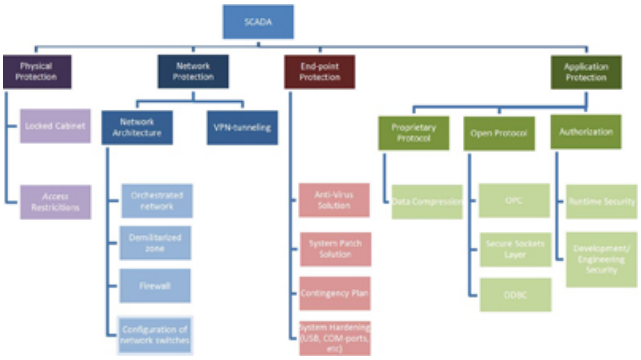
industrial ethernet book
Enhancing Automation and Internet Connectivity

Industrial Ethernet Book Issue 79 / 39

Cyber security a priority to protect SCADA systems

Engineers are being asked to connect absolutely everything to a network. The network protocol of choice is Ethernet or one of the myriad variations. Some of these assignments can look great on paper but suffer serious setbacks once realized in the modern world.



A structured overview shows SCADA cyber security elements, and important measures that can be deployed to provide secure operation of data acquisition systems.

DUE TO TARGETED VIRUS ATTACKS such as Stuxnet and Flame, the demand for cyber security has become high priority for industrial automation. From the beginning, the global approach for security technologies has been reserved and there was a valid reason for 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. But this philosophy has changed significantly since the introduction of Supervisory Control and Data Acquisition (SCADA) and Manufacturing Execution Systems (MES).

Conformance testing process

Information Technology (IT) systems provide well developed IT security solutions but unfortunately not all solutions are applicable for industrial automation and control. A notable difference is when the need for high availability complicates security. The differences between ANSI and ISA-99 highlight the priorities of the two environments. As a result, there is a need to understand the range of vulnerabilities in current use of SCADA systems, and how to mitigate cyber-attacks.

High availability a priority

Industrial control systems including SCADA are known for their high availability. The demand for high availability remains the number one requirement within industry. But more recently, industry desires an additional strong requirement, more accessibility by interconnecting SCADA and process systems with the enterprise network. Introducing accessibility to control systems can compromise availability because systems also become more exposed to cyber security vulnerabilities.

The most common vulnerabilities can be found in:

• Improper Input Validation

• Permissions, Privileges and Access Controls

• Improper Authentication

Insufficient attention to cyber security by industrial automation end users can have a tangible negative impact on health, safety, quality of the environment and lead to economic loss.

Physical Protection

The first layer of defense is Physical Protection. Attacks can be carried out by malicious individuals who have unsecured physical access to the system, and 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 and the effects of internet and public networking are inevitable. This requires a different IT security strategy and network plan. 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. The network architecture must be not only configurable in hardware and software to mitigate vulnerabilities. Added measures include 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.

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 . Use of a 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. Process machines can be configured via a dedicated machine in the DMZ, further mitigating inter Level accessibility.

Network Communication

Use of a 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.

But 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 case a device is stolen, 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

According to Eugene Spafford, a renowned security expert, "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." Perhaps this quote is 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.

Yokogawa and McAfee have a partnership to enhance the security of industrial control systems, and 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 approved update has been released. The necessity of Anti-Virus solutions is obvious. The number of known viruses 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.

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 hardware/ software solutions.

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. If a system infection would occur, this can lead to reduced performance, loss of visualization, loss of control or a hacker has control or shut 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 appropriately 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

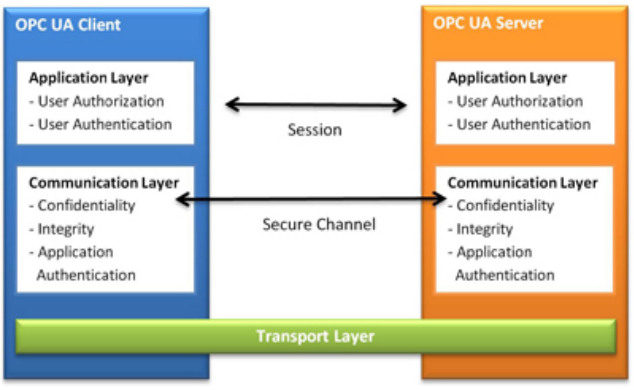
• The frequency of backups.

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 system's configuration. Source 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 hard disk failure or virus infection, this image provides for a quick system recovery.

Application Protection



OPC UA Security Architecture communicates over a Secure Channel that is managed by the Communication layer.

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:

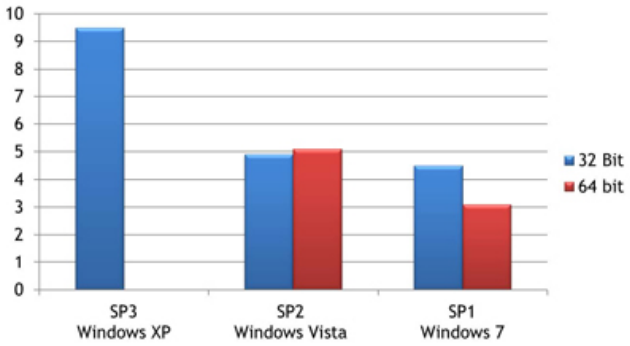
• Buffer overflow

• Lack of bounds checking

• Command Injection

• Cross site scripting (XSS)

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. Use of protocol or transferring data via a secure connection by VPN can mitigate the risk due to buffer overflow/lack of bound checking.



Number of infections per 1000 examined systems (1st half 2012), by Microsoft.

Of all vulnerabilities identified by the 2009-2010 CSSP assessment, a staggering 47% were due to Improper Input Validation.

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 communication between machines that are normally open to allow ease of use of client software, typically in office environments.

There are smart concepts to cope with these vulnerabilities. An OPC Tunneler provides a solution to embed 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.

These issues have been addressed by the OPC Foundation with the Unified Architecture (UA). This ¡®next generation OPC standard' offers a secure solution in the transport layer. This enables data communication between network Levels using signatures to authorize and authenticate communication between client and server using encryption technology.

The client and server application primarily exchange process information, which is executed in the Application Layer by setting up a Session. 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 using data transport over the internet. 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 and enables sending sensitive information while mitigating the risk of interception.

ODBC/SQL

Open database connectivity (ODBC) 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 a cyber-security vulnerability, while it 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 to communicate within the database. The vulnerability can occur when the SQL-statement 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 or SQL-injection. The awareness of these vulnerabilities is very important when setting up a SQL-based database. To guard the system against these attacks sufficient attention must be given to database permissions, use of predefined statements and rejections of incorrect input. By concentrating on secure engineering, the SCADA environment is protected.

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 most common ICS vulnerability as defined by the CSSP product assessment was permissions, privileges and access controls. 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 runtime and development/ engineering authorizations.

Runtime Security requires an engineer to set user permissions and 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. By use of Development Security tooling integrated in the SCADA Engineering environment an engineer can also easily configure user/group definitions.

This includes 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.

*Article by **Yokogawa's Global SCADA Center**.*

www.yokogawa.com

Source: Industrial Ethernet Book Issue 79 / 39