SAFE AND SOUND:

THE JOURNEY TO SUSTAINABLE NERC CIP COMPLIANCE AND UNITED STATES POWER GRID RELIABILITY AND SECURITY

Accenture Security

To improve the reliability and security of the U.S. power grid, the North American Electric Reliability Corporation (NERC) has created a series of critical infrastructure protection (CIP) standards. All U.S. bulk electric system (utility) owners and operators must comply.

These standards are applicable to multiple components of the bulk electric system, including generation, substations and energy management systems. They cover both physical and information technology security (cybersecurity). Achieving and maintaining CIP compliance is expensive, but so are the consequences of failing to do so. Unfortunately, the compliance processes that many utilities use are not fully sustainable, especially as NERC continues to publish new and updated standards. It is possible, however, to create a sustainable NERC CIP program that not only assures compliance, but also does even more to protect critical infrastructure assets from attacks.

MOUNTING THREAT LEVELS

Over the past several years, multiple cyber attacks on industrial control systems (ICS) have made domestic and international headlines. These examples illustrate the danger and impact of ICS cyber attacks on energy and utilities systems worldwide:

2007

Estonia: Serious attacks on the government ICS Network.

Brazil: Over three million people affected by attack on the world's largest iron ore producer.

United States: Controlled hacking experiment (Project Aurora) destroyed a diesel-electric power generator through remote control, raising public awareness of the possible impact to critical infrastructures.

2008

Multiple countries outside the United States: Extortionists attacked overseas electrical utilities in multiple cities, demanding payments prior to the disruption of power.

United States: Energy entity hired a "penetration-testing consultant" whose actions impacted operations and exposed the company's internet connectivity as a key vulnerability.

2010

Iran: Stuxnet computer virus covertly inserted into ICS equipment that was running more than 1,000 nuclear uranium enrichment program centrifuges, causing destruction and major political consequences.

2011

United States, Greece, Kazakhstan and Taiwan: Night Dragon Trojan attacks targeted and assumed remote control of ICS at major global oil, petrochemical and energy entities.

Australia: Disgruntled former employee initiated cyber attack on ICS controlling a wastewater facility to convince the water treatment company to employ him to "solve" the problem he had created.

2012

Saudi Arabia: Shamoon virus infected more than 30,000 ICS at Saudi Aramco, erasing all of the data on computer hard drives and resulting in serious and irreparable damage.

Middle East: Flame virus with cyber espionage capabilities stole large amounts of data (believed to have been active for approximately two years prior to detection).

2013

United States: Snipers firing on a California electrical substation knocked out 17 giant transformers, highlighting the risk and severity of physical attacks on an electric entity.

2014

United States, Canada and Europe: Energetic Bear (Dragonfly) cyber espionage campaign used various malware to infect multiple ICS at energy, aviation and defense companies.

2015

Worldwide: Multiple cyber attacks on power grids, including control center lockouts, and ransomware attacks requiring payment in order to regain control of ICS used by utilities.

Ukraine: Sophisticated attack impacted almost a quarter of the country's power grid, through reconnaissance, customized malware and help desk denial-of-service attacks.

OVERCOMING NERC CIP CHALLENGES

Whether through cyber attacks or some other source of disruption to its infrastructure, the U.S. power grid is at high risk of being targeted by a rogue entity or enemy nation. A successful attack could result in major power outages that would impact large populations for long periods.

Utilities invest a great deal of time and energy in interpreting NERC CIP standards and defining the policies, processes, roles and responsibilities and technical controls that the utilities must implement to assure compliance. In this context, some of the greatest challenges include:

- Categorizing assets.
- Identifying compliance requirements.
- Managing the collection of evidence.
- Identifying where gaps exist.
- Ensuring robust management and reporting on those gaps.
- Defining and executing prioritized remediation plans to address the gaps in a consistent and timely fashion.
- Documenting auditable results.

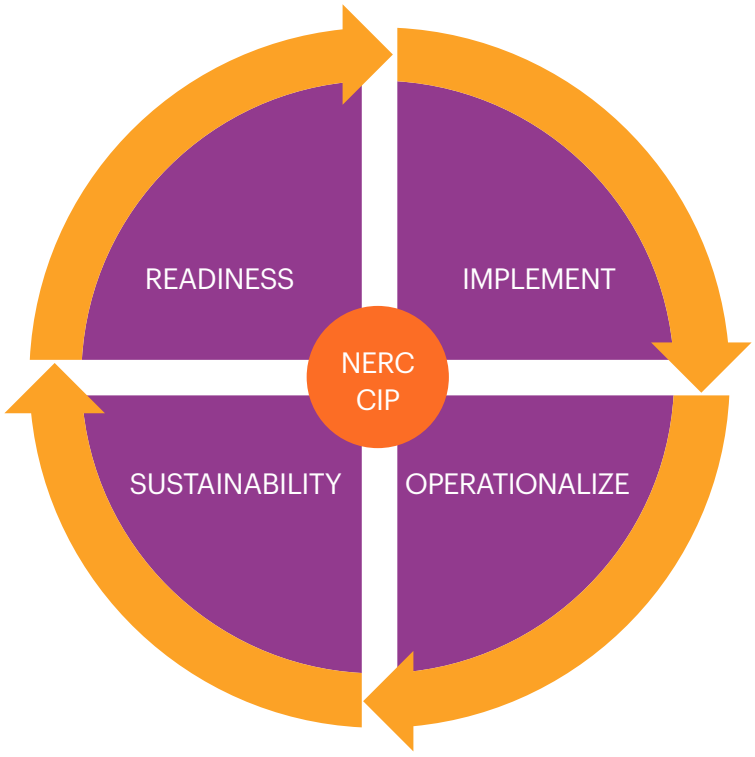
Overcoming these challenges requires a continuous cycle of activities that can be called a "life cycle of sustainability." It begins with a readiness phase, in which the utility assesses and prepares for ever-evolving standards, including updated and newly approved standards. Understanding the impacts of these changes, the timeline for enforcement and their potential implications is fundamentally important in staying a step ahead. The implementation phase follows, which includes planning and delivering the program of work and bringing together a broad set of security and compliance skills combined with deep industry knowledge.

The next phase is operationalization, which is about putting in place the people and processes to maintain protective controls, the auditability of these controls and the collection of evidence. The fourth phase is sustainability. It includes streamlining and industrializing processes and procedures to bring down the cost of maintaining compliance and ultimately increase the reliability and security of the grid through effective and consistent application of controls, in addition to highly repeatable compliance and audit processes.

Life Cycle of Sustainability

Preparing for ever-evolving standards.

Version 5, 6, 7 and beyond.



Delivering the program of work.

Bringing together a broad set of cyber skills, combined with deep industry knowledge.

Streamlining and industrializing processes and procedures.

Bringing down the cost of compliance.

Putting in place the people and processes to maintain security and reliability.

Keys to overcoming identified CIP challenges:

Repeatable process engineering (automation and integration), which can make exception management, evidence collection, validation and reporting both repeatable and automated. Escalations can also follow an automated protocol that alerts the enterprise when exceptions are due to expire and remediation plans are overdue.

On-demand services, which can flex up and down to provide optimal management of operational costs and overheads. While CIP controls require ongoing oversight, many compliance activities are periodic (for example, access and authorization reviews, cybersecurity vulnerability assessments, incident response planning and recovery planning) that drive peaks and troughs in the skillsets and resources required to maintain NERC CIP controls effectively. Using on-demand services enables utilities to focus their people on core roles and responsibilities and drive significant cost efficiencies by avoiding the need to staff for peaks permanently.

The right steps bring multiple benefits:

- Significantly decrease the time and effort required of staff members across the business.
- Allow staff members to focus on their core responsibilities.
- Deliver consistent compliance data that will prevent potentially large fines for non-compliance.
- Ensure that utilities can sustainably remain compliant, and provide evidence of compliance, even in the face of changing and new standards.
- Eliminate the need for intense, costly and time-consuming manual processes by replacing them with automated, integrated processes and on-demand services that ramp up and down as required.

Many utilities have established NERC CIP compliance by working in a piecemeal, reactive fashion—viewing standards and controls in isolation, building compliance and reporting solutions incrementally. Such processes are highly unlikely to lead to sustainable solutions.

Building a comprehensive, sustainable, repeatable and automated evidence management approach as an afterthought is also unlikely to be successful. In fact, it's more likely to lead to expensive, time-intensive and fragmented activities. Worse still, it could result in pockets of non-compliance.

By taking a more proactive approach—instilling consistent processes and approaches across the full CIP life cycle—more strategic and sustainable controls can be planned for and implemented from the outset, therefore avoiding the need for expensive retrofitting or replacement in the future.

REACHING OPTIMAL PROTECTION

Utilities find themselves at various stages along a CIP maturity curve that ranges from merely maintaining compliance with NERC CIP standards, to the more mature position of achieving sustainability and automation, to the optimal level of implementing advanced security for high-risk assets.

A series of clear steps can lead utilities along the maturity curve to a point at which they not only maintain compliance as efficiently as possible, but also experience business benefits beyond avoiding expensive penalties and negative publicity. Such benefits can include greater operational control, improved situational awareness, reduction of risk, better control of operations and maintenance costs, better preparedness for future disruptive technologies and most importantly, stronger power-grid protection.

Understand the current posture. Utilities should diagnose their NERC posture through an analysis of their processes and controls. They must develop an in-depth understanding of the audit trail before engineering an end-to-end process to obtain required evidence of compliance.

Establish a sustainability strategy and governance framework. It should include determining which staff members' roles and responsibilities include assessing the impacts of inevitable, new standards on an ongoing basis.

Establish an actionable plan to build the foundational components of a sustainable program—one that will underpin automated and repeatable processes and evidence collection for compliance demonstration.

Begin industrializing key NERC CIP processes. Initially target high-value areas, which are those shown by an assessment to pose the greatest need for manual efforts.

After a utility has put in place a sustainable program for managing compliance, and the principles and practices of physical and cybersecurity permeate the enterprise, it can begin the journey to advanced security for high-risk assets.

ADVANCED SECURITY: BECAUSE COMPLIANCE ALONE DOESN'T ENSURE PROTECTION

Attackers routinely breach infrastructures and systems that are 100 percent compliant with regulatory standards. Truly protecting the power grid—and the American people—requires more than regulatory compliance.

For example, a manual process that tracks access authorizations might meet CIP standards, but because it relies on human intervention, it's prone to stagnation and errors. An automated identity—and access—management system is an example of advanced security that provides better protection.

Another example is security monitoring. Simply logging security events from devices might comply with current standards. Greater protection requires a security monitoring system that integrates with a broader cybersecurity operations center. It also requires a security-information-and-event-management (SIEM) platform that correlates operational technology and information technology events. The result is automatic alerting of cybersecurity analysts to any sequence of related events that might indicate a wider breach.

Advanced security requires a concept of operations that spans the entire business and takes into account the processes, procedures, stakeholders (and their responsibilities), tools and technologies that underpin the NERC CIP program. It also requires the collaboration of physical security and cybersecurity stakeholders and making security intrinsic to every area of utility operations.

> **Advanced security requires a concept of operations that spans the entire business.**

CONTACTS

James Wright
Senior Manager | Accenture Security
Utilities Cybersecurity
j.a.wright@acccenture.com

Brian Walker
Managing Director | Accenture Security
Utilities Cybersecurity Leader
brian.d.walker@accenture.com

Michael Rossman
Managing Director | Accenture Security
Utilities Cybersecurity
michael.rossman@accenture.com

Jim Guinn, II
Global Managing Director | Accenture Security
Energy, Mining, Chemicals & Utilities
james.s.guinn.ii@accenture.com

Michael Rogers
Senior Manager | Accenture Security
Utilities Cybersecurity
michael.p.rogers@accenture.com

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

Copyright © 2017 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.

CONTRIBUTORS

Alex Habre
James Wright
John Fridye
Michael Rogers
Michael Rossman
Sergio Martinez
Terry Bjerken
Thomas Duffey

FOLLOW US

@AccentureSecure

https://www.linkedin.com/company/accenture_security

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 394,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.