SIERRA ENERGY GROUP
Market Intelligence and Research Solutions

A division of ENERGY CENTRAL

Author/Editor
Warren B. Causey
VP, Sierra Energy Group

Dealing with NERC/CIP standards – a new ballgame

Prepared for:

Microsoft

Table of Contents

Executive Summary

Dealing with regulatory reporting is nothing new for utilities. However, the new North American Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) standards, which have been given the force of law by the Federal Energy Regulatory Commission (FERC), have presented a whole new ballgame. They are extensive and are backed by audits that can be enforced with fines of up to $1 million per day for utilities found out of compliance.

The NERC-CIP standards touch virtually everything utilities do with computers related to the operation of the grid, data collection and data dissemination throughout the enterprise. As such, it is an added burden on employees, especially IT (Information Technology) staff members and others who are not accustomed to dealing with regulations and regulatory reporting.

Since this expanse of regulation is new in the utility industry, many utilities are at a loss for how to deal with the new requirements. Many are struggling to establish a direction or are taking a "wait and see" attitude until there is more clarity around the still-evolving regulations. However, the wait and see approach won't work much longer as the first of the standards go into effect in the second half of 2007 and then deployment accelerates through 2010.

Many companies, that serve the industry, are stepping up to fill the solutions void using Microsoft technology to address the NERC-CIP standards. Six companies that already have software available to help utilities address these standards are profiled herein.

Because of Microsoft's ubiquity in utility enterprises, its enabling technologies and architectures are making it easier, and faster, to develop the necessary solutions to deal with these new requirements.

NERC-CIP standards are a new ballgame

Utilities have had to deal with regulatory compliance almost since they were invented by Thomas Edison more than 100 years ago. However, the new North American Reliability Corp. (NERC) Critical Infrastructure Protection (CIP) standards are a new ballgame due to the complexity of the reporting and auditing requirements as well as their reach within the utility organization. Only Sarbanes-Oxley regulations, which were the previous high-water-mark for complex, intrusive regulation among utilities, come close to what utilities will have to accomplish in order to deal with NERC-CIP.

When the Federal Energy Regulatory Commission (FERC) named NERC the Electric Reliability Organization (ERO), NERC's role in setting standards rose in importance, notes Gerry Cauley, vice president and director of standards at NERC, which is based in Princeton, NJ. FERC standards now are mandatory, not voluntary, and fines ranging between $1,000 and $1 million per day can be imposed on utilities that violate those standards.

"It's our opportunity to put teeth behind what NERC was doing on a volunteer basis," says Rick Sergel, President and CEO of the organization. "Voluntary standards aren't enough and weren't getting the job done."

"Getting the job done" involves securing the North American grid from terrorist threats, as well as providing an overall boost to reliability to prevent blackouts such as those that have occurred periodically across the country. But the process is long, complicated and potentially very expensive for utilities.

This is not to denigrate the regulations or the efforts aimed at securing the computer and communications systems that increasingly control the electrical grid. An aging infrastructure, aging workforces, the threat of terrorism and other issues justify a close examination of utility cyber operations and assets. Those assets are indeed "critical" to the control, continuity and reliability of the grid, which is critical to the continuity and well-being of the United States and Canada-whose utilities also must comply with NERC-CIP. And, as utilities increasingly integrate their far-flung systems to work toward the goal of "Intelligent Enterprises" and "Intelligent Grids" in the future, cyber assets will become ever more critical.

"In the case of NERC, it isn't that utilities haven't had to deal with standards before," notes Mike Tobias, CEO of ember Corp., a Toronto, Canada, firm that specializes in risk and compliance productivity solutions. "The real issue is the specificity and complexity of it all."

In fact, there are eight new NERC-CIP standards, CIP-002 through CIP-009 that touch virtually everything a utility does, from generation and transmission through distribution and corporate operations. Included in these eight sets are more than 160 individual requirements which must be complied with, reviewed every year, and audited by NERC according to a staggered timetable that begins in 2007 and continues through 2010. This is in addition to the fourteen other classes of standards utilities must also comply with which contain nearly 1200 requirements. Documenting and demonstrating compliance with all of these requirements on an ongoing basis can be a truly daunting task unless a utility uses a rigorous approach and leverages technology to make the job easier.

A simplified listing of the broad standards categories, grouped by type, includes:

Electronic Security (CIP-002, 003, 005, 007, 009)

Under these standards, utilities must:

- Maintain an inventory of all electronics that either are part of the critical assets list or are necessary to the operation of critical assets.
- Protect access to these critical cyber-assets on a need-to-know basis.
- Create an electronic security perimeter that prevents unauthorized users from accessing any critical cyber-asset, whether they are outside or inside the corporate network.
- Ensure that all electronic cyber-assets are secure via user account management, equipment, password management, and secure networking policies.
- Implement and test a critical cyber-asset recovery plan.

Physical Security (CIP-006)

Utilities must ensure the physical security of all critical cyber-assets by:

- Ensuring that there is a physical security perimeter around all critical cyber-assets.
- All physical access points to critical cyberassets must be identified and controlled.
- An access log must be maintained for all critical cyber-assets, via keycards, video or manual log.

Personnel Security (CIP-004)

- Each person who accesses critical cyber-assets, including the utility's personnel, contract workers and vendors, must be investigated to assess the risk that he or she poses to security.

Training and Awareness (CIP-004)

- Everyone who has access to critical cyber-assets, including utility personnel, contract workers and vendors, must be trained in cyber-security.

Audits and Documentation (All CIP standards)

- All CIP standards make it mandatory to document and review all procedures and policies every year. NERC will audit compliance on all the standards on a schedule provided by the organization.

Recovery Plans (CIP-009)

The CIP standards make a recovery plan mandatory. The plan must include:

- Backup strategies
- Data restoration strategies
- Spare parts and equipment.

Obviously these standards affect virtually all parts of utilities and all facets of their operations and computer systems. And there are those stiff penalties of up to $1 million per day for failure to comply. It is a new ballgame.

Utilities are aware of the problem; the solution still may be a little elusive

Most utilities are in various stages of preparing for the CIP standards that go into effect in the second half of 2007. However, they are using a wide range of methodologies to get into compliance, according to interviews with various utility CIOs and others in the industry. "I don't think any one system has emerged and utilities are using an eclectic collection of software and tools to comply," said Ray Johnson, CIO at Entergy, New Orleans. Most other CIOs report a similar situation, according to Sierra Energy Group research.

"All of this is still very much in flux," agrees Jim White, chief security strategist at WiredCity, a subsidiary of OSISoft, San Leandro, CA. "The broadness of the standards lend themselves to a variety of solutions." White says he believes that "broadness of the standards" has caused both utilities and the vendors who serve them to look more closely at cyber architectures and assets and, "it's been a good push for the whole industry."

"A lot of people are dragging their feet and waiting to see what happens," says Tamar June, vice president, Strategic Marketing, with Assurx, Inc., Morgan Hill, CA "The whole NERC compliance issue is complex. Utilities don't have personnel in place to handle and manage it. We've been gearing up to provide that assistance."

"People involved in day-to-day operations at utilities have their own real jobs to perform," points out Andre Chon, principal and director at AUS Inc., a utility consulting firm in Mount Laurel, NJ. "NERC Standards are requiring employees to do extra things. The CIP standards are being tackled by IT people at many utilities, but most people in IT at utilities don't have a lot of experience in dealing with regulatory bodies. IT is running as fast as it can to try to comply with CIP standards and the rest of the company is trying to comply with the other standards. They're often attacking the problem separately with separate applications. At most of the companies I've talked to, people are doing this the old-fashioned way, with spreadsheets. Think of it as 160 (CIP requirements) plus 1,200 (other non-CIP requirements) separate on-going projects for which work has to be delegated, information collected, compiled, reported and audited. This puts a new and special burden on general employees."

Help is on the way

Despite the lack of continuity in utility efforts, however, a number of tools already have emerged, or are emerging, to assist with the process. These vendor-provided tools, like the utilities themselves, tend to attack the problem from different directions. However, a lot of them have one thing in common. Most of them are built on the Microsoft tools, (see additional information from Microsoft at the end of this white paper) architectures, operating systems and office software that utility personnel are already familiar with. That helps make them easier to deploy and use over the long run.

All of the companies mentioned in the previous section have developed new tools to assist utilities in complying with the new CIP standards and prepare for the upcoming audits. Others, including Subnet Solutions Inc., Calgary, Alberta, Canada, Assurx Inc., Flexnova, Cleveland, OH, Mentor Process Technologies, Houston, TX, also have developed tools and systems to deal with the CIP issue. What they all share in common, in addition to the use of Microsoft technologies, is that they all are Microsoft partners. Microsoft has worked with each of them to help enable their solutions and through them, Microsoft is working to help the utility industry deal with this new ballgame in a variety of different ways.

Many approaches, a common platform

The following more detailed look at the six companies mentioned above, and their NERC-CIP tools, will give a good idea of the complexity of the problem and the variety of the solutions, as well as the flexibility of the Microsoft enabling architectures and systems. Companies and their products are listed alphabetically in the following descriptions.

Assurx, Inc.

AssurX, Inc., Morgan Hill, CA, is a privately held company founded in 1993. Assurx has been offering an entirely browser-based quality management and compliance tool called

CATSWeb since 1998. CATSWeb is a flexible, all-in-one platform that automates quality management & regulatory compliance-related processes so issues can be globally managed from detection to corrective action to trend analysis. It helps collect, organize, analyze and share information to better manage and improve quality and compliance performance everywhere in the enterprise. Customers use the application to manage their manufacturing defects, customer complaints, corrective/preventive actions, regulatory issues, supplier quality, audits and findings, R & D problem reports, plus much more. CATSWeb includes analytical tools that help companies solve problems, and has proven to be instrumental in helping firms achieve and maintain ISO/QS 9000 certification and comply with the FDA's requirements for electronic records, electronic signatures and time-stamped audit trails (21 CFR Part 11). The CATSWeb application currently serves more than 300 companies with customers spanning a broad range of industries including medical device, pharmaceutical, energy, semiconductor, contract manufacturing, high technology, biotechnology, aerospace, telecom, as well as service industries such as finance and insurance.

AssurX now is offering CATSWeb-ER (Electric Reliability) to utilities for tracking and complying with the evolving NERC Electric Reliability Compliance Standards. CATSWeb-ER was developed in 2006 in anticipation of the Mandatory NERC Standards. It is built on Microsoft .NET technology and supports Microsoft Office and Windows SQL Server 2005. It is entirely a zero-client browser-based system. As more NERC Standards are released this year and the standards are updated, revised, etc., Assurx releases updates for CATSWeb ER to all customers automatically.

AUS, Inc./Flexnova

AUS and Flexnova are separate companies that work in close partnership with each other, as well as both being Microsoft partners. Founded in 1967, AUS specializes in financial consulting services to the public utility industry. Most of its work has been in the traditional rate-making process, testifying, rate design, cost of allocation and depreciation. Flexnova develops information worker solutions for the utility industry, focusing especially on business process enablement through the use of Microsoft technologies such as SharePoint and Office. AUS partnered with Flexnova to develop CaseWorks, a software system that is used by some of the nation's leading utilities to manage Rate Case, Regulatory and Public Policy Management processes.

AUS and Flexnova have now developed a sister application to CaseWorks called ComplianceWorks which is designed specifically to enable utilities to comply with all NERC and regional reliability standards, including the critical infrastructure protection (CIP) standards.

Key features of the software include:

- Coordinated management of compliance across all legal entities and functional roles.
- Relational database which serves as system of record for legal entities, functional roles and corresponding NERC and regional standards, requirements and measures, ISO tariffs, etc.
- Configurable tasks, roles and statuses.
- Automated task assignment and tracking based on regional and NERC audit schedules.
- Flexible and intuitive workflow for standards, requirements, measures and compliance planning.
- Automated audit preparation and submission of information to Regional Reliability Organizations (RRO's).
- Audit trails and automated document indexing, storage and retrieval.
- Ad hoc and canned reporting and statistics on all compliance management data.
- Ability to effective date the addition and deletion of functional roles and legal entities for historical reporting.
- Robust search capabilities.
- Ability to automatically populate workspaces and repositories with template forms, documents and folder structures.
- Ability to manage and view compliance information by voluntary, pending, approved or mandatory standards.
- Configurable event based notification and escalation processes.
- Ability to add/modify/delete navigational elements of the application to suit business needs.
- Ability to expand and collapse standard requirement sections and sub-sections for granular or aggregated delegation and reporting.

ComplianceWorks is built on Microsoft technologies including Microsoft Office 2007, Microsoft Office SharePoint Server 2007 and SQL Server 2005.

Ember

Founded in 1998 as a custom software development boutique, ember launched its first Risk and Compliance product, ember.HeatShield, in 2002. Since that time, ember has exclusively focused on providing Risk and Compliance Productivity solutions that reduce the cost and complexity of risk and compliance management while eliminating the mundane, tedious and repetitive tasks that are normally associated with compliance activities.

HeatShield leverages the capabilities of the Microsoft Office Suite, providing a holistic approach to Enterprise Risk and Compliance Management through low-risk, configurable, modular and iterative deployments.

"We have been watching the progress within the NERC Standards and Requirements process since early 2006," says Mike Tobias, "and we made a significant commitment to the Utilities market once it became clear that people were looking for help managing the growing burden of NERC compliance."

HeatShield for NERC offers the following capabilities:

- A pre-populated catalogue of all NERC Reliability Standards and Requirements, with an ability to add other Regulations and Standards.
- Automated Notifications, Compliance Workflows, and Documentation functions specific to NERC.
- Dynamic, Profile-driven Functionality and Reporting based on the user's Role and responsibilities in the organization.

- Automated, granular Audit Trails of all actions taken by anyone involved in meeting the NERC Standards.
- Real-time reporting based on rolled-up data from across the organization.

HeatShield is a pure Microsoft platform, utilizing SharePoint and SQL Server on top of a .NET architecture with integration to existing systems using XML and Web Services.

Mentor Process Technologies

Mentor Process Technologies™ (MPT) was founded in 2005 specifically to create an automated compliance solution for the electric power industry. MPT executives, including CEO Bill Addington, have a legacy of producing software solutions with a patent for intelligent software and the sale of two prior software ventures to Microsoft and America On Line.

The company's NERC compliance product is called Operations Mentor™ and was designed from the ground up to help electric utilities meet all the requirements of NERC CIP-002 through CIP-009 standards. Mentor includes hundreds of predefined automated processes that enable traceable compliance with the CIP standards, from assisting in defining critical assets and tracking critical cyber assets through helping manage recovery plans and training. Operations Mentor is designed to enable utilities to meet and automate the extensive documentation requirements of the CIP standard.

At the heart of Operations Mentor is the Intelligent Ramifications Engine™ which helps determine the direct and indirect effect of every change and ensures that tasks don't "fall through the cracks." Operations Mentor uses patent-pending technologies to link the CIP requirements to the workflows in Operations Mentor and then to the record of activities that prove compliance to the standard. Through automatic notifications, everyone in the organization with CIP responsibilities is notified of required tasks via the built in intelligence that guides users through the process.

Operations Mentor is an ongoing service as well as a product. Services include compliance update services, patch notifications, asset configuration updates, vulnerability notifications and security awareness alerts. Operations Mentor was released on May 1 after two and a half years of development.

Operations Mentor is built on top of MS Windows Workflow and SQL Server 2005 and uses Office 2007 with SharePoint as a document repository. It also uses MS Ident Server with add-on Centrify.

OSIsoft/Wired City

OSIsoft, founded in 1980 is best known for its PI System enterprise historians, as the core of its real-time infrastructure platform. PI System gathers real-time data from utility SCADA (supervisory control and data acquisition) and DA (distribution automation) systems. The company has a global client base of more than 11,000 installations across manufacturing, energy, utilities, life sciences and other process industries. The OSIsoft PI System is designed to safeguard data and deliver enterprise-wide visibility into operational health in order to manage assets, mitigate risks, and identify new market opportunities.

Wired City was founded in 1999 as a division of OSIsoft. Wired City has been working with a number of utility customers to focus on NERC-CIP requirements. Wired City's IT Monitor platform is used by utility customers to meeting the requirements of CIP 5, 7 and 8. IT Monitor enables monitoring of sign-on authorizations, perimeter device logs, network traffic, as well as other system parameters.

IT Monitor leverages the inherent capabilities of the Microsoft .NET platform and uses Microsoft's WMI, Performance Monitor and Windows Event Monitoring features in the product. IT Monitor also uses Microsoft's SharePoint for visualization of key performance and security indicators and is supplied with an

Excel add-in to aid in data analysis.

While all of OSIsoft's products are built on Microsoft platforms, they also can capture data from Linux and Unix systems.

Subnet Solutions

SUBNET Solutions Inc, based in Calgary, Alberta, Canada, is a software development and engineering services company. SUBNET Solutions has developed a solution that provides access control for utility employees so they can centrally manage access to IEDs (Intelligent Electronic Devices). For NERC-CIP requirements, utilities must be able to control user access to IEDs on a per-user basis.

SUBNET's solution uses Microsoft’s encryption capabilities, as well as Microsoft interfaces to authenticate tokens, smart cards, fingerprint scanners, etc. In many cases, utilities will need these capabilities not only for IT systems, but also for physical access and log-on to substations and other systems.

Conclusion

Obviously the NERC-CIP standards still are evolving and are likely to continue to do so for some time. This has put tremendous pressure on utilities and the vendors who serve them to develop procedures and systems for compliance. It's a matter of hitting a moving target.

However, as can be seen in the descriptions in the previous section, many Microsoft Partners are leveraging Microsoft technology to solve all or part of the problem. Because of Microsoft's ubiquity in the utility industry, it's natural for utilities and vendors to turn to MS enabling technologies to meet just the latest regulatory challenge faced by utilities.

Why Microsoft for Regulatory Compliance?

By Larry Kuhl, P.E., Utilities Solutions Executive, Microsoft Corporation

Recent corporate scandals and the increasing number and scope of compliance regulations have increased pressure on companies to effectively meet compliance requirements without bogging down business processes. Most companies recognize the importance and value of technology in the design and development of solutions for regulatory compliance, but they are challenged when it comes to mapping regulatory requirements to software implementations.

The ease-of-use and scalability of the 2007 Microsoft Office system includes built-in compliance features which enable organizations to address regulatory requirements without adversely affecting employee productivity. The 2007 release provides fundamental components required for regulatory compliance such as document and records management, versioning control, workflow processes, and auditing capabilities without ever leaving the familiar environment of Microsoft Office. These components and the system's extensible architecture have made it a favorite foundation for developing optimized solutions for regulatory compliance.

"We're tying in and leveraging some of the same corporate infrastructure from Microsoft that utility companies use to control what file and printer resources people have access to based on user name and password," says Subnet Solution's Hamdon (see Subnet Solutions section in main paper). We also are using the encryption capabilities that are part of Microsoft and tying in and leveraging Microsoft interfaces to authentication for RSA Tokens, etc. By using all these Microsoft technologies, utilities can leverage all these solutions not just for information technology, but for physical access, log-in access and other things."

The 2007 release is not only an application suite, it is also a full-featured development platform that is being exploited by developers for utility specific applications such as North American Reliability Corp. (NERC) compliance. With this release developers are building NERC compliance applications for collaboration, workflow, knowledge management, and business process automation with fewer lines of code than on other platforms. And utilities get a solution where users are immediately comfortable and productive due to the ease-of-use and users' familiarity with the most widely deployed desktop productivity environment.

In particular, 2007 Microsoft Office system lends itself to being a platform for powerful compliance solutions thanks to its advanced audit trail, encryption, information rights management, records and document management.. The 2007

Microsoft Office system includes desktop programs such as Microsoft Office 2007 and server based systems including: Live Communications Server, PerformancePoint Server, Project Portfolio Server, Project Server, SharePoint Server and SharePoint Server for Search.