Antti Hurttila

Cybersecurity in SCADA Engineering

Engineering
2019

VAASAN AMMATTIKORKEAKOULU
Sähkötekniikan koulutusohjelma

TIIVISTELMÄ

Tekijä	Antti Hurttila
Opinnäytetyön nimi	Cybersecurity in SCADA Engineering
Vuosi	2019
Kieli	englanti
Sivumäärä	35 + 4 liitettä
Ohjaaja	Jukka Matila

Kyberturvallisuus on kasvava huolenaihe valvontaohjelmistoalalla. Monilla yrityksillä tietoturvan tuominen osaksi järjestelmän kehitystyötä on ongelmallista.

Opinnäytetyön tarkoitus oli määrittää, dokumentoida ja tuoda kyberturvallisuuteen liittyvät ABB:n minimivaatimukset osaksi projektin kehitysprosessia.

Opinnäytetyön aikana luotiin kyberturvallisuusohje, jossa tarvittavat toimenpiteet olivat yksityiskohtaisesti listattu, jotta saataisiin aina standardisoitu lopputulos. Kyberturvallisuusohjeen lisäksi luotiin mallipohjat projektin kyberturvallisuuden seurannalle sekä esimerkki proseduureja tehdas- ja hyväksymistestaukselle.

Avainsanat Kyberturvallisuus, ohjeet, tietojärjestelmät, systeemityö

VAASAN AMMATTIKORKEAKOULU
UNIVERSITY OF APPLIED SCIENCES
Sähkötekniikan koulutusohjelma

ABSTRACT

Author	Antti Hurttila
Title	Cybersecurity in SCADA Engineering
Year	2019
Language	English
Pages	35 + 4 appendixes
Name of Supervisor	Jukka Matila

Cybersecurity is a growing concern in the SCADA market and many companies have difficulties adapting the security into the engineering process.

The focus of this thesis was to determine, implement and document the needed actions what needs to be taken to fulfil the minimum cybersecurity requirements of a system during project deployment. Minimum cybersecurity requirements were defined by ABB at the business level.

As a result, multiple documents were created to standardize the cybersecurity practices during the project. The documentation included a practical guide, a project tracking document and cybersecurity procedures to be included in the factory as well as site acceptance testing.

Keywords Cybersecurity, instruction, guide, system, engineering

TABLE OF CONTENTS

ABBREVIATIONS

BIOS	Basic Input-Output System
CD-ROM	Compact Disc Read-Only Memory
HMI	Human Machine Interface
ICS	Industrial Control System
IT	Information Technology
LAN	Local Area Network
PLC	Programmable Logic Controller
ROM	Read-Only Memory
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus
WAN	Wide Area Network

LIST OF FIGURES AND TABLES

LIST OF APPENDIXES

* Only available for the client of the thesis.

1 INTRODUCTION

Industrial control systems (ICS) such as SCADA system play a vital role in critical infrastructure. These systems require high availability and proper functioning, so they need to be protected from both intentional and unintentional incidents which may cause operational outages. In the past risks were mitigated by completely isolating systems from external networks and the only way to access the system was physically from the operational facilities itself.

Today organizations are rapidly deploying modern networking technologies to enhance productivity and reduce costs by integrating ICS with external connections. However, these integrations often expose ICS to cyberthreats through existing vulnerabilities in the connected networks. These are new risks to once isolated systems.

Many companies have acknowledged the risks and have developed cybersecurity policies and baselines to follow. These documents are usually broad in scope and they do not specifically describe how to achieve the required results. Therefore, the people working during the project must take the responsibility of the implementation.

However, the knowledge of the engineers might vary, which may lead to different results in cybersecurity. The objective of this thesis is to standardize the methods of cybersecurity implementation to ensure the required actions have been taken. It needs to be kept in mind that each project might have additional cybersecurity requirements defined by the customer which are not in the scope of this thesis.

The thesis will make use of existing infrastructure, implementation methods and tools which are available at ABB. Many of these are internal tools and are not disclosed. The security design of network architecture is not in the scope of the thesis.

At first the thesis introduces a simplified introduction of what SCADA systems are, what cybersecurity is about, potential threats to the system and selected techniques which can strengthen the protection of the system. The next chapters describe the

minimum requirements and the implementation of them into the project deployment.

2 ABB

ABB is a multinational corporation headquartered in Zürich, Switzerland. The company is operating in more than 100 countries with about 147,000 employees. The operations of the company are organized into four global divisions – power grids, electrification products, industrial automation and robotics and motion. /1/

In Finland ABB is one of the largest industry employers operating in about 20 districts with around 5,300 employees. ABB owns four large manufacturing plants in Finland located in Helsinki, Vaasa, Hamina and Porvoo. /1/

2.1 ABB Grid Automation

ABB is divided into multiple business units which acts as their own divisions with their own metrics and goals. This thesis is based on Grid Automation which is a part of Power Grids division. /1/

The business unit markets, designs, engineers and delivers SCADA and DMS systems for various customers including the ones in electrical grid, public transportation and industrial companies. The business also offers various additional services such as maintenance, remote support, operational training and spare parts. /1/

The main products of the unit are software and expertise based. The software are MicroSCADA Pro SYS600, MicroSCADA Pro DMS600 and MicroSCADA Pro Historian. Each software has its own purpose and one cannot replace perfectly another. Expertise includes but is not limited to service agreements and spare part supplies. /2/

2.2 Software

There are several companies offering SCADA systems where each has its own products to cater the needs of the industry. ABB main offerings are divided into three solutions which together forms the MicroSCADA Pro product family. /2/

The software has been developed with redundancy in mind and each of the systems can have a duplicate standby variant running in the background on different machine. /2/

2.2.1 MicroSCADA Pro SYS600

SYS600 is the main product which provides the SCADA system its fundamental and advanced functions so the system can be classified as a SCADA system. The system was developed at first to provide means to control and monitor transmission and distribution of electricity, but nowadays it is a feasible way of managing almost any system. Applications can vary from a simple building environment condition monitoring system to a complex system monitoring the activity in a nuclear power plant. The most common systems today built are for substation automation and process industry applications. /3/

2.2.2 MicroSCADA Pro DMS600

DMS600 is a distribution management system which extends the functionality of a SCADA system by providing geographically based network views and advanced distribution management functions over the entire electrical network. /4/

A geographically presented network helps operators of the electric companies to visually determine the state of the entire network. During a fault operators can instantaneously determine fault location along the feeder from the geographic view. /4/

DMS also provides additional advanced functionality, for instance automatic fault location, restoration and network reconfiguration. /4/

2.2.3 MicroSCADA Pro Historian

Historian is specifically made to collect, archive and organize the data collected from the SCADA system. The data which is logged is freely chosen from the objects in the SYS600 database. The chosen variables can be made into a report template which updates itself with the data archived in the system. /5/

There are multiple types of reports varying from precise numerical data like Excel to visualized graphs to provide the overview of the state with a glance. /5/

3 SCADA SYSTEMS

SCADA systems are designed to collect field information, transferring it to a centralized location and providing the employees access through the use of HMI software. This enables the employees to monitor or control an entire system from a central location in near real time. /1, 6/

Therefore, SCADA systems are widely adopted in distribution systems such as water distribution systems, electrical utility transmission and distribution systems and public transportation systems. In these systems the assets are usually dispersed to one or more geographically distributed field sites, so the centralized control and monitoring system provides enormous value. /1, 6/

Typical hardware for SCADA system includes a control server placed at a control center, communication equipment and one or more geographically distributed field sites consisting of remote terminal units and programmed logical controllers or intelligent electrical devices. /1, 6/

The control server stores and processes the field information from the remote terminal unit, while the RTU or PCL controls the local process. The communication hardware enables the communication between the control server and the RTU. /1, 6/

SCADA systems are usually designed to be fault-tolerant with significant redundancy. This means the servers, workstations and communication equipment is essentially doubled. This is done to provide the highest availability at all times but is not a sufficient protection against cyberthreats. /1, 6/

3.1 Network Architecture

Figure 1 shows the system components in a general configuration of a SCADA system. The control center facilitates control server, data historian, operator workstations and communication router. The control server collects the information from field devices in field sites and displays the information to the HMI. The data historian communicates with the control server and stores the collected information,

which can be used to generate trend analyses and reports from a certain time period. Routers enables communication between the control center and multiple field site through the LAN or WAN. The communication type is chosen on the basis what is available. The customer may have a dedicated fibre backbone to support he communication or the communication could be through WAN using multiple communication channels. Common WAN channels are leased line or power line based, cellular and satellite. /1, 6/

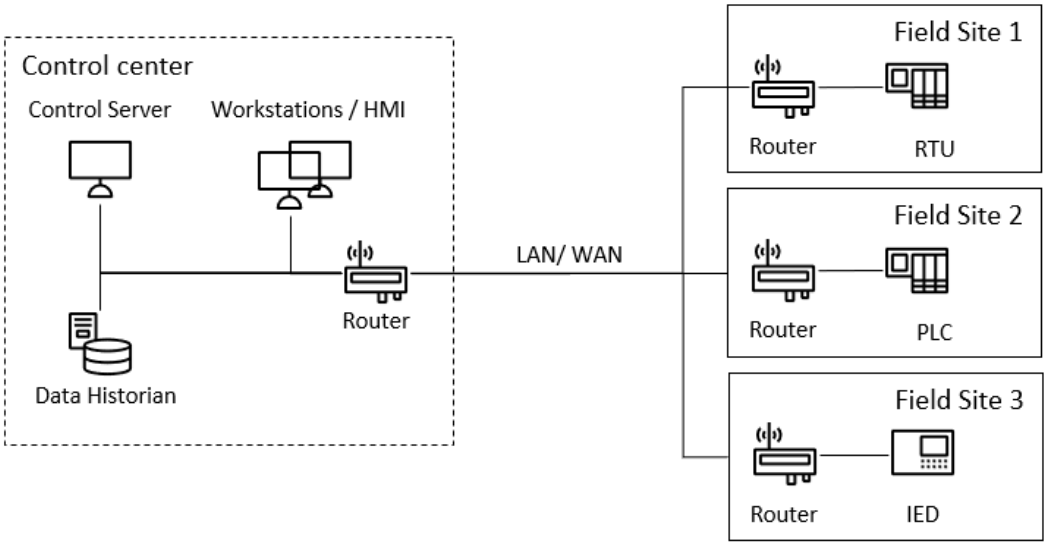

Figure 1. SCADA system general topology.

Large SCADA systems containing hundreds of field sites often alleviate the burden on the control center by employing sub-control centers. With this type of implementation, the main control center communicates with the sub-control centers and sub-control centers communicate with the field sites. This is commonly seen in electrical distributions systems. An overview of sub-control center implementation is shown in Figure 2. /1, 6/

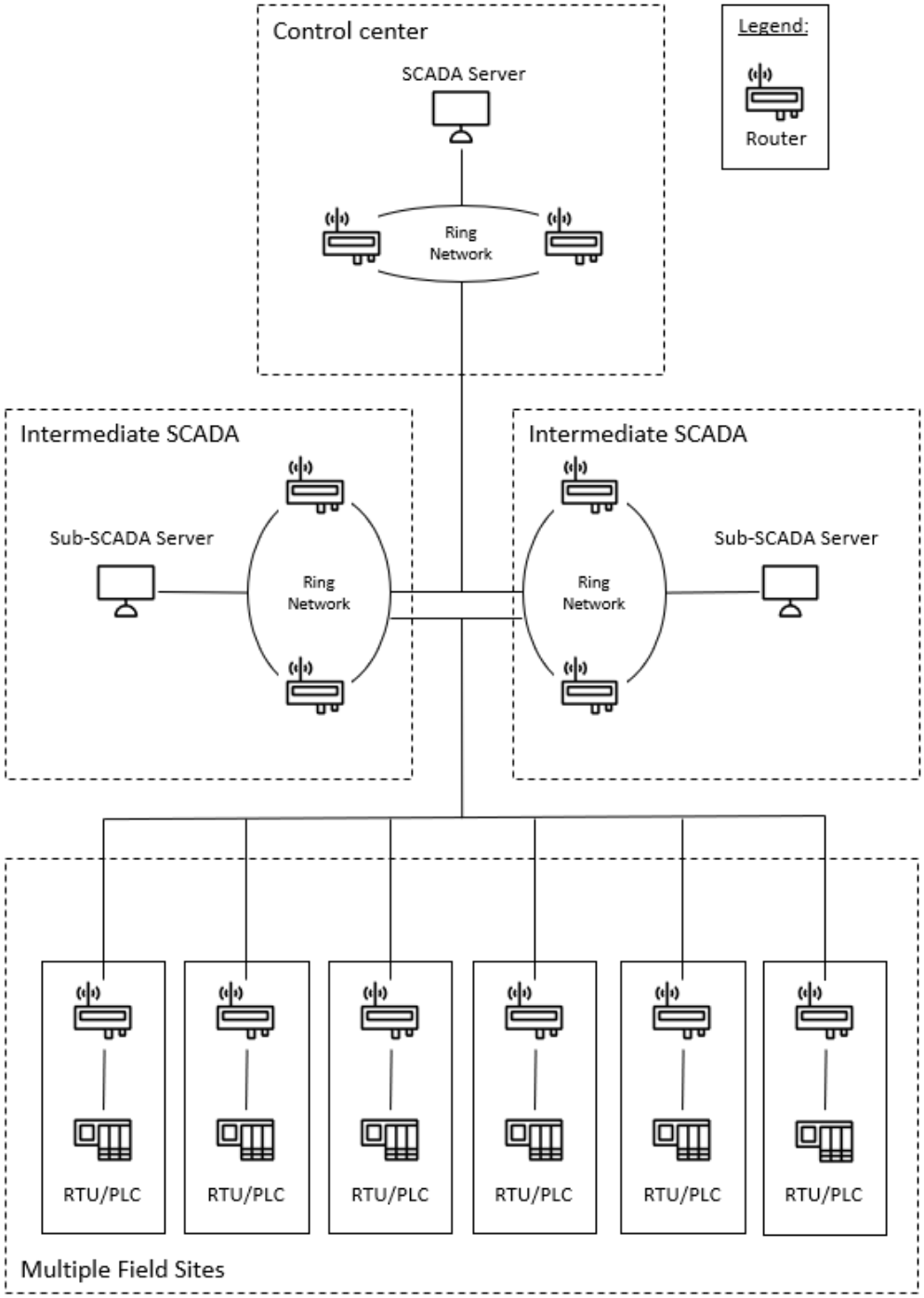

Figure 2. Simplified large SCADA communication topology with limited redundancy.

4 CYBERSECURITY

Cybersecurity is formally defined as “Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation”. /8/

When comparing the ICS such as SCADA and tradition IT systems there are many characteristics which differs from each other. The main differences are the risks and the priorities. While the risk on an IT system may be the loss of data, the risks on ICS may introduce significant risks to the health and safety of human lives or environmental damage which may have impact on national level. /1, 6/

The priorities in IT systems are on security and confidentiality while on ICS systems the priorities are on system availability and integrity. Table 1 summarizes the main differences between an information system and an industrial control system. /1, 6/

Table 1. Differences between an IT system and an industrial control system.

	Information Systems	**Industrial Control Systems**
Primary subject for protection	Information	Physical process
Primary risks	Information disclosure, financial	Safety, health, environmental, financial
Security focus	System security	Control device stability
Availability	95 – 99 %	99,9 – 99,999 %
Determinism	Hours to months	Milliseconds to hours

Timeliness	Interactive, transactional	Interactive, real-time
Problem response	Reboot	Fault tolerance, on-time repair

4.1 Cyberthreats

In order to implement any security features to a system, the definition of threats is required. The threats can be classified by multiple ways, in example by characteristics of the attack or the goal of the attack. /1, 8, 6/

Threats actors may be classified as:

- Recreational hackers
- Professional hackers
- Organized groups
- Malware
- Internal.

Recreational hackers try to break into system for fun and honour. This type of an attacker has most likely low consequences but may be difficult to stop. /1, 8, 6/

Professional hackers commonly break into systems for financial reasons. The consequences vary from medium to high depending on the purpose. Professional hackers are usually very difficult to stop. /1, 8, 6/

Organized groups such as terrorists or foreign state agencies break into systems to gather intelligence or cause societal disruption by sabotage. If a system is a target of this type of attacker, it is almost impossible to stop. By proper detection methods in place the breach can be detected in timely manner and the losses can be minimized. /1, 8, 6/

Malware-based threats rely on automated attack software. The intention might vary from building a botnet to extortion of ransom. Malware attacks are easier to stop

than human based ones as the methods can be detected by commercial security software such as antivirus. /1, 8, 6/

Internal threats can be intentional or unintentional depending on the case. Unintentional threat could be a misconfiguration of a device which could potentially compromise the whole system. Intentional threat could be creation of backdoor to a system or insertion of malware-laced external media to the control system. /1, 8, 6/

Threats may be classified as:

- Denial of service
- Man-in-the-middle
- Network monitoring
- Escalation of privilege
- Storage modification
- Compromised portable media
- Phishing
- Social engineering.

The purpose of denial of service attacks is to block legitimate access to network. This is achieved by saturating the communication channels of a device by requests. The device response time grows to the point where the system is practically unusable until the requests stop. The main strategy for preventing denial of service is to use firewalls and switches to keep all non-required network traffic out of the critical network. /1, 8, 6/

Man-in-the-middle attacks are used to assume a trusted role in a communications network. The basic idea is to intercept the message from one computer and inspect or manipulate the data before forwarding it to the intended computer as shown in Figure 3. Neither system detects the presence of the attacker. The main strategy for preventing man-in-the-middle attacks is to use safe protocols that include encrypted authentication mechanisms. /1, 8, 6/

Figure 3. Man-in-the-Middle attack.

Network monitoring is using passive surveillance software to identify key devices and vulnerabilities of the network or even gain passwords if not used safe protocols. Network monitoring is easier on systems where wireless communications are used. This technique is most commonly used by Nation-States or criminal groups to avoid detection before trying to cause disruption. The main strategy for preventing network monitoring is to encrypt traffic using strong encryption protocols and to use properly zoned network. /1, 8, 6/

Escalation of privilege is a technique that exploits bugs in the operating system to gain administrative privileges after gaining basic access to the system. This is usually needed when making changes to the system. Main strategy for preventing escalation of privilege is to give only minimum amount of privileges per user to do their daily work and by keeping the operating system up to date to prevent usage of already patched bugs. /1, 8, 6/

In storage modification the attacker modifies files or programs to execute attacker-assigned task on next task execution. In example a malware can modify hosts list to disable communication of system. The main strategy for preventing storage modifications is to restrict file access by authentication and security mechanisms and using virus scanners and whitelisting to detect and prevent unauthorized storage modification. /1, 8, 6/

Compromised portable media attacks use the greedy nature of people. As an example, attacker can leave malware-laced USB-sticks around parking lot of employee in hope that someone will insert it in to the system infecting it. The main strategy for preventing this type of attack is by user training and using up-to-date virus scanners. /1, 8, 6/

Phishing attacks use email and websites to persuade users to give up information or to install malware by disguising as a trusted party. Phishing attacks are effective when firewalls are configured to only filter inbound communication as when the malware is already in the system it only needs the outbound to send the data. The main strategy for preventing phishing is by user training, proper network zoning and properly configured firewalls. /1, 8, 6/

Social engineering attacks including phishing is to exploit the willingness to help of an employee. As an example this can be achieved by calling known employees and impersonating a trusted person to gain "forgotten" password to the system. With good speech skills attacker can gain access to the system and gain valuable data or to cause disruption to the system. The main strategy for preventing social engineering attacks is by training the user to recognize and counter these attacks. /1, 8, 6/

4.2 Defence in Depth

The most recommended approach to secure any industrial control system is based on the principle of defence in depth. The principle originates from military strategies to provide barriers to impede the progress of intruders while monitoring the progress and implementing efficient response to repel them. In cybersecurity this appears in multiple independent and redundant prevention and detection methods. This reduces the risk that the system is compromised if one security measure fails or is circumvented. /1, 6, 7, 8, 12/

The layers of cybersecurity protection are represented in Figure 4.

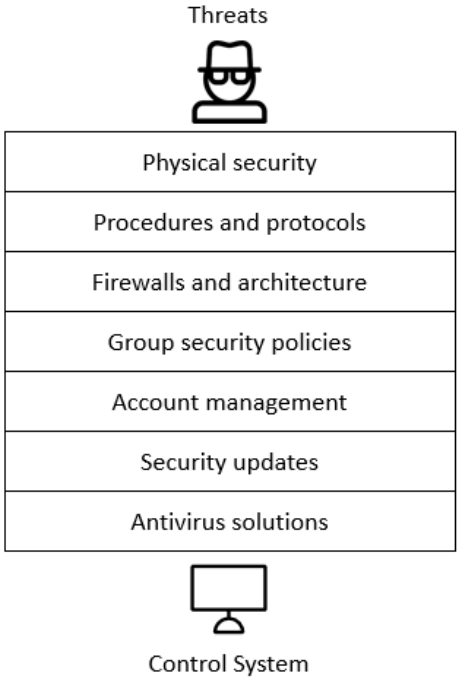

Figure 4. Layers of defence in depth.

Physical security refers to prevention to gain unauthorized access to the system hardware. Even as simple as disconnecting or moving a system cable can cripple a system. This should be taken in consideration when designing a system and it is recommended to hardware cabinets to include physical locks to provide a basic level of protection. /1, 8, 6/

Procedures and protocols refer to creation of security policies which guides to a proper security practice such as determination of secure password or how to securely handle and store digital data. /1, 8, 6/

Firewalls and architecture refer to securing the network communication. Firewalls are key components in securing communication networks as they are designed to protect the network by blocking communication from unauthorized source or unauthorized types while allowing legitimate traffic through. This is done by configuring the device with a set of rules and other criteria. /1, 8, 6/

Group security policies are settings that are centrally controlled. Group security policies include rules such as media access control, password requirements, user account settings and system security auditing. /1, 8, 6/

Media access control impacts features such as disabling auto-run on new USB devices or CD-ROM should be enforced as it is known method to attackers to try infecting the system with an external storage media. Password requirements are defined to prevent the most common brute force type attacks and to prevent unauthorized use. User account settings may include restrictions to file systems or locking out account after certain number of failed logon attempts for a certain time. System security auditing ensures that the attempts to access system resources are properly logged to be able to verify a source of attack if needed. /1, 8, 6/

Account management is based on the “least privilege” principle where the different accounts have different uses and have different restrictions. As a good practice it would be good to restrict the access of operator to the needed operations on SCADA application and restrict any changes to the filesystem. Centralized account management solutions help managing user specific restrictions. /1, 8, 6/

Security updates should be applied in timely manner as attackers often exploit known bugs in software to gain unauthorized access to the system. In SCADA systems the updates should be verified to be compatible with the SCADA software, so the functionality is not compromised. /1, 8, 6/

Antivirus software can recognize known malware and attack mechanisms by identifying patterns in the code. The software is effective against known threats but is not effective against so called zero-day malware which pattern is not included in the definitions database. Therefore, it is important to update the definitions database frequently to be able to detect newly discovered malware patterns. Zero-day malware is usually used by organized groups. Therefore, any antivirus software does not give a complete protection against the malware. Antivirus software often include basic host-based intrusion detection system which can detect suspicious activities on ports and web browsers. /1, 8, 6/

5 MINIMUM REQUIREMENTS

ABB has set the minimum baseline for cybersecurity requirements which should be met in any project deployment which involves configuring or commissioning of any kind. The requirements are only for the use of ABB, so the detailed list of specifics is not given in this thesis.

Generally, the requirements consider following categories:

- Contractual requirements
- Employee training
- Policies
- Patch management
- Project documentation

Contractual requirements describe what needs to be included in the contract of the project between ABB and the customer. The requirements are set in place to prevent any confusion in responsibilities or of the scope during project.

Employee training requirements are listed to ensure that any employee involved in the project deployment is aware of the internal security policies and common cyber threats such as social engineering. The training is supervised by the functional managers.

Cybersecurity policies outlines the security rules and controls that are made in place to protect the assets and the information of a project. For example, existing policies include but are not limited to password requirements, handling of sensitive data and removable devices and malware propagation protection.

Patch management requirements are in place to ensure that any system node or software included in the project have the latest validated or available patches applied to ensure the known vulnerabilities countered.

Project documentation requirements describe the required documents that should be part of the project documentation that is handed over to the customer. The documentation should include at minimum:

- Network diagrams of all system nodes (physical and logical connections)
- Inventory of all system nodes
- Inventory of installed software
- List of used ports and services
- List of user accounts.

Multiple documentation requirements can be created automatically by available internal software and scripts.

6 SCADA ENGINEERING

At ABB the SCADA engineering is project-based and the scope of the project varies per project.

A typical SCADA project where the customer does not have the existing system can be split into stages shown in Figure 5.

Figure 5. Lifetime of a project.

All cybersecurity related tasks are listed in Appendix 4 and should be tracked during the different stages of the project.

6.1 Sales

During sales the cybersecurity focus is on the contractual features of the project. Most cybersecurity features are introduced to the project by the customer. The features determine the type and amount of hardware and software-based solutions are being used in securing the system. An example feature could be securing of external connections by the use of virtual private network connection. A typical solution is to add a virtual private network gateway to the main system and virtual private network clients to the remote sites.

The contract should also specify the cybersecurity responsibilities during a project's lifetime. Extra attention should be given to certain points when the system nodes are being transferred to another location which could potentially allow third party to intervene with the system. This could happen after shipping the hardware to customer location.

As an example the responsibility of patch management would be transferred to customer after the shipment of the system nodes as the customer location might not have proper infrastructure to support it.

The contract should also specify a certain point when the responsibility is fully transferred to customer. The usual point is when project is handed over to customer.

6.2 Design

Cybersecurity features and the responsibilities defined in the contract of the project must be carefully read and understood by the people involved in the system design as the project requirements affect the choice of hardware, software and protocols that are used in the project.

The system architecture is developed with cybersecurity in mind and incorporates defence in depth principle to fulfil the project requirements. The minimum project requirements do not consider any architectural choices and they are left outside the scope of thesis. During the system architecture development, security expert should be consulted.

When the architecture is known the following documentation concerning cybersecurity should be generated:

- Inventory of system nodes
- Network diagram with physical and logical connections.

System nodes include but are not limited to servers, workstations, network equipment and embedded devices. Embedded devices include but are not limited to remote terminal units and intelligent electronic devices.

A template for system node inventory is available as an appendix (Appendix 1).

6.3 System Engineering

System engineering is a crucial phase of any project. Even the most secure system design does not matter if the system nodes have not been configured to be secure in the first place.

During system engineering the principles of “least privileges” and “least functions” should be kept in mind. Essentially, this means providing access to the privileges

that are essential to a specific user and removing or disabling unnecessary programs and services on any system node to reduce the potential attack surface.

The basic cybersecurity process of securing a system node is represented in Figure 6.

Figure 6. Simplified system node cybersecurity process.

6.3.1 Firmware Updating

When the system node is unpacked the first thing to do is to check the availability of firmware updates for the node. Firmware is a software which provides the necessary instructions for how the device works or communicates with other hardware.

Firmware is typically stored in the flash ROM of a system node. However this can usually be updated by erasing and rewriting the memory by a firmware updater. Updates generally provide better compatibility, more efficient operation or security enhancements. /10, 11/

The most common firmware is known as BIOS or. It resides on the motherboard of a computer system. It is necessary to keep the firmware up to date as old software might be vulnerable to exploits. Additional security measurements that should be done on BIOS or UEFI when available are:

- Enabling password protection
- Enabling secure boot
- Disabling remote wake-up on LAN. /1, 12/

Password protection prevents unauthorized access, a secure boot helps a computer resist attacks and infection from malware by validating the digital signatures of boot loaders, key operating system files and unauthorized option ROMs /9/. Disabling remote wake-up on LAN provides protection against possible remote exploitation.

When the firmware has been verified to be the latest and the version has been documented, the main features of system node should be configured. Different types of system nodes have varying configurable features which can make the configuration complex. To be able to clarify the configuration the system nodes are split into two categories: Windows-based system nodes and general system nodes.

6.3.2 Configuration of Windows-based System Node

As ABB has the existing infrastructure to centrally manage the Windows-based system nodes, it should be used to significantly reduce the engineering workload so the focus of the project can be on SCADA application engineering.

Figure 7 is the simplified process of initial configuration process.

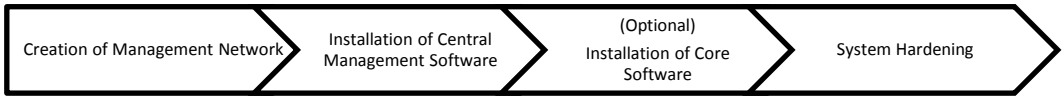

Figure 7. Initial configuration process of Windows-based system node.

To be able to make use of the existing infrastructure the Windows-based system nodes should have a connection to central management network. This is implemented with the use of LAN and network switches. When the connection is made the central management is enabled by installing a software-based agent which communicates with the central management server.

The central management server is administered by service employees, who remotely executes the following tasks:

- Updating and activation of Windows operating system
- Updating of antivirus definition database
- Delivery of latest installers of core pre-determined software

After the system is up to date the core software should be installed where needed to be able to restrict the file path privileges of user accounts. Software which is considered as a core are listed in Table 2.

Table 2. List of core software.

Core Software	**Description**
MicroSCADA Pro SYS600	Control of ICS.
MicroSCADA Pro DMS600	Distribution management system.
MicroSCADA Pro Historian	Data logging and reporting.
System Data Manager (SDM600)	IEC 61850 central management.

Windows-based system nodes are ready for hardening after the installation of the core software. The hardening is done using an internal software of ABB which has pre-determined baselines for different operating systems and core software. The project engineer has to pick the correct baselines according to the software installed on the system node and run the tool. The tool configures the following categories listed in Table 3.

Table 3. List of categories of hardening software.

Hardening category	**Description**
Application whitelisting	AppLocker is enabled and configured to block running software from specific user groups.
Audit policies	Increases the user actions that are audited and tracked by Windows.
Custom scripts	Any custom scripts made by user can be ran.
Firewall	Replaces the default firewall rules with pre-defined set according to least privileges.

Local security policies	Configures password, account and user right policies and varying security policies.
Services	Enables / disables Windows services.
User management – Groups	Creates user groups which are used by other security categories.
User management – Users	Creates default user accounts and assigns them to specific user groups.
Windows apps	Removes unnecessary built-in apps which are bundled with operation system.
Windows standard user with less privileges	Restricts user access to product installation folder and assigns permissions for non-admin user accounts.

Additional manual configuration should be done according to the deployment guidelines of system nodes and software when needed.

6.3.3 Configuration of General System Node

The configuration of any other system node should be done according to the deployment guidelines. Common cybersecurity configuration tasks are listed in Appendix 4, which should be followed and the progress should be tracked.

The most common tasks are:

- Removing, disabling or renaming default user accounts
- Creation of additional user accounts and configuring password and permissions
- Removal or disabling of unnecessary features.

6.3.4 Configuration Backup

When the initial configuration is complete, and the operation is verified the system node configuration should be backed up to external location. This is done to ensure no work is lost if the system node malfunctions or an unexpected environmental event occurs such as flooding or destruction from overvoltage by lightning.

Backups from Windows-based system nodes can be taken with image backup software such as Acronis True Image or built-in Windows backup tool. Built-in Windows backup tool can be set to take a system backup as a scheduled task to the network drive of the management network where feasible.

Backups from general system nodes such as firewalls and network switches should be taken manually.

The external backups should be stored according to the file handling policies of ABB.

6.4 Factory Acceptance Test

Factory acceptance test consist of system-wide testing procedures. During the thesis example cybersecurity procedures were developed to be used as a part of the official factory acceptance testing. The testing procedures can be found on Appendix 2.

6.5 Shipping

Before the shipment the following tasks should be conducted to satisfy the requirements:

- (Optional) Removal of the central management software agent
- Creation of system security audit report
- Storing of successful antivirus report
- Backup of each system node.

If the central management software is not sold as a service, the agent should be removed before delivery. The system data for the security audit report can be collected with ABB's internal software. The auditing software collects various information of the system which include but are not limited to:

- Group policies
- State of antivirus
- Software firewall state and rules
- List of installed programs
- List of services
- Windows security updates.

A successful antivirus report should be backed up so there is proof that the system was clean of known malware at the time of the shipment. The report should include the antivirus engine and database version, the scope of the scan and the results. A successful scan means that all the content has been scanned and no malware was found.

The system security audit report should be compiled from the data mentioned above and stored according to the internal file handling policy.

The backups should be taken according to paragraph 6.3.4 to ensure that any system node can be recovered if anything unexpected happens such as destruction of system hardware in transit.

6.6 Site Acceptance Test

Site acceptance test consist of system-wide testing procedures at the customer is location. During the thesis example cybersecurity procedures were developed to be used as a part of the official site acceptance testing. The testing procedures can be found on Appendix 3.

If any changes are made in between the shipment and completion of the site acceptance tests the system node backups should be taken again on external media as typically there is a warrant period. During the warrant period the backups are stored

according to the internal file handling policy in case the recovery of a system node is needed.

In addition, the system data could be collected again with the audit software to compile a new version of system security audit report, if needed.

6.7 Hand-over

Hand-over is a symbolic project phase, when the system responsibility for a system is transferred to the customer as it is. At this point at the latest the required documentation listed in the minimum requirements is delivered to the customer.

7 CONCLUSIONS

Cybersecurity is not a trivial part of the SCADA engineering process and requires multiple steps during the project to be done. Some of the steps can be automated with the use of software and scripts but in the end the responsibility, is in the hands of the project engineers.

The policies and requirements are usually not enough by themselves to ensure that the system is compliant with the minimum requirements and therefore more detailed project steps should be in place. With the use of documentation created during the thesis, the outcome of the cybersecurity should be standardized and at on acceptable level.

In the future the possibilities to integrate advanced cybersecurity functions into standard workflow of the project engineering should be studied. For example, these functions could include:

- two factor authentication
- centralized logging services
- centralized user management.

REFERENCES

/1/ ABB Oy. 2018. Intranet. Accessed 12.1.2019.

/2/ ABB Oy. 2018. MicroSCADA Pro. Accessed 24.10.2018. https://new.abb.com/network-management/network-management/microscada-pro

/3/ ABB Oy. 2018. MicroSCADA Pro SYS600. Accessed 24.10.2018. https://new.abb.com/network-management/network-management/microscada-pro/sys600

/4/ ABB Oy. 2018. MicroSCADA Pro DMS 600 – Leading Distribution Management System. Accessed 24.10.2018. http://www.abb.com/cawp/seitp326/61ad3b3d1774e87bc125799c004c92b8.aspx

/5/ ABB Oy. 2018. Knowing the past improves the future. Accessed 27.10.2018. https://new.abb.com/network-management/network-management/microscada-pro/sys600/historian

/6/ National Institute of Standards and Technology. 2015. Guide to Industrial Control Systems (ICS) Security. Accessed 2.12.2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

/7/ Cisco. 2018. What is Cybersecurity? Accessed 27.10.2018. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

/8/ National Institute of Standards and Technology. 2016. Small Business Information Security: The Fundamentals. Accessed 29.10.2019. https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf

/9/ Intel Corporation. 2018. Frequently Asked Questions about Secure Boot. Accessed 18.5.2019. https://www.intel.com/content/www/us/en/support/articles/000006942/boards-and-kits/desktop-boards.html

/10/ Sharpened Productions. 2018. TechTerms - Firmware. Accessed 4.12.2018. https://techterms.com/definition/firmware

/11/ Tech-FAQ. 2018. Firmware. Accessed 4.12.2018. http://www.techfaq.com/firmware.html

/12/ U.S. Department of Homeland Security 2016. Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Accessed 4.12.2018. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf