utility horizons QUARTERLY

Automation Rising

Fourth Quarter 2013

The Digital Magazine of Automation & Information Technology for Electric, Gas and Water Utilities

Utility Automation & Information Technology...

PLAN...

DESIGN...

AUTOMATE...

ANNIVERSARY ISSUE

FOCAL POINT: Learn how Haiti is evolving to become a Smart Grid model for developing regions in our cover story, starting on page 16

By Wayne Hartmann | Protection & Smart Grid Solutions Manager | Beckwith Electric

The ABCs of CIPs

What the NERC-CIP Standards Mean for Automation

Intersections in Automation

Some prominent examples of DACs are load tapchanger, regulator, capacitor and recloser controls. The Responsible Entity (RE) – which in most cases is the utility – usually provides the overall system approach to meeting the NERC CIP requirements, which includes but is not limited to DACs, SCADA and various head-end computing, processing and data storage systems. Here's how the various sections break out and their relevance for the distribution automation environment…

◆ **CIP 001-2a, "Sabotage Reporting,"** defines methods, processes, and procedures for reporting any disturbances or unusual occurrences to appropriate authorities. Intrusion detection for DAC enclosures, combined with the ability of the DAC to provide unsolicited reporting of any enclosure intrusion to SCADA, help meet this requirement. The use of a Flash SD Card that functions as a cyber-security hard key with alphanumerical character passwords (multiple passwords for multiple users and roles) will help prevent unauthorized local access through the DACs keypad or HMI. In addition, an SD Flash Card can record and time stamp log-ons and log-offs, and access session duration for each event.

◆ **CIP-002-4, "Critical Cyber Asset Identification,"** mandates critical assets that use a routable protocol to communicate or that are dial-up accessible are identified when accessed. This can be accomplished with the RE keeping records of DAC individual model and serial numbers. These can be embedded on the DACs to provide positive identification of these assets. Additionally, the model and serial numbers can be electronically communicated to SCADA, engineering work stations, planning workstations, or any other entity deemed necessary as part of the cyber security protocol.

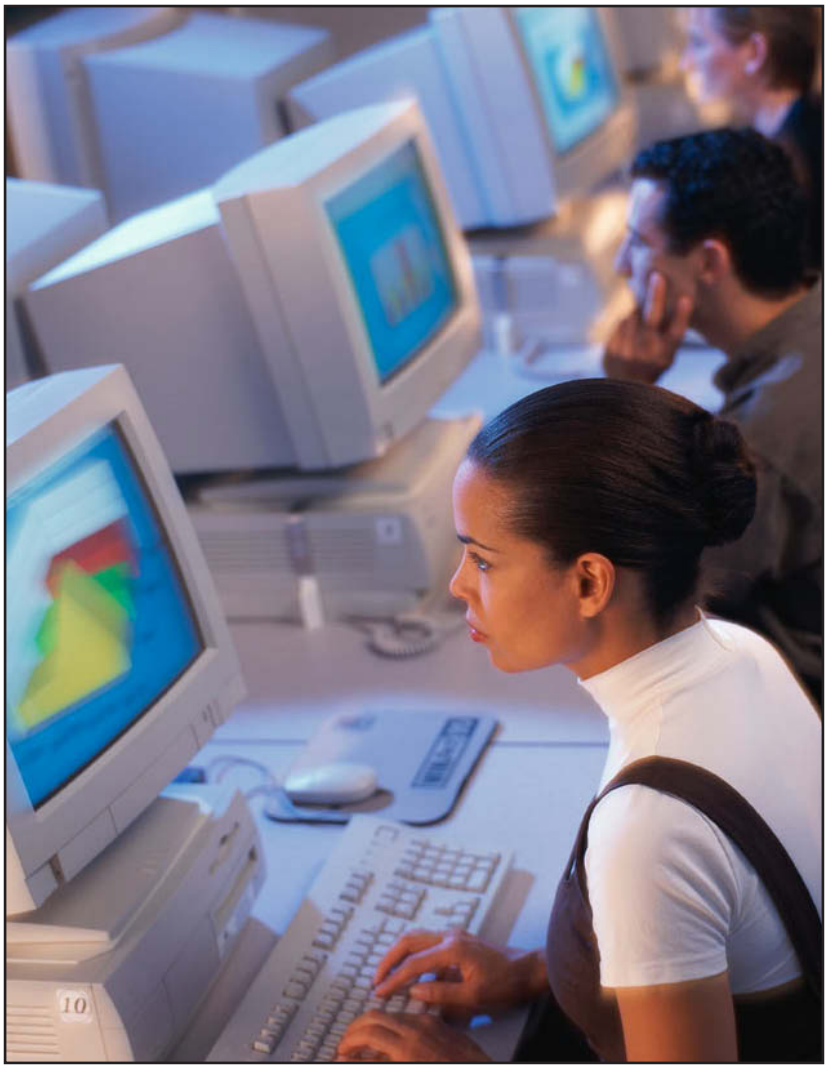
◆ **CIP-003-4, "Cyber Security – Security Management Controls,"** states requirements for the RE to document

As is the case across many critical industries and services, the bulk electric power system is subject to intrusion by unauthorized and often malicious attacks of a physical and/or cyber nature. As most utility practitioners now know, the North American Reliability Corporation (NERC) has developed Critical Infrastructure Protection (CIP) standards to meet the challenges posed by these threats and is responsible their enforcement across the electric utility marketplace.

In order to meet the NERC CIP standards, many elements of a distribution management system (DMS) must all work in concert. This article focuses in on certain of the CIP requirements and describes recent implementations available in modern distribution automation controllers (DAC) that form the field building blocks of many integrated DMS or SCADA interfaced applications and implementations.

Continued from page 57

and implement a cyber security policy to ensure protection of the Critical Cyber Assets. DACs can provide intrusion detection, cyber security "hard key" functionality using a SD Flash Card, multi-actor/multi-role alphanumerical passwords, logging of usage time, and recording of the model and serial number, all of which can be part of the procedural protection policy for protecting Critical Cyber Assets (CCA).



◆ **CIP-004-4, "Cyber Security – Personnel and Training,"** defines the requirements to properly create awareness of security precautions, training in security protocols, maintain a personnel risk assessment, and monitor the list of personnel with access to CCAs. DACs can provide intrusion detection, cyber security "hard key" functionality using a Flash SD card, multi-actor/multi-role alphanumerical passwords, logging of usage time at the control, and recording of the model and serial number. The RE would develop the training and awareness program to explain use of these security precautions and training in security protocols.

◆ **CIP-005-4a, "Cyber Security – Electronic Security Perimeter,"** defines methods, processes, and procedures for maintaining an Electronic Security Perimeter. DACs can use a Flash SD card for hard key access control.

◆ **CIP-006-4c, "Cyber Security – Physical Security of Critical Assets,"** defines methods, processes, and procedures for maintaining the physical security for CCAs. This is accomplished by the RE maintaining records of DAC access to help prevent unauthorized access. DACs can provide Flash SD card hard key access with multi-actor/multi-role alphanumerical passwords, logging of usage time at the control, and recording of the model and serial number. These would be employed as part of the RE's CCA scheme. Additionally, DAC user interface software can be used to download a log of each user's unique access code, date and time stamped, as well as recording the access duration time.

◆ **CIP-007-4, "Cyber Security – Systems Security Management,"** defines methods, processes, and procedures for securing CCAs within the Electronic Security Perimeter.

◆ **Subclause R2, "Ports and Services,"** states that only the ports and services required for normal and emergency operations are enabled. DACS can accomplish this by selectively enabling and disabling communication ports, and implementing communications session timeouts on selected ports.

◆ **Subclause R5, "Account Management,"** states the RE shall establish, implement, and document technical and procedural controls to

minimize risk of unauthorized use. DACs can help with this requirement by generating access logs to create historical audit trails of individual users. In addition, DAC access passwords may provide graduated capabilities to the assigned user in accordance to their roles. Capabilities limitations may be defined in levels, and by access location (remote or local). Example of such access definitions are:

◆ **Remote Communications:** Separate password to access unit with remote communications may be employed

- Level 1: Ability to read set points, monitor status, view targets
- Level 2: Level 1 capability, plus the ability to read/write setpoints, implement remote control, reset target history, set time, clear logs
- Level 3: Total access capability including changing all passwords

◆ **Subclause R6, "Security Status Monitoring,"** states that automated or manual alerts are created for CCA access occurrences DACs help meet this requirement by employing an enclosure access switch, logging of all users (local and remote), and initiating unsolicited reporting of any enclosure intrusion to SCADA.

◆ **CIP-008-4, "Cyber Security – Incident Reporting and Response Planning,"** defines methods, processes, and procedures for maintaining a plan to respond to Cyber Security Incidences. DACs help meet this requirement by using a Flash SD card as a hard key for multi-actor/multi-role passwords, logging of usage time, log in and log off times, recording of the model and serial number, and logging of date and time each access code was used.

◆ **CIP-009-4, "Cyber Security – Recovery Plans for Critical Cyber Assets,"** states the requirements for action plans for disaster recovery, including techniques and practices. These plans should establish the responsibility of responders and the backup and restore of system settings. DACs have the ability create downloadable backups of setpoints, configurations, settings logging, communication and cyber security settings

Although no single system or device can be expected to meet and provide all NERC CIP requirements, as part of integrated DMS or SCADA interfaced applications and implementations, modern DACs can provide a set of tools to help realize the overall goal of the CIPs – to prevent unauthorized and malicious intrusion so the reliability of the bulk power system can be maintained. uhQ

Author Profile

Wayne Hartmann is a broadly and deeply experienced power engineering and automation technology veteran, who is widely considered an expert in electric power protection and control and various other aspects of generation, transmission and distribution automation. Over the past three decades Wayne has conducted hundreds of formal and informal training classes, attended by thousands of suppliers, consultants, utilities and various other industry participants.

Wayne has performed in Project, Application, and Sales & Marketing Management capacities with Siemens Energy, Alstom T&D, General Electric and PowerSecure. He is presently a Smart Grid and Protection Solutions Manager for Beckwith Electric. Wayne is an IEEE Senior Member, serving on the IEEE Power System Relaying Committee (PSRC) as a Main Committee Member. He has also contributed to numerous IEEE Transactions, Standards, Guides, Tutorials and