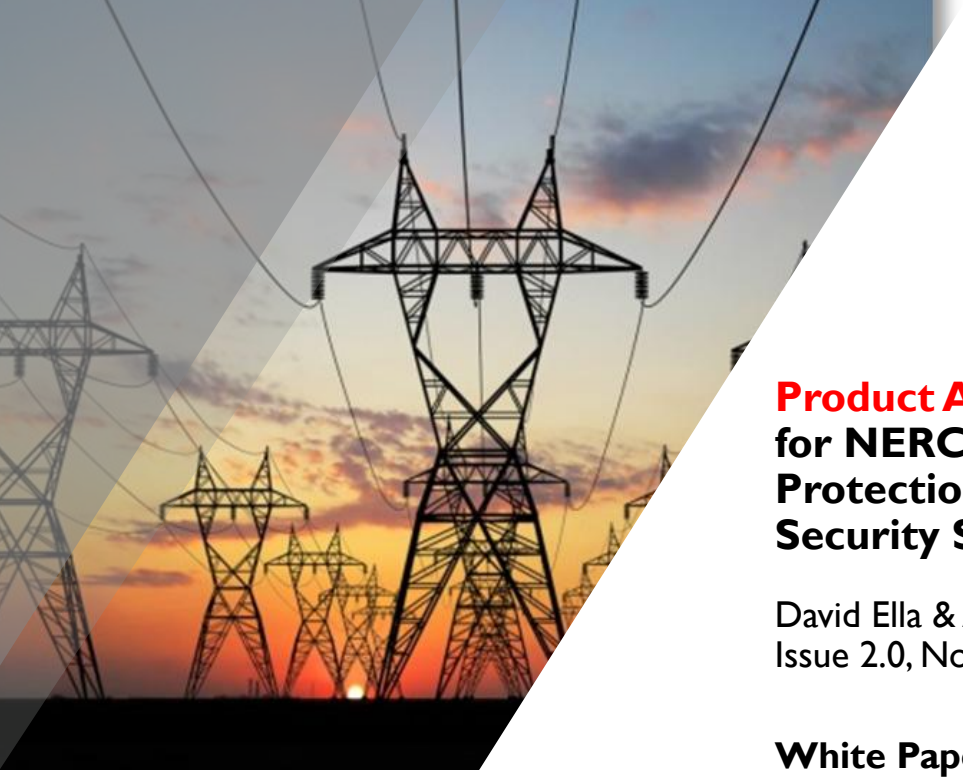

AMAG TECHNOLOGY
An ALLIED UNIVERSAL Company

Product Applicability Guide for NERC Critical Infrastructure Protection (CIP) Cyber Security Standards

David Ella & Adam Shane
Issue 2.0, November 2016

White Paper

The Symmetry Security Management System is a Physical Access Control System (PACS) and a significant component of the physical security measures used to secure the physical perimeter. This represents but one small part of the regulations imposed on the critical infrastructure that makes up the Bulk Electric Power System (BES) in North America. Symmetry provides functionality which enable conformance to the CIP requirements and can be used to further the efforts of BES producers and suppliers in documenting compliance.

EXECUTIVE SUMMARY

The North American Electric Reliability Corporation (NERC) has as its mission to ensure the reliability of the bulk power system in North America. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada. NERC develops, releases and maintains Critical Infrastructure Protection (CIP) Cyber Security Standards. Presently these cover the following topics:

- Cyber System Categorization
- Security Management Controls
- Personnel and Training
- Electronic Security Perimeter(s)
- Physical Security of Cyber Systems
- Systems Security Management
- Incident Reporting and Response Planning
- Recovery Plans for Cyber Systems
- Configuration Change Management and Vulnerability Assessments
- Information Protection
- Physical Security of Transmission Facilities

The Physical Access Control System (PACS) is a major component of the physical security measures used to secure the physical perimeter. The PACS runs on cyber assets (servers and workstations) and relies on the network architecture for communications. Therefore, the PACS is not only a system that must be identified for protection (as a non-critical cyber asset) but is also integral

in the solution developed by the Responsible Entity for protecting Critical Cyber Assets and transmission facilities.

Many facilities responsible for the generation or distribution of electric power through North America may also be regulated to comply with the Transportation Worker Identification Credential (TWIC) smart card program implemented by the US Government Transportation Security Agency (TSA). AMAG Technology has a long history of supporting US Government smart card credentials for physical access control. Support of the TWIC is another example of this. AMAG has deployed large scale systems that utilize the TWIC as well as local ID cards and biometrics.

This white paper describes how the proper installation and operation of a PACS from AMAG Technology will support the Responsible Entity in complying with the NERC CIP requirements. It should be noted that the PACS and services from AMAG Technology are not a replacement for sound security policies, but work in concert with best practices to bring the facility into NERC CIP compliance.

The paper is organized by the CIP requirement topics. Where the PACS offers a mechanism to meet the requirement, it is described in more detail. In this version of the white paper CIP requirements that are strictly based in policy or aren't otherwise supported by the PACS are not discussed in detail.

INTRODUCTION

The North American Electric Reliability Corporation (NERC) has as its mission to ensure the reliability of the bulk power system in North America. NERC is a self-regulatory organization, subject to oversight by the U.S. Federal Energy Regulatory Commission and governmental authorities in Canada. NERC develops, releases and maintains Critical Infrastructure Protection Cyber Security Standards. Presently these number from CIP-0021 through CIP-014 and are titled as follows:

CIP-002: BES Cyber System Categorization

CIP-003: Security Management Controls

CIP-004: Personnel and Training

CIP-005: Electronic Security Perimeter(s)

CIP-006: Physical Security of BES Cyber Systems

CIP-007: Systems Security Management

CIP-008: Incident Reporting and Response Planning

CIP-009: Recovery Plans for BES Cyber Systems

CIP-010: Configuration Change Management and Vulnerability Assessments

CIP-011: Information Protection

CIP-014: Physical Security

This white paper was originally based on Version 2 of the CIP standards, and over time was updated to include Versions 3 and 4. Version 5 of the existing standards were subsequently introduced, with an implementation date of July 1, 2016, and these have also been added. Additional standards have also been introduced, most notably the CIP-014 Physical Security standard which extended the standards to the physical protection of transmission facilities. The purpose of these various revisions and new standards has been to clarify interpretations and expectations and, in many cases, to strengthen the requirements.

The physical access control system (PACS) is a major component of the physical security measures used to secure the physical perimeter. The physical security perimeter is defined in CIP-006 as the 6-wall perimeter that encloses the cyber assets and the electronic security

[1] CIP-001 relates to Sabotage Reporting. It was in effect prior to the CIP-002 through CIP-014 standards and is not included in the current Cyber Security Standards.

perimeter. The PACS runs on cyber assets (servers and workstations) and relies on the network architecture for communications.

Therefore, per CIP-006 R2, the PACS is not only a system that must be identified for protection (as a non-critical cyber asset) and afforded all of the protective measures identified, but it is also integral to the solution developed by the Responsible Entity for protecting Critical Cyber Assets and transmission facilities.

CIP-014 is a newly implemented standard which relates to the physical security of transmission stations, sub-stations and their control centers. These facilities were largely outside the scope of the previous standards, and access control and video systems form one part of the physical protection of these assets.

Many facilities responsible for the generation or distribution of electric power through North America may also be regulated to comply with the Transportation Worker Identification Credential (TWIC) program implemented by the US Government Transportation Security Agency (TSA). AMAG Technology has a long history of supporting U.S. Government smart card credentials for physical access control. Support of the TWIC is another example of this. AMAG has deployed large scale systems that utilize the TWIC as well as local ID cards.

This white paper describes how the proper installation and operation of a PACS from AMAG Technology will support Responsible Entities in complying with the NERC CIP regulations.

AMAG SYMMETRY SECURITY MANAGEMENT SYSTEM

Symmetry is an enterprise level Security Management System developed by AMAG Technology, Inc. Symmetry combines building Access Control with various other capabilities which are relevant to the BES and the CIP standards. Key relevant elements include:

- Access Control to buildings and remote facilities incorporating smart cards and integration with biometrics
- Video Management through the advanced integration of alarms and access control events to Video Management Systems
- Alarm Management including integration with fence protection systems and intrusion alarm panels
- Identity Management through CONNECT which provides workflow-based authorization and identity and access control auditing
- Visitor Management through GUEST
- Audit and Reporting through Symmetry Advanced Reporting and Audit

CIP-002-5.1: BES CYBER SYSTEM CATEGORIZATION

In a change of emphasis from previous versions of the standard, the focus in Version 5 is now on systems rather than the individual assets which make up that system.

Per the standard, the purpose is to:

- Identify and categorize BES Cyber Systems and their associated BES Cyber Assets
- Commensurate with the adverse impact that loss, compromise, or misuse could have on the reliable operation of the BES

Facilities operated by Generation, Distribution and Transmission providers which meet certain criteria are impacted by this standard.

The Responsible Entity identifies and categorizes the Critical Systems. The Critical Cyber Assets are those components that are essential to the operation of the Critical Systems. The responsible entity determines the level of granularity with which these systems are defined

BES Cyber Systems have associated Cyber Assets which, if compromised pose a threat by virtue of the security control function they perform. These Cyber Assets include Physical Access Control Systems (PACS). Therefore, AMAG Symmetry is relevant to compliance with CIP-002-5.

For these reasons, the servers and associated workstations should be included in the list of assets that will be afforded the protective measures offered in CIP-006-6.

Certain hardware such as access control nodes, door controllers and input/output devices are used for data collection and interface to the environment but are pass-through devices without autonomous authorization or logging responsibility; and thus, these devices need not be considered cyber assets.

The Symmetry Security Management System uses access control panels with purpose-built firmware. There is no Operating System, and there is no anti-virus or malicious code detection software available for these hardware components. However, due to their purpose-built nature, they are not subject to traditional viruses, worms, Trojan horses, or other malicious network attacks. Additionally, there is no human user interface to these devices (they are strictly used for machine-to-machine communication).

AMAG Technology recommends that the correct control is to use network-based malicious code detection, equipment should be installed in a physically protected area (wiring closet or IDF), and that communications to these devices (where available) be encrypted thus providing the intended protections suggested in CIP-006-6.

CIP-003-6: SECURITY MANAGEMENT CONTROLS

CIP-003 requires that the Responsible Entity implement consistent and sustainable security management controls to protect BES Cyber Systems against compromise. The various requirements of this section include Cyber Security Policy, Leadership, Exceptions, Information Protection, Access Control, and Change Control and Configuration Management.

The Responsible Entity has a responsibility to review and gain approval of policies which include – for high and medium impact BES Cyber Systems - the Physical Security of BES Cyber Systems (CIP-006), and for low impact systems the Physical Security Controls.

Policies for high and medium impact Cyber Systems can be used for low impact assets or separate plans can be developed to control physical access based on need to the asset or the locations of the low impact BES Cyber Systems within the asset. Additionally, there is a requirements to protect Low Impact BES Cyber System Electronic Access Points (LEAPS).

Evidence for Physical Security Controls can include documentation of the selected access controls, monitoring controls (including alarms systems and human observation), or other operational, procedural or technical physical security controls that control physical access to the asset or the locations of the Cyber Systems or of cyber assets containing LEAPS.

R5, Access Control

Symmetry from AMAG Technology supports individual logon credentials for each operator. The logon credentials include a username and a password. Passwords can be made up of letters, numbers and symbols. Passwords can be up to 16 characters long, can be set to expire in a specified number of days, and to meet the NERC CIP requirements a strong password requirement can be enforced.

Within Symmetry a strong password is one that is case sensitive; has at least 6 characters; must have at least one lowercase character, one uppercase character, one numeric character and one special character. In addition, a password will not be able to contain any full word of the user's username.

The operator account is assigned to a specific role. The PACS supports various roles within the software thereby preventing a user from performing functions they are not authorized to perform.

The system comes with a small number of default accounts and roles. These can be deleted, or the passwords changed from their default to meet requirements of CIP-007. The default accounts are listed in the following table.

Table 1: Default Accounts

Default Account Name	Default Role Assignment
Installer	Installer
Manager	System Manager
Guard	Security Guard
Engineer*	
Administrator	Card Admin

*The Engineer account has special privileges in the system. It cannot be deleted but the password can be changed from the default.

Furthermore, a default role of "Visitor Management" is assigned to any cardholder that is enabled login to the visitor management system (this feature is disabled by default).

One of the requirements for Critical Cyber Asset Information (CCAI) protection is to set forth privileges for access. Symmetry enforces a role-based privilege model. Each operator logging into the system is assigned a personal account so that their activity in the system can be tracked and associated with the individual responsible for the activity. The account is assigned to a role within the system. The role is made up of a list of which capabilities and features in the system the operator is allowed to utilize.

The privileges are designated by None, View, Modify and Delete.

- "None", the operator will not be able to initiate or manage this feature,
- "View", the operator will be able to review the information already entered or report on these fields, but will not be able to modify or delete the data,
- "Modify", the operator can view and edit the data in question, but will not be allowed to delete the data,
- "Delete", the operator can perform any function allowed in the software with regard to that particular feature.

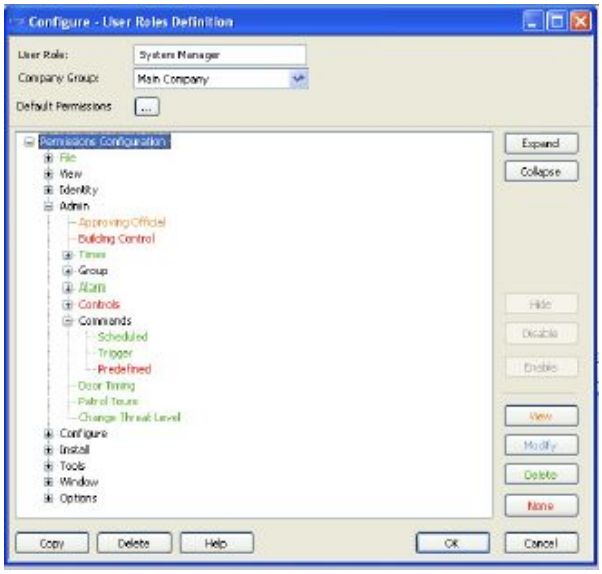

Figure 1: User Roles Definition Example

If the operator role is assigned the "None" designation, then generally the buttons are grayed out or not displayed on the screen. Data fields are not displayed. Therefore, the operator does not have an opportunity to attempt to make the change rather than reporting an error back to the operator when a disallowed function is attempted.

The System Manager, Installer and Engineer roles generally have the privilege enabled to modify the privileges of other operator accounts. Symmetry provides built in reports to describe privileges associated with defined roles in the system as well as a report to list all operator accounts and which roles they are assigned to.

CIP-004-6: PERSONNEL AND TRAINING

Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to BES Cyber Systems, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness.

Elements of the requirements of the standard which are directly applicable to physical access control and Symmetry include:

- Training content on physical access controls, incident identification and recovery plans for BES Cyber Systems (in this context the PACS) [R2]
- Recording of completion and current validity of relevant training before granting authorized unescorted physical access [R2]
- Repeat training at least once every 15 months [R2]
- Process to confirm identity and seven-year criminal record check (CONNECT) [R3]
- Personnel risk assessments for employees, contractors and service providers completed within the last seven years [R3]
- Process to authorize access to physical security perimeters and BES Cyber System storage locations (CONNECT) [R4]
- Verification at least once each calendar quarter that those with unescorted physical access have authorization records (Symmetry and CONNECT) [R4]
- Verification at least once every 15 months that user accounts, user roles and their privileges are correct, and that those with Cyber System storage locations are restricted to those with the necessary need to gain access (Symmetry) [R4]
- Process to remove access on termination within 24 hours and to revoke specific access no longer required on reassignment or transfer by the end of the next calendar day (Symmetry and CONNECT) [R5]

Compliance monitoring of the standard can include audits and self-reporting.

R3, Personnel Risk Assessment

Enforcement of time thresholds for access grants and revocation is essential for compliance. This area is one of the top violations of the standard being cited in the NERC spot checks. Symmetry can generate the reports necessary for inclusion in quarterly reviews to prove compliance.

Symmetry supports up to 50 customizable personal data fields. The fields can be configured to be mandatory and therefore must be filled in before the card record can be saved. These fields can be used to record, display, and report on CIP-specific information such as dates Cyber Security training and Personnel Risk Assessments (PRA) were completed. By including these records with the cardholder identity information in the Symmetry system, it enforces the validation of these dates prior to issuing access privileges. Symmetry can be configured to automatically inactivate card records or access rights based on dates stored in personal data fields.

In support of logging requirements, Symmetry supports procedures for the review of access authorization requests and revocation of access authorization through history and configuration reports that can be run as needed or on a scheduled basis. The optional Audit database can be used alongside Symmetry Advanced Reporting in order to retain full detail of changes made to access authorizations.

R4, Access

The physical security system is an integral part of compliance to this standard. The PACS can be used to prevent unescorted physical access to BES Cyber Systems unless authorization is provided. The PACS can be used directly to manage access control rights or can be used in conjunction with an Identity Management or other similar solution integrated with the Symmetry system (solutions covering IDMS, HR, Workflow/Policy Enforcement, and Compliance Management have been integrated). The policy manager tracks the training, clearances, and other requirements for each individual and if they are not in compliance to fulfil their function access rights can be automatically withheld.

The policy manager can also be used to document who has appropriate qualifications for access to BES Cyber Systems, and to manage the revocation of these privileges as necessary.

If the PACS is used directly to manage these privileges, then this system can also support the requirement to maintain a list of personnel with unescorted physical access to critical cyber assets. The PACS allows the operator to:

- Report on cardholder access filtered to only include a personal data title or reader group,
- Revoke access for terminated employee or change in responsibility,
- Maintain audit records for 3 years or longer as needed,
- Maintain online records from previous full calendar year (the amount of data required to be kept online will determine the database size). Symmetry Enterprise is recommended for facilities with this requirement.

CIP-005-5: ELECTRONIC SECURITY PERIMETER(S)

Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all BES Cyber Systems reside as well as all access points on the perimeter.

The standard goes on to require "any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005." Therefore, since the Symmetry PACS server resides within the Electronic Security Perimeter, it must be afforded the same protection as Critical Cyber Assets.

This standard does not specifically refer to physical security or physical access control systems at any point. However, this standard needs to be implemented in conjunction with all the other CIP standards which often refer to physical security and PACS.

R2, Electronic Access Controls

This requirement is specific to the network and the devices that a Responsible Entity installs to protect it (e.g., firewall, switch, router, electronic access control monitor). There are various aspects to this requirement and Symmetry may be used to support each of them in the following manner:

1. The software denies access to logon attempts by default. An active operator account and a correct matching password must be entered to gain access to the software.
2. Per this requirement, the Responsible Entity shall enable only ports and services required for operations. A list of ports and services used by Symmetry is included in the Appendix.
3. The Responsible Entity will have to implement and maintain a procedure for securing dial-up access. The Symmetry system supports dial-up access, but it does not have to be implemented.
4. Symmetry supports strong authentication as a technical control on access to the software. Since the Windows-based computers that the Symmetry software resides on also supports strong technical controls this combination provides the RE with many tools.

   The nodes (or access control panels) support TCP/IP through their NIC. The node does not provide an interactive interface and therefore is excluded from this discussion. The nodes do provide an option for password restriction.

   Additionally, encryption can be used to secure the information in transit. Encryption is available from Client to Server and from Server to field panel (when using appropriate network interface cards). Symmetry has received NIST FIPS 140-2 certification on the encryption subsystem.
5. The Responsible Entity is responsible for documenting the above procedures.
6. An appropriate use banner can be implemented at the Windows OS level by changing the wallpaper. Furthermore, this can be implemented on the logon screen for Symmetry by inserting the appropriate use text as a bitmap image (logo.bmp) in the Security Management System folder. The following figure provides an example.

R2, Monitoring Electronic Access

The nodes support TCP/IP through their NIC, but the node does not provide an interactive interface and therefore is excluded from this discussion. However, it may be useful to note that the node would temporarily cease communications with the communications service if an external attempt at communications was being attempted, and this break in traffic flow would be noted by the communications service. Furthermore, the node supports AES encryption which would be a further preventative measure.

CIP-006-6: PHYSICAL SECURITY OF BES CYBER SYSTEMS

Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of BES Cyber Systems. The Responsible Entity shall create and maintain a Physical Security Plan. Symmetry will be an integral part of the plan to demonstrate protection of all BES cyber systems, electronic security perimeters and the physical assets that are used to perform the cyber functions for proper operation of the facility and the business.

CIP-006-06 relates to Generation, Transmission and Distribution facilities which meet certain criteria set out within the standard.

Physical Access Control Systems such as Symmetry, and locally mounted hardware such as motion sensors, electronic locks and card readers are specifically included within the scope of the standard. However, it should be noted that perimeter devices that do not store access information or make access decisions are excluded from the definition of a PACS.

Elements of the requirements of the standard which are directly applicable to physical access control and are supported as standard features of Symmetry include:

- For Medium Impact BES Cyber Systems utilize at least one physical access control to allow unescorted physical access, including proof that physical access is restricted to only authorized individuals, accompanied by access logs [R1]
- For High Impact BES Cyber Systems utilize – where technically feasible – two or more different physical access controls including explanation in the physical security plan and evidence that such access is restricted only to authorized individuals, accompanied by access logs [R1]
- Monitor for unauthorized access through physical access points in perimeters for high and medium impact BES Cyber Systems [R1]
- Issue an alarm in response to detected unauthorized access through a physical access point in a secure perimeter to personnel identified in the incident response plan within 15 minutes of detection [R1]
- Monitor each PACS for unauthorized access to the PACS and issue an alarm to personnel identified in the incident response plan within 15 minutes of detection [R1]
- Log entry into each physical security perimeter with name, date and time [R1]
- Restrict physical access to cabling and components of High and Medium Impact BES Cyber Systems [R1]
- Require continuous escorted access of visitors [R2]
- Require logging of visitor entry into the physical security perimeter and retain logs for 90 days [R2]
- Maintain and test each PACS at least once every 24 months [R3]

Physical Security Plan

The Responsible Entity (RE) must document and identify the physical security perimeter (PSP). The PSP is a six-wall border surrounding the Electronic Security Perimeter (ESP). The Symmetry software supports the import of maps in various file formats that can be used to provide a graphical representation of the security system. The map can have icons added to it to show the physical location of card readers, intrusion sensors, and other physical security related items. The map with icons can be printed (screen capture) and included in RE reports for evidence of the measure taken to secure the PSP. Symmetry supports configuration reports as well that may assist in the documentation requirements.

In addition to the PSP as defined in the NERC CIP requirements, the facility will typically have a perimeter that will be incorporated in an overall facility security plan and will be partially defined by the physical barricades (gates, walls, fences, etc.) and entry points (doors, turnstiles, mantraps) both attended and unattended, that make up the edge of the protected environment. There will be various means of protecting the physical area including video surveillance, security patrols, and access control.

Access control at different levels of secure areas should be identified. For instance, the facility may have some areas that are uncontrolled (open to the public), other areas that are controlled (only employee access), some areas that allow limited accessibility (financial records, or special use areas), and finally certain areas may be at an exclusion level (cyber assets such as servers, etc.). Physical security will be in place to protect all of these areas to different levels.

Controlled areas may only require an employee badge. Limited areas may rely on the access control system to allow access or may require higher levels of authentication – two-factor - such as card + PIN. Exclusion areas may require biometric authentication. The level of authentication required will be determined based on a risk assessment.

The RE must put in place processes and procedures to monitor physical access to the perimeter. Such monitoring can be the activity screen on a Symmetry client monitoring "Granted Access" messages as all alarm messages. The RE is required to implement procedures that enforce appropriate use: visitor pass management, response to loss and preventing the inappropriate use of physical access controls.

Symmetry comes complete with a simplified electronic visitor pass management system. The advantage of this is that it is embedded in the graphical user interface of the Symmetry software, uses the same types of controls and has the same look and feel thereby reducing training requirements. The Symmetry Visitor Management System tracks all of the relevant information in an SQL database and can be used to generate reports. Information such as visitor name, escort, date and time of check in and check out; and up to 50 customizable personal data fields to capture affiliation, purpose of visit, whether they are US citizen or what type of ID was provided.

If the simplified system doesn't meet local facility requirements, then there are a number of integrated solutions available including GUEST, AMAG's hosted Visitor Management System which is available for on-premise deployment. Contact your AMAG regional sales manager for additional information.

Response to loss is also captured by the Symmetry system. Every alarm type can be defined with instructions to the operator and will display these instructions when an alarm is acknowledged. The alarm acknowledgement window also allows (or optionally requires) the operator to insert comments on their response to the alarm. Alarm comments can be pre-defined and are selectable or can be entered in free-form text. These alarm records and response reports may provide evidence for CIP-008 Incident Reporting & Response, and CIP-009, Recovery Plans.

Symmetry has many features that support the prevention of inappropriate use of the access control system. First, it requires a valid operator account name and password to operate the system. The operator is limited to the functions authorized by their assigned role in the system. The system also can be configured to automatically log off after a specified period of inactivity (from the operator) thereby preventing a passer-by from using the system inappropriately. External solutions should be implemented that automatically log off or lock the workstation when they move away from the workstation in support of CIP-007 hardening of the system.

Symmetry supports procedures for the review of access authorization requests and revocation of access authorization through history and configuration reports

that can be run as needed or on a scheduled basis. This also supports efforts to meet CIP-004 logging requirements.

The RE must implement procedures for escorted access. By implementing access control at various interior doors, escorted access is required. Video surveillance and security communications systems (such as Stentofon) can also be used to monitor escorted and unescorted persons through the facility.

Protection of Physical Access Control Systems The reader is directed to those specific sections of this document to review how Symmetry facilitates this requirement.

This requirement indicates that protective measures of CIP-003-6, CIP-004-6-R3, CIP-005-5- R2 and R3, CIP-006-6 R2 and R3, CIP-007-6, CIP-008-5, CIP-009-6 and CIP-014-2 are afforded for Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access points such as electronic locking control mechanisms and badge readers.

In general, one might consider the Symmetry node as authorizing access when it commands the door controller to unlock a door in response to an authorized credential presentation. However, this is not the case. The "authorization" referred to in CIP-006 R2 is that provided by the personnel operating the Symmetry client. The operator modifies the access privileges assigned to the cardholder, thus authorizing them for access to the area. The Client refers this information to the server for storage in the database and referral to the access control nodes (field hardware). The node itself is simply executing a rule.

Similarly, "logging" as referenced in the standard is being performed at the server. The node merely collects this information temporarily until the server is able to store it more permanently. Certain additional hardware such as door controllers and input/output devices should be mentioned to demonstrate they are also used in the data collection process and interface to the environment but are pass-through devices without autonomous authorization or logging responsibility; and thus, these devices (along with the Symmetry nodes) need not be considered for the specific protections identified above.

The Symmetry Security Management System uses access control panels (the Symmetry nodes) with purpose-built firmware with no Operating System. Due to their purpose-built nature, they are not subject to traditional viruses, worms, Trojan horses, or other malicious network attacks; and there is no anti-virus or malicious code detection software available for these hardware components. Additionally, there is no human user interface to these devices (they are strictly used for machine-to-machine interface).

AMAG Technology recommends that the correct control is to use network-based malicious code detection, equipment should be installed in a physically protected area (wiring closet or IDF), and that communications to these devices (where available) be encrypted thus providing additional protections.

Physical Access Controls

Symmetry provides means for implementing operational control as well as supporting the documentation requirement for all access points to the Physical Security Perimeter. AMAG Technology offers solutions that cover all aspects indicated in the standard:

- Card keys – card access offers the most management control and is extremely cost effective compared to deploying security personnel for 24 hour per day, seven days a week access control. Card access also speeds personnel throughput and simplifies logging and reporting requirements.
- Special locks – such as those offered by Assa Abloy, Sargent and Allegion to allow electronic security for remote or disconnected doors are now able to be managed by Symmetry. Other solutions such as physical keys, electronic keys or cipher locks are not directly by Symmetry but electronic key safes from several manufacturers can be tightly integrated into a Symmetry solution.
- Security Personnel – mobile solutions from AMAG Technology allow the owner/operator to deploy security personnel in the most cost-effective way possible by allowing them to perform multiple functions simultaneously. Mobile solutions allow the security officer at the perimeter gate or on patrol to have access to their security system at all times.
- Other authentication devices: biometrics, keypads, tokens, or equivalent devices are all supported by Symmetry.

Symmetry supports the use of AES 256 bit encryption throughout the system. The communication between access control nodes and the communications server can be encrypted using AES encryption and supported NICs. The client to server communications can be encrypted using IPsec enabled NICs in the workstations and/or by providing layer 3 encryption on the network. Symmetry can operate across VPN tunnels.

Mobile solutions support encrypted Wi-Fi communications. However, if these solutions are deployed it allows for communications outside the ESP and therefore, may require other mitigating measures.

Documentation requirements can be further facilitated by the generation of configuration reports from Symmetry. This will show the access points along the physical perimeter, what equipment is assigned to the location, and how the equipment is configured. History reports can be generated to show who has requested access through various points and whether those access requests were granted or denied.

Monitoring Physical Access

Symmetry supports the Responsible Entity's requirement to implement the technical controls for monitoring physical access at all access points to the Physical Security Perimeter. Alarm monitoring is performed through the Symmetry client software (either on a PC or on a handheld unit). All alarms are presented to those clients authorized for alarm routing. Furthermore, clients can filter alarms to show only those alarms for their jurisdiction.

In Symmetry monitored input points are alarm sensor inputs. Since a sensor can be tampered with (or the device removed in an attempt to circumvent the detection) Symmetry supports line supervision. This is implemented through end-of-line resistors that provide specific signals to the PACS when a device is removed, or a cable is cut or shorted out. Symmetry reports all of these as alarms to the operator. Additionally, tamper switches can be employed for equipment in cabinets, etc. If the tamper switch is triggered, an alarm will be generated.

Per the standard, unauthorized access attempts shall be reviewed immediately. The Symmetry system presents all configured alarms to the operator in near real time. Operators can acknowledge the alarm, read the pre-defined instructions, enter comments (either pre-defined or free-form) and either clear or acknowledge the alarms.

- Alarm systems – the Symmetry system can be used directly to monitor alarm inputs, control access through doors, and trigger outputs. Additionally, Symmetry offers the ability to integrate with intrusion systems from other companies such as DMP and DSC.

- Human observation of access points – video surveillance can be used to make best use of available staff levels.

Symmetry also supports an automation feature that allows the configuration of actions to occur automatically on a trigger event. For instance, if a smoke detector signals an alarm, locked doors can be opened for free egress. Therefore, alerting not only occurs at the control station but can include any number of additional automated responses such as e-mails, paging, mass notification, video recording, or other.

Logging Physical Access

The Symmetry security management system logs all activity (at access points as well as operator functions) thereby supporting the requirement to record sufficient information to uniquely identify individuals and the time of access.

- **Computerized logging** – all transactions (at access points as well as operator functions) are logged in a database. The database can be used to generate reports showing the activity as well as who (card number, first, middle, and last name), what (the description of the event), where (the configured name of the location of the device whether card reader or alarm point), and when (the time and date stamp of the event at the time of the event – not the time it was stored in the database).

  The system supports non-repudiation in that all operator activities are also logged in the database and can be reported for audit purposes. Any changes to access control privileges, roles or accounts are logged as well as other typical operator activity.

- **Video recording** – video recording is supported through the Symmetry Video Management System – Symmetry CompleteView. Additionally, Symmetry provides a totally integrated solution with Video Management Systems from many other manufacturers including Milestone, Genetec, Avigilon, Pelco, Verint, Qognify, 3VR, Bosch, Flir, Exacq, March Networks, Salient, and others. The Symmetry graphical user interface is used to monitor alarms as well as to view live video or to access recorded video on any of the integrated platforms. Video clips can be associated with activity in the access control or intrusion detection system.

The system records all activity (cardholder transactions, operator activity and system events) in a SQL database. The database is made up of tables of data and as new events occur, they are appended to the appropriate tables. Therefore, data is never overwritten. When the tables get too large, a manual process to backup and purge the data can be implemented by policy.

Access Log Retention

Physical access logs shall be retained for at least ninety (90) calendar days. The Symmetry Enterprise system uses the Microsoft SQL Server database, and this database can grow to large size as supported by the local hardware. This ensures that at least ninety (90) calendar days of history will be retained.

Furthermore, other CIP regulations such as CIP-008 (Incident Reporting) and CIP-009 (Recovery Plans) require retention of records for at least three (3) years. History transactions can be archived to long-term storage. Doing so maintains high performance in the database system. Archived data can later be re-incorporated into the system for reporting on older events. The retention of archived data is only limited by the amount of storage the user has available on the system.

Maintenance and Testing

The Responsible Entity is required to develop the maintenance and testing program. This program is required to include, at a minimum, the items below. Symmetry can support the documentation of the maintenance and testing requirement.

- Test and maintenance of all physical security mechanisms shall be performed on a cycle of no longer than three (3) years. Schedules of maintenance can be configured using the built in Task Manager within Symmetry or through external scheduling applications. Other maintenance includes applying patches and service packs as recommended by AMAG Technology as well as operating system security patches and service packs as approved by AMAG Technology. These are not scheduled but a monthly notice of available and supported patches and service packs is made available by AMAG Technology. Firmware changes to field hardware is also covered under this requirement, although this occurs very rarely.

- Retention of records – the notes field and document attachment capability in the Symmetry system can be used to record information regarding the maintenance and testing performed on the system, any issues identified, and their resolution.

- Retention of outage records for minimum of one calendar year – Symmetry will raise an alarm if there is an outage in the system. These alarms will be retained along with other transactional data. Reports can be generated on the specific outage related information and retained themselves.

CIP-007-6: SYSTEM SECURITY MANAGEMENT

Standard CIP-007 requires Responsible Entities to define technical, operational and procedural requirements for securing those systems determined to be BES Cyber Systems, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s).

Physical Access Control Systems such as Symmetry are identified as an Applicable System to which this standard applies for PACS associated with high and medium impact BES Cyber Systems.

R1, Ports and Services

The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. A list of ports and services required by the Symmetry PACS for normal and emergency operations is included in the Appendix.

R2, Security Patch Management

This requirement is supported by AMAG Technology. OS and PACS patches are made available from time to time. AMAG Technology recommends that the Responsible Entity install critical OS patches when they become available, but that service packs and non-critical patches should not be applied until such time as AMAG has had an opportunity to test them. AMAG releases a compatibility report on a monthly basis.

The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. AMAG Technology recommends applying patches and service packs to the PACS software as required or to maintain current support requirements. Additionally, operating system security patches and service packs should be applied as approved by AMAG Technology. From time-to-time AMAG releases a list of supported patches and service packs. Firmware changes to field hardware is also covered under this requirement, although occurs very rarely.

Such updating to the system is considered significant per this requirement. In order to test that such changes will not adversely affect existing cyber security controls, a separate installation of the Symmetry application and all associated systems should be maintained as a test bench. Patches and upgrades can be applied to the test bench to validate that there have been no adverse effects before applying the patches and upgrades to the production system.

R3, Malicious Software Prevention

This requirement is supported by AMAG Technology. A white paper, "Notes on the Application of Virus Scanning Software" has been developed and is available that specifically addresses the use of Anti-Virus/Anti-Malware scanning on the operation of the PACS cyber assets. That white paper also addresses port usage and database optimization utilities. The white paper includes recommendations for the Responsible Entity on excluding certain folders from AV scanning.

R4, Security Event Monitoring

Responsible Entities must implement processes to log events at the BES Cyber System level or Cyber Asset level for identification and after the fact investigations of cyber security incidents.

Cyber security incidents include successful and failed access and login attempts and detected malicious code. Additionally, alerts must be generated in defined circumstances.

Logs must be retained for a 90 days to allow a review by the Responsible Entity at intervals no greater than 15 calendar days.

Symmetry contains extensive logs of all system activity, and with the addition of Symmetry Advanced Reporting and Audit Reports an additional layer of audit reporting is included.

R5, System Access Control

The Responsible Entity shall enforce access authentication of, and accountability for, all user activity. In support of this requirement the Symmetry security management system allows the RE to delete default accounts, change the passwords, and create specific accounts for all operators to enforce accountability. Symmetry also supports the generation of reports showing operator activity.

In further support of this requirement, Symmetry supports an option for the requirement of strong passwords. Within Symmetry a strong password is one that is case sensitive; has at least 6 characters; must have at least one lowercase character, one uppercase character, one numeric character and one special character. In addition, a password will not be able to contain any full word of the user's username. The password can be set to expire in a set number of days per policy.

The Engineer account in the Symmetry application has specific use and various measures can be employed to limit use of this account. The password can be changed after each use of the account.

The system comes with a small number of default accounts and roles. These can be deleted, or the passwords changed from their default to meet requirements of CIP-007, R7. The default accounts are listed in the following table.

Table 2: Default Accounts

Default Account Name	Default Role Assignment
Installer	Installer
Manager	System Manager
Guard	Security Guard
Engineer*	
Administrator	Card Admin

*The Engineer account has special privileges in the system. It cannot be deleted but the password can be changed from the default.

Furthermore, a default role of "Visitor Management" is assigned to any cardholder that is enabled login to the visitor management system (this feature is disabled by default).

Symmetry has many features that support the prevention of inappropriate use of the access control system. The system can be configured to automatically log off after a specified period of inactivity (from the operator) thereby preventing a passer-by from using the system inappropriately. External solutions should also be implemented that automatically log off or lock the workstation when they move away from the workstation.

CIP-008-5: INCIDENT REPORTING AND RESPONSE PLANNING

Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to BES Cyber Systems. The requirements in this section necessitate policies, procedures, and applications external to the PACS although operations within the PACS may be used as part of the incident response plan.

Alarm events that come into the PACS are acknowledged by an operator. That acknowledgement can include response instructions, comments by the operator, and logs of when the alarm was acknowledged and cleared from the alarm hot list. This procedure and the details of the configuration can be included in the incident response procedure documentation.

Symmetry provides advanced features for incident response including:

- Control Desk, a unified display of integrated security capabilities for one or more selected Monitor Zones
- Threat Level Manager, the ability to totally reconfigure the access control system in the event of a threat level change
- Integrated Video Management, the ability to interactively operate with video management systems in the response to any alarm event
- Triggers, the ability to automatically carry out "if … then …" responses to any security event

Symmetry supports integration with other systems as well. An XML API as well as database connectivity are available for developers writing middleware between two systems such as Symmetry and an incident reporting and management system.

It should be noted that Risk360 an advanced Incident Management and Case Management system, is part of the wider range of products available from G4S, AMAG's parent company.

CIP-009-6: RECOVERY PLANS FOR BES CYBER SYSTEMS

Standard CIP-009 ensures that recovery plans are put in place for BES Cyber Systems and that these plans follow established business continuity and disaster recovery techniques and practices. AMAG Technology has long been a proponent of consideration of the PACS as a high availability service. Toward that end we have been providing solutions for high availability and business continuity for many years.

Physical Access Control Systems are defined as an Applicable System in this standard for high and medium impact BES Cyber System, and therefore recovery plans must be put in place for these systems.

R1, Recovery Plan Specifications

AMAG Technology has solutions that take advantage of Microsoft Cluster Services in Windows Server 2014 Enterprise edition, and we support NEX Express Cluster software for data replication over the local or wide area networks. AMAG has also partnered with NEC to provide our customers with options for the fault tolerant servers. AMAG can also assist in a design that incorporates both high availability and disaster recovery. AMAG Technology has produced a white paper, "Business Continuity and High Availability Options" on these disaster recovery options.

Response to communication loss is also captured by the Symmetry system. Every alarm type can be defined with instructions to the operator and will display these instructions when an alarm is acknowledged. The alarm acknowledgement window also allows (or optionally requires) the operator to insert comments on their response to the alarm. Alarm comments can be pre-defined and are selectable or can be entered in free-form text. These alarm records and response reports may provide additional evidence of support for CIP-009.

R2, Recovery Plan Implementation and Testing

Recovery plans for these systems must be tested at least once every 15 months. AMAG can assist with such planning and testing through the use of AMAG Professional Services and an AMAG Platinum Site Support Agreement.

CIP 010-3: CONFIGURATION MANAGEMENT AND VULNERABILITY ASSESSMENTS

Standard CIP-010-2 specifies configuration change management and vulnerability assessment requirements to prevent and detect unauthorized changes to BES Cyber Systems.

PACS are an Applicable System as defined by the standard for high and medium level BES Cyber Systems.

Although PACS are encompassed within the standard there are no specific requirements for PACS within the standard which are different for any other Cyber Asset to which the standard relates.

Symmetry's activity logging, Advanced Reporting and Audit capabilities will provide evidence of any configuration changes within the Symmetry system.

CIP 011-2: INFORMATION PROTECTION

The purpose of CIP-011-2 is to prevent unauthorized access to information in BES Cyber Systems by specifying information protection requirements against compromise.

CIP-011 was a new standard implemented in 2014 and updated by CIP-011-2.

As with some of the other CIP standards PACS are an Applicable System but there are no specific requirements related to PACS.

The standard covers:

- Identification of data that meets the definition of the standard
- Protection of data (both in storage and in transit)
- Documenting a process for date re-use and disposal

CIP 014-2: PHYSICAL SECURITY

CIP-014-2 is the only standard within the CIP family of standards which has no specific cyber security element. It was the most recently implemented standard and relates to the identification and protection of Transmission stations and sub-stations.

The standard resulted from a directive from FERC dated March 7, 2014, and was implemented in a very short time scale due to the pressing need for additional physical security measures in these facilities.

The purpose of the standard is to "Identify and protect Transmission stations and Transmission sub-stations, and their associated primary control centers that if rendered inoperable or damaged as a result of a physical attack could result in instability, uncontrolled separation, or Cascading within an Interconnection."

The standard relates to all transmission facilities rated at over 500kV and all those over 200kV which pass certain line weight value criteria.

Symmetry as a PACS and Security Management System is able to integrate various transmission station physical security systems and devices including cameras, video management systems, fence detection, motion sensors, ground-based radar, intrusion alarm systems and various other sensors and devices.

A transmission station Symmetry system can be confined to that local site, organized across an area on a hub-and-spoke basis or fully integrated into the overall Symmetry PACS/Security Management System of the organization.

The elements of the standard are as follows:

R1: Transmission owners are required to carry out an initial risk assessment consisting of a transmission analysis to identify the results if the station is made inoperable. They must also identify the primary control center for each of the transmission stations

Subsequent risk assessments are to be carried out at least once every 30 months.

R2: The risk assessment must be verified by an unaffiliated third party.

R3: Where the primary control center is not under the control of the transmission owner, they must notify the owner that they have been identified as having such a role.

R4: All transmission owners and primary control center with facilities which have been identified must carry out an evaluation of potential threats and vulnerabilities from physical attack. The evaluation must take into account unique characteristics, prior history of attack on similar facilities, and intelligence or threat warnings from approved sources.

R5: Each owner or control center must develop and implement a physical security plan for each facility within 120 days of following completion of R2.

R6: Each owner must have an unaffiliated third party review the results of R4 and R5 within completion f R5.

Summary

The Symmetry security management system from AMAG Technology is used by a large number of electric energy generation and distribution companies. This white paper has highlighted areas within the NERC Critical Infrastructure Protection BES Cyber Security Standards where the Symmetry system supports the efforts of the Responsible Entity in securing the physical perimeter of their facility. Furthermore, being a cyber-asset (server and workstation) itself, the PACS inherently supports the features necessary to facilitate the RE policies, procedures, and documentation requirements.

Some of the CIP requirements and/or TWIC support necessitate specific implementations of the Symmetry system. If Symmetry has not been installed in a way to support the efforts of the local Responsible Entity, AMAG Technology is available to assist in your efforts to become compliant with the regulations. AMAG Technology has Regional Sales Managers, Regional Sales Engineers, Professional Services teams, and Technical Support ready to assist with your security challenges.

Transportation Worker Identity Credential

Many of the electric power generation and distribution companies have facilities that are regulated to comply with the TWIC program implemented by the Transportation Security Agency. The TWIC card is an electronically enabled (smart card) identity document. The TWIC has biographic and biometric data that associate the card with the individual. By registering the credential ID number in the physical access control system, the card can also be used to associate the individual with their access privileges as assigned by the security administrator at the facility.

The TWIC program requires that all individuals with unescorted access to secure areas of regulated facilities must have their TWIC card within 5 minutes of their person. If the card is used to gain access to secure areas, it is a further assurance that the person has their card with them. To provide the irrefutable connection between the person and the card, biometric authentication must be applied at the gate.

Use of the TWIC as the access control credential also simplifies the process for the cardholder. They no longer have to carry multiple cards to gain access at various facilities. The TWIC is based on Federal Information Processing Standard (FIPS) 201 and therefore is interoperable with other systems that also support this standard. Support of the standard means that the system is capable of reading the card – the cardholder must still register in the PACS and be assigned appropriate access rights.

Support for the TWIC and other FIPS 201-based credential solutions is achieved by implementing the Symmetry Homeland Security Management System. This version of the access control system supports the various identity fields on the TWIC and similar smart cards.

GLOSSARY

AV	Anti-Virus – in particular the software running on a computer responsible for the detection and removal of viruses and other "malware."
BES	Bulk Electric System – these are essentially transmission and power resources operated at 100kV or higher .
CIP	Critical Infrastructure Protection
DMP	Digital Monitoring Products – a company that produces intrusion detection equipment.
DSC	Digital Security Corporation – a company that produces intrusion detection equipment.
ESP	Electronic Security Perimeter
FIPS	Federal Information Processing Standard – NIST is responsible for developing standards and guidance for the Federal government's use of information processing. FIPS 201 is a standard for Personal Identity Verification.
ID	Identity – for instance, an ID card is a credential that represents one's identity.
IDS	Intrusion Detection System – a hardware system made up of a control panel, user interface (typically a keypad/display), and various sensors that is designed to enable the detection of anomalous behavior in a particular area. There are physical and cyber versions of IDS.
LEAP	Low Impact BES Cyber System Electronic Access Point
NERC	North American Electric-Reliability Corporation – the organization responsible for the regulation of electric energy production and distribution facilities.
NIC	Network Interface Card – provides the interface between the computer system and software running on it to the network physical layer.
NIST	National Institute of Standards and Technology
OS	Operating System – such as Microsoft Windows, provides a means of controlling applications (software) running on a computer system and providing services to that application, including access to the network.
PACS	Physical Access Control System
PRA	Personnel Risk Assessment
PSP	Physical Security Perimeter – this is a six-wall perimeter (therefore totally enclosed and defined). The PSP completely encloses the ESP and all equipment.
RE	Responsible Entity
TCP/IP	Transmission Control Protocol/Internet Protocol – a fundamental protocol used to communicate across Ethernet networks.
TSA	Transportation Security Agency – a Federal agency under Department of Homeland Security responsible for the safety and security of all modes of transportation and regulation of the facilities that are involved in transportation.
TWIC	Transportation Worker Identity Credential – the identity card issued by TSA and the TWIC program office to individuals that qualify and meet the identity vetting and proofing requirements. The card is required by US Coast Guard regulated facilities for unescorted access to secure areas.

APPENDIX: PORTS AND SERVICES

The Symmetry security management system from AMAG Technology uses a number of TCP/IP ports. The following identifies those ports that are required for proper operation and their use.

21/tcp	FTP
25/tcp	SMTP (Email)
25/udp	SMTP (Email)
53/tcp	DNS
53/udp	DNS
80/tcp	HTTP
110/tcp	POP3 (Email)
123/udp	NTP/SNTP (Windows time)
135/tcp	RPC (DCOM/DTC/MSMQ/CLUSTER)
137/udp	File/Printer Sharing, NETBIOS Name Resolution
138/udp	File/Printer Sharing
139/tcp	File/Printer Sharing
443/tcp	HTTPS
445/tcp	File/Printer Sharing
554/tcp	RTSP

1433/tcp	MS SQL Server
1434/udp	MS SQL Server[2]
1801/tcp	Microsoft Message Queue
1801/udp	Microsoft Message Queue
1900/udp	UPnP
2869/tcp	UPnP
3001/tcp	NIC module (MN-2, M2100, 8DBC)
3343/udp	Cluster Services
3389/tcp	Terminal services (Web Client)
3527/udp	Microsoft Message Queue
6456 -> 7456/tcp	RTP
12090/tcp	SMS client network messaging
12290/tcp	SMS CCH client network messaging
14090/tcp	SMS global alarm monitor network messaging

[2]Microsoft SQL Server database engine default instance (Symmetry is always installed as the default instance) listens for requests on TCP port 1433. The MS SQL Server browser service uses UDP port 1434 to establish communications links from applications that are attempting to discover the SQL Server database. Therefore, the UDP port 1434 can be closed when no third-party applications are attempting to discover the database.

NETWORK CAMERAS

80/tcp	Web interface to camera, firmware upload and so-called tcp tunneling via HTTP (specific cameras)
443/tcp	Encrypted communication via SSL
1756/tcp	RCP+ communication
1758/udp	Network scan target
1759/udp	Network scan response

1818/tcp	Alarm notifications (specific cameras)
1900/udp	Multicast network scan target
4000/udp	Device discovery response (specific cameras)
10669/udp	Device discovery response (specific cameras)

SYMMETRY SERVICES

The following services are installed at the server and are required for proper operation:

- SMS Services
- SMS Transaction Service
- SMS Integration Server
- Message Queuing
- MSSQL Server
- SQL Server Agent

The following services are installed at the client and are required for proper operation:

- SMS Client Service
- Message Queuing

The following services are installed with the Video Management Option:

- Message Queuing
- IIS Admin
- FTP Publishing
- World Wide Web Publishing
- SMS Streaming Archiver
- SMS Archived Index
- SMS Streaming Server
- SMS Transaction Parser

Revision History

01/04/2010 Initial document draft, 0.1

01/11/2010 Completed content, 0.2

01/18/2010 Released as version 1.0

01/20/2010 Added info on TWIC, 1.1

01/29/2010 Incorporated feedback, 1.2

02/11/2010 Incorporated additional feedback, 1.3

05/08/2012 Updated document for version 4 CIP requirements, 1.5

01/16/2014 Added detail and description around protection of equipment, 1.6

01/28/2014 Corrected inconsistencies throughout document, 1.7

01/24/2016 New title. Full update. Incorporate of v5 and CIP-014 standards, 2.0