Supervisory Systems
FAST/TOOLS™

SCADA Cyber Security

Information on Securing SCADA systems
Version: 1.0

Erik Daalder, Business Development Manager

Yokogawa Electric Corporation— Global SCADA Center

T: +31 88 4641 360 E: erik.daalder@nl.yokogawa.com

Executive Summary

Due to current events of target virus attacks such as Stuxnet and Flame, the demand for cyber security has become high priority within Industrial Automation (IA). Since the beginning of IA, the global approach for security technologies has been reserved. There was a valid reason for the industry wide reticence, given that there were no direct vulnerabilities. Initially, the internet and office domain were not in direct connection with the process control network. This philosophy has changed significantly since the introduction of Supervisory Control and Data Acquisition (SCADA) and Manufacturing Execution Systems (MES). The general purpose Information Technology (IT) systems provides well developed IT security solutions with proven technology. Unfortunately not all solutions are applicable for IA and control systems. The demands by IA differ from the usability requirements within general purpose IT. Most notable difference is the high availability demand within IA, which complicates security. Figure 1 ANSI/ISA-99 shows the different priorities of the two environments. The objective of this report is to inform about the range of vulnerabilities in the current use of SCADA systems and to provide solutions to mitigate cyber-attacks.

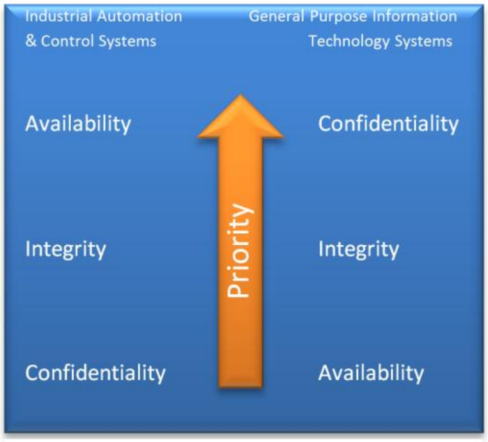

Industrial Automation & Control Systems
General Purpose Information Technology Systems
Availability
Confidentiality
Integrity
Priority
Integrity
Confidentiality
Availability

Figure 1 ANSI/ISA-99

CONTENTS

Introduction

The Industrial Control Systems (ICS), including SCADA, are known for their high availability. The demand for high availability remains the number one requirement within the industry. More recently the industry desires an additional strong requirement, namely more accessibility by interconnecting the SCADA, therewith the process systems, with the enterprise network. By introducing accessibility to ICS it can compromise the availability, because it becomes more exposed to cyber security vulnerabilities. As figure 1 shows most common vulnerabilities in ICS can be found in:

- Improper Input Validation
- Permissions, Privileges and Access Controls
- Improper Authentication

Insufficient attention to cyber security by IA end users can have a tangible negative impact on Health, Safety, Quality of the Environment and lead to economic loss.

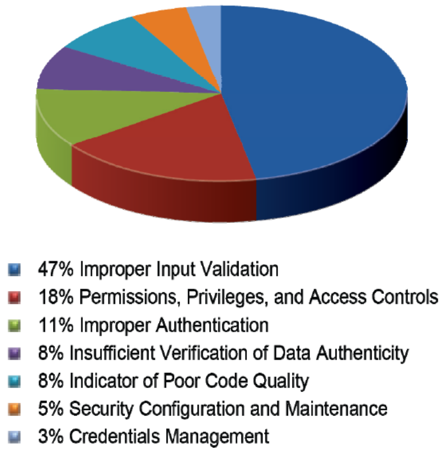
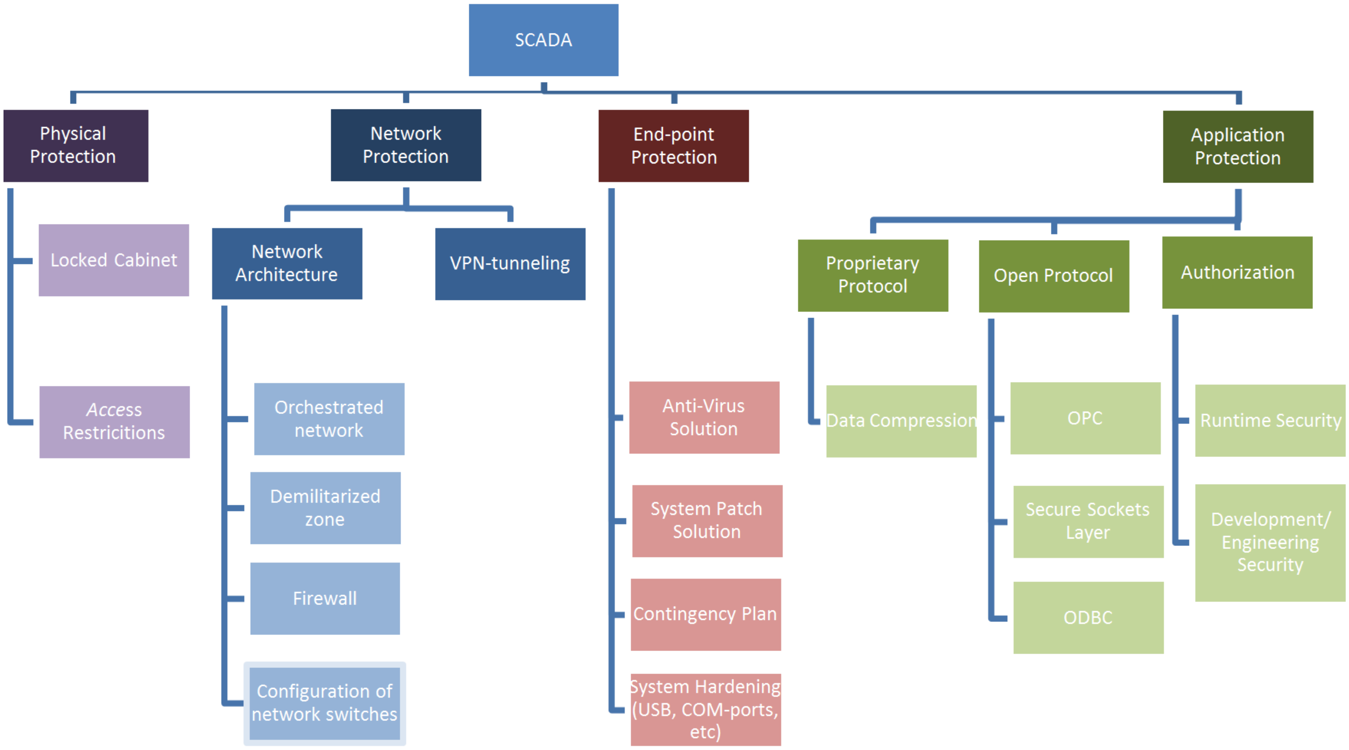


Figure 1 Categories of vulnerabilities identified in 2009-2010 CSSP product assessment. [*1]

General Overview

The diagram below displays a structured overview of SCADA cyber security elements. The following chapters will go into detail on these topics.



**1 CCSP stands for Control Systems Security Program.*
Part of the U.S. Department of Homeland Security (DHS) National Cyber Security Division.

Physical Protection

The first layer of defense is by Physical Protection. Attacks can be carried out by malicious individuals who have unsecured physical access to the system. These attacks can range from disconnecting a cable to deliberately pushing a virus by USB or installing a key logger for espionage purposes.
Aside from malicious incidents, unexpected infections are becoming more common, for instance by using an infected USB stick.
By implementing proven methods of system hardening and company security regulations these risks are mitigated.

Network Protection

From a stand-alone process network, SCADA has developed into a geographically distributed system. With that, the effects of internet and public networking are inevitable. This requires a different IT security strategy and network orchestration.

By dividing the plant and/or process network into separate areas with, for example dedicated Virtual Local Area Networks (VLAN), it decreases the risk of vulnerability in case of a cyber-attack.
The SCADA environment should enable users to only access the assigned dedicated areas. In this manner with SCADA the orchestrated network architecture is not only configurable hardware wise but also software wise, mitigating the vulnerabilities.
Aside from these measures, there are well developed Network Security Solutions practices, such as firewalls and Demilitarized Zones (DMZ).
When entering a different network level, securing the accessibility by integrating a firewall on either side prevents unwanted access.
When using SCADA, it is advised to differentiate network Levels specified by ISA-99, as shown in figure 3.

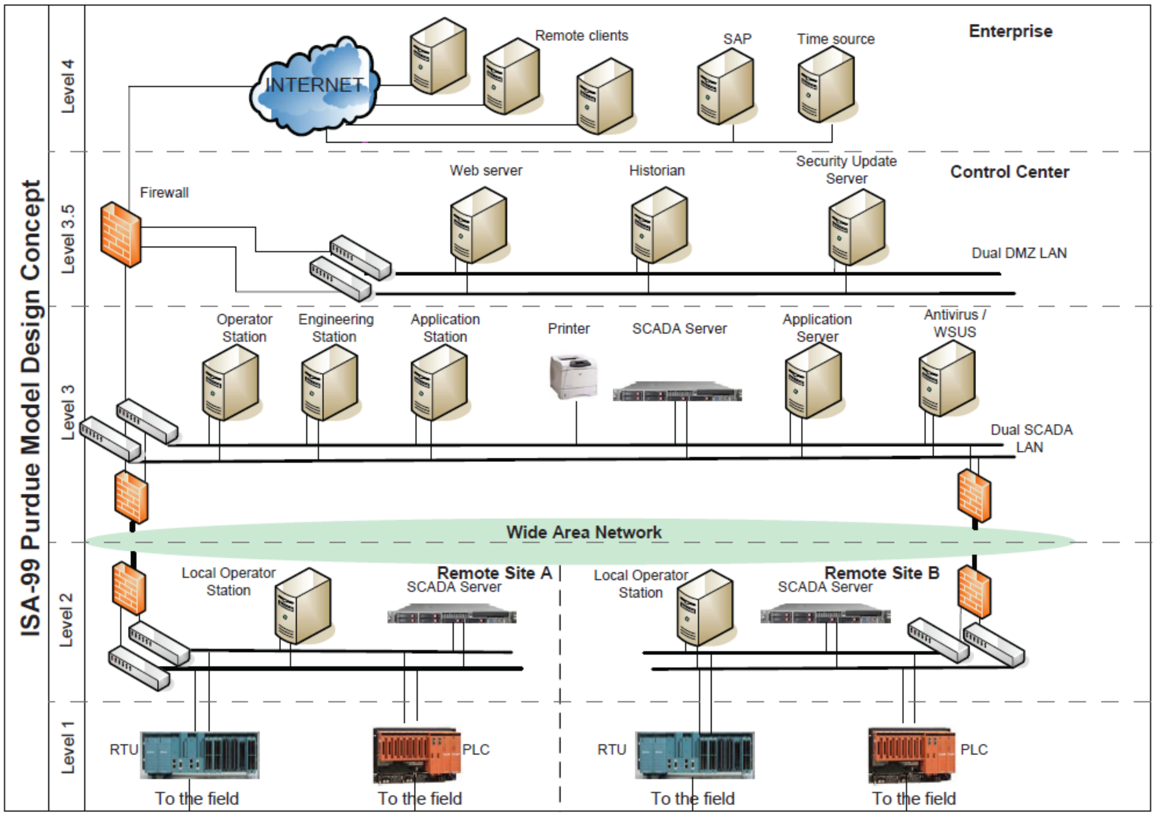


Figure 2 SCADA Network, in accordance with ISA-99

By applying a firewall in an ICS network environment enables:
- Setting ports that are allowed to communicate.
- Setting applications that are allowed to communicate
- Event logging of transactions through the firewall.
- Restriction of data transactions between different domains.
- Allowing wanted IP-addresses, denying unwanted IP-addresses.

DMZ contributes to further mitigate Inter Level accessibility. This solution strives to disable direct communication between Level 3,4 and Level 1,2 (see figure 3) . As shown in figure 4, the firewall disables all direct communication between the Process network (Level 1,2) and the Corporate network (Level 3,4). Nevertheless controlling and data acquisition is applicable to this design. **Only machines in the DMZ have connection to applications outside it. Data exchange is routed through these machines, avoiding the need for a direct connection between corporate and process applications.**

Instead of directly approaching the process machine you configure via a dedicated machine in the DMZ, hence a further mitigation of inter Level accessibility.

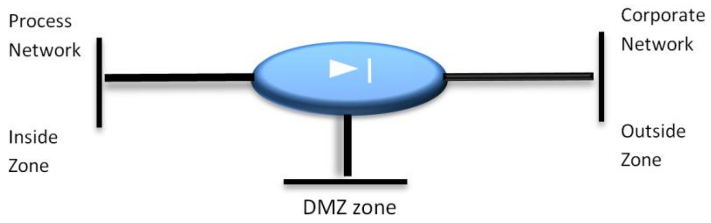
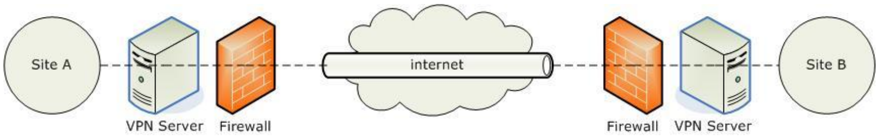


Figure 3 DMZ design

Network Communication

Virtual Private Network tunnel (VPN) ensures the integration, authorization and authentication of data transactions between various networks. VPN enables private use of the public network, such as the internet. This is done by creating an encrypted tunnel between the client and server. The encrypted tunnel is owned and controlled by one of the connected parties. Commonly Secure Socket Layer and IP Security are technologies used for creating a VPN. Transactions through VPN mitigate the vulnerability of a cyber-attack. Even with VPN vulnerabilities can still occur. For instance, when a device is used to login via VPN to the company server, this device must have the same level of end-point protection which is configured on the company server. In the unfortunate case of a device is stolen, due to lack of physical security, an attacker can try to use the device with VPN connection for their own purpose. Therefore prudence must be taken when authenticating an individual to use a device that can connect to the network.



End-Point Protection

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts."
- Eugene Spafford, renowned security expert

Perhaps this quote is over exaggerated, but nonetheless the core message is true; a computer is a vulnerable device which should be protected from outside influences.
Preferably each computer should be secured by means of anti-virus software, system hardening procedures and regular system patching.

Anti-Virus Solution

Yokogawa and McFee have a partnership to enhance the security of industrial control systems. Therefore Yokogawa recommends the use of McAfee solutions for cyber threat protection. These packages use a Centralized Management Server to control the updates of client systems. This station keeps an up-to-date overview of the client status. Updates can be pushed from this station whenever a new Yokogawa approved update has been released.
The necessity of Anti-Virus solutions becomes more obvious when figure 5 is considered. This displays all known Malware Samples in the database of McAfee. (Malware is an abbreviation for Malicious Software) As shown the amount of known virus is significant, and these numbers are still growing. The use of Anti-Virus solutions enables protection of the system against known Viruses. Yokogawa frequently tests the releases of McAfee to exclude any features which could influence the continuity of Yokogawa`s control systems.

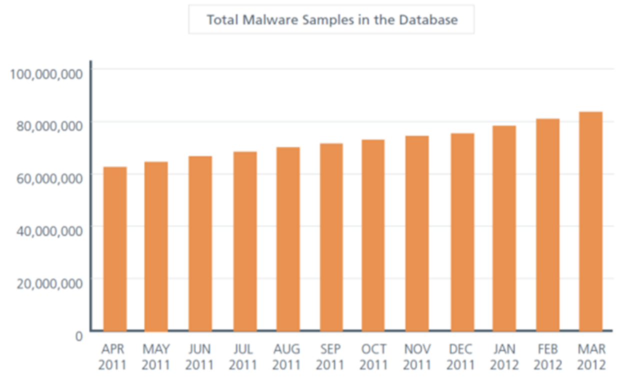


Figure 4 source McAfee

System Update Solution

Yokogawa uses the Windows Server Update Services (WSUS) as its management console. Pushing updates from a management server makes it possible to plan system maintenance and reduce downtime. The WSUS retrieves the Microsoft security patches from the Microsoft website or a WSUS server located at the customers office and is installed on the Centralized Management Server. This station gives an up-to-date overview of all clients' status. Updates are distributed from this station whenever a new patch (tested and approved) has been released. Updates are collected and installed manually for the same reasons as for the anti-virus. Security patches and Service Packs are typically released after Yokogawa have tested them against our hardware/software solutions. Figure 6 shows the number infected systems per 1000 examined Microsoft systems. Microsoft develops patches in order to close these kinds of security leakages. However, if we would take Windows XP for example, the security patch developments will cease per 8 April 2014.
Microsoft has announced that they will cease the Extended Support on Windows XP, which will include closing new security leakages. As a result XP will become more vulnerable, a vulnerability that cannot be fixed by patching or service packs. This will likely lead to a high number of OS-platform migrations in the industry.

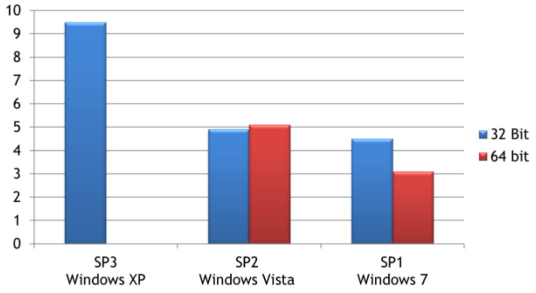


Figure 5 Number of infections per 1000 examined systems (1^{st} half 2012), by Microsoft

Contingency plan

If the unfortunate situation of system infection would occur this can lead to reduced system performance, loss of visualization, loss of control or that a hacker has control over the process or shuts down the process.

For these cases, ISA guidelines provide a contingency plan.

This definition states that a backup and systems restoration procedure shall be established, used, and appropriate tested. Backup copies must be well protected to ensure critical systems can be restored in the event of a disaster situation. Part of the IT security management system is the determination of:

- The amount of time/resources required for system restoration
- The location of backup files
- The hardware
- The frequency of backups

For back-ups and image creation by the backup controller, for instance a backup package can be used. This package can be tailored to the specific requirements of an industrial environment.

The Central Managed Station creates application backups of the systems configuration data. Engineering source files and database files are backed-up after synchronization.

Once collected on the backup server Hard Disk, the data is transferred onto an external storage device (disk-2-disk-2-tape principle). This approach enables a quick system restoration and has the assurance of security as the files are on an external backup device.

Making images of hard drives is a useful way of backing up all your information, including your entire operating system. In case of a disaster - hard disk failure or virus infection - this image provides for a quick system recovery.

It is advisable that backups are stored at a safe place (ideally outside your perimeters).

Application Protection

Of all vulnerabilities identified by the 2009-2010 CSSP assessment a staggering 47% were due to Improper Input Validation. Examples of improper input validation are:

- Buffer overflow
- Lack of bounds checking
- Command Injection
- Cross site scripting (XSS)

Bufferoverflow/lack of bound checking

Command injection enables an attacker to implement and perform run malicious code. This is done by detecting unsecured buffer, and exploiting changing of variables which changes program behavior.

Mitigation of command injection can be achieved via numerous ways, e.g. by use of safe libraries.

By use of protocol or transferring data via a secure connection by VPN can mitigate the risk due to bufferoverflow/lack of bound checking.

Open Protocol

OLE for Process Control (OPC) is a generally accepted open protocol within the Process Control Industry. OPC and common Operating Systems facilitates an easy to use interface of ICS equipment. Unfortunately this can result in vulnerabilities, where accessibility to malicious users becomes more available. The main reason is that classic OPC makes use of DCOM, a Microsoft technology for application communication between machines. DCOM services are normally open to allow ease of use of client software, typically in office environments.

There are smart concepts to cope with these vulnerabilities. For instance an OPC Tunneler provides a solution which has embedded the OPC functionality, while remaining secure, plain configurable and highly available. The OPC Tunneler enables the SCADA system to communicate with OPC-servers without transporting OPC-protocol over the underlying networks. The SCADA server communicates to a local OPC Tunneler using a Proprietary Protocol. The OPC Tunneler in turn communicates with the OPC Server.

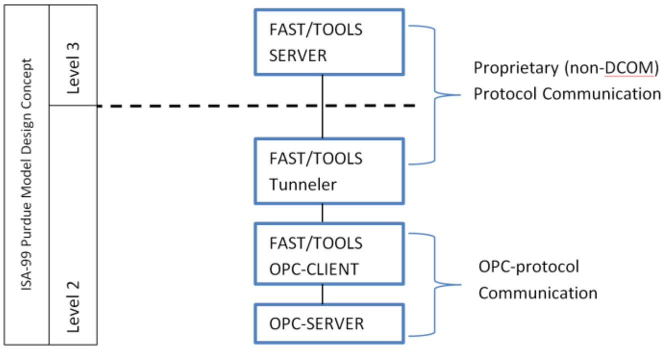

ISA-99 Purdue Model Design Concept
Level 3
Level 2
FAST/TOOLS SERVER
FAST/TOOLS Tunneler
FAST/TOOLS OPC-CLIENT
OPC-SERVER
Proprietary (non-DCOM) Protocol Communication
OPC-protocol Communication

Figure 7 OPC Tunneler Architecture

The security issues above have been recognized by the OPC Foundation. The OPC Foundation has developed the Unified Architecture (UA). This so called 'next generation OPC standard' provides a secure solution in the transport layer. This gives the convenience of enabling secure OPC data communication between different network Levels. OPC UA uses signatures to authorize and authenticate communication between client and server via encrypted communication. The OPC UA security architecture is show in Figure 8.

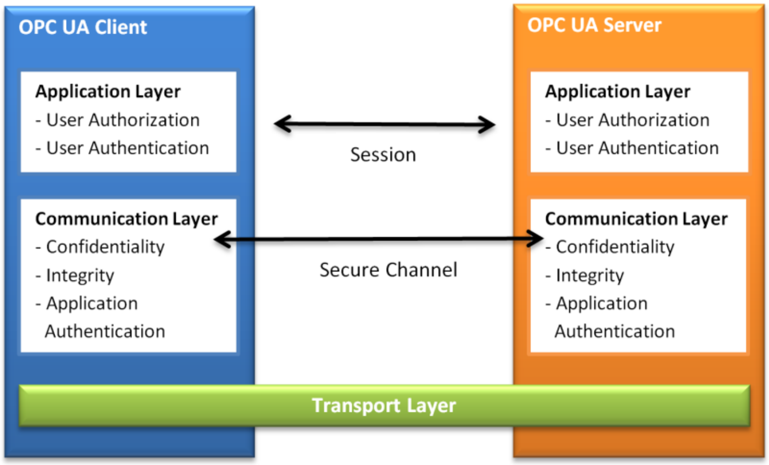


Figure 8 OPC UA Security Architecture

The client and server application primarily exchange process information, this is executed in the Application Layer by setting up a Session (see figure 8). This layer manages all User Authorization and User Authentication. When a session is initiated by the Application Layer it communicates over a Secure Channel that is managed by the Communication layer. All communication over the Secure Channel is encrypted to ensure data Confidentiality. By exchanging Message Signatures the Integrity is assured. Furthermore secured communication is achieved by exchanging Digital Certificates between client and server to provide application Authentication.

Secure Sockets Layer

Currently the high end SCADA applications enable users to Monitor, Control and Engineer their SCADA system in a wide geographical distributed network configuration.
The central SCADA Server can be located at great distance from the SCADA Web-Client. This can be achieved by data transport over the internet. Transporting process data via the Internet requires well considered Cyber Security. Vulnerabilities can be mitigated by securing data transport using Secure Sockets Layer and if necessary equipped with a VPN connection.

Secure Sockets Layer (SSL) presently better known as Transport Layer Security (TLS) has three basic functionalities:
1. Message encryption
2. Detection of Message alteration
3. Authentication between Client & Server

TLS ensures the user that all communication transactions via the internet are encrypted. This enables the user to send sensitive information while mitigating the risk of interception.

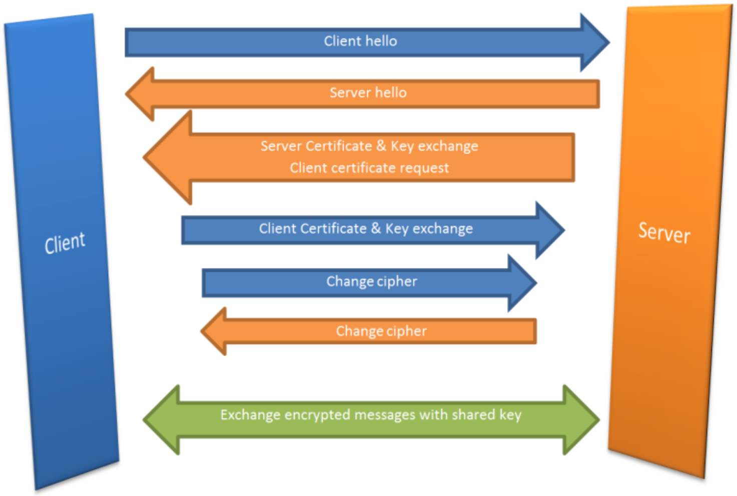

Client
Client hello
Server hello
Server Certificate & Key exchange
Client certificate request
Client Certificate & Key exchange
Change cipher
Change cipher
Exchange encrypted messages with shared key
Server

Figure 9 Communication flow for TLS

ODBC/SQL

Open database connectivity (ODBC) was developed by the SQL Access Group in 1992. This standard enables any program to communicate with a database, independent of the database type. Examples of industry standard databases connected with SCADA systems are Oracle and MS-SQL. Often ODBC is considered cyber-security vulnerability, while this is actually not the source of the vulnerability. The databases to which the ODBC connects, e.g. MS-SQL, would be the source of the vulnerability.
These relational databases make use of SQL (Standard Query Language) to communicate within the database. The vulnerability can occur when the SQL-statement (a command) is insufficiently secured. This unsecured statement leaves room for malicious users to add an additional command to the statement, with the intention to kick off an unwanted SQL-query. This is also known as SQL-injection. The awareness of these vulnerabilities is very important when setting up a SQL-based database. In order to guard the system against these attacks sufficient attention must be given to e.g. database permissions, use of predefined statements, rejections of incorrect input, etc. By concentrating on secure engineering of the SQL-database, the SCADA environment is protected simultaneously. Therewith the consideration of vulnerabilities due to the ODBC connection lapsed.

Authorization

Unwanted access to the SCADA system can lead to extensive problems, for instance the malicious user can perform unwanted control actions. Remarkably the 2nd common ICS vulnerability the defined by the CSSP product assessment was:

- Permissions, Privileges and Access Controls

As mentioned earlier, this can have a tangible negative impact on Health, Safety, Quality of the Environment and lead to economic loss.

For the specific SCADA environment of FAST/TOOLS, all the privileges for a specific type of user can be specified in user profiles which define the Runtime and Development/Engineering authorization.

Runtime Security requires an engineer to set user permissions. Subsequently Runtime Security will validate if a user has permission to execute a certain command. In case a user is not authorized to employ the request, the request will be denied.
For instance, the FAST/TOOLS Runtime Security customizable components are:

- Login/password (application level)
- Process areas (items, displays, reports, etc. in access right groups)

By use of the Development Security tooling integrated in the SCADA Engineering environment a engineer can easily configure the following user/group definitions:

- Authorization groups
- Which actions (delete, modify, etc.) are allowed on SCADA definitions (displays, items, objects, classes, etc.)

When an Authorization Group is defined the Developer can configure user settings.

FAST/TOOLS and SCADA Security

Increasing cyber threats require extensive cyber security. Cyber security consists of physical, network, end-point and application protection together with system recovery back up. Besides all these measures, it is of high importance that security is integrated in the company`s philosophy, because the awareness by users is the foundation of the effectiveness of cyber security..

FAST/TOOLS is Yokogawa`s SCADA solution. FAST/TOOLS provides a reliable high performance geographically distributed Industrial SCADA System. Being the interface to multiple assets, tens of thousands of field controllers, multimiljoen I/O points located over a widely spread area makes that reliable and extended security is a high priority.

FAST/TOOLS is positioned to leverage standard and proven web security techniques as administered by IT departments. FAST/TOOLS communication is built to provide reliable and continuous data transportation.
As of FAST/TOOLS release R9.05 the new OPC standard, OPC Unified Architecture, is supported. Providing flexible data integration combined with a secure architecture solution. Since Yokogawa considers cyber security developments paramount, FAST/TOOLS started to develop the integration of OPC UA in an early stage, making FAST/TOOLS the world`s first SCADA Client to be OPC UA Certified.

FAST/TOOLS has a truly Web-based HMI to be deployed on the web. All the workflow processes, business logic, and database links are designed after careful studies both technical and ergonomically. Applications and process information can be rapidly deployed and is easily maintained centrally on the server. This so called “zero deployment” means that client applications can be run from any web-browser and the users always get the most recent version of an application. The web-based nature of the HMI asks for reliable communication, FAST/TOOLS achieves this by integration of Secure Socket Layers (SSL) security, delivering flexible server/client architecture, while maintain the security of the system.
By combining application security with hardened systems and a well-designed network architecture, FAST/TOOLS van offer a solid SCADA solution and mitigation of security vulnerabilities, giving an orchestrated network architecture.

Yokogawa provides high end Security Consultancy, that provides advice on which actions there must be taken to achieve the most secure possible system. For any questions regarding Network- or Application Security please contact the Yokogawa Global SCADA Center or the Yokogawa Network & Security Team. FAST/TOOLS Installation Manual and TIPS provides proven methods of system hardening.

Please be advised that this document solely provides a global overview on Cyber security. The most suitable solution must be determined on a per case basis. Yokogawa Global SCADA Center and the Yokogawa Network & Security Team can be contact to give advice on these matters.