

Securing SCADA Communications following NERC CIP Requirements

Mira Zafirovic-Vukotic, Roger Moore, Michael Leslie, Rene Midence, Marzio Pozzuoli,
RuggedCom Inc.

Asia Energy Week 2008, Kuala Lumpur, Malaysia, May 2008

Abstract

Electric utilities require secure network and control system communications that conform to the recommendations of the NERC (North America Electric Reliability Corporation) CIP (Critical Infrastructure Protection) cyber security framework for identification and protection of critical cyber assets to support reliable operation of the bulk electric system. This paper summarizes the major technological requirements of secure control networks and illustrates solutions for control networks and equipment, SCADA data and communications that are a foundation for conformance to the regulatory security requirements and industry standards for control network operation, like NERC CIP, IEC and NIST. It also introduces the newly developed IEC 62351 security standard for SCADA data and communication protocols. The paper also includes guidelines and requirements for secure network equipment that form a technological foundation for secure SCADA system and network equipment planning, as well as a sound basis for network security management. Secure communications equipment and network communication methods are addressed in the paper.

1. Introduction

The loss of integrity or of availability of data has the potential to adversely affect power utility core operations. The overall security concern facing the designers and operators of SCADA and, more generally, of industrial control systems typically originates either from malicious threat agents attempting to disrupt the control system operation, e.g. to create a power outage, or it originates from inadvertent actions, equipment failure, or similar.

NERC CIP standards 002-009 provide a cyber security framework for identification and protection of critical cyber assets to support reliable operation of the bulk electric system. The utility's security risk analysis determines

security requirements based on an assessment of threats, vulnerabilities and impacts. Security functions in the cyber security perimeter are derived from the risk analysis.

End-to-end communication between any two devices e.g. located in a control center and in a substation, is typically structured according to IEC 60870, IEC 61850, etc. To address security vulnerabilities, organizations primarily install security retrofits or upgrades to their existing SCADA systems. The corresponding standardization bodies and regulatory agencies also deal with the design of new secure systems. For example, security enhancements to IEC control protocols are available and being further developed in IEC 62351 standards.

SCADA communications include a diverse set of layered protocols and physical media. A large class of SCADA protocols is implemented using

TCP/IP protocols. Utilities' communications network of choice, dedicated for control applications is typically a private IP (Internet Protocol) network (referred to as intranet) and/or an Ethernet. Corresponding open data communications security methods that may be used include firewalling, VPN (Virtual Private Network), tunneling, authentication, cryptography, and IDS (Intrusion Detection System). These methods are standardized by organizations like NIST (National Institute of Standards and Technology), IETF (Internet Engineering Task Force) and ISO (International Standards Organization) in the framework of IP communications and information security standardization. One example is the NIST 800 standards series.

Typically there are two major analysis methods in regard to security which form the basis for discussion: enterprise based analysis and technology/threat based analysis. Both approaches have disadvantages.

There are vendors who can offer integrated solutions that meet important technical requirements of secure control networks, SCADA data and protocol communications that are conformant to the regulatory security requirements and industry standards for control network operation, like NERC CIP [1], IEC [2] and NIST [3]. They are the reference standards for diverse implementations, without being the only possible solutions.

The requirement of a high level of network security is related to other critical requirements of SCADA communication networks, including [5]:

- Electrical and environmental requirements for communications equipment in substations addressing harsh environmental conditions
- Bounded response times for real-time SCADA applications
- Network resilience, or the ability to heal around failures

In each particular control system and network, the security risk must be assessed and security measures determined accordingly. One should be aware that there is often a trade-off between security, cost, and performance when choosing one method over another. In general, multiple levels of security mechanisms and measures are needed to ensure robust control system communication.

In this paper we provide at first the historical background and the state of the art related to security guidelines. We then introduce cyber security incident and attack scenarios in brief. Newly standardized secure SCADA protocols are briefly described next. Secure communication network topology, methods, techniques and equipment are outlined. Finally, we show reference SCADA network architecture and draw conclusions.

2. SCADA Security

Current State

Diverse institutions publish guidelines and provide related security services addressing the electric utility SCADA network and its components.

NERC has provided a number of standards related to cyber security of electric power systems. The old ones, UA 1200 – Urgent Action Cyber Security Standards, have been replaced by NERC CIP, see [1]. We derive requirements for communication equipment based on the CIP 002-009 standard, see the remainder of Section 2.

FERC (Federal Agency Regulatory Commission) has accepted NERC CIP requirements as the obligatory ones for power utilities and designated them as Electric Reliability Organization (ERO) [12]. NERC will continue to monitor the development and implementation of cyber security standards by NIST to determine whether they contain provisions that can enhance the CIP reliability standards.

IEC SCADA control systems and protocols are being extended by the security methods and protocol mechanisms in IEC 62351, see the remainder of Section 2 for a quick introduction.

A few reference documents have been developed over the past few years that provide guidance for secure SCADA, e.g. NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security [3]. This document identifies typical threats and vulnerabilities to these systems and recommends security countermeasures to mitigate the associated risks, including a few reference network architectures.

In addition, NIST, ISO, IETF, IEEE and other bodies are developing standards and

recommendations that apply to general purpose, open communication systems security, see e.g. [8] and [9]. These recommendations are often applicable to SCADA networks, but require appropriate interpretation, see e.g.[3].

Equipment and NERC CIP Standards

NERC (North American Electric Reliability Corporation) CIP (Critical Infrastructure Protection) standards 002-009 [1] provide a cyber security framework for identification and protection of critical cyber assets to support reliable operation of the bulk electric system. NERC CIP requirements can be mapped onto requirements for communications equipment that is used within an Electronic Security Perimeter (ESP), deriving the following main ones that we refer to here in brief:

- Security monitoring that detects, logs and issues notifications related to cyber security
- Security audit logs that are easily retrievable and stored reliably
- Strong technical controls at interactive access points to ensure the authenticity and authorization of accessing parties
- Logging of access attempts at access points to the ESP, including dial-up devices
- Anti-virus software, IDS and other tools to prevent malicious software, along with related updates
- Ports and services required for normal and emergency operations should be enabled at any point in time, and the others should be disabled or not accessible.
- Security patches and security upgrades to software
- Passwords of diverse types of characters and of mandatory minimum length
- Resource availability is a prerequisite for any security method, thus a high level of availability is required for all resources.

Secure SCADA Protocols

The IEC 62351 standard defines security for SCADA data and protocols that are in the scope of IEC, see [2] and [4]. IEC 62351 defines end-to-end security methods for SCADA protocols and security in diverse protocol layers in layered

communications architecture. We explain them in brief in the following.

Most importantly, message origin authentication and data integrity is introduced to SCADA protocols, e.g. by means of hash function. This ensures that spoofed or replayed SCADA messages are discarded. Note that data may be exchanged in the clear.

For user authentication, both asymmetric and symmetric keys may be used. Public Key Infrastructure (PKI) and certification authorities may provide digital certificates that include asymmetric keys.

Data encryption in SCADA communication protocols is performed by means of running a SCADA application level protocol over TLS (Transport Layer Security), which encrypts data end-to-end. RFC 4346 TLS runs in the layers beneath application protocols such as SCADA or HTTP, is comparable to TCP (Transmission Control Protocol). TLS provides one of the most commonly available mechanisms to secure TCP/IP protocols.

Data encryption is not required by the standard for SCADA end devices that do not use TLS/TCP and that access the network through a serial interface, see IEC 62351-5, or via Ethernet without TCP, e.g. GOOSE (Generic Object Oriented System Event), see IEC 62351-6.

Applying cryptographic and protocol mechanisms such as IEC 62351-3, and -4 to SCADA communications provides end-to-end authentication, integrity, confidentiality, and non-repudiation. Additional data encryption should not be implemented in the communication network in order to avoid redundant processing and to keep the end-to-end delays small.

If a SCADA protocol does not provide end-to-end authentication, integrity and non-repudiation, then the overall communication is not fully secured, e.g. if IEC 62351 is not implemented. A control system communications network should therefore implement security methods as appropriate. For example, IPsec can provide security functions between firewalls and/or routers that include authentication and encryption.

3. Secure SCADA Network

Technology and Methods

Network resource, routing and management information exchange should be secured in a communications network used for control purposes. Multiple levels of security measures may be implemented. The level of security protection strongly depends on risk assessment and performance requirements.

Topology, Routing and Protocols

Network reliability should be ensured by making use of redundant topology and functionality. This includes layer 2 mesh topologies with RSTP (Rapid Spanning Tree Protocol) on the substation LAN (Local Area Network) [5], [6], [7], OSPF (Open Shortest Path First) on the intranet and VRRP (Virtual Router Redundancy Protocol) for redundant access to the IP network and backup links between the routers.

In addition, traffic may be segregated using VLANs to further increase security. Some protocols, such as IPv6, OSPFv3 (see RFC 2740) and SNMPv3 (e.g. see RFC 3826), provide their own mechanisms for authentication and data encryption.

MAC address filtering should be used on Ethernet switches and IP address filtering, i.e. IP access lists, should be used on firewalls to define the end devices that are permitted to connect to network devices.

QoS (Quality of Service) mechanisms should be used to ensure bounded latencies for real-time SCADA applications and to ensure network resource availability. Messages should be prioritized and PQ (Priority Queuing), CBWFQ (Class-Based Weighted Fair Queuing) or similar queuing mechanisms should be used on routers and switches. IEEE 802.1p prioritization should be used on LAN switches and IP based prioritization should be used on routers.

User and Device Authentication

The most often used AAA (Authentication, Authorization and Accounting) server is the Remote Authentication Dial-In User Service (RADIUS) (RFC 2865 and 2866) using IEEE 802.1x with the Extensible Authentication Protocol (EAP). It plays a key role in user

authentication at all levels in the network. For example, firewalls and access routers can act as authenticating agents, intermediaries for client devices or entities connecting to them, such as wireless devices and end user equipment. The authenticating agent challenges the entity, which authenticates itself, e.g. using a username and password, which are forwarded to and processed by the authentication server, e.g. RADIUS, that gives authorization and access rights to the client.

Passwords should be encrypted when sent across a network. Some form of cryptographic hash should be used that is specifically designed to prevent replay attacks e.g. approved by FIPS (Federal Information Processing Standards), see [6].

One may supplement password authentication with other forms of authentication such as challenge/response or by using biometric or physical tokens. Physical tokens are suitable in physically secure area.

Role Based Access Control (RBAC) should be used to restrict user privileges to only those that are required to perform a task. Currently, IEC TC57 WG15 has initiatives to develop standards to define RBAC for SCADA communications.

All system administrator communication must be authenticated, confidential and its integrity protected. The following methods provide such security: SSHv2 (Secure Shell), rather than Telnet and HTTPS (Hyper Text Terminal Protocol over Transport Layer Security), RFC 2818, rather than HTTP

Firewalls

Network firewalls control data flow between networks employing differing security postures. NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, provides general guidance for selection of firewalls and firewall policies [8].

In a SCADA environment, a firewall must be deployed between the SCADA control network and the business network. Firewalls should include the following features: extensive logging of events, IDS, DMZ (DeMilitarized Zone) based policy routing, access lists, etc.

Firewall use depends strongly on network topology. Their use in SCADA networks will be explained further in the reference scenario presented in coming sections.

IPsec VPN

An IPsec-based VPN can provide tunneling between physical security perimeters. It typically runs between the corresponding firewalls, or as needed, between routers. A remote user can also gain access to a secure perimeter by connecting via an IPsec VPN. IPsec can ensure integrity, authenticity and confidentiality of data, see e.g. [11] and [9].

The technique involves establishing an IPsec tunnel over an arbitrary, possibly insecure, IP network, and transmitting data through the tunnel. Each IP packet is encrypted and encapsulated within an additional IP packet at the IPsec tunnel ingress. Routers use the new IP header information to forward the packet between the tunnel endpoints. The original frame is extracted and decrypted at the tunnel egress. IPsec uses one or both of the Authentication Header (AH) and Encapsulating Security Payload (ESP) protocols. AH provides data integrity and packet origin authentication. ESP encrypts the IP packet. IPsec including both AH and ESP is a mandatory part of IPv6 implementation. Its use is optional both with IPv4 and IPv6. See RFC 4301–4309, for further explanation

IPsec devices use Internet Key Exchange (IKE) to authenticate the peer, negotiate and distribute symmetric encryption keys, and establish IPsec security associations. IPsec often uses pre-shared key and signature for device authentication.

IPsec can use shared secret keys only, or it can make use of PKI. Efficient IPsec VPN management in a smaller network may imply that the administrator can easily configure secret keys.

An IPsec-based VPN should be implemented only if necessary to augment the end-to-end security methods already in use by a SCADA application. IPsec authentication may be used without SCADA performance degradation. IPsec encryption should not be implemented if SCADA runs over TLS as in IEC 62351-3 and -4. Re-encrypting data traffic is generally redundant, costs additional processing resources, and causes the traffic to incur additional latency in transit.

Intrusion Detection System

An Intrusion Detection System (IDS) issues alerts when a system is being probed or attacked, see [8]. It generally collects information from different sources at strategic points in the network, analyzes the content of individual packets for malicious traffic, and then issues alarms, drops data, logs events and activities, and initiates other responses as necessary. IDS vendors also develop and incorporate attack signatures for various application protocols such as DNP (Distributed Network Protocol) and ICCP (Inter-Control Center Communications Protocol), in addition to the usual signatures, see [3].

Network based IDS are deployed on control network equipment. Host based IDS are deployed on SCADA servers, systems that use general purpose operating systems, and those running SCADA protocols, etc. Integrated IDS control of agents in network equipment and in SCADA devices is the most efficient implementation of IDS, since they include host-based and network based IDS. Note that the addition of IDS agents has the potential to adversely affect system performance.

Wireless and Modem Links

Modems are often used to provide backup links. Callback systems can be used to ensure that a dialer is legitimate by using the callback number stored in a trusted database. Remote control software should use unique user names and passwords, encryption, and audit logs. Link layer neighbor authentication should be done e.g. using CHAP (Challenge Handshake Authentication Protocol) of RFC 1994.

Wireless user access and links between network equipment may be implemented in several ways. Users or nodes may act as wireless clients of an IEEE 802.11b/g network access point, or two or more nodes may form a point-to-point or multipoint fixed installation using 802.11 Ad-Hoc mode. All wireless communication should be protected by the available security features such as strong data encryption protocols e.g. IEEE 802.11i with AES support. Wireless access should use IEEE 802.1x authentication which authenticates clients either via user certificates or via a RADIUS server. Hardware accelerators may be needed to perform cryptographic functions to reduce encryption latency. For an overview of 802.11 wireless networks see e.g.

Reference SCADA Control Network

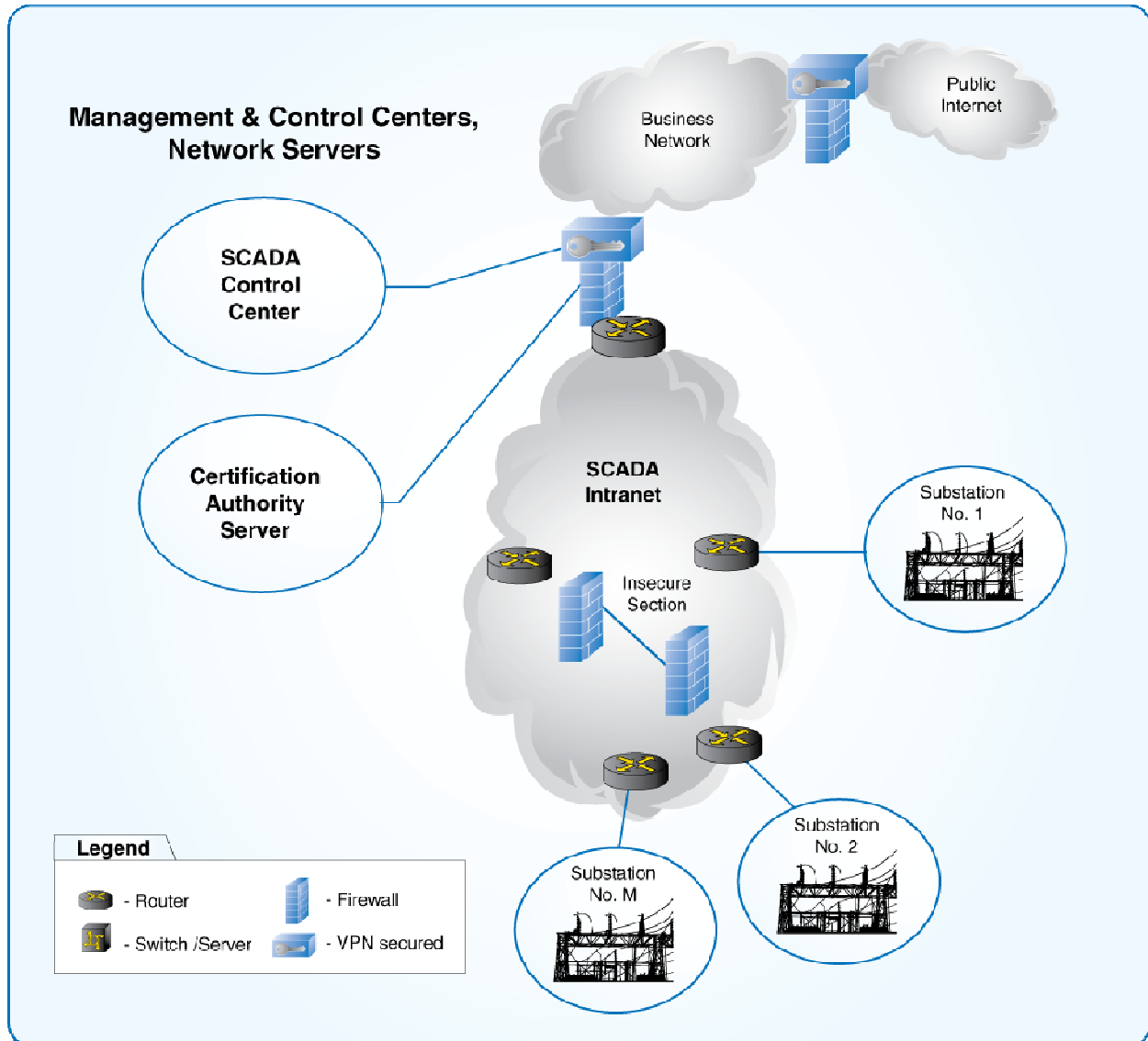


Figure 1. Reference SCADA control network.

[14] and for a quick overview of wireless access implementation within substation, see e.g.[13].

Time Synchronization

Real-time clocks in each piece of SCADA and network equipment should be synchronized, and

the correct time should be logged along with each entry in the event log. To that end, NTP (Network Time Protocol) and IEEE 1588 are used. The older NTP is widely used throughout the Internet and is accurate in the face of a wide range of network latencies and varying conditions. The much newer IEEE 1588

addresses the clock synchronization requirements of measurement and control systems.

Service for both protocols may be provided by standalone equipment or by components of other network equipment or of general purpose computer equipment. The required time precision is not in the scope of NERC CIP, although it does require extensive logging on all equipment to make security event analysis possible and effective.

Network and Security Management

SCADA protocols, telecommunication networks, and TCP/IP networks may use different management methods. Standardization effort on IEC 62351 should also lead to a generic management information model and a MIB (Management Information Base) module for security management of control protocols and communication networks. It is not in the scope of this paper to discuss security aspects of management protocols in detail.

SNMP (Simple Network Management Protocol) is traditionally used to manage IP network resources such as routers, firewalls and servers. SNMP may also be used to provide integrated management of SCADA applications and control networks. SNMPv3 includes the security features fundamentally required by NERC CIP: message integrity, authentication and encryption. See RFC 2574 and RFC 3826.

Security management applied to SCADA networks and applications includes monitoring, analyzing, providing security and responding to incidents. This includes dynamic adaptation to new security requirements as they change, prioritization of security vulnerabilities, and mapping them onto management of the following: AAA (e.g. RADIUS), security keys, traffic filtering, IDS, logging, etc.

Integrated security management systems for SCADA and general networks are emerging on the market. An integrated security system can include easy audit log accessibility, centralized user authentication, integrated key management, security logging and dynamic firewall configurability through a centralized control centre, see e.g.[10].

4. Secure SCADA Network

Architecture

Starting from the security requirements of NERC CIP, in particular as mapped onto network equipment requirements, as well as starting from the cyber security incident scenarios and possible attacks on SCADA systems, secure SCADA and network protocols, security key management and secure control network technologies, all presented in previous sections, we now take the next step and derive a reference SCADA control network (illustrated in Figure 1). It includes the following:

- substation communications network
- control centre communications network
- core network
- security firewalls to separate the network
- network servers and SCADA hosts

When planning a control network, the organization, and the network planners in particular, interpret the security risk assessment and implement security measures for the SCADA network. In the scope of this paper, we outline general solutions, rather than specifics and variations. Requirements and best practices vary and should be analyzed on an organization by organization basis. Numerous variations on the reference configuration are possible.

The control network core is typically an intranet, i.e. a private IP network that is based on routers and other technology that has the functionality of the equipment used on the public Internet. Substation and control centre sites run Ethernet locally and connect to the IP core network via firewalls, see Figure 2.

The core network may also be implemented entirely as a single Ethernet network, using switches only, with no IP routing. Industrial control systems (ICS) networks often have such a topology. This is often due to one of the following reasons: small core network area, large control sub-system area, a single physical security perimeter, fiber link availability, etc.

Transmission networks and link types that may be used to connect routers and firewalls include the following:

- Frame Relay (FR) or ATM (Asynchronous Transfer Mode) circuits
- SONET (Synchronous Optical Network) or SDH (Synchronous Digital Hierarchy), PDH

(Plesiochronous Digital Hierarchy) links e.g. T1/E1 links

- Modem, DSL (Digital Subscriber Line) and other access lines.
- Wireless access e.g. IEEE 802.11b/g.

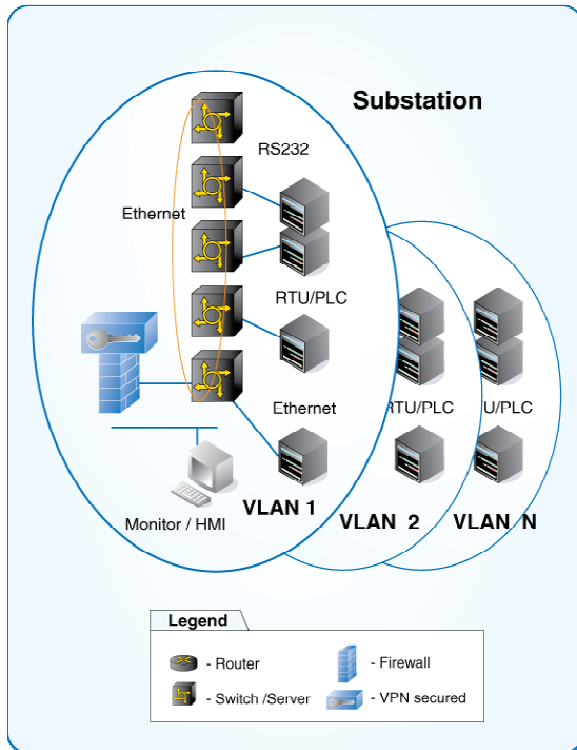


Figure 2. Reference substation control network.

The SCADA control network and the business network are separate networks connected across a firewall. This way, security and performance issues on the business network do not affect the control network. The business network and the control network should not communicate directly with each other and there should be no direct path between them. There should be one or more DMZs connected to the firewall such that restricted communication occurs between the business network and the DMZ, and the control network and the DMZ. Stations and servers for the SCADA system and control network that need to be accessed from the business network are placed in the DMZ [3].

There should be a firewall at the substation network interface to the core IP network, since this is typically an access point to the physical security perimeter of the substation. The firewall can connect to one or more routers on the core

IP network. It may also be a part of the core IP network or just be providing high availability access to the core.

SCADA intranet firewalls should typically include the following functions:

- A stateful firewall between the control network and business network
- Site firewalls operate at the connection level, e.g. on a TCP connection.
- The firewall is an IPsec tunnel end point.
- Access from insecure sections of the SCADA network should be protected by firewalls.
- Policy based routing by means of access lists and firewall zones
- Packet filtering based on IP destination or source address, port number, MAC address

IPsec VPNs in the SCADA intranet should have the following properties:

- An IPsec authentication function should provide site-to-site authenticated VPN connectivity.
- An IPsec encryption function may be used to traverse insecure sections of the IP network if needed, e.g. to connect two routers or firewalls through a less secure carrier, but only if encryption is not implemented by a SCADA application as in IEC 62351 for some protocols.
- Remote access to the network and application resources should be done using an IPsec VPN. Remote user authentication should preferably use smart tokens and PKI based authentication.
- VPN management should be implemented efficiently including a VPN monitor.

Note that remote access from other networks or hosts to SCADA network resources cannot be said to be completely without risk since the same mechanism used for legitimate access can also be attacked by an intruder. Remote access may be needed, for example, for data exchange between two power utilities, or to allow engineers to respond quickly to a situation.

Environmentally hardened switches, firewalls and routers should be used in substations and in any location that has harsh electrical and environmental conditions. Critical control system and network components have high availability requirements that typically include redundancy. Examples of the kinds of redundancy that might be used are:

- A critical network link may be implemented with provision for a backup link.

- A networked host may have a backup NIC (Network Interface Card).
- Redundant communication protocols such as VRRP may be used.
- Network topology should include redundant paths, either at layer 2 using RSTP, at layer 3 using OSPF, or in combination.

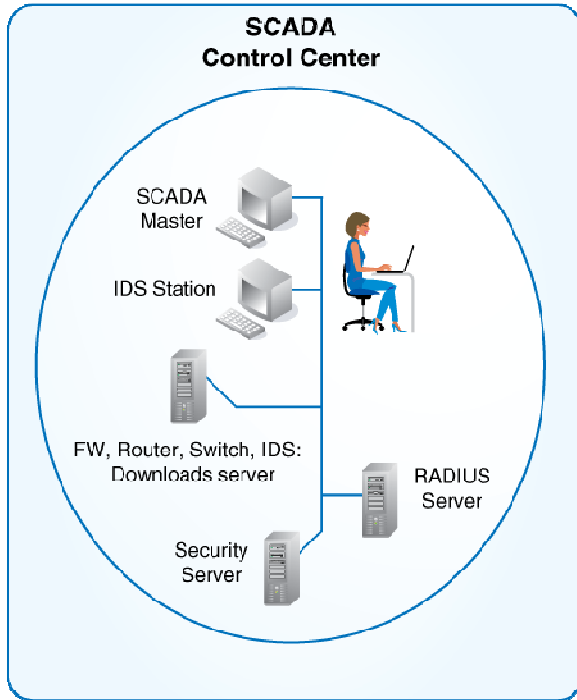


Figure 3. Reference control centre network.

Ethernet networks may benefit further from the following techniques:

- Virtual networks, isolated from one another, may be implemented on a single Ethernet using VLANs (IEEE 802.1q).
- Traffic may be prioritized using IEEE 802.1p, i.e. traffic with critical latency requirements may be configured to take priority over all other traffic on an Ethernet.

See the reference scenario in Figure 1 for illustration of some of the above.

Other methods to provide security include the following; see the previous sections for more explanation:

- SSH and HTTPS administrator access
- SNMPv3 management
- Integrated IDS
- Extensive logging

A SCADA control and network management center, see Figure 3, may include the following functions which apply to SCADA applications and to control networks in general:

- SCADA system management of end devices and applications
- Substation LAN management
- Transmission and link layer management
- IDS and anti-virus management
- Authorization server for access control
- Security key management
- Certification authority server for the control network, along with a backup mechanism, deployed within PKI
- Security policy management server
- Audit server to track security related events
- IPsec VPN management
- Diverse patch and download servers
- Time synchronization server

For the purpose of security, control and management centre functions should be located in one or more dedicated DMZs behind a firewall, and may be implemented on a number of different computers.

5. Conclusion

A networked SCADA application can be secured to a high level by implementing, as appropriate, the techniques, protocols, network topologies, and policies illustrated in the reference SCADA control network in this paper.

Whether planning a new SCADA implementation or securing an existing one, the selection of equipment, software, and techniques used to ensure security must take into account the following:

- an evaluation of security risks and of the vulnerability to those risks,
- corporate security policy, which itself should reflect the requirements of NERC CIP, and
- an evaluation of the trade-offs between complexity and performance.

The critical asset cyber security framework that applies to SCADA systems and networks is provided in NERC CIP standards 002-009. In this paper, we have shown how these requirements map onto and can be realized using secure communications equipment that includes the following general features: security monitoring, logging and security notifications,

authentication control at interactive access points, access logging including dial-up devices, anti-virus software, IDS, security patches, security upgrades to the software, and the ability to enable only those ports and services required for operations.

We have also provided an introduction to the newly developed IEC 62351 security standard for SCADA data and communications. Taking into account the levels and types of security methods implemented by SCADA protocols, we derived a reference secure SCADA control network architecture that is a sound basis for organization conforming to the security requirements of NERC CIP, see Figure 1. Secure communications equipment and methods include the following:

- Encrypted authentication at all levels and authorization service e.g. RADIUS
- Secure SCADA control protocols e.g. using TLS, see IEC 62351
- Firewalls to protect each SCADA site and dedicated DMZs for servers and hosts
- Secure management e.g. via SNMPv3, secure administrator access e.g. via SSH and HTTPS
- IPsec tunnels on insecure network sections which implement authentication but not necessarily encryption
- Time synchronization for SCADA and network equipment
- Integrated IDS system for SCADA and network equipment
- PKI for cryptographic public key management, and/or efficient cryptographic secret key management
- Integrated security management for SCADA and network systems that includes security audit log retrieval and user authentication

References

- [1] North American Electric Reliability Council (NERC), Critical Infrastructure Protection Committee, NERC Standard CIP-002 through -009, Cyber Security, June 2006
- [2] IEC 62351 Power systems management and associated information exchange Data and communication security, 2006-2007.
- [3] NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, Second Public Draft, Sept. 2007.
- [4] Cleveland, F., IEC TC57 Security Standards for the Power System's Information

Infrastructure – Beyond Simple Encryption, Transmission and Distribution, Conference and Exhibition 2005/2006 IEEE PES, Page(s):1079 – 1087 Digital Object Identifier 10.1109/TDC.2006.1668652

- [5] Marzio Pozzuoli, RuggedSwitch™ Reliability, Immunity, Performance, available at <http://www.ruggedcom.com>
- [6] The Automation of New and Existing Substations: Why and How, CIGRE Study Committee B5, available at http://grouper.ieee.org/groups/1525/CIGRE3_4.07/Document/, August 2003.
- [7] Michael Galea, Marzio Pozzuoli, Redundancy in Substation LANs with Rapid Spanning Tree Protocol (IEEE 802.1w), Electric Energy T&D Magazine, Sept.-Oct. 2003, pp. 66-68.
- [8] NIST SP 800-41, Guidelines on Firewalls and Firewall Policy, provides general guidance for the selection of firewalls and the firewall policies.
- [9] NIST SP 800-77 Guide to IPsec VPNs, December 2005
- [10] Gauntlet security system, available at <http://www.teltone.com>
- [11] John Mairs, VPNs: A Beginner's Guide, McGraw-Hill Co., 2002, ISBN 0-07-219181-3.
- [12] Federal Agency Regulatory Commission (FERC) "FERC approves new reliability standards for cyber security", <http://www.ferc.gov/news/>, January 2008
- [13] A. MacDonald, Make the most of maintenance resources with wireless substation monitoring, Joseph, 03/23/2007, Energy Tech Magazine.
- [14] 802.11 Wireless Networks: The Definitive Guide, Matthew S. Gast, O'Reilly, CA, April 2005.

Biographies

Mira Zafirovic-Vukotic is the R&D quality manager of RuggedCom. She graduated from Faculty of Mathematics, University of Belgrade, with major in computer science, in 1981 and obtained a PhD in tele-informatics from University of Twente, the Netherlands in 1988. Her previous employers were M. Pupin Institute and Agilent. Her experience includes communication protocols, performance analysis, security and control systems. She authored 6 IEEE/ACM journal papers related to communication systems, as well as numerous

other publications. Mrs. Zafirovic-Vukotic is a senior member of IEEE and member of IEC TC57 WG15.

Roger Moore is the Engineering Vice President of RuggedCom. He graduated from the University of Toronto in 1990 with a B.A.Sc. degree majoring in computer science and physics. He was previously a project manager for GE Power Management. He lead development of networking, substation automation and advanced protective relaying technology. Mr. Moore holds patents related to advances in communications and protective relaying technology. He is a member of the IEEE and is involved in developing the IEEE 1588 standard.

Michael Leslie is an Application Engineer with RuggedCom Inc. For more than 15 years, he has developed embedded software and solutions in fields as diverse as communications-based train control, broadcast video editing and distribution, network routing and services, DSP for multimedia, telephony, and paging, precision timekeeping, and custom cellular data networks.

Rene Midence is the Utility Market Manager of RuggedCom. He graduated from the University of Honduras in 1983 in Electrical and Industrial Engineering. He previously worked for GE Multilin. His experience covers the design and commissioning of power substations and power plants for over 25 years, including protection and control, SCADA, substation automation and LANs. Mr. Midence is a member of IEEE and of IEC TC57 WG10.

Marzio Pozzuoli is the founder and president of RuggedCom Inc. He graduated with a BEE from Ryerson Polytechnical Institute, Toronto in 1986. He was the Technology Manager for GE Power Management / Multilin,. Mr. Pozzuoli lead development and holds multiple patents related to advances in communications, protective relaying technology, and automation technology. As a member of the IEEE PES Substations Committee C2TF1 Mr. Pozzuoli participated in standardization of communications networking devices.