

industry reports

79

Cyber Security Standards Under Review



NERC- the North
American Electric
Reliability Corporation

THE NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION'S (NERC) MISSION is to ensure the reliability of the bulk power system in North America.

To achieve that, NERC develops and enforces reliability standards; assesses adequacy annually via a 10-year forecast and winter and summer forecasts; monitors the bulk power system; audits owners, operators, and users for preparedness; and educates, trains, and certifies industry personnel.

NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. Learn more at www.nerc.com.

Multi-Phase Development Approach Will Address Short and Long-Term Goals.

by Kelly Ziegler, NERC, USA

Revised Phase I under review

As part of its efforts to better address cyber security and critical infrastructure protection, the North American Electric Reliability Corporation and its Cyber Security Standard Drafting Team have recently released phase one of proposed revisions to eight Critical Infrastructure Protection reliability standards for industry comment and review.

The standards (CIP-002 through CIP-009) are designed to ensure utilities and other users, owners, and operators of the bulk power system in North America have appropriate procedures in place to protect critical infrastructure from cyber attack.

Scheduled to be filed with regulatory organizations for final approval this spring, phase I revisions address a number of wording changes to the existing standards as specifically outlined in the Federal Energy Regulatory Commission's Order 706, released in January 2008.

Importantly, the proposed modifications to the standards address the directive in Order 706 to "remove references to reasonable business judgment (in the standards) before compliance audits begin in 2009." This phase also closes a key gap in the existing standards, specifying a compliance schedule for newly identified critical assets.

Phase II CS Standards

Work on Phase II has already begun and will result in more significant revisions which may change some of the philosophical foundations of the standards. These efforts will include a more thorough evaluation of the National Institute of Standards and Technology standards and risk management framework and their applicability to the bulk power system.

"Developing the multi-phase approach has enabled us to address pressing concerns around the existing standards in the short term while devoting the appropriate resources to thoroughly address more

complex revisions in the long term," commented Jeri D. Brewer of the United States Bureau of Reclamation, the Chair of the Cyber Security Standard Drafting Team. "We are firmly committed to drafting stronger standards that will better protect our continent's bulk power system infrastructure and achieving this goal on a schedule that will make these standards mandatory and enforceable promptly and effectively."

"These phase I revisions represent an unprecedented effort to improve existing standards in a short, two-month revision cycle and are evidence of the volunteer-based team's dedication to this important work," commented Gerry Adamski, Vice President of Standards Development at NERC. "We all recognize, however, that there is still much work to be done. I am confident that industry-based standards development process will meet the high expectations set out for this critical project and look forward to working closely with the drafting team as this project progresses."

The proposed modifications to the eight Critical Infrastructure Protection reliability standards are available at:

http://www.nerc.com/filez/standards/Project_2008-06_Cyber_Security.html.

The drafting team is comprised of 24 cyber security experts from across the electric industry. View the team members online at:

http://www.nerc.com/docs/standards/sar/Drafting_Team_Roster_External_Version.pdf

Get a high-level update on drafting team activities by subscribing to our e-mail notifications list. Send an e-mail to: subscribe-cipdt-info@listserv.nerc.com. Leave the subject and body of the message blank. ■

To comment -
visit NERC's web site.

IEEE PES Power Systems Relaying

A TECHNICAL COMMITTEE OF THE
POWER & ENERGY SOCIETY.

NOW BEARING THE TITLE C37.2 –IEEE STANDARD for Electrical Power System Device Function Numbers, Acronyms, and Contact Designations, this standard was perhaps the first substation configuration language when published by the American Institute of Electrical Engineers in 1928 as AIEE No. 26. It provided a means to describe, on an elementary diagram, the control and protection systems in automatic substations. Yes, even with just electromechanical relays, the control systems in these unattended substations could start and put on line rotary dc converters as the trolley or subway car loads grew (and take them off line in light load periods), detect dc overcurrent events and trip the affected 600 volt feeder. Then, based on the fault current's rate of rise, block reclosing for downed trolley conductors but reclose for slower rates of rise (most likely a misoperation by a motorman).

The standard has been revised and updated many times since its

original issue, and the 2008 revision was substantial. Of particular value to the users of IEC 61850 was the addition of a means to describe and document a communications network in a substation, even one with redundant communications elements. Added to IEEE C37.2 is a new device (Device number 16) defined as:

“data communications device - A device that supports the serial and / or network communications that are a part of the substation control and protection system.” Device number 16 is now used for data communications devices handling protective relaying or other substation communication traffic. The following suffix list identifies specific functions of a component identified as device 16. The first suffix letter must be either S (serial devices for RS-232, 422, or 485 communications) or E (for Ethernet components). The second and subsequent suffix letters may be one or more of the following letters to further define the device:

C - Security processing function [Virtual Private Network (VPN), encryption, etc.]

F - Firewall or message filter function

M - Network managed function [e.g., configured via Simple Network Management Protocol (SNMP)]

R - Router

S - Switch (Examples: Port switch on a dial up connection is 16SS, and an Ethernet switch is 16ES)

T - Telephone component (Example: auto-answer modem)

Annex B of the standard provides this additional information on the use of Device number 16 and its suffixes:

“In certain electric utility and industrial applications, data communications connections to protective relays are critical to the protection application. The data communications devices to which the relays connect are as important as auxiliary relays in protection system design and documentation.

For example, Ethernet local area networks (LANs) and wide area networks (WANs) are used for message transmission to carry out high-speed control and protection. A prime example for utilities is the use of IEC 61850 Part 8-1 GOOSE or GSSE messages in a substation Ethernet LAN environment to convey relaying element status, to provide interlocking, or to transmit a primary or backup trip command from one relay to another without conventional wiring. The Ethernet networks in substations are comprised of wired connections or fiber optic links, connecting protective relays and other IEDs in LANs based on managed Ethernet switches. The switch is, in fact, an elaborate message-processing computer with a list of settings that define how the protection messages are sent from one relay to another. Thus, Ethernet switches are the auxiliary relays for Ethernet-based protection and control systems. Furthermore, in some architectures, these substation LANs are connected to the utility

enterprise WAN via Ethernet router(s) with broad functional capabilities and configuration settings. The configuration settings impact remote access to relays for monitoring, control, data collection, and wide-area protection, and are critical in the implementation of data communications security. See IEEE Std 1615™-2007 for more information. Similarly, serial data communications devices are important for communicating with relays for fault data retrieval, settings access, configuration, and for condition monitoring as part of a formal maintenance program.”

The C37.2 standard includes example diagrams showing the use of Device 16 for a serial network, for an Ethernet network, and for a dual redundant Ethernet network. It should be noted that the Substation Configuration Language in IEC 61850-6 deals only with logical nodes (not physical nodes) in describing the communications between elements. In addition, it does not include such devices as Ethernet routers, switches, firewalls, etc. All are included in Device 16, as shown in this example diagram for a dual redundant Ethernet based substation protection system. It shows how dual redundant relays might be integrated with an Ethernet LAN connected to the utility enterprise WAN. Each of the linked Ethernet connections shown for System A and System B in the diagram comprises a pair of noise-immune optical fibers for conveying Ethernet message



The Power System Relaying Committee is in the Power & Energy Society of IEEE.

