HIRSCHMANN
A BELDEN BRAND

WP 1004HE – Part 5

White Paper – Data Communication in Substation Automation System (SAS)

Cyber security in substation communication network

Table of Contents

1. Cyber Security

1.1 What is Cyber Security in Substation Communication Network?

A substation is a critical infrastructure. Security threats generally consist of attacks against assets. These assets may not only be physical facilities, but also cyber information, databases and software applications. Cyber data security is a vital element of a substation system's reliability. It decreases cyber crimes and increases the security and availability of the substation communication network.

Cyber security in substations is not currently recognized as a serious issue. Many utility personnel are unaware of the number of security threats. They think their substations are already safe and do not see any reason to add security measures to their systems. However, most of substation communication networks are open and additional information access requirements are growing. Protocols (like TCP/IP) and the network itself are vulnerable. Attacks can be easily instigated by using standard tools and are difficult to trace in a modern substation, IEDs are progressively interconnected. Remote access to IEDs via modern IP networks, Internet and WAN (Wide Area Network) technologies present many security threats.

Targets such as IEDs, SCADA (Supervisory Control And Data Acquisition) systems, EMS (Energy Management Systems), databases, applications and web services can be attacked. Even if the network is completely isolated and no remote equipment is connected, attacks may even be initiated by operational personnel who lack special training and awareness.

In general, there are four types of cyber security threats:

- Unauthorized access to information
- Unauthorized modification or theft of information
- Denial of service
- Lack of repudiation/unaccountability

Countermeasures for cyber security must be applied to achieve the expected utility and societal benefits.

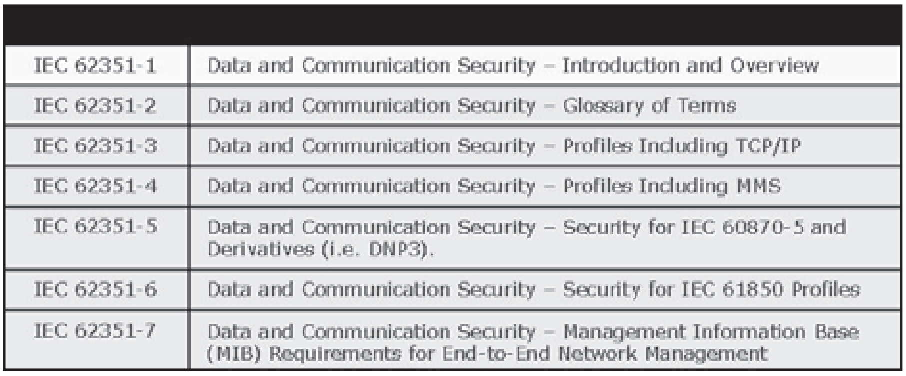
1.2 Which Standard Should be Applied for Cyber Security in Substation Communication?

IEC 61850

Substation communication security requirements are described in the standard IEC 61850 security recommendations (IEC 62351-6: Data and Communication Security – Security for IEC 61850).

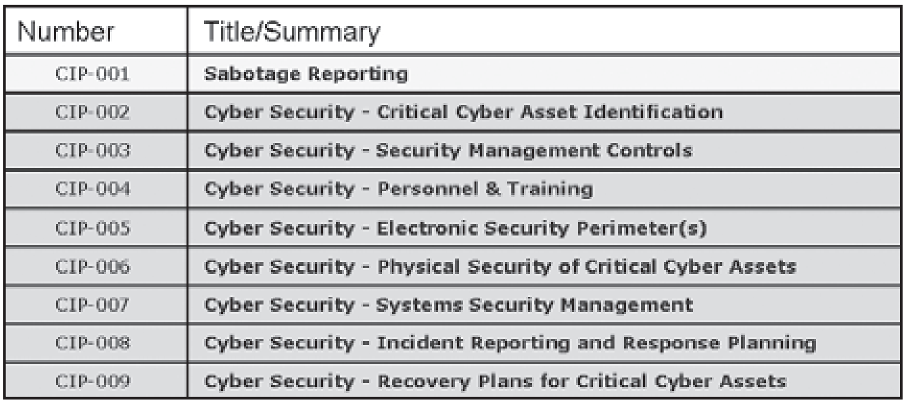
IEC 62351

IEC 62351 standards cover information security for power system control operations.



IEC 62351-1	Data and Communication Security – Introduction and Overview
IEC 62351-2	Data and Communication Security – Glossary of Terms
IEC 62351-3	Data and Communication Security – Profiles Including TCP/IP
IEC 62351-4	Data and Communication Security – Profiles Including MMS
IEC 62351-5	Data and Communication Security – Security for IEC 60870-5 and Derivatives (i.e. DNP3).
IEC 62351-6	Data and Communication Security – Security for IEC 61850 Profiles
IEC 62351-7	Data and Communication Security – Management Information Base (MIB) Requirements for End-to-End Network Management

EN 60950-1 Information technology equipment, Safety – Part 1: General requirements
UL 60950-1 Effective date and will be harmonized with IEC 60950-1 First Edition (issued October 2001)
EN 61131-2 (Class 1 Equipment)



Number	Title/Summary
CIP-001	**Sabotage Reporting**
CIP-002	**Cyber Security - Critical Cyber Asset Identification**
CIP-003	**Cyber Security - Security Management Controls**
CIP-004	**Cyber Security - Personnel & Training**
CIP-005	**Cyber Security - Electronic Security Perimeter(s)**
CIP-006	**Cyber Security - Physical Security of Critical Cyber Assets**
CIP-007	**Cyber Security - Systems Security Management**
CIP-008	**Cyber Security - Incident Reporting and Response Planning**
CIP-009	**Cyber Security - Recovery Plans for Critical Cyber Assets**

This table summarizes the content of NERC CIP

NISTIR 7628

NISTIR 7628 is a tool and a set of reference guidelines for implementing smart grid cyber security and is published by the National Institute of Standards and Technology (NIST).

The smart grid is a growing digital information network with modernized power generation, transmission, and distribution systems. All of these network segments can be targets for an attack. Substation automation is the backbone for a secure transmission grid operation and must be protected.

NERC CIP

Another important specification for cyber security is NERC CIP. NERC stands for the North American Electric Reliability Corporation. It is an international regulatory authority established to evaluate the reliability of the bulk power system in North America. CIP stands for Critical Infrastructure Protection and is a cyber security framework for the identification and protection of critical cyber assets to increase reliability and protection from terrorist attacks.

NERC CIP 002-009 requires a consolidation of utility policies, procedures and vendor technologies to prepare asset databases and reports on access controls. It uses different authentication methods and authorization privileges to identify critical cyber assets and define who has the rights to those assets and who approves them, etc.

IEEE 1686-2007

IEEE 1686-2007 is a security standard for IEDs. It establishes requirements for IED security in accordance with NERC CIP. This standard defines the functions and features to be provided in substation IEDs to accommodate critical infrastructure protection programs. IEEE 1686-2007 also provides a table of compliance which must be used by vendors to indicate a level of compliance with the requirements.

1.3 What are Common Technologies for Cyber Security in Substation Communication?

In order to increase availability in substations, enhanced security is required. Deep threat defense measures should be implemented to defend the network edge, protect the interior and guard the endpoints.

The basic idea for security in substations is to establish what information traffic (data) in which protocol is allowed. For example, who is the sender and where is the destination? Even if the network is completely isolated and no remote equipment is connected, security mechanisms such as syslogs, security audit trails, passwords, access control, port security, and encryption should be applied to increase resiliency against configuration and installation errors.

Generally there are different types of cyber security in substation communication networks: physical security and network security.

For physical security, the following countermeasures can be implemented: Lock communication switch in cabinet. Use a special M12 connector. Switch off unused switch port and protect unused network ports from unwanted use. Apply port security. Limit network access via a port to a specific device according to MAC address and IP address. Only allow registered devices to connect to the network. For network security, general security mechanism is AAA.

AAA is a standard for Authentication, Authorization and Accounting traffic and user access to network infrastructure devices. It can be implemented by identitying and controlling who or what has access to which resources, Rules can be set by filtering incoming traffic against an access list. For instance, password protection can be used to authorize access to the switch, with multi-level passwords for user and administrator. The following technologies can be applied using the AAA standard.

SNMPv3

SNMP stands for Simple Network Management Protocol. It is an interoperable standards-based protocol that allows external monitoring of the content engine through an SNMP agent. SNMPv3 introduced security functions including User-based Security Model (USM), encrypted authentication and integrity, timeliness verification of messages, privacy through encryption and view-based access control security to protect against manipulation of information, replay, spoofing and sniffing. Utility users can securely collect management information from their SNMP agents in IEDs.

RADIUS

RADIUS stands for Remote Authentication Dial in User Service. It is a client/server protocol that provides AAA management. The RADIUS server is usually a background service to authenticate users or devices before granting them access to a network. In addition, the RADIUS function authorizes users or devices for certain network services and accounts for usage of those services. All gateways that control access to the network have an IEEE 802.1x RADIUS client.

TACACS

TACACS stands for Terminal Access Controller Access-Control System. It is a remote authentication protocol that is used to communicate with an authentication server. A remote access server can communicate with an authentication server with TACACS to determine if the user has access to the substation network.

SSH

SSH stands for Secure Shell. SSH can be used to log into communication devices (e.g. IEDs) for secure data communication, remote shell services or command execution and other secure network services between two networked computers. SSH uses public-key cryptography to authenticate the remote computer and allow it to authenticate the user. SSH only verifies whether the same person offering the public key also owns the matching private key.

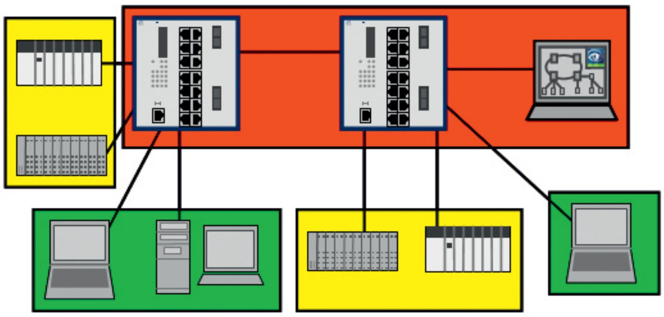
1.4 What Other Technologies Can be Used for Cyber Security in Substation Communication?

Besides the cyber security at physical and AAA mechanism level, there are other different security levels. The following technologies can address data security issues in substation communication networks.

Switch Level Security

Substation networks are primarily built with switches. Logically isolated substation network segments can be built by creating Virtual LANs within a physical LAN. Devices connected to different physical switches can communicate with each other as long as they are in the same VLAN. Devices which are in different VLANs cannot communicate with each other. This complete separation ensures a first level of security with switches. Multiple VLANs per switch would be required.

Figure: Multiple VLAN per switch



HIRSCHMANN

A BELDEN BRAND

Router Level Security

A router is a device that forwards data packets over standard or redundant data lines between communication networks in substations, between substations, or from substations to control centers. A VLAN-aware router can also be deployed between VLANs. When a data packet is transferred over one of the lines, the router reads the address information in the packet to determine the ultimate destination. Access Control Lists (ACLs) are vital to security and are a fundamental part of router administration. They prevent unauthorized access to the network. Every packet in a substation network must be processed by the router before it can be forwarded.

An ACL can be used as a packet sniffer to filter packets that do not meet certain requirements. It can not only be used to control route access and management, but also to control debug output. ACLs should be defined in routers between different VLANs or communication interfaces in the substation automation network to achieve cyber security.

Firewall Level Security

Some routers are also firewalls and secure cells of network can be created. A firewall is a system or group of systems that enforces an access control policy between two networks. It can protect against attacks from insecure networks and may hide the internal network structure. Transparent (bridging) firewalls can also be used to add security to an existing network.

Firewalls can log, administer, and audit network access in order to create alerts during attacks and failures. They provide secure control functions like stateful inspection, content inspection, access control, user control, protocol and services control, as well as data control for secure substation automation networking.

Generally firewalls can be used to create secure cells and secure zones inside a network and set restricted communication outside a cell and zone. This is known as defense in depth.

Gateway Security

When the substation network is connected to a WAN or remotely accessed, gateways must be applied to achieve cyber security against a variety of cyber attacks. A gateway collects metering, status, event, and fault report data from IEDs and RTUs and creates an interface between substation automation systems and external connections like a web browser or ERP systems. It can manage, filter and control data traffic and secure IEDs and other devices against external access. Normal gateways can be achieved by VPN and Encryption.

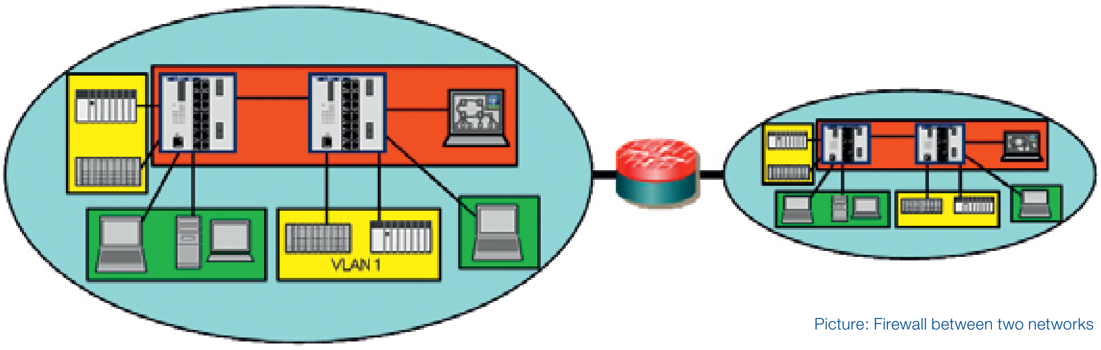
VPN

A Virtual Private Network (VPN) is a secure, encrypted connection between two points across an insecure network. A VPN uses a secure “tunnel” between two networks. Information is sent via tunneling, which is the practice of encrypting and encapsulating IP packets.

There are two main ways to create a VPN:

- OpenVPN
  OpenVPN is an open-source tool and implements VPN techniques to create secure point-to-point or site-to-site connections. This is done in routed or bridged configurations and remote access facilities. OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. OpenVPN creates a TCP or UDP tunnel and then encrypts the data inside the tunnel over an unsecured network.

- IPSec
  Internet Protocol Security (IPSec) is a framework of open standards that helps to ensure private and secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPSec provides data security at the IP packet level. IPSec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection to provide defense in depth against network based attacks, data corruption, data theft, user-credential theft and administrative control of servers, other computers, and the network.



Picture: Firewall between two networks

1.5 Summary

Substation communication networks are mission-critical infrastructures. IEDs and substation applications can be easily hacked even by using free tools like Nessus (the world's most popular vulnerability scanner). Security mechanisms like port security, AAA, VLANs, firewalls, routers, gateways, and syslogs must be applied to increase resiliency against configuration and installation errors or even cyber attack. Cyber security maintains the reliability and safety of control systems and reduces operational expenses in substations.

Hirschmann™ provides state-of-the-art security for substation automation networks and offers a full range of unique products and solutions that meet even the most demanding security requirements.

The Hirschmann™ industrial firewall and VPN router family EAGLE and EAGLE Tofino security system are designed specifically for automation angineers and little IT knowledge is required.

The following are features of the Hirschmann™ Security Appliance EAGLE 20:

Stateful inspection firewall	Firewall rules (incoming/outgoing, modem access, management), IP masquerading, 1-to-1 NAT, DoS limiter, MAC filter, user firewall for external activation of FW rules
Multipoint VPN	IPSec, IKEv2, DES, 3DES, AES (-128, -192, -256), Pre-Shared Key, X.509v3 certificates, MD5, SHA-1, NAT-T, Firewall rules for every VPN connection, configuration assistant in the web interface, remote enable/disable of connections

The EAGLE 20 Tofino system offers the following benefits:

- Rule definition using a graphical drag-and-drop editor. Traffic that does not match the rules is automatically blocked and reported.
- Over 50 pre-defined IT and industrial communication protocols.
- Over 25 pre-defined controller templates.
- Pre-defined "special rules" for advanced traffic filtering and vulnerability protection.
- Protects controllers with known vulnerabilities.

Hirschmann™ cyber security technology facilitates the seamless sharing of information throughout the substation facility to maximize security and productivity.

References:

1. IEC 61850 Communication Networks and Systems in Substations, IEC standard in ten main parts, 2002

2. NERC, Critical Infrastructure Protection (CIP) at http://www.nerc.com/page.php?cid=2

3. SGIP, Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security, 2010, at http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf

4. IEC 62351-1, Data and communication security – Part 1: Introduction and overview, 2006
Shailendra Fuloria, Ross Anderson, The Protection of Substation Communications, at http://www.cl.cam.ac.uk/~sf392/publications/S4-2010.pdf

5. Hirschmann White Paper, Get Smart About Electrical Grid Cyber Security, at http://www.belden.com/pdfs/techpprs/PTD_Cyber_SecurityWP.pdf

6. Hirschmann Service and Support: http://www.beldensolutions.com/de/Service/index.phtml

HIRSCHMANN

A BELDEN BRAND

Appendix: Further Support

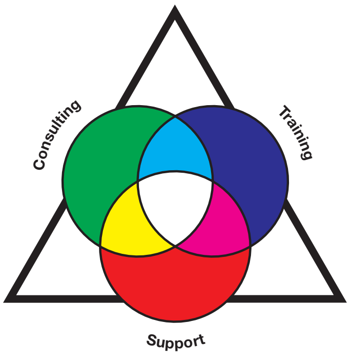
Technical Questions and Training Courses

In the event of technical queries, please contact your local Hirschmann™ distributor or Hirschmann™ office. You can find the addresses of our distributors on the Internet: www.hirschmann.com

Our support line is also at your disposal:

Tel. +49 (0)1805 14-1538
Fax +49 (0)7127 14-1551

Current training courses for technology and products can be found under http://www.hicomcenter.com.



Belden Competence Center

In the long term, excellent products alone do not guarantee a successful customer relationship. Only comprehensive service makes a difference worldwide. In the current global competition scenario, the Belden Competence Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Belden Competence Center, you do not have to make compromises. Our client-tailored package enables you to choose the service components you want to use.
Internet: http://www.hicomcenter.com