Research Trend on Secure SCADA Network Technology and Methods

Farkhod Alsiherov[1], Taihoon Kim[1*]
[1]Dept. Multimedia Engineering
Hannam University
Daejeon, South Korea
sntdvl@yahoo.com, taihoonn@paran.com

Abstract: 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. Electric utilities require secure network and control system. This paper illustrates solutions for control networks and equipment, SCADA data and communications.

Key-Words: SCADA security, Secure SCADA networks, SCADA systems

1 Introduction

SCADA controls Critical Infrastructure. Aside from SCADA's internal vulnerabilities, the fact that it controls Critical Infrastructure makes it more vulnerable and gains many threats.

SCADA refers to the combination of telemetry and data acquisition. SCADA includes the collecting of the information via a RTU (remote terminal unit), PLC's (Programmable Logic Controllers) and IED's (Intelligent electronic devices), transferring it back to the central site, carrying out any necessary analysis and control and then displaying that information on a number of operator screens or displays. Three of the most important part of a SCADA system are Master Station, Remote Terminal (RTU, PLC, IED) and the communication between them. Unlike application or operating systems, These systems usually sold as bundled packages by the vendors, so the end-user really doesn't know what is inside and what needs patching to keep it safe from emerging vulnerabilities and threats.

SCADA affects the daily lives of millions because it caters services which include power generation plants, potable water systems, wastewater treatment facilities, oil and gas production and transportation/distribution networks. SCADA systems are vulnerable to both cyber and physical attacks. Cyber Vulnerabilities includes attacks by worms, spam, virus and more others which cause inauspicious degrees of harm to the critical infrastructures ranging from the controllable to the severe attacks.[1][2]The critical data such as consumer specific information are often the target of shrewd thieves who prey on the financial services industry. On the other hand, physical vulnerabilities which include electricity blackouts, floods, earthquakes and hurricane which are although great disasters can be resisted with a strategic protection and exploiting the vulnerabilities of a SCADA systems so as to generate a more efficient protective measures.

The size and scope of critical infrastructure is gigantic. The critical infrastructure systems encompass almost everything that's why a destruction of such type of system would greatly affect a nation.

Several problems were posted in most SCADA R&D such as in the Standard and Methodology. This includes the issue of inability to test the security of infrastructure systems and to describe the industry's security readiness in a consistent manner. Another is the modeling and analysis issue which means the inability to model the entire infrastructure and represent the interdependences. Most R&D focuses on the development and extensible models of the critical infrastructure to enable planning, simulation and predictions of response to change and anomalies. This will have a great impact in the economic, human interaction, organizational structure, and technology development, accidental and malicious faults.

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)

*Corresponding author

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.

Typically there are two major analysis methods in regard to security:

1. Enterprise based analysis
2. 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.

2. SCADA Components

While exceptions exist, such as self-contained and stand-alone SCADA systems that are purpose built for a given application, most SCADA systems are comprised of
several components that communicate across a network.

2.1 Remote Terminal Units (RTUs)

An RTU (Remote Terminal Unit) provides intelligent I/O collection and processing, such as reading inputs from switches, sensors, and transmitters and then arranging the representative data into a format that the SCADA system can understand. The RTU also converts output values provided by the SCADA system from their digital form into that which can be understood by field-controllable devices such as discrete (relay) and analog outputs (current or voltage).

2.2 Programmable Logic Controllers (PLC)

The PLC can be regarded as the " brain" of the SCADA system. The actual control program for a given process or its control systems is executed within the PLC. A PLC can either work with local physically connected inputs and outputs or with remote inputs and outputs provided by an RTU. Typical PLCs can provide for two different types of control: discrete and continuous.

Discrete Control

In discrete control applications, the PLC works with inputs and outputs that have defined states (on/off) and can perform actions based on time, events, or a particular sequence (for example, turn on an output at a given time, turn off an output after the input from a field device, such as a limit switch closes; turn on a series of outputs in a given sequential order).

Continuous Control

In continuous control applications, the PLC typically works with analog input and output devices and uses special algorithms to maintain a steady operating state. For instance, the PLC has a set point that is provided by the SCADA system for the desired temperature of a given process. It receives an analog input value of 0 to 100 percent, representing the process temperature. The PLC uses specialized algorithms (such as PID algorithms) to generate an analog output value of 0 to 100 percent that is then used to position a valve or to control the speed of a motor in an effort to continuously keep the temperature at the desired set point.

Combinations of both discrete and continuous control are often used in what is referred to as batch control. In batch control applications, both discrete control and
continuous control are used together. In the simplest of terms, discrete operations could be used to mix the given ingredients of a recipe and place the batter in a pan
in the oven, while continuous control would be used to maintain the oven at a specific temperature to create the finished product—the cake.

2.3 Human Machine Interface (HMI)

The HMI (Human Machine Interface) is the means by which the user (operator) interacts with the SCADA

*Corresponding author

system. Simply put, the HMI provides a clear and easy-to-understand computer representation of what is, in fact, being controlled or monitored by the SCADA system. Further, it provides for interaction, either in the form of a touch screen, a specialized keyboard, or both.
Current-generation SCADA HMIs are not just a replacement for push buttons and pilot lights of the past. In fact, they provide a simpler user interface for even the most complex SCADA systems. The "usability" of the HMI is the measure by which a user can effectively interact with the SCADA system. HMI implementations that offer high levels of usability provide SCADA systems that are intuitive, efficient, and effective. A good and effective SCADA HMI design makes the interaction with the SCADA through the HMI seem natural to the operator—in other words, clear and easy to understand, with no need for explanation.

2.4 Distributed Control Systems (DCS)

Historically, the term DCS could best be defined as a dedicated control system that did not rely upon a single central computer to control a given process, was comprised of multiple computers, did not require operator intervention, and afforded for interaction between those computer systems to provide for the total control of a given manufacturing or process control system.
The distinction between DCS and SCADA systems has become difficult since SCADA systems have evolved to become more powerful and capable with many SCADA solutions today offering DCS-like capabilities. In fact, vendors of SCADA systems today would argue that the current-generation SCADA system gives the distributed control capability of a large DCS system, while still affording the ease of use found in a SCADA system. At the same time, of course, DCS vendors are today claiming that their DCS systems are able to handle much more complex processes with the ability for operator interaction through an HMI that rivals the ease of use found in a SCADA system

2.5 Hybrid Controllers

Hybrid controllers are specialized devices that provide for capabilities not found in standard discrete and continuous control modules for PLC systems. Capabilities such as adaptive control, artificial intelligence, and fuzzy logic are afforded by typical hybrid controllers. The capability of hybrid controllers is one of the primary mechanisms that is blurring the line between SCADA and DCS systems. Benefiting from Moore's Law (computing power nearly doubles every 18 months), the most complex control algorithms and intricate mathematical capabilities previously reserved only for powerful DCS systems are quickly finding their way into today's increasingly more powerful hybrid controllers for SCADA systems.
A SCADA system may utilize multiple hybrid controllers distributed as needed to perform the tasks at hand across a given process while still operating under the supervisory control of the SCADA system.

2.6 Event Loggers

Event loggers provide for the capturing of events as they happen within a SCADA system and provide time/date stamping, which affords a complete audit trail of the events that have occurred in the SCADA system. Typically, time within a SCADA system event logger provides for usable resolution down to 1/10 of a second.
While this is more than fast enough for many typical applications, it is not suitable for applications where multiple events can happen only milliseconds apart, such as in the switch gear for power distribution systems and safety shutdown systems for critical processes. In these applications, specialized event loggers that can capture events occurring perhaps just milliseconds apart are typically required.
In SCADA systems that utilize the integrated event logging capability of multiple individual components, it is critical that the time across the SCADA system be synchronized. Hence, it is not uncommon today for a SCADA system to use a single time reference such as that found in a Global Positioning System (GPS) satellite receiver as a time-synchronizing source to assure that all real-time and historical data timestamps are accurate across all HMIs, PLCs , hybrid controllers, and other devices within the SCADA system.

3. Protocols in SCADA Communication

In order for SCADA systems to obtain its functionality, it needs a protocol for transmitting data. Some of the SCADA protocols include Modbus RTU, RP-570, Profibus and Conitel. [1] These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850 (in which T101 branched out), IEC 60870-5-101 or 104, and DNP3. These communication protocols are standardized and recognized by all major SCADA vendors. Many of these protocols is now improved and contain extensions to operate over TCP/IP. These two open communication protocols that provide for interoperability between systems for telecontrol applications. Both are now competing within the world market. DNP is widely used in North America, South America, South Africa, Asia

*Corresponding author

and Australia, while IEC 60870-5-101 or T101 is strongly supported in the Europe.

3.1 IEC 60870-5

IEC 60870-5 is the collection of standards produced by the IEC(International Electrotechnical Commission). It was created to provide an open standard for the transmission of SCADA telemetry control and information. It provides a detailed functional description for telecontrol equipment and systems for controlling geographically widespread processes specifically for SCADA systems. The standard is intended for application in the electrical industries, and has data objects that are specifically intended for such applications. It is also applicable to general SCADA applications in any industry. But IEC 60870-5 protocol is primarily used in the electrical industries of European countries.[18]

When the IEC 60870-5 was initially completed in 1995 with the publication of the IEC 870-5-101 profile, it covered only transmission over relatively low bandwidth bit-serial communication circuits. With the increasingly widespread use of network communications technology, IEC 60870-5 now also provides for communications over networks using the TCP/IP protocol suite. This same sequence of development occurred for DNP3.

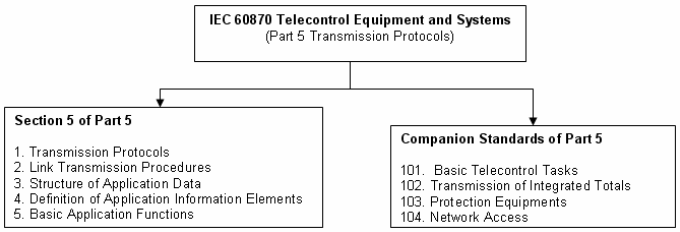

Fig. 2. IEC 60870 Structure

3.1.1 T101

T101 or IEC 60870-5-101 (IEC101) is an international standard prepared by TC57 for power system monitoring, control & associated communications. This is compatible with IEC 60870-5-1 to IEC 60870-5-5 standards and uses standard asynchronous serial tele-control channel interface between DTE and DCE. The standard is suitable for multiple configurations like point-to-point, star, mutidropped etc.

3.1.2 T101 features

60870-5-101 or T101 have many features such as the following:

- Supports unbalanced (master initiated message) & balanced (master/slave initiated message) modes of data transfer.
- Cyclic & Spontaneous data updating schemes are provided.
- Facility for time synchronization
- Schemes for transfer of files

3.2 DNP3 Protocol

The DNP3 or Distributed Network Protocol is a set of communications protocols used between components in process automation systems. It is usually used is in utilities such as water and electric companies. It is also technically possible to use it in other utilities. It was specifically developed to facilitate communications between various types of data acquisition and control systems. It plays a crucial role in SCADA systems. It is used by SCADA Master Stations or Control Centers, Remote Terminal Units, and Intelligent Electronic Devices. It is primarily used for communications between a master station and IEDs or RTU's. DNP3 supports multiple-slave, peer-to-peer and multiple-master communications. It supports the operational modes of polled and quiescent operation. The latter is also referred to as reporting by exception.

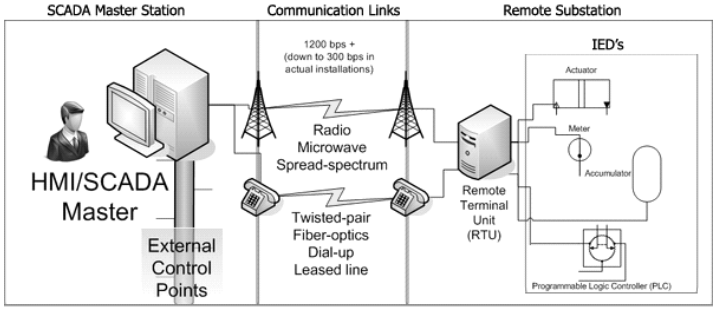

Fig. 3 Overview of the DNP3 Protocol

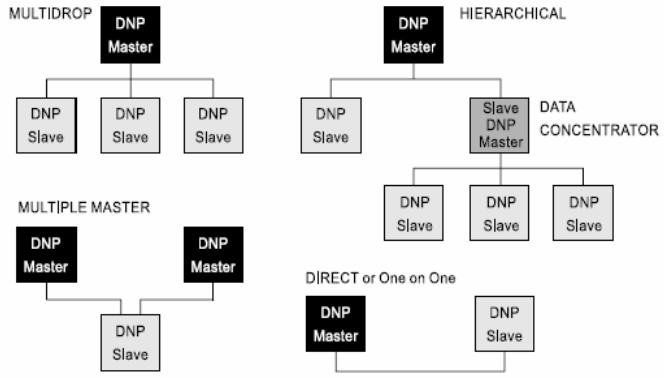

Fig. 4 Network Topologies of DNP3

3.2.1 DNP3 in SCADA Communication

The DNP3 protocol is utilized in communication between various SCADA system components. These system components include the SCADA master or HMI, the

*Corresponding author

Remote Terminal Units, and Intelligent Electronic Devices.
Operators of SCADA systems can monitor the DNP3 protocol within their operations to increase system reliability. This will reduce customer roil by decreasing downtime. DNP3 protocol was designed to avoid being distorted by legacy equipment, as well as EMI noise and low-grade transmission channels. While it adds network reliability, the DNP3 protocol does not make provisions for communications security.

3.2.2 Advantages of using DNP3

DNP3 was designed to optimize the transmission of data acquisition information and control commands from one computer to another. It is intended for SCADA (Supervisory Control and Data Acquisition) applications. It is not a general purpose protocol like those found on the Internet for transmitting email, hypertext documents, SQL queries, multimedia and huge files.
The reasons for the adoption of DNP3 by users are primarily:
- It is an open protocol;
- It is optimized for SCADA communications;
- It provides interoperability between different vendor's equipment;
- It is supported by a substantial number of SCADA equipment manufacturers;
- It will provide immediate and long-term benefits to users;

4. SCADA Security

4.1 Guidelines

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. 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. 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 [8] and [9]. These recommendations are often applicable to SCADA networks, but require appropriate interpretation [3].

4.2 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.

4.3 Protocols

The IEC 62351 standard defines security for SCADA data and protocols that are in the scope of IEC [2] and [4]. IEC 62351 defines end-to-end security methods for SCADA protocols and security in diverse protocol layers in layered communications architecture. Most importantly, message origin authentication and data integrity is introduced to SCADA protocols, e.g. by

*Corresponding author

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, or via Ethernet without TCP, e.g. GOOSE (Generic Object Oriented System Event).

Applying cryptographic and protocol mechanisms such as IEC 62351-3, and -4 to SCADA communications provides end-to-end authentication, integrity, confidentiality, and nonrepudiation. 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-toend
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.

5. Secure SCADA Network Architecture

Specific terminology is associated with the components of SCADA systems.

These SCADA elements are defined as follows:

Operator: Human operator who monitors the SCADA system and performs supervisory control functions for the remote plant operations.

Human machine interface (HMI): Presents data to the operator and provides for control inputs in a variety of formats, including graphics, schematics, windows, pull-down menus, touch-screens, and so on.

Master terminal unit (MTU): Equivalent to a master unit in a master/slave architecture. The MTU presents data to the operator through the HMI, gathers data from the distant site, and transmits control signals to the remote site. The transmission rate of data between the MTU and the remote site is relatively low and the control method is usually open loop because of possible time delays or data flow interruptions.

Communications means: Communication method between the MTU and remote controllers. Communication can be through the Internet, wireless or wired networks, or the switched public telephone network.

Remote terminal unit (RTU): Functions as a slave in the master/slave architecture. Sends control signals to the device under control, acquires data from these devices, and transmits the data to the MTU. An RTU may be a PLC. The data rate between the RTU and controlled device is relatively high and the control method is usually closed loop.

Modern SCADA architectures rely heavily on standard protocols and digital data transmission. For example, a communications protocol such as the Foundation Fieldbus, is applied in conjunction with industrial Ethernet radios. These Ethernet radios provide data rates of 512 Kbps, a large increase over those provided by EIA-232 serial links. For security, industrial Ethernet access points use spread-spectrum frequency hopping technology with encryption.

A SCADA architecture comprises two levels: a master or client level at the supervisory control center and a slave or data server level that interacts with the processes under control. In addition to the hardware,
the software components of the SCADA architecture are important. Here are some of the typical SCADA software components:

SCADA master/client
Human machine interface
Alarm handling
Event and log monitoring
Special applications
ActiveX or Java controls
SCADA slave/data server
Real-time system manager
Data processing applications
Report generator
Alarm handling
Drivers and interfaces to control components
Spreadsheet
Data logging
Archiving
Charting and trending

A SCADA substation control network (illustrated in Figure 1) 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

*Corresponding author

risk assessment and implement security measures for the SCADA network. In the 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. 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.;

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.

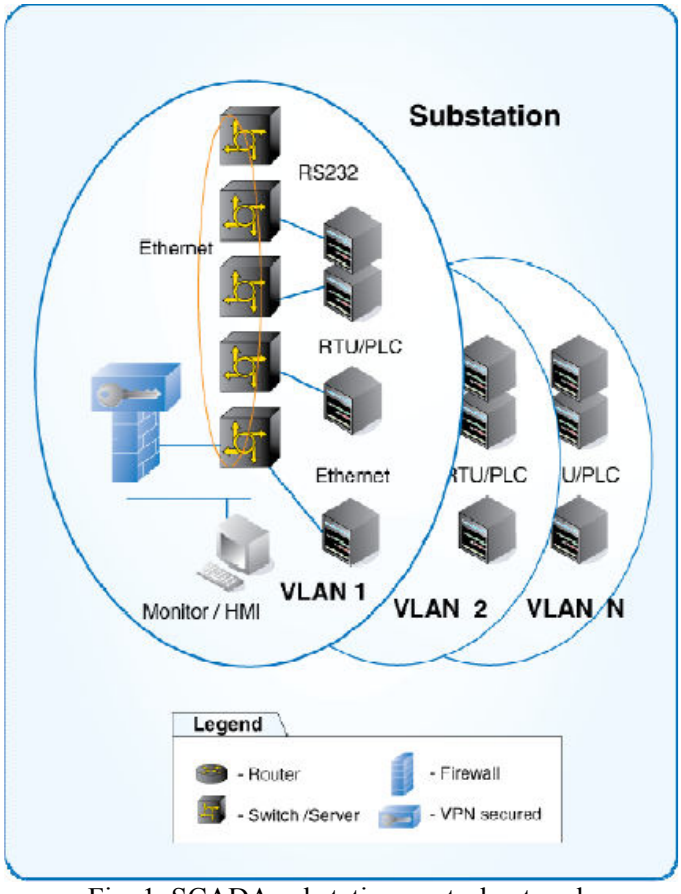

Fig. 1. SCADA substation control network

- 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.

*Corresponding author

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. 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.

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.

6. 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.

6.1 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 (RFC 2740) and SNMPv3 (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.

6.2 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

*Corresponding author

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) [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

6.3 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.

6.4 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, [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. 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 preshared 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. Reencrypting data traffic is generally redundant, costs additional processing resources, and causes the traffic to incur additional latency in transit.

6.5 Intrusion Detection System

An Intrusion Detection System (IDS) issues alerts when a system is being probed or attacked [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 8as DNP (Distributed Network Protocol) and ICCP (Inter-Control Center Communications Protocol), in addition to the usual signatures [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 hostbased and network based IDS. Note that the addition of IDS agents has the potential to adversely affect system performance.

6.6 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.

*Corresponding author

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.

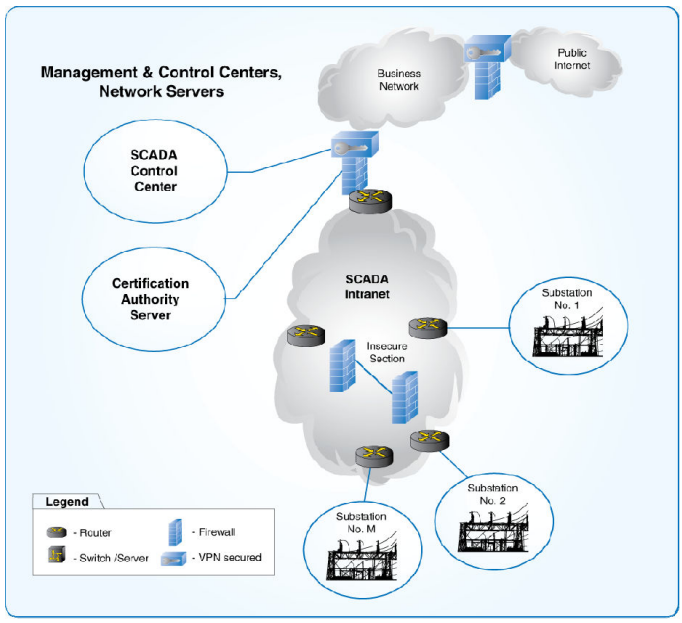

Fig.2 Reference SCADA control network

6.7 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.

6.8 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 [10].

7 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

*Corresponding author

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.

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

[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

[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.

[15] Scale Free Networks – A Challenge in Modeling Complexity, Radu Dobrescu, The 6th WSEAS International Conference on Multimedia, Internet & Video Technologies (MIV '06)

[16] Smart control system for LEDs traffic-lights based on PLC, Ramon Martinez-Rodriguez-Osorio, Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006

[17] Remote Data Acquisition System for Hydro Power Plants, Costin Cepisca, Proceedings of the 6th WSEAS International Conference on Power Systems, Lisbon, Portugal, September 22-24, 2006

[18]C. Clarke, D. Reynders, E. Wright (2004) Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems

*Corresponding author