Data Comm for Business, Inc.
2949 County Road 1000 E
Dewey, IL 61840
217-897-6600, FAX 217-897-1331
Outside Illinois: 800-4DCBNET
http://www.dcbnet.com

NERC Cyber Security Standards

CIP-005-2 Electronic Security Perimeter and the Security Modem

Overview:

CIP standards CIP-002 through CIP-009 may be met using standard DCB SCADA products along with proper management and procedural standards. System control centers and other designated facilities must be compliant or auditably compliant with the CIP standards by the end of the June, 2009.

The one instance where a special DCB product should be used in meeting CIP-005-2 section R2 is guarding the electronic security perimeter. This section requires strong procedural or technical controls at the electronic security perimeter access points. The DCB SM Security Modem is the product of choice to meet this requirement for modem connections to the public telephone network. While most DCB products are "CIP standard compliant", the standards also require adequate management and procedural standards to complete the compliance.

Applications for a Security Modem

There are often requirements for management access to remote equipment management or configuration ports. This is frequently accomplished using dial-in modems attached to routers for PPP connections, bridges for ethernet bridging, or directly connected to RS-232 management ports on SCADA equipment. The new CIP standards do not allow traditional dial in modems as this is considered . To meet the CIP standards, the modem must have strong procedural or technical controls to ensure authenticity of the accessing party.

SM Security Modem

The SM security modem functions as a standard dial-in/dial-out modem with enhanced features. These features provide the enhanced security and logging/audit ability required to meet NERC requirements. Features include comprehensive logging, one-time passwords, dial-back, and the ability to connect only to other SM modems with proper AES encryption Most of these features may be used in conjunction with each other, or for simplicity, unneeded features may be disabled.

NERC Cyber Security Standards CIP-002-2 through CIP-009-2
Although these standards contain some far-reaching concepts and are subject to differing interpretations, they are relatively straightforward to read and understand at the basic level. The following overview descriptions are the interpretation of DCB engineers and should be verified for applicability and correctness by the utility engineers.

CIP-002-2 - Critical Cyber Assets: This section is requires that all utilities must identify and enumerate the critical cyber assets that support reliable operation of the Bulk Electric System. This is purely an accounting and documentation process. Basically, it requires annually re-certifying to CIP-002 and keeping the documentation current. If the utility uses DCB products in a manner that supports the reliable operation of the Bulk Electric System (often considered to be the electrical transmission system), those products should be listed in the inventory. Obviously SCADA equipment and SCADA communications equipment fall in this category.

Data Comm for Business, Inc.
2949 County Road 1000 E
Dewey, IL 61840
217-897-6600, FAX 217-897-1331
Outside Illinois: 800-4DCBNET
http://www.dcbnet.com

CIP-003-2 – Security Management Controls: This requires that there be minimum security management control in place. That means that the officials who check and verify the controls are different people than those who authorize access. This is another management procedure control, and is not directly related to any DCB SCADA communications equipment.

CIP-004-2 – Personnel and Training: This standard requires that personnel with authorized access to critical cyber assets be well trained and that their training be documented. This is another management control not directly related to any DCB SCADA communications equipment.

CIP-005-2 – Electronic Security: This section requires the definition of an electronic security perimeter (ESP) around all all critical cyber assets. This security perimeter includes all externally connected communication end points terminating at any device within the ESP. It states that the utility must secure dial-up modem connections and implement procedural or technical measures to ensure the authenticity of the accessing device or application. This standard also requires that the utilities control the electronic access as well as the historical record on monitoring that access. There are additional management and procedural controls associated with this. DCB equipment that is declared to be the terminating point of the ESP falls within this standard and the SM security modem or ET ethernet tunnels are used to meet this requirement.

CIP-006-2 – Physical Security: This requirement covers the physical aspects of a physical security perimeter (PSP). There are both procedural, management, and physical aspects of this PSP requirement. This is another management procedure control, and is not directly related to any DCB SCADA communications equipment.

CIP-007-2 – Systems Security Management: This is another management program that requires audits of user activity and change control procedures as well as general management of the security aspects of their critical cyber assets. This is another management procedure control, and is not directly related to any DCB SCADA communications equipment.

CIP-008-2 – Incident Reporting and Response Planning: This standard requires that there be proper identification, reporting, documentation, and record retention of cyber security incidents. This is another management procedure control, and is not directly related to any DCB equipment.

CIP-009-2 – Recovery Plans for Critical Cyber Assets: This is another management requirement for recovery plans, business continuity, exercises and drills, and documentation of same. This is another management procedure control, and is not directly related to any DCB SCADA communications equipment.

References:
DCB SM-Security Modem: http://www.dcbnet.com/datasheet/smmodemds.html
DCB SCADA Products: http://www.dcbnet.com/products_scada.html#scada

FAQ for cyber security Standards CIP-005-1:
http://www.nerc.com/fileUploads/File/Standards/Revised_CIP-005-1_FAQs_20090217.pdf

Downloadable CIP standards and discussions from NERC:
http://www.nerc.com/filez/standards/Cyber-Security-Permanent-RF.html

NERC Implementation Plan Schedule:
hhttp://www.nerc.com/files/2009_NERC_CMEP_Implementation_Plan_final.pdf

NERC Electronic library of downloadable standards and discussions, probably the best resource for individual utilities:
http://www.nerc.com/elibrary.php