PROTECTING INDUSTRIAL CONTROL SYSTEMS AND SCADA NETWORKS

Cyber attacks on industrial control systems and in particular critical and manufacturing infrastructures is now a reality. Power generation facilities, metropolitan traffic control systems, water treatment systems and factories have become targets of attackers and have been hit recently with an array of network breach, data theft and denial of service activity. Service uptime, data integrity, compliance and even public safety require that organizations implement steps to deal with these security concerns. It is time to take action.

Industrial Control Systems from leading vendors are vulnerable and exploits are now freely available on the Internet. The vulnerabilities vary from basic issues like systems without passwords or with hard-coded passwords to configuration issues and software bugs. Once an attacker is able to run software that has access to a controller, the likelihood of a successful attack is very high.

This paper presents a summary description of the threats to industrial control systems used in critical infrastructure and manufacturing and suggests guidelines for mitigating this risk using a multi-layered security strategy.

THE THREAT

Industry, manufacturing and critical infrastructure facilities (electricity, oil, gas, water, waste, etc.) rely heavily on electrical, mechanical, hydraulic and other types of equipment. This equipment is controlled and monitored by dedicated computer systems known as controllers and sensors. These systems are connected to management systems—together they form networks that leverage SCADA (Supervisory Control and Data Acquisition) and ICS (Industrial Control System) solutions. Both ICS and SCADA enable efficient collection and analysis of data and help automate control of equipment such as pumps, valves and relays.

The benefits that these systems provide have contributed to their wide adoption. Their ruggedness and stability enable critical infrastructure-related facilities to use ICS and SCADA solutions for long periods of time—often in excess of 10 and sometimes 20 years and beyond.

Stuxnet

Probably the most well-known Critical Infrastructure attack was Stuxnet—a sabotage of the operation of an Iranian nuclear facility that targeted Siemens Programmable Logic Controllers (PLCs) used in the facility for process automation and control.

Stuxnet exploited several previously undisclosed vulnerabilities in Microsoft Windows. It was initially propagated via intentionally infected USB memory devices. These were inserted into Windows PCs that were connected to the PLC network, with subsequent infection of the PLCs.

However, the benefits provided by ICS and SCADA systems make them equally capable of damaging infrastructure operations and processes. By altering the commands sent to the controllers, or by changing sensors readings, attackers can create changes in electrical, chemical, mechanical or other processes. These changes can introduce sudden and apparent or slow and hard to notice modifications to factory processes. The results can be defective products, loss of productivity, disruption of service or worse—genuine risk to public safety.

Individuals or organizations perform attacks against ICS and SCADA systems with a detailed understanding of the environment in which these systems operate and with specific motivation—these can be disgruntled employees, foreign governments, business competitors, criminals or political/ideological activists.

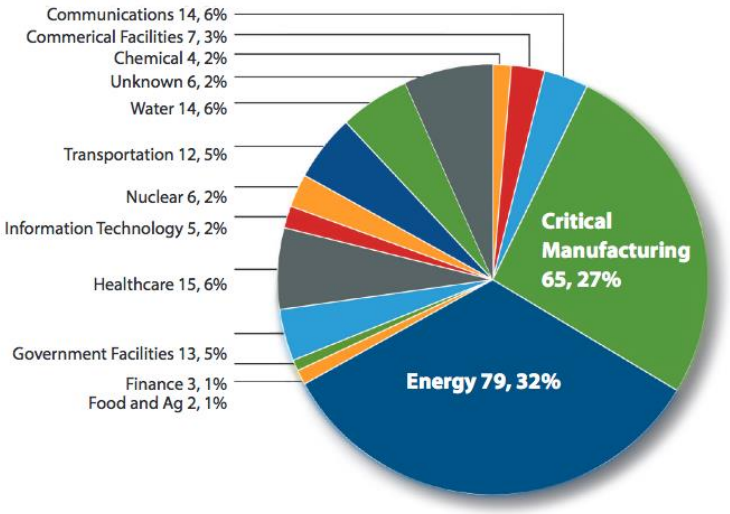
In order to alter a controller command or change a sensor reading, an attacker needs to either access the controller/sensor itself or to access a remote system which is communicating with it. This requires either physical or remote access to some computer or network that is connected to the controller/sensor.

Most SCADA/ICS networks have some level of perimeter defense, including network segmentation and firewall technologies. Bypassing such perimeter defenses from the outside is typically relatively difficult, and so attackers are always looking for alternative ways to get inside—for instance, through a gate that is left open, or by triggering some operations from inside the organization that opens up a communication channel to the outside. For example:

- Using a remote access port used by vendor for maintenance
- Hacking a legitimate channel between IT systems and ICS/SCADA systems
- Convincing an internal user to click on a URL link in an email from a workstation that is connected both to the ICS/SCADA network and to the Internet
- Infecting laptops and/or removable media while outside the ICS/SCADA network, later infecting internal systems when they're connected to the network for data collection, controller/sensor software updates, etc.
- Making use of configuration mistakes in security or connected devices

Once inside, the attackers might leverage information that they have about the network, or else conduct reconnaissance to learn the environment. Or, they might just try well-known access methods to see if they work due to weak or incomplete network security policies. Very frequently, weaknesses in specific vendor implementations of a protocol or typical system/security configuration mistakes are taken advantage of.

Infrastructure attacks are happening daily all around the world, as indicated by hundreds of cases in just the last few years. They are a relevant and imminent threat to any organization.



245 incidents reported and investigated by US ICS-CERT in 2014
Source [ICS Cert Monitor September 2014 – February 2015]

ICS AND SCADA NETWORK SECURITY

ICS/SCADA networks and devices were designed to provide manageability and control with maximum reliability. Often they do not feature mechanisms to avoid unauthorized access or to cope with the evolving security threats originating from external or internal networks that have become common in the IT world.

While their implementation is often proprietary, SCADA controllers are essentially small computers. They use standard computer elements such as operating systems (often embedded Windows or Unix), software applications, accounts and logins, communication protocols, etc. Moreover, some of the management environments use standard computing environments such as Windows and Unix workstations.

As a result, the familiar challenges associated with vulnerabilities and exploits apply to ICS and SCADA systems, with the additional challenge of such systems operating in environments that can be physically difficult to reach or that can never be brought offline.

Industrial Control Systems from most leading vendors are vulnerable as demonstrated by hundreds of exploits that are now freely available on the Internet from various sources. The vulnerabilities, which vary among the products examined, include backdoors, lack of authentication and encryption, and weak password storage that would allow attackers to gain access to the systems. The security weaknesses also make it possible to send malicious commands to the devices in order to crash or halt them, and to interfere with specific critical processes controlled by them, such as the opening and closing of valves.

A common belief is that ICS and SCADA networks are physically separated from corporate IT networks. This might be accurate physically, in the sense that some companies operate distinct LANs or air gap their control and corporate networks from one another. In other cases, companies use the same LANs and WANs, but encrypt their ICS and SCADA traffic across a shared infrastructure. More frequently however, networks require some level of interconnectivity in order to obtain operational input from and/or export data to external 3rd party systems.

Programmable Logic Controllers (PLC) are purpose-built computers used for automation of electromechanical processes such as control of pumps, valves, pistons, motors, etc. PLCs are used to control functions in many industries such as water, power and chemical plants; gas pipelines and nuclear facilities; manufacturing facilities such as food processing plants and automobile and aircraft assembly lines and even in correctional facilities to control large doors.

	A-B	Schneider Electric	GE	SEL	Koyo
Firmware	!	7	!	!	!
Ladder Logic	!	!	7	!	7
Backdoors	!	7	7	3	3
Fuzzing	7	7	7	!	!
Web	!	7	N/A	N/A	7
Basic Config	!	!	7	!	!
Exhaustion	3	3	7	3	3
Undoc Features	!	7	7	!	!

3 = OK 7 = Vulnerable and Exploit is available ! = Vulnerable, exploit not available

SCADA network devices have specific characteristics which can be very different than regular IT systems:

- They are often installed in locations that are difficult to access physically (e.g. on towers, on an oil rig, on a working robot) and are environmentally more challenged than regular IT systems (e.g. outdoors, extreme temperatures, vibrations) or require special input voltages and mounting options
- They often use propriety operating systems that have not been subjected to security hardening
- Their software cannot be updated or patched frequently, due to access limitations, concerns over downtime or the need to re-certify
- They use proprietary or special protocols

In the last 20 years, the IT world has gained significant experience in protecting computer networks—dealing with the growing problem of operating system and application software vulnerabilities by developing practices and processes that enable them to function in a secured manner. Reusing the know-how and technologies developed over the years can save significant time and money, but this can only be done when understanding the differences between SCADA and IT environments and while using specialized security practices and technologies as part of the solution.

SCADA PROTOCOLS

SCADA networks make use of specific and sometimes proprietary protocols. Many of these protocols have known shortcomings that make them susceptible to attack. Here are a couple notable examples:

"In conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the Enterprise network. On average, we see 11 direct connections between those networks and in some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise environment."

May 2011 Testimony of National Cybersecurity and Communications Integration Center Director Sean McGurk

MODBUS is an application-layer communication protocol. It provides client/server communication between devices connected on different types of buses or networks. MODBUS is mainly used for supervision and control of automation equipment. The protocol provides no security against unauthorized commands or interception of data.

An attacker with IP connectivity and a Modbus client simulator (available from the Internet and potentially embedded in malware) can create various types of attacks:

- Run a reconnaissance attempt using a scanner to determine what function codes are supported in a Modbus TCP server to help plan an attack
- Issue write requests to the Programmable Logic Controller (PLC) device, which could result in the device being corrupted, or displaying other undesired behavior
- Send Force Listen Mode commands to PLCs to create a state of chaos—subsequently, PLCs will not respond to request packets
- An attacker with physical or logical access to a PLC intercepts or blocks Modbus requests to the PLC and responds with an exception response message, allowing the attacker additional time to modify the PLC or other field systems and avoid detection

DNP3 (Distributed Network Protocol) is a set of communication protocols used between components of process automation systems. Its main use is in utilities such as electric and water companies (usage in other industries is not common). Although the protocol was designed to be very reliable, it was not designed to be secure from attacks. Typical DNP3 implementations do not employ encryption, authentication or authorization—the devices simply assume that all messages are valid. Common DNP3 attacks rely on the ability to intercept, modify or fabricate DNP3 messages. This can happen in the link or application layers. Typical attack scenarios include:

- An attacker with network access captures and analyzes DNP3 messages, providing the attacker with information about network topology, device functionality, memory addresses and other data
- Based on knowledge of normal DNP3 traffic patterns, the attacker can simulate responses to the master while sending fabricated messages to remote devices
- An attacker can install a “man-in-the-middle” device between the master and outstations, that can read modify and fabricate DNP3 messages and/or network traffic
- Link layer attacks can insert incorrect values in messages messing with protocol implementation of some DNP3 devices

These attacks can result in extremely serious Denial of Service or changes in the industrial process without the knowledge of operators.

SCADA TRAFFIC SECURITY

Security solutions working in SCADA environments must be able to:

- Perform protocol validation and anomaly detection—i.e. identification and prevention of traffic that does not comply with protocol standards and that can create device malfunction

- Provide identification and enforcement of allowed commands, queries and responses within the protocol based on allow/block rules
- Provide prevention of transmission of payloads that are not known or can potentially exploit a specific vulnerability
- Provide prevention of excessive rates of communication that can create Denial of Service
- Log traffic details such as source, destination, users, time, protocol methods, queries and responses, login attempts, etc., used for forensic and trend analysis
- Ensure connectivity and minimal latency at all times including any hardware and software failures
- Be managed and updated from remote locations without the need to physically access them
- Be updated without any interruption/downtime to the SCADA network traffic

SECURING ICS AND SCADA PROCESSES

This section suggests guidelines for protecting ICS and SCADA infrastructures through an understanding of the environment, analysis of the security risks and implementing a comprehensive security strategy to deal with the security concerns.

UNDERSTAND YOUR ENVIRONMENT

We can protect what we know. The problem is that many legacy environments include devices, communication links, software versions, accounts and users, which were added over time, and for which there are incomplete records.

Step one in securing any network is making sure there is an up-to-date mapping and list of its components.

The mapping should include:

- Inventory of devices and communication links
- Diagram of the physical and logical locations and connections between devices
- Hardware and software versions
- List of accounts and users in each device and their access privileges

INITIAL ANALYSIS

Based on the mapping conducted, it is possible to start with an initial analysis of security risks. This process assesses what would be the severity, probability and business impact of an attack—that is, how severely a successful attack would affect the environment, how easy it would be for the attacker to launch an attack and what would be the business consequences of the attack.

The following are some of the major points to consider when conducting such an analysis:

1. Physical Access

Physical access to SCADA networks components enables network configuration sabotage, configuration changes that are difficult to notice and the installation of devices for eavesdropping or changing communication controls.

2. Logins
Computer systems and controllers among them have logins. Many times these systems are left with factory defaults that allow access using a well-known user name and password. In many organizations, when people leave, accounts are not disabled and passwords are not changed.

3. Configuration and Hardening
Most computer systems allows configuration, which limits some operations that are not necessary for specific deployment scenarios. This is an important line of defense not just for attackers, but also for avoiding mistakes.

4. Software Versions and Patches
Due to concerns about system stability, software versions of controllers are rarely updated. This results in organizations running code that is known to have vulnerabilities for months and even years. Malware designed to exploit common vulnerabilities could easily access such systems.

5. Logging
One important aspect of any security model is the monitoring of the network and systems. Most devices are capable of issuing logs that contain valuable information for real time security event management, security evaluation, forensic analysis and trend analysis.

Lack of logging information can hide successful attacks attempts over months or years, and can make the analysis of attacks after the fact extremely difficult.

6. Interfaces and Interconnects
Interfaces and Interconnects are a major source for infiltration into ICS networks. It is critical to map and regulate them at all times. In cases where an interface is needed, a careful security analysis should be conducted and proper policy, user education and enforcement technology must be deployed.

Examples:

a) Remote administration channels (out-of-band ports, modem dial-in)
b) Removable media (thumb drives, smart phones)
c) Portable equipment (laptops)
d) File and data transfer to other systems
e) Network connections
f) Wireless interfaces
g) Serial interfaces

A SECURITY STRATEGY

To achieve the level of protection needed for industrial and critical networks, security needs to grow from a collection of disparate technologies and practices to an effective business process. Check Point recommends organizations to look at three dimensions when deploying a security strategy and solution:

1. Policies
Security starts with a widely understood and well-defined policy—closely aligned to business needs rather than a collection of system-level checks and disparate technologies. Policies should take into account that the priority is the business and

suggest ways to conduct them in a secure manner as part of the business instead of appearing in a completely different context.

2. People

Users of computer systems are a critical part of the security process. It is often users who make mistakes that result in malware infections and information leakage. Organizations should pay much attention to the involvement of users in the security process. Employees need to be informed and educated on the security policy and their expected behavior when surfing the Internet or sharing sensitive data. At the same time, security should be as seamless and transparent as possible and should not change the way users work.

Implementation of a security program should include:

- Education program—ensuring that all users are aware that systems are potentially vulnerable to attack and that their own actions may allow or help prevent it
- Technology that advises people in real time as to why certain operations are risky, and how they could conduct them in a secure manner

3. Enforcement

Deployment of security technology solutions such as security gateways and endpoint software is critical for automated analysis of traffic, prevention of attacks and regulation of work procedure. It should meet three main goals:

a) Ensure the security of the SCADA network devices perimeter and interface points:

- It is recommended to maintain physical network separation between the real time components of the SCADA network (e.g. PLCs) and other networks
- Security gateways should be installed at all interconnects, ensuring that only relevant and allowed traffic is entering/leaving the network. This validation should be done on all communication, protocols, methods, queries and responses and payloads using firewall, application control, IPS and antivirus.
- Anti-Bot solution can deal with identification of malware that may have infiltrated and reside in the devices network.
- Threat Emulation (sandboxing) can identify malicious software embedded in files (Excel, Word, Power Point, PDF, EXE)

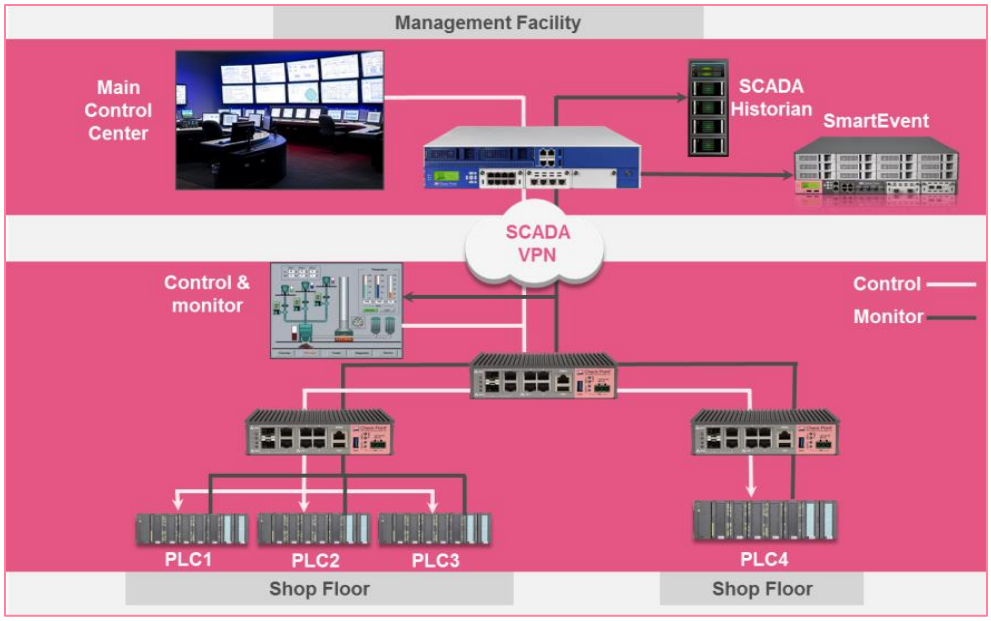
b) Ensure that all workstations and portable equipment used for management and maintenance is free from malware and secured.

- It is recommended to assign separate workstations for SCADA management software
- Dual homed workstations that connect to both an internal critical network and to other less sensitive networks or even the Internet is a major risk. In cases where such configuration is mandatory:
    - Users must be fully aware of the risks
    - Software and security configuration should limit the operations that can be performed on the workstation
    - Strict analysis of all traffic, files and payloads must be performed in real time

- All workstations must be hardened and controlled by endpoint security that includes firewall, application control, port control, media authentication/encryption, host IPS and antivirus.

c) Ensure SCADA traffic within the perimeter is valid and free of exploit attempts

The following diagram demonstrates how within the production networks specialized SCADA capabilities can prevent undesired communication and attacks as well as baseline white-list allowed commands.



RUGGED SECURITY DEVICES

Security devices for SCADA networks must often be installed in environments which are not friendly to standard IT equipment. In those cases it is essential for security devices to have robust mechanical design. Industrial specifications for dust, extreme temperatures, humidity, and vibration should be complied with to ensure physical durability. Durable devices would have an extremely high MTBF (mean time between failures) and contain a minimum number of moving parts such as fans and hard drives.

MANAGEMENT

Managing a large network consisting of hundreds or thousands of devices is a complex task. Remote central management of security policies and effective situational visibility are key to effectively securing the infrastructure.

As security of organizations is comprised of many layers, it is important to have a single view of all security incidents in one place. Standardizing and unifying security solutions can allow use of expertise already present in the organization and provide a better overall view of the security posture across ICS security devices, IT systems security devices and endpoint computers.

SUMMARY

A MULTILAYERED APPROACH TO PROTECT INDUSTRIAL CONTROL SYSTEMS AND SCADA NETWORKS

Securing ICS and SCADA networks is critical for ensuring manufacturing capability, service continuity and public safety. It is a complex task that can be achieved by employing planning, common sense, understanding of business requirements and people aspects—as well as employing the right technologies.

In the last 20 years, the IT world gained significant experience in protecting computer networks. Reusing some of the know-how and technologies developed over these years can save significant time and money, buy it can only be done when understanding the difference between SCADA and IT environments.

As security of organizations is comprised of many layers—it is important to have a single view of all security incidents in one place. Standardizing and unifying as much as possible security solutions can allow use of expertise already present in the organization and better overall view on the security posture.

For more details about how Check Point products, technologies, consulting, deployment and security services can help you implement an ICS security strategy, please contact us.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

CHECK POINT OFFICES Worldwide Headquarters
5 Ha'Solelim Street Tel Aviv 67897, Israel Tel: 972-3-753 4555
Fax: 972-3-624-1100
email: info@checkpoint.com

U.S. Headquarters
959 Skyway Rd., Suite 300
San Carlos, CA 94070
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
URL: http://www.checkpoint.com