

# CYBER SECURITY AND ELECTRIC UTILITY COMMUNICATIONS

## WHAT NERC/SIP MEANS FOR YOUR MICROWAVE

# TABLE OF CONTENTS

1.0	INTRODUCTION.....	3
2.0	MODERN ELECTRIC UTILITY COMMUNICATIONS .....	4
2.1	DOMAINS AND APPLICATIONS .....	4
2.2	EVOLUTION OF ELECTRIC UTILITY COMMUNICATIONS .....	4
2.3	THE ROLE OF MW RADIO IN THE MODERN UTILITY COMMUNICATIONS ARCHITECTURE.....	5
2.4	CYBER SECURITY NEEDS AND DRIVERS .....	5
3.0	SUMMARY OF RELEVANT SECURITY STANDARDS AND GUIDELINES FOR THE ELECTRIC SECTOR .....	5
3.1	NERC CIP .....	5
3.1.1	PURPOSE OF THE NERC CIP STANDARDS.....	5
3.1.2	COMPLIANCE TO THE NERC CIP STANDARDS .....	6
3.1.3	OVERVIEW OF REQUIREMENTS .....	7
3.1.4	EVOLUTION OF STANDARDS .....	7
3.2	ADDITIONAL REFERENCES.....	8
3.2.1	NISTIR 7628 .....	8
4.0	MAPPING OF CYBER SECURITY REQUIREMENTS TO COMMUNICATIONS SYSTEMS.....	9
4.1	REQUIREMENT CATEGORIES AND ASSOCIATED REQUIREMENTS .....	9
4.1.1	CIP 002-4 CRITICAL CYBER ASSET IDENTIFICATION .....	10
4.1.2	CIP 003-4 SECURITY MANAGEMENT CONTROLS.....	11
4.1.3	CIP 004-4 PERSONNEL AND TRAINING .....	11
4.1.4	CIP 005-4 ELECTRONIC SECURITY PERIMETER(S) .....	11
4.1.5	CIP 006-4 PHYSICAL SECURITY .....	12
4.1.6	CIP 007-4 SYSTEMS SECURITY MANAGEMENT .....	13
4.1.7	CIP 008-4 INCIDENT REPORTING AND RESPONSE PLANNING.....	14
4.1.8	CIP 009-4 RECOVERY PLANS FOR CRITICAL CYBER ASSETS.....	14
4.2	REQUIREMENTS SIGNIFICANT TO MW RADIO SYSTEMS.....	14
4.3	AVIAT MW RADIO FEATURES SUPPORTING REQUIREMENTS .....	15
4.3.1	SECURE MANAGEMENT .....	15
4.3.2	PAYLOAD ENCRYPTION .....	15
4.3.3	INTEGRATED RADIUS CAPABILITY.....	15
	ABOUT AVIAT NETWORKS.....	16

## 1.0 INTRODUCTION

The modernization of the electric power grid, often referred to as "smart grid", is critical to meet the changing needs of electric utilities. Better visibility and control of the power grid improves its reliability and efficiency and, as applications are developed for end users, point-of-use monitoring and control of power usage will benefit utilities by reducing peak loads and benefit consumers by providing a way to save on their energy costs.

In order support this modernization effort, utilities are relying more than ever on communications and IT infrastructure which has become an integral part of the overall landscape. Traditional point-to-point, circuit switched communications with limited external system interfaces are evolving to packet and IP based services along with the need to share data outside the traditional system boundaries.

As a result of this evolution, heightened awareness of cyber security needs have arisen that must be addressed at all levels of the utility's communications architecture. While the emphasis has been placed on the applications and end devices, the communications infrastructure, which connects them, also plays a critical role in the overall security of the system and therefore the power grid itself.

While there are numerous standards and guidelines that can be applied to this domain, two specific documents specific to this domain are worthy of examination; The North American Reliability Corporation (NERC) - Critical Infrastructure Protection (CIP) standards (CIP 002-009) and the National Institute of Standards and Technology (NIST) – NISTIR 7628 Guidelines For Smart Grid Cyber Security. This paper will provide a general introducing to these documents. It will also summarize the relevance of the NERC CIP standards to communications systems utilized by electric utilities in general with emphasis on MW radio.

### Conceptual Model

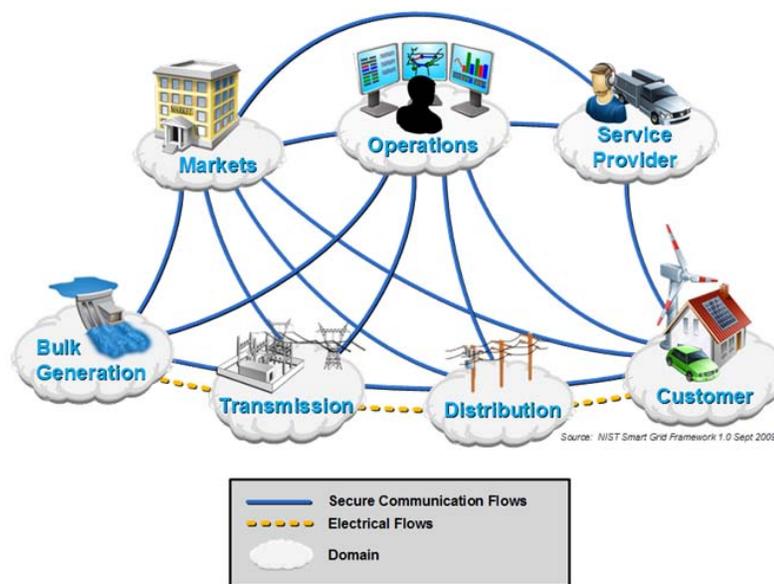


Figure 1: NIST Smart Grid Conceptual Model

## 2.0 MODERN ELECTRIC UTILITY COMMUNICATIONS

### 2.1 DOMAINS AND APPLICATIONS

While one may think of the power grid as a single unified system, the electric utility industry in reality has many facets. The recent work by NIST provides a basis for outlining these facets, referred to by NIST as domains, of the electric utility industry.<sup>1</sup> Each domain has specific needs driven by the applications needed to support the utility's operational and business needs within that domain however communications and IT infrastructure are often a common elements between them.

A brief explanation of the role of each of these domains is shown in Table 1.

Domain	Description
Customer	Where electricity is consumed
Markets	Where grid assets are bought and sold
Service Provider	Includes services to support the business processes of power system producers, distributors and customers
Operations	Responsible for grid operations
Bulk Generation	Large scale, centralized generation
Transmission	Covers bulk transfer of electrical power from generation sources to distribution through multiple substations
Distribution	Covers the electrical interconnection between the Transmission domain, the Customer domain and the metering points for consumption, distributed storage, and distributed generation.

Table 1: NIST Smart Grid Domains.

The focus of this paper shall be on the Operations, Transmission, and Bulk Generation domains

### 2.2 EVOLUTION OF ELECTRIC UTILITY COMMUNICATIONS

In order support the ongoing modernization effort, electric utilities are relying more than ever on communications and IT infrastructure which has become an integral part of the overall landscape. Point-to-point, circuit switched communications with limited external system interfaces were traditionally employed for critical communications with dial-up communications utilized for non-critical needs. While this model served the industry well for many years, it has now become cumbersome and costly architecture to maintain given the current needs of the utilities to evolve the manner by which they monitor and control the power grid. As a result of this evolution, the utilities needs for increased visibility of the power grid and faster, broader access to power system data has resulted in the underlying communication architecture which supports these goals also evolving.

While utilities will continue to utilize circuit switched technology for certain applications in the short term, many applications are now being deployed based on packet or IP based services. From the utility perspective, some of the benefits for the migration to the converged IP based services include:

- More efficient use of bandwidth
- More economical solutions available
- Multi-user architecture supported
- Standardized solutions

---

<sup>1</sup>Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, (NIST Special Publication 1108); January 2010.

### **2.3 THE ROLE OF MW RADIO IN THE MODERN UTILITY COMMUNICATIONS ARCHITECTURE**

In grid monitoring and control applications, the control system is the core of the design with the communications media being a secondary consideration that can be implemented in a number of ways. While each technology may have advantages and disadvantages, North American utilities typically select the technology for certain applications based on two primary factors: functionality and cost. In an ideal scenario, a utility may desire to deploy a 100% fiber optic based system for maximum functionality. In reality, the associated costs are often prohibitive and therefore necessitate choosing more economical solutions. As this process is repeated throughout the evolution of the utilities communication architecture to support the power grid, a hybrid communications architecture typically emerges utilizing several underlying technologies (such as fiber optic, MW radio, satellite, MAS radio, etc).

In today's utility communication architecture, MW radio systems are utilized as part of the utilities communications backbone, spurs from the utility communications backbone, or for last mile connectivity.

### **2.4 CYBER SECURITY NEEDS AND DRIVERS**

As the communication and IT infrastructure which support the monitoring and control of the power grid have evolved, so has the risk associated with the increased attack surface which comes with the evolved architecture. The need to provide power system data beyond the traditional control center boundaries has led to an increasing number of external and internal connections between traditionally isolated systems. As a result, heightened awareness of cyber security needs have arisen that must be addressed at all levels of the utility's communications architecture. While the emphasis has been placed on the control systems and end devices, the communications infrastructure which connects them also plays a critical role in the overall security of the system and therefore the power grid itself. The power grid is changing from a relatively closed system to a complex, highly interconnected environment. Each organization's cyber security requirements should evolve as technology advances and as threats to grid security inevitably multiply and diversify.

Adding to the drivers are the NERC CIP standards which are mandatory and enforceable to most entities which can be classified in the Operations, Transmission, or Bulk Generation domains.

## **3.0 SUMMARY OF RELEVANT SECURITY STANDARDS AND GUIDELINES FOR THE ELECTRIC SECTOR**

### **3.1 NERC CIP**

The North American Electric Reliability Corporation's (NERC) mission is to ensure the reliability of the North American bulk power system. As a result of the Energy Policy Act of 2005, it now serves as the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk-power system. The Critical Infrastructure Protection (CIP) standards are among these standards.

#### **3.1.1 PURPOSE OF THE NERC CIP STANDARDS**

The overall goal of CIP-002 through CIP-009 is to ensure the bulk electric system is protected from unwanted and destructive effects caused by cyber event. Essentially, FERC, via NERC, wants assurance that the owners and operators of the bulk electric system in North America are addressing these risks.

The bulk electric system includes electrical generation resources, transmission lines, interconnections with neighboring electric grids, and associated equipment, generally operated at voltages of 100,000 volts or higher. Distribution systems operating at lower voltages are not included in the NERC CIP standards as NERC has no authority over these entities.

The NERC CIP standards are aimed at the IT infrastructure that supports the operation of the bulk electric system and these standards provide guidelines for the security of what are defined as critical cyber assets. To determine the critical cyber assets, entities must first understand what their "critical" assets are. These are facilities, systems and equipment which, if destroyed, degraded or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system. These assets include system control centers, large generation facilities and critical transmission facilities. Entities must then examine these critical assets and identify the cyber aspects that could directly affect the general critical assets in the event that they are unavailable or compromised.

### 3.1.2 COMPLIANCE TO THE NERC CIP STANDARDS

Compliance enforcement activities are carried out on behalf of NERC by the eight regional entities based on the NERC Compliance Monitoring and Enforcement Program and their respective delegation agreements.<sup>2</sup> NERC oversees these programs to ensure consistency and fairness.

- Florida Reliability Coordinating Council - FRCC
- Midwest Reliability Organization - MRO
- Northeast Power Coordinating Council - NPCC
- Reliability First Corporation - RFC
- SERC Reliability Corporation - SERC
- Southwest Power Pool Regional Entity - SPP RE
- Texas Reliability Entity - TRE
- Western Electricity Coordinating Council - WECC

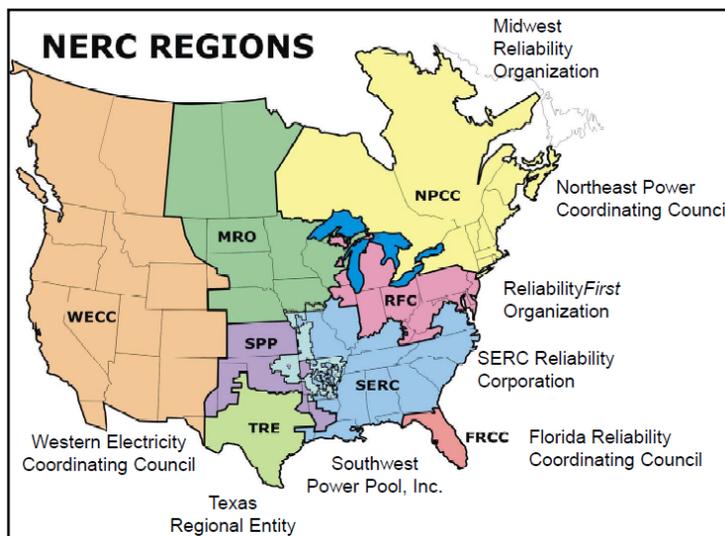


Figure 1: NERC Regional Entities

<sup>2</sup> Source: North American Electric Reliability Corporation (NERC)

The NERC CIP standards apply to a range of entities that impact the reliability of the bulk power system. In general, these entities are owners, operators and users of any portion of the bulk power system

### 3.1.3 OVERVIEW OF REQUIREMENTS

CIP-002 Critical Cyber Asset Identification - requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-003 Security Management Controls - requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets.

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

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

CIP-006 Physical Security of Critical Cyber Assets - intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets.

CIP-007 Systems Security Management - requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s).

CIP-008 Incident Reporting and Response Planning - ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets.

CIP-009 Recovery Plans for Critical Cyber Assets - ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices.

### 3.1.4 EVOLUTION OF STANDARDS

The NERC CIP standards have undergone several revisions since initially approved and continue to evolve. Upon initial approval of version 1 of CIP 002-009, NERC embarked upon a series of revisions to address the directives issued by FERC, in Order 706 relative to these standards under Project 2008-06: Cyber Security Order 706.

#### 3.1.4.1 Version 4 - CIP 002-009-4 (Current Approved Version)

As part of the ongoing efforts of Project 2008-06: Cyber Security Order 706, NERC has produced version 4 of CIP 002-009. This only significant change in this version was to CIP 002 (Critical Cyber Asset Identification) and CIP 003-009 revisions consist of reference updates only. Once Version 4 becomes effective, assuming FERC approval, the identification of Critical Assets will be based on a set of identification criteria (sometimes referred to as "bright line" criteria) included as an attachment to the CIP-002-4 Standard itself instead of on entity-defined risk-based assessment methodologies. For many Responsible Entities, this new approach to identifying Critical Assets will increase their total number of Critical Assets, and that this will often result in a larger inventory of Critical Cyber Assets that must be in compliance with CIP-003-4 through CIP-009-4. Version 4 of CIP 002-009 was approved by industry on December 30, 2010. FERC approval for this version is anticipated summer 2011.

In a separate effort, Project 2010-15: Expedited Revisions to CIP-005-3, NERC has developed additional changes to CIP-005. These consist of the addition of additional requirements identified in R6 covering interactive remote access to critical cyber assets for support or maintenance activities. Support or maintenance includes non-operational activities associated with the upkeep, testing and modification of Cyber Assets or networks within the Electronic Security Perimeter. Examples of support or maintenance activities include, but are not limited to, configuration changes, power system model maintenance, vulnerability assessments, incident response, troubleshooting, computer system monitoring, and application of software patches.

#### 3.1.4.2 Version 5

This version of the reliability standards is still in draft. Version 5 potentially eliminates the terms “critical asset”, “cyber asset” and “critical cyber asset” defined in CIP-002 and moves to a low, medium, high impact criteria related to “BES Cyber Systems” (very similar to the categorization process used in the NIST Risk Management Framework (specifically FIPS-199). Once the impact categorization for each identified BES Cyber Systems is completed, then establishes baseline cyber security requirements for the BES Cyber Systems based on the impact categorization (very similar to the control selection process of the NIST Risk Management Framework (specifically NIST SP800-53). It is anticipated that the compliance footprint (i.e. the number of cyber systems for which compliance must be achieved) for most utilities will increase with this process as opposed to the categorization method used under CIP-002 which yielded only a subset systems deemed critical by the asset owner.

While the exemption for communication systems may still be in effect, the new impact criteria may result in systems which were not classified as Critical Cyber Assets under the Version 4 criteria to be categorized as low or medium impact.

## 3.2 ADDITIONAL REFERENCES

### 3.2.1 NISTIR 7628

In the broader context of the Smart Grid, NIST has developed high level guidelines to evaluate the overall cyber risks to a Smart Grid. Under the Energy Independence and Security Act (EISA) of 2007, the National Institute of Standards and Technology (NIST) was assigned “primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems...”

As part of the cyber security efforts associated with this task, the three-volume NISTIR 7628, Guidelines for Smart Grid Cyber Security was produced by the Cyber Security Working Group (CSWG). These guidelines cover the Bulk Generation, Transmission, Distributions, and Customer domains outlined in the NIST conceptual architecture.

## 4.0 MAPPING OF CYBER SECURITY REQUIREMENTS TO COMMUNICATIONS SYSTEMS

### 4.1 REQUIREMENT CATEGORIES AND ASSOCIATED REQUIREMENTS

The requirements identified in the NERC CIP standards are primarily policy based and not prescriptive in nature. Their primary purpose is to ensure that the entity has a comprehensive security program in place. Ultimately, it's not the IT or communication systems that are compliant to the standards but rather the entities security program around the systems that is assessed at the compliance level.

None the less, when overlaying these requirements specifically onto the communications infrastructure utilized to transport data between physical locations, one will find that there are cases where these standards directly apply if any portion of the infrastructure is classified as Critical Cyber Assets (and therefore the utility's operations of the communication system(s) come into play when addressing compliance to the standards). In other cases, the standards apply more indirectly in that the communication systems must support various functionality needed by the utility to address compliance to the standards for its identified Critical Cyber Assets.

Figure 2 summarizes the individual requirements contained in CIP 002-009, Version 4 and those requirements which are either directly or indirectly applicable to communications infrastructure.

CIP-002	CIP-003	CIP-004	CIP-005	CIP-006	CIP-007	CIP-008	CIP-009
<b>CRITICAL CYBER ASSET IDENTIFICATION</b>	<b>SECURITY MANAGEMENT CONTROLS</b>	<b>PERSONNEL AND TRAINING</b>	<b>ELECTRONIC SECURITY PERIMETER(S)</b>	<b>PHYSICAL SECURITY</b>	<b>SYSTEMS SECURITY MANAGEMENT</b>	<b>INCIDENT REPORTING AND RESPONSE PLANNING</b>	<b>RECOVERY PLANS</b>
R1: CRITICAL ASSET IDENTIFICATION	R1: CYBER SECURITY POLICY	R1: AWARENESS	R1: ELECTRONIC SECURITY PERIMETER	R1: PHYSICAL SECURITY PLAN	R1: TEST PROCEDURES	R1: INCIDENT RESPONSE PLAN	R1: RECOVERY PLANS
R2: CRITICAL CYBER ASSET IDENTIFICATION	R2: LEADERSHIP	R2: TRAINING	R2: ELECTRONIC ACCESS CONTROLS	R2: PROTECTION OF PHYSICAL ACCESS CONTROL SYSTEMS	R2: PORTS AND SERVICES	R2: DOCUMENTATION	R2: EXERCISES
R3: ANNUAL APPROVAL	R3: EXCEPTIONS	R3: PERSONNEL RISK ASSESSMENT	R3: MONITORING ELECTRONIC ACCESS	R3: PROTECTION OF ELECTRONIC ACCESS CONTROL SYSTEMS	R3: SECURITY PATCH MANAGEMENT		R3: CHANGE CONTROL
	R4: INFORMATION PROTECTION	R4: ACCESS	R4: CYBER VULNERABILITY ASSESSMENT	R4: PHYSICAL ACCESS CONTROLS	R4: MALICIOUS SOFTWARE PREVENTION		R4: BACKUP AND RESTORE
	R5: ACCESS CONTROL		R5: DOCUMENTATION	R5: MONITORING PHYSICAL ACCESS	R5: ACCOUNT MANAGEMENT		R5: TESTING BACKUP MEDIA
	R6: CHANGE CONTROL		* R6: INTERACTIVE REMOTE ACCESS	R6: LOGGING PHYSICAL ACCESS	R6: SECURITY STATUS MONITORING		
				R7: ACCESS LOG RETENTION	R7: DISPOSAL OR REDEPLOYMENT		
				R8: MAINTENANCE AND TESTING	R8: CYBER VULNERABILITY ASSESSMENT		
					R9: DOCUMENTATION		
<b>APPLICABLE TO COMMUNICATION SYSTEMS</b>	* PROPOSED REVISION NOT YET APPROVED BY NERC						

Figure 2: Summary of NERC CIP 002-009 Requirements.

The following tables provide further details of these requirements as they apply to communications systems.

4.1.1 CIP 002-4 CRITICAL CYBER ASSET IDENTIFICATION

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Critical Asset Identification	Policy	None
R2: Critical Cyber Asset identification	Policy	Direct
R3: Annual Approval	Policy	None

Table 2: CIP 002 Mapping to Communication Systems

R1: Communications infrastructure is not explicitly included in the list of critical asset criteria.

R2: CIP-002 specifically excludes Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters. There are however, some cases where this exclusion would not apply and would therefore bring the communications links into play under NERC CIP.

In some instances, a portion of the communication equipment associated with transport links may come directly into play as cyber assets, and therefore must be evaluated under the CIP 002, R2 criteria. These instances are primarily centered on two architecture scenarios:

- The communication link is logically inside the Electronic Security Perimeter. While there may be numerous applications for this type of architecture, one specific example would involve a layer 2 network spanning two or more locations. This type of network architecture may be utilized to support a special protection application such as a Remedial Action Scheme (RAS). In this scenario, the overall protection system encompassing the communications link may have been designated as a Critical Asset by the entity.
- The management interface of the communications terminal is within the same Electronic Security Perimeter as a Critical Cyber Asset. This is further clarified in CIP 005; R1.4.

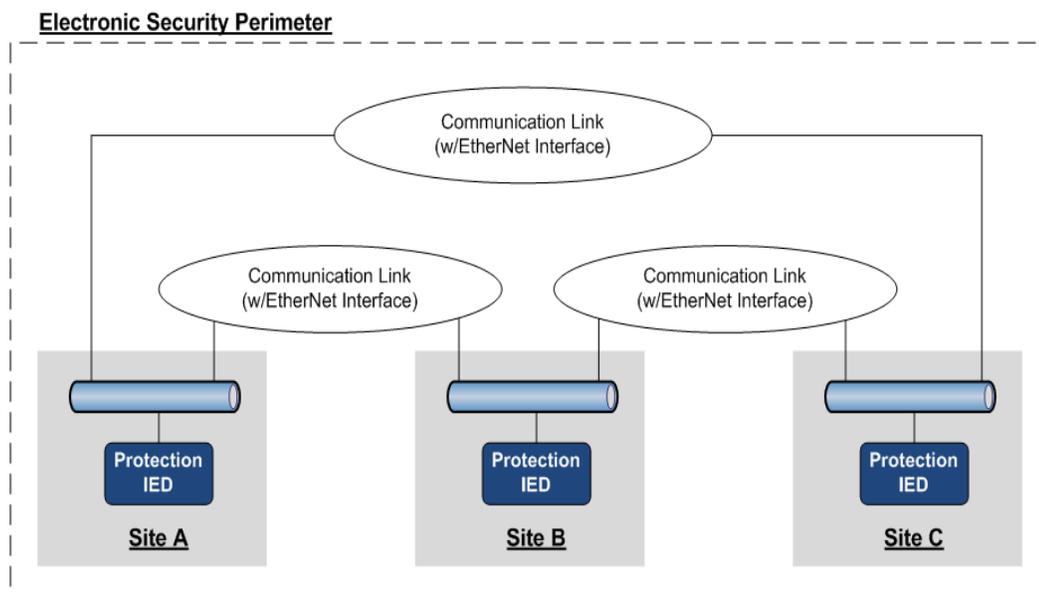


Figure 3: Architecture Example (Communications Link Inside ESP)

In both cases, this is ultimately an issue concerning how the system is implemented by the entity rather than the specific features of the communications equipment.

R3: This is a policy based requirement applicable to the entities security program and not the communications systems.

4.1.2 CIP 003-4 SECURITY MANAGEMENT CONTROLS

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Cyber Security Policy	Policy	None
R2: Leadership	Policy	None
R3: Exceptions	Policy	None
R4: Information Protection	Policy	None
R5: Access Control	Policy	None
R6: Change Control and Configuration Management	Policy	None

Table 3: CIP 003 Mapping to Communication Systems

All requirements outlined in CIP 003-4 are policy based requirements applicable to the entities security program and not the communications systems.

4.1.3 CIP 004-4 PERSONNEL AND TRAINING

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Awareness	Policy	None
R2: Training	Policy	None
R3: Personnel Risk Assessment	Policy	None
R4: Access	Policy	None

Table 4: CIP 004 Mapping to Communication Systems

All requirements outlined in CIP 004-4 are policy-based requirements applicable to the entities security program and not the communications systems.

4.1.4 CIP 005-4 ELECTRONIC SECURITY PERIMETER(S)

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Electronic Security Perimeter	Policy/Technical	Direct
R2: Electronic Access Controls	Policy/Technical	Direct
R3: Monitoring Electronic Access	Policy/Technical	Direct
R4: Cyber Vulnerability Assessment	Policy	None
R5: Documentation Review and Maintenance	Policy	None
R6: Interactive Remote Access [Proposed]	Policy/Technical	Direct

Table 5: CIP 005 Mapping to Communication Systems

R1: While normally accomplished utilizing routers or firewalls, communication systems may play a part in creating the ESP if they provide a mechanism for segmentation of Critical Cyber Assets from non-Critical Cyber Assets such as the creation of VLANs.

R2: In cases where the communication system is providing access to the ESP, three specific features need to be supported:

- Centralized authentication
- Role based access control
- Port and service filtering

In cases where the communications system is providing layer 2 access to the ESP, the following functions additionally need to be supported:

- Port Based Network Access Control (PNAC) such as 802.1x
- Disabling of unused physical ports

R3: To compliment the requirements in R2, utilities must be able to validate that only authorized users have access to the ESP and specifically the cyber assets within it. To facilitate this, the communications system should support features such as:

- Alerting and logging of authorized and unauthorized attempts to access the ESP
- Non volatile storage for logs during communications outages

R4/R5: These are policy based requirements applicable to the entities security program and not the communications systems.

R6: The change to CIP 005 adding this requirement pertaining to interactive remote access has not yet been approved by NERC. As it is currently written, the proposed requirement would be applicable to remote access of any communications terminal for the purposes of maintaining or supporting the communications system. Any external management application for the communications system could serve the function of an intermediate device. Any remote access to the management application should be encrypted and require multi-factor authentication.

#### 4.1.5 CIP 006-4 PHYSICAL SECURITY

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Physical Security Plan	Policy	None
R2: Protection of Physical Access Control Systems	Policy/Technical	None
R3: Protection of Electronic Access Control Systems	Policy/Technical	Direct
R4: Physical Access Controls	Policy/Technical	Indirect
R5: Monitoring Physical Access	Policy/Technical	Indirect
R6: Logging Physical Access	Policy/Technical	None
R7: Access Log Retention	Policy	None
R8: Maintenance and Testing	Policy	None

Table 6: CIP 006 Mapping to Communication Systems

R1: This is a policy based requirement applicable to the entities security program and not the communications systems.

R2: This requirement is applicable to physical access control systems and not communications infrastructure.

R3: While this requirement may be applicable to communications infrastructure which provides access control to the ESP, it is aimed at the entities physical protection of these systems.

R4/R5: While the communications systems are not directly covered under these requirements, they can be critical to the utility’s ability meet these requirements as a majority of the solutions available for remote facilities require reliable communications between these facilities and the centralized access control systems.

Availability of the communications may be an issue if the physical access controls can be circumvented and/or unauthorized access can go undetected by interrupting or disabling the communications systems in any way.

R6: This requirement is applicable to physical access control systems and not communications infrastructure.

R7/R8: These are policy-based requirements applicable to the entities security program and not the communications systems.

4.1.6 CIP 007-4 SYSTEMS SECURITY MANAGEMENT

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Test Procedures	Policy	None
R2: Ports and Services	Policy/Technical	Direct
R3: Security Patch Management	Policy	None
R4: Malicious Software Prevention	Policy/Technical	Direct
R5: Account Management	Policy/Technical	Direct
R6: Security Status Monitoring	Policy/Technical	Direct
R7: Disposal or Redeployment	Policy	None
R8: Cyber Vulnerability Assessment	Policy	None
R9: Documentation Review and Maintenance	Policy	None

Table 7: CIP 007 Mapping to Communication Systems

R1/R3/R7: These are policy based requirements applicable to the entities security program and not the communications systems.

In cases where the communications systems have been designated as Critical Cyber Assets or reside within the same ESP as a Critical Cyber Asset, the following functions need to be supported as noted for the specific requirements in CIP 007. This would apply to any logical interfaces to the communications equipment accessible from within the network such as is used for monitoring and management.

R2: Disabling of unused logical ports and services

R4: Anti-virus and malware prevention

R5:

- Logging of all user activity
- Role based access controls
- Least privilege
- Password policy enforcement

R6:

- Alerting and logging of unauthorized attempts to access the communications system
- Non volatile storage for logs during communications outages

4.1.7 CIP 008-4 INCIDENT REPORTING AND RESPONSE PLANNING

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Cyber Security Incident Response Plan	Policy	None
R2: Cyber Security Incident Documentation	Policy	None

Table 8: CIP 008 Mapping to Communication Systems

R1/R2: These are policy based requirements applicable to the entities security program and not the communications systems.

4.1.8 CIP 009-4 RECOVERY PLANS FOR CRITICAL CYBER ASSETS

Requirement	Type of Requirement	Applicability to Communication Systems
R1: Recovery Plans	Policy	None
R2: Exercises	Policy	None
R3: Change Control	Policy	None
R4: Backup and Restore	Policy/Technical	Direct
R5: Testing Backup Media	Policy	None

Table 9: CIP 009 Mapping to Communication Systems

R1/R2/R3/R5: These are policy-based requirements applicable to the entities security program and not the communications systems.

R4: In cases where the communications systems have been designated as Critical Cyber Assets or reside within the same ESP as a Critical Cyber Asset, the communications system should support the backup of all configuration settings and restoration to normal system operations from the backup.

4.2 REQUIREMENTS SIGNIFICANT TO MW RADIO SYSTEMS

Virtually all of the requirements identified in the previous section are significant to MW radio systems in various circumstances.

For cases when the MW radio system is providing a layer 2 interface to transport traffic between locations, the following security features should be supported.

The management interface to the MW radio system:

- Secure SNMP (SNMPv3)
- Secured Syslog
- Disable unused physical ports and services
- Disable “back door access”
- TLS for secure communication over unsecured networks
- Keys and Certificate management per ITU-T X.509
- Strong authentication:
  - Choice of Role-based or Identity-based (superior) authentication
  - Ability to assign different privileges to each user
  - RADIUS protocol for centralized user authentication.
  - Local user account information as a contingency for AAA server
  - Password complexity policing
- Secure (authenticated) software download
- Secure configuration storage/backup/restore
- All information stored on radio must be encrypted
- Secured Event Log with viewing policy to control user activity and what each one can see

- User craft interface viewing limited by permission-based filtering
- Access Control List
- Mechanized Attack Prevention
- Session timeout mechanism
- Warning banners for users
- Solution based on widely recognized standards (ex: FIPS 140-2)

The payload interface to the MW radio system:

- Encrypt payload (with negligible impact on latency)
- Use widely recognized encryption (ex: AES 128 and above)
- Solution based on widely recognized standards (ex: FIPS197)

### 4.3 AVIAT MW RADIO FEATURES SUPPORTING REQUIREMENTS

#### 4.3.1 SECURE MANAGEMENT

Management of the Eclipse Packet Node platform can be secured over unsecured networks. Strong Security supports secure management interfaces based on secure management protocols that have been validated against FIPS-140-2 requirements.

Secure Management is very flexible and provides the security customers need for microwave transmission management. Using a craft interface tool for configuration and maintenance, the Eclipse Packet Node radio can be securely managed via TLS v1.2 tunneling. For centralized monitoring from a network operations center (NOC), Eclipse Packet Node can be securely accessed by way of any network management system (NMS) that supports SNMP v3.

#### 4.3.2 PAYLOAD ENCRYPTION

To provide Strong Security, data and management payloads on Eclipse Packet Node radios can be encrypted. Payload Encryption through Strong Security prevents wireless communications from being eavesdropped on. Any eavesdropping equipment, or sniffers, along the transmission path between links or in the transmitter's vicinity will only receive a garbled transmission.

With AES encryption and 128-, 192- or 256-bit symmetric keys, a randomly generated encryption combination protects each Eclipse Packet Node wireless link pair. These combinations are created and negotiated between links using the industry-standard Diffie-Hellman Key agreement method, which supports groups with modulo of at least 2048 bits. Given this level of support, no particular encryption combination will be repeated within 835 years. Therefore, Payload Encryption is fully compatible with the AES encryption standard and complies with FIPS-197, which provides the definition for AES encryption.

#### 4.3.3 INTEGRATED RADIUS CAPABILITY

For an even higher level of protection, Strong Security on Eclipse Packet Node configures RADIUS capability into existing customer IT infrastructure. With integrated RADIUS capability, access control based on more sophisticated permission attributes can be provided. Eclipse Packet Node RADIUS capability enables authentication, authorization and accounting of remote user accounts, and integration also allows customers to manage user accounts within existing IT infrastructure from a central location—the same way PC user accounts are managed. With integrated RADIUS capability and the Security Event Logger feature on Eclipse Packet Node, all management activity attempts on Eclipse are tracked, including actions that affect traffic, logins and logouts, any changes to user accounts and other security events. It does this by recording user logins and IP addresses.

If communications to the RADIUS server are interrupted for any reason, Strong Security supports a fallback position. RADIUS credentials can be cached for a user-defined period. When the RADIUS server is unavailable, the cached credentials may be used to log in. For extended periods where the RADIUS server cannot be reached, the user-based security model allows logging in with the local SNMP user database.

#### ABOUT AVIAT NETWORKS

Aviat Networks, Inc. is a leader in wireless transmission solutions. We apply innovation and IP networking expertise toward building a carrier class foundation for future energy and mobile broadband networks. With more than 750,000 systems installed around the world, Aviat Networks has built a reputation as a leader in offering best-of-breed solutions including LTE-ready microwave backhaul and a complete portfolio of service and support options to public and private telecommunications operators worldwide. With a global reach and local presence in more than 46 countries, Aviat Networks works by the side of its customers allowing them to quickly and cost effectively seize new market and service opportunities. Aviat Networks, formerly Harris Stratex Networks Inc., is headquartered in Santa Clara, California, and listed on NASDAQ (AVNW). For more information or to join the dialogue, please visit:

[www.aviatnetworks.com](http://www.aviatnetworks.com)

For additional information and a copy of this paper, please visit [www.aviatnetworks.com](http://www.aviatnetworks.com)

WWW.AVIATNETWORKS.COM

Aviat, Aviat Networks and Aviat logo are trademarks or registered trademarks of Aviat Networks, Inc.

© Aviat Networks, Inc. 2011. All Rights Reserved.

Data subject to change without notice.

\_w\_Utility\_Electric\_Grid\_Security\_UNIV\_EcliPktNd\_04May11

