Cyber Security of Process Automation

Panu Harmo, Dimitar Boyadzhiev, Arto Visala
Aalto University, School of Electrical Engineering, P.O. Box 15500, FI-00076 Aalto University, Finland
Tel: +358 50 331 6803, panu.harmo@aalto.fi, http://autsys.aalto.fi/en/Autonomous

KEY WORDS cyber security, process automation

ABSTRACT

The developed world is totally dependent on continual operation of its industries and its automated technical infrastructure. The increased use of open, networked systems in process automation have resulted in previously inexistent vulnerabilities and cyber threats that can cause wide damage not only in the process plants but to the society in large. This paper discusses the cyber threats, their technical implementations, and ways to encounter these threats. Six automation system providers and system users were interviewed about cyber security. The importance of the subject was acknowledged by all. Cyber security was more advanced in large companies. Aside from the technical implementation of cyber defences the interviewed stressed appropriate good cyber practices, training for cyber awareness, and cooperation between the stake holders. Remote maintenance, remote data acquisition, and remote operations were seen necessary in today's process automation environments. All agreed that security and integrity of remote connections must be maintained at all times.

1 INTRODUCTION

Over the years, there has been some serious misapprehension that Industrial Automation and Control Systems (IACS) networks have remained electronically isolated from other networks in a facility and therefore impossible to breach /1/. The truth is, however, that IACS networks have been increasingly adopting open, networked systems architecture due to the pressure to improve connectivity between them, the corporate networks and even the Internet. Carlson /1/ emphasises on the importance to "realise that with current networking technology there can be multiple access points to any network, including SCADA networks, and physical isolation does not guarantee network security." As a result, the potential threats of cyber-attacks from both internal and external origins are growing exponentially /2/.

2 CYBER SECURITY

The word cyber security is defined as the "state of being protected against criminal or unauthorized use of electronic data, or the measures taken to achieve this" (Oxford Dictionary). Successful cyber security involves the use of the latest technology available but this alone is not enough. In addition to this, companies must educate their employees and make them aware of the cyber risks, adopt an appropriate organizational structure and create a security strategy that matches it, as well as do regular risk assessments and undertake the correct measures. /3/ There exists a noteworthy difference between cyber security in IACS and cyber security in Information Technology (IT). The acronym CIA, for Confidentiality, Integrity and Availability is widely used to describe this type of security handling. On the contrary side, industrial control security is mainly concerned with keeping the manufacturing process running (availability) together with integrity and confidentiality where possible. Therefore, the acronym used here is AIC as shown in Figure 1.

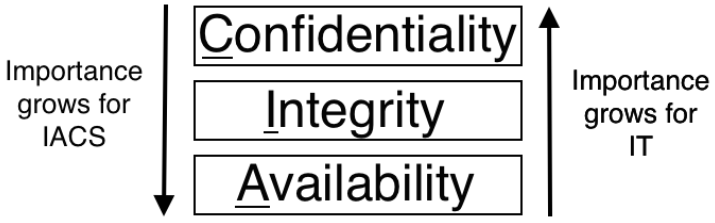

Figure 1: The difference between cyber security in IT and IACS. It is AIC for IACS.

3 CYBER THREATS

Deliberate actions that aim is to "alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" are called cyber-attacks /4/. Cyber exploitations on the other hand focus on gathering intelligence rather than being destructive activity. Cyber Security Combined Glossary Project (2007) /5/ defines the main cyber threats:

> **Virus**: "A code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data."
>
> **Worm**: "A self-contained program that can propagate itself through systems or networks. Note: Worms are often designed to use up available resources such as storage or processing time"
>
> **Trojan Horse**: "A program that appears to be useful or harmless but that contains hidden code designed to exploit or damage the system on which it is run. Trojan horse programs are most commonly delivered to users through e-mail messages that misrepresent the program's purpose and function. Also called Trojan code."
>
> **Denial of Service (DoS) Attack**: "An attempt by a malicious (or unwitting) user, process, or system to prevent legitimate users from accessing a resource (usually a network service) by exploiting a weakness or design limitation in an information system. Examples of DoS attacks include flooding network connections, filling disk storage, disabling ports, or removing power."

The **deliberate cyber-attacks**' goals differ from each other but typically they would infiltrate a computer network to steal secret information, cause a malfunction, destroy a physical part of a process, or in the very extreme cause human death. These acts can range from a denial-of-service (DoS) attack aimed at Human-Machine Interface (HMI) servers to an upload of a malicious ladder logic code onto a Programmable Logic Controller (PLC), and always require the use of cracking techniques and malicious software.

Cyber espionage, is the act of using computer networks to obtain secrets and classified information illegally, without the permission of the owners of the information and is thus an act of cyber exploitation. The penetration into the control network can occur internally or externally. Examples of internal espionage can include trained, professional spies and moles specifically infiltrated into foreign governments or a normal worker that is being paid by hackers to internally provide them with access to an industrial control network. External espionage happens without any involvement of internal personnel but rather by hackers from outside the network that find weak spots in the control network and explore them, gaining eventually access, for example using viruses, Trojan Horses or worms. /6/.

Cyber sabotage can be at a national level, where one nation may attempt to destroy parts of the critical infrastructure of other nations in order to get economic and military advantage. The Stuxnet incident is a good example of a sabotage attempt at a national level. The focus of a sabotage can also be on a single process or industry, with the motivation behind being to gain advantage over direct competitors.

Cyber terrorism is defined as the "politically motivated use of computers and information technology to cause severe disruption or widespread fear" (Oxford Dictionary).

Cyber vandalism could be thought of as the group of individual computer hackers without any real motives for damaging information infrastructures other than just personal pleasure and joy.One specific subgroup of cyber vandalism is the group of insiders (disgruntled employees, fired employees etc.), which is also the most common internal adversary.

Accidental events would typically be due to users (employees) making a mistake that enables a cyber-attack to occur. The user performed non-malicious attacks result from the lack of understanding, carelessness or the intentional bypassing of security measures to get a job done quicker. Examples could range from an employee hitting the wrong button on the keyboard that causes a crash in the control system, to plugging in an infected USB flash disk into a computer connected to the control network without knowing of it, to unintentional errors and omissions in data entries and programming. /6/.

4 CYBER SECURITY CHALLENGES

4.1 Access control

The first and very substantial step in securing industrial networks is to maintain control of the people allowed to access the system assets, such as HMIs, control networks, field devices and servers. The network access control can be broken down into physical and cyber access control: /3/ Once the physical barriers are bypassed, cyber access control would regulate which of the people that are already in the control room to be able to login to the control system. This type of access is usually in the form of usernames and passwords. Furthermore, people having the cyber access could be given a variety of authorisation and clearance levels, which would restrict the functions they are allowed to execute. /3/

4.2 Firewalls

Every firewall's underlying task is to block any unauthorised incoming connections to a protected network. It achieves this by checking whether the traffic passing through meets certain predefined security criteria and if this is not the case, it disregards this messages. Byres et al. /7/ note that firewalls have been used in the IT industry for very long time, but their effectiveness in IACS networks is still in question. The reason is because the firewalls used in IT are typically not familiar with the process control protocols, may violate the time-critical criteria by impermissibly high latencies and be unable to handle operational constraints unknown to the IT world. /7/

4.3 Communication Protocols

In an interview /8/, Eric Byres highlights the importance of security in protocols by stating that whenever Stuxnet encountered a firewall, it managed to get past it by riding on top of protocols allowed through the firewall. In that way, Stuxnet managed remain undetected and not set off any alarms. Brändle and Naedele /9/ emphasise that security measures, such as encryption, message integrity protection, authentication and authorisation, are not intrinsic to most of the communication protocols used in IACSs. Thus, one way of improving the overall cyber security of IACSs is to refine the security features in the communication protocols. Protocol vulnerabilities can be typically divided into two main groups: the group of improperly implemented protocols and the group in which vulnerabilities arise from specification of the protocol /10/.

4.4 Operating Systems

Initially, industrial automation and control systems used to run on DOS, VMS and UNIX-based operations systems /11/. Microsoft Windows and Linux have been increasingly becoming the more popular choice in recent years with new versions of Windows released every few years. The first step of most cyber-attacks is to breach into the operating system itself, as was the case with Stuxnet worm. Therefore, decreasing the number of vulnerabilities in OSs will have a direct impact on the cyber security of IACSs. One way to decrease the vulnerability level of OSs is through a method called system hardening. This method manages to reduce risks by removing all software applications and processes that are not related to the primary function of the computer, thus closing "back-door" access to the computer system that some applications enable. /12/

4.5 Security Management and Updates

In addition to the efficient use of properly chosen security technologies, good security management is vital for greater cyber security. In comparison to traditional IT systems, Krutz /6/ highlights that software patches in IACSs are done deliberately far less frequently. The process sometimes requires the involvement of vendors and the need for off-line testing of the patches to ensure their harmfulness to the plant. These lead to the process being far more time-consuming in IACSs. Johnson /7/ notes that the reason for the rarely patched IACSs is hugely due to the concern of automation engineers that the patch itself might have negative effects on the operation of the system. Managers must note that common security policies for all firms cannot be developed due to the difference of companies' goals and requirements. A good implementation of a cyber secure control network at the start of a facility is crucial but it can quickly become insecure with new technologies being invented and new vulnerabilities found in already existing technology. Thus, IACS networks must be constantly tested for vulnerabilities in security, as well as the existing software and hardware must be regularly updated and maintained. /13/

5 RISK REDUCTION

Once the risks and vulnerabilities in IACS networks are identified and evaluated, the next stage is to reduce them or even eliminate them entirely wherever feasible.
Intrusion Detection (ID) is a "security service that monitors and analyses system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner" /14/. Network-based IDSs inspect network events, including traffic volume, IP addresses and protocol usage. IDS can be attached to monitor a network through a independent hardware based "network packet sniffer" or the IDS can be integrated into the source code of a firewall, router or another standalone device. Network-based IDSs can search for known attack signatures by comparing them to an up-to-date database of recognised attacks (e.g. worms), or for anomalies in the network traffic, which are any statistically suspicious variations in the traffic patterns. /3/ **Intrusion prevention** differs from normal IDSs is that it can also automatically execute a prearranged action at the sign of intrusion, such as blocking all incoming traffic from the Internet.

Virus detection and elimination can be deployed at three levels within an industrial network. /3/ The first one is at the perimeter of the network, for example it could be built into the firewall. The second level is at the control server level and the third one is at individual workstations, such as antivirus software installed on a HMI console. The first two levels are oriented to prevent viruses entering from outside the control network, whilst the last one is for preventing viruses infecting from within the control network, such as an employee inserting flash drives or CDs containing a virus into a workstation within the control network.

Cyber security awareness and training are frequently conducted in typical IT industries, but the case is completely the contrary in automation control networks. /6/ The goal of cyber security awareness and training is to provide all employees with a clear, general overview of the cyber security vulnerabilities and threats faced by the control network, the security measures that all workers have to keep in mind and the possible consequences, if they are not followed closely. Companies can have a general security training program meant for all workers but it is also possible to create different programs for each worker individually based on his daily activities within the control network. /3/ Tumid /3/ suggests that IACSs should use **periodical audits** to assure the proper set-up, configuration and operation of cyber security. It includes also **physical security** measures, such as guards, intrusion alarms, windows, fences, locks and pass keys that are used to prevent an unauthorised entry by both intruders and insiders. **Personnel security** is another important component that can contribute to the overall cyber security of an IACS.

6 INTERVIEWS

Interviews concerning cyber security of process automation systems were carried out with six companies and organizations. There were two large and one small company using process automation, and two were large and one small company providing process automation. The automation systems in focus were both DCS and SCADA systems. The in depth discussions lasted up to two hours each. Same questions were asked from all participants, but often the discussions led to other topics of interest, as well. An overview of the results and contents of the interview is presented below. Everyone agreed that, if the **electricity** network is down, most processes would shut down. Even in the case where there is reserve power that would in most cases only last a certain time or only parts of the processes could be kept up and running.

Availability of the automation was the main concern for both the system providers and the users. Loss of control means loss of safety and loss of production. The seriousness of the incidents depends on the processes. If a large process must be driven down, the financial losses can be substantial. SCADA systems are often designed so that even when the operator interface or the communications to the remote stations are lost, the system can operate safely some time. Loss of **confidentiality,** that is theft of information, is more related to office systems, where business data, production plans, and product information etc. are stored. In some cases confidential data can be found in the automation systems as well.

Internal threats were considered more common that **external threats**. Internal threats are in most cases due to lack of understanding, less often due to carelessness or neglect. Using unchecked USB memory sticks, installing programs that can contain malware, connecting unsafe laptop computers to automation networks, written passwords on computers, and using unsafe computers to connect remotely to automation networks, can be sources of cyber threats, but according to the respondent these bad practices are not common any more. A new possible threat comes from the so called BYOD's (Bring Your Own Device), that is personal smart phones and tables that are used both at home and at work. Intentional internal threats by personnel can be serious, because usually only

knowledgeable people can harm the process seriously. However, this threat was seen most unlikely by all respondents.

Remote connections were seen as possible external threats. Remote maintenance of automation systems is often carried out by remote service crews and automation system providers, who can debug, fix and update the systems through the remote connection. This is often done through the Internet. If proper procedures for these connections are not performed, they can be a security risk. SCADA systems use various different communication channels; company internal field networks, GSM-networks, proprietary radio networks and the Internet. They are a risk, if not properly shielded. All interviewed, except in one case, said that their systems had some type of connections from the outside world to their automation system. The remote connection usually go through the company office network whose security, firewalls etc. are administered by the IT department.

Windows operating systems were used in all automation systems. The complexity of the operating systems, the available knowledge of its vulnerabilities, and the various malware and cyber-attack tools require that the Windows computers are carefully protected. Window PC is in practice the door to automation systems, where hackers can get in and where damage can be done. Windows computers in automation are always hardened by removing and uninstalling all unnecessary Windows services, which could provide back doors to attackers. Even when they are a possible vulnerability they are hard to replace. How could one make sure that the new replacement system would be any safer?"

Software updates, especially Windows operating system updating is a source of possible incompatibilities between various automation programs. These can cause some features of the automation systems to malfunction or stop working all together. Here the company IT department policies and the automation department policies often conflict. Due to the stringent requirement of automation system availability the system cannot be run down many time of the year for system updates. Some processes have scheduled shut-downs once a year, but Windows security patches come much more often. One company advised their customers not to update the Windows at all. Others had less frequent Windows update schedule, which was performed after they had tested the compatibility of the update with their system.

Small companies and large companies have obviously different resources to implement cyber security. Both of the smaller companies said that they did not have a cyber security strategy. But that did not mean that their practices were unsafe, but obviously without a strategy the development of cyber defence is more difficult. Smaller companies wanted practical training that combines IT and automation. The large interviewed companies had various levels of cyber security strategies in use or in final phases of implementation. They also had much knowledge about different cyber security standards and practices and they cooperated nationally and internationally actively with officials, organisations and companies.

Cyber security strategy describes a continuous process that spans the whole life cycle of the system, from the initial plans and designs to the destruction and recycling of the equipment. There are various guides, best practice documents and even industry specific rules how to make and keep a process and its automation safe. Some guidance can be gotten for IT system security guides as well. The automation system providers said that they have their own documents how their customers can keep the automations system secure. In the end, however, the users are responsible for cyber security and they must create their own strategies and educate their personnel in a way that fits their companies. One of the interviewed put it in a nut shell. Make your guidelines easy to understand and simple to use. It was also noted that cyber security has a price tag meaning that too many restrictions, protocols and equipment may affect the effectivity of the day to day operations of the plant. The following documents and sources came up in the discussions about where to find material for building company cyber security practices and strategies.

- ISA99/IEC62443
- Cyber Security Procurement Language for Control Systems by ICS-CERT
- HUOVI-portal, advice to cyber security issues for critical infrastructures
- CERT-FI, Finnish Communications Regulatory Authority
- The North American Electric Reliability Corporation (NERC)
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security

Technical solutions to cyber security depend on firewalls, demilitarized zones, intrusion detection and protection systems, multiple levels of cyber defences, virtualised, hardened PCs, and VPN connections, virus detection and elimination software. These must be regularly updated and tested according to company cyber strategies. However, new possibilities and threats emerge constantly: industrial internet, wireless sensor networks, cloud computing and cloud services, and virtualised PC-computers to name a few.

7 CONCLUSIONS

Cyber security is essential part of company security. At the same time it has an important role in ensuring the safety and functionality of whole societies. Process automation differs from office IT systems in that it emphasises availability, real time responses and physical safety issues, which must be understood when implementing cyber security issues for process automation. Cyber security is a process that must be incorporated into the lifecycle of an industrial automation and control system. Because the cyber scene is changing constantly, companies must develop their practices and train their personnel. Formal automation system cyber security procedures and strategies are already used in larger companies but lack in many smaller companies.

8 REFERENCES

/1/ Carlson, Rolf. 2002. “Sandia SCADA Program High-Security SCADA LDRD Final Report.” Sandia National Laboratories.

/2/ Culling, Thomas. 2006. Control System Cyber Security Risk Assessment, Isa Expo 2006. ISA Transactions.

/3/ Tumid, David. 2010. Industrial Network Security. 2nd ed. United States of America: The International Society of Automation (ISA).

/4/ Straf, Miron, Margaret Martin and Constance Citro. 2009. Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities. National Academies Press.

/5/ Cyber Security Combined Glossary Project. 2007. Technical report PCSF Congress of Chairs.

/6/ Krutz, Ronald. 2013. Industrial Automation and Control System Security Principles. United States of America: The Internattional Society of Automation (ISA).

/7/ Byres, Eric, John Karsch and Joel Carter. 2005. “NISCC good practice guide on fire- wall deplo

/7/ Johnson, Robert. 2010. Survey of SCADA security challenges and potential attack vectors. In International Conference for Internet Technology and Secured Transactions (ICITST). IEEE pp. 1–5.

/8/ Lydon, Bill. 2011. “Cyber Security Threats: Expert Interview with Eric Byres, Part 1.” Personal Interview.

/9/ Brändle, M. and Martin Naedele. 2008. “Security for process control systems: An overview.” Security & Privacy, IEEE, 6(6):24–29.

/10/ Franz, Marcel. 2004. Protocol implementation testing: challenges and opportunities. Technical report National Infrastructure Security Co-ordination Center (NISCC) workshop.

/11/ Sung-Hwan, Kim, Eom Jung-Ho and Chung Tai-Myoung. 2012. “A study on optimization of security function for reducing vulnerabilities in SCADA.” Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, pp. 65–69.

/12/ System Hardening. N.d., URL: http://www.techterms.com/defidening

/13/ Igure, Vinay, Sean Laughter and Ronald Williams. 2006. “Security issues in SCADA networks.” Computers & Security, 2(7):498–506.

/14/ ANSI/ISA-99.00.01. 2007. “Security for Industrial Automation and Control Systems, Part 1: Terminology, Concepts and Models.”