting you to change and ensuring that configurations remain in a known, trusted state.

Tripwire Enterprise assesses critical systems against over 60 NERC CIP requirements. Through its remediation guidance organizations can quickly and easily bring their systems into a secure and compliant state. From that point forward, Tripwire's change auditing continuously monitors your configurations, alerting you to change and ensuring that configurations remain in a known, trusted state.

With Tripwire Enterprise, organizations quickly achieve integrity of their IT configurations, effortlessly manage internal and external policy, and streamline continuous compliance with even the most stringent NERC requirements.

1. <http://www.tswg.gov/subgroups/ps/infrastructure-protection/documents/SustainableSecurity.pdf>



www.tripwire.com

ABOUT TRIPWIRE

Tripwire helps over 6,500 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency across virtual and physical environments. With its industry leading configuration assessment and change auditing software solutions, IT organizations achieve and maintain configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.