(No) Security in Automation!?

Dr. S. Lüders[1)]

[1)] CERN, Geneva, Switzerland

Abstract

Modern Information Technologies like Ethernet, TCP/IP, web server or FTP are nowadays increasingly used in distributed control and automation systems. Thus, information from the factory floor is now directly available at the management level (“From Shop-Floor to Top-Floor”) and can be manipulated from there. Despite the benefits coming with this (r)evolution, new vulnerabilities are inherited, too: worms and viruses spread within seconds via Ethernet and attackers are becoming interested in control systems. Unfortunately, control systems lack the standard security features that usual office PCs have.

This contribution will elaborate on these problems, discuss the vulnerabilities of modern control systems and present international initiatives for mitigation.

CERN-OPEN-2008-014
30/06/2008

Kurzfassung

Moderne Prozeßsteuerungs- und Automatisierungssysteme übernehmen heutzutage gängige IT-Techniken wie Ethernet, TCP/IP, Webserver oder FTP. Während dies eine direkte Kommunikation mit übergeordneten Managementsystemen erlaubt, erhalten nun aber auch Viren, Würmer und Angreifer Zugang zur Kontrollebene. Im Gegensatz zu üblichen Büro-PCs mangelt es vielen Automatisierungssystemen leider jedoch an etwaigen Schutzmechanismen.

Dieser Beitrag geht auf diese Problematik ein, diskutiert die Verwundbarkeit moderner Kontrollsysteme und präsentiert internationale Ansätze zur Verbesserung der Situation.

1 Control Systems Inherit Information Technologies

The enormous growth of the worldwide interconnectivity of computing devices (the “Internet”) and the “industrialization” of common IT-technologies during the last decade has given automation systems new means to share and distribute information and data. Following this (r)evolution, the corresponding IT-protocols (e.g. TCP/IP, SNMP, SMTP, FTP or HTTP), methods (e.g. VPN, wireless access), standards (e.g. USB, Unix/Linux, Microsoft Windows, OPC), and devices (e.g. notebooks,

web-cameras, voice-over-IP telephones) have been integrated into control systems. In industry, this has resulted in an adoption of modern Information Technologies (IT) to their plants and, subsequently, in an increasing integration of the production facilities, i.e. their process control and automation systems[1], and the data warehouses. Thus, information from the factory floor is now directly available at the management level ("From Shop-Floor to Top-Floor") and can be manipulated from there.

1.1 The Risk: The Critical Infrastructure

However, with a 100% vertical integration of production and management networks the risk of a cyber-security related incident inside the control system also increases. This risk is usually proportional to the probability of occurrence and the final consequential costs. With respect to cyber-security, the probability depends on the frequency and severity of the threats as well as the number and extent of the vulnerabilities. Thus, one can express the risk as: *risk = threats × vulnerabilities × consequences.*

1.1.1 The Threat: Viruses, Worms, Attacker & Co.

This interconnected world based on a common (IT-) technology at the level of control systems is, however, by far more hostile than a local private controls network using proprietary technologies[2]. The number of potential threats increases as worms and viruses can now easily propagate into control systems. Furthermore, attackers are starting to become interested in control systems too. It is a fact that the corresponding attack procedures were already presented on the usual "Black-Hat"-conferences. In addition, competitors might resort to such illegal practices, not to speak of terrorists.

Additional threats can be operators or engineers, who unconsciously download configuration data to the wrong device, or broken controls devices, which flood the controls network with data packets and, thus, bring all communication to a halt.

Unfortunately, the major part of the factor "threat" originates from outside and cannot be significantly reduced. Thus, protective measures have to be implemented to prevent external threats

[1] Commonly denoted in the following as "control systems", where a "system expert" has the expertise in its configuration.

[2] For example, PROFIBUS and Modbus are more and more replaced by PROFINET and Modbus/TCP, respectively.

penetrating control systems. These protective measures should also prevent insiders from (deliberate or accidental) unauthorized access.

1.1.2 Vulnerabilities: Failing Automation Devices

The adoption of standard modern IT in control systems also exposes their inherent vulnerabilities to the world. Programmable Logic Controllers (PLCs) and other controls devices (even valves or temperature sensors) are nowadays directly connected to Ethernet, and come with integrated web-servers and emailing functionality. Security measures, on the other hand, are often completely lacking.

In order to get an overview of the cyber-security of their installed control systems, CERN launched the “Teststand On Control System Security” (TOCSSiC) project. More than thirty different devices (PLCs and power supplies) from seven different manufacturers have been tested [1]. Including different firmware versions, 53 tests were made in total. The results revealed serious security problems. After a “Denial-of-Service“ attack using the freely available program package “Netwox“[3], only 75% of the PLCs were able to respond properly to an ICMP “ping“ request, while the other 25% did not respond anymore and needed to be restarted by power-cycling the device. A full Nessus[4] scan was successfully completed on 68% of the PLCs. Only a few minor security problems were found, which are also frequently present on up-to-date and properly patched office PCs. In 17% of the Nessus tests, the device crashed during the scan. In the remaining 15%, Nessus reported significant security holes like e.g. the unprotected access via FTP or HTTP. However, the results often improved after testing the same PLC with more recent firmware versions. Unfortunately, an update to a more recent firmware version is not always possible on production systems.

Additionally, some tests were conducted with a set of PLCs configured for, and run in, production mode (i.e. continuously exchanging data). The results have shown that under these circumstances the loss of communication is much more likely. Similar results have been presented by the U.S. Sandia National Laboratories [2].

On the user interface side, operator consoles and Supervisory Control And Data Acquisition (SCADA) systems are now based on the Microsoft Windows platform or are ported to a standard Linux installation. Both are dedicated for office or server applications, but not adapted to the requirements of control systems. For example, controls PCs cannot be patched and updated as fast

[3] “Netwox” offers a selection of tools for the verification of the network security.

[4] The “Nessus” program performs about 10000 different penetration tests and vulnerability scans. It is quite frequently used within IT to assess the cyber-security of web servers and alike.

as office PCs. The corresponding interventions need to be planned with care. Furthermore, some patches might not be compliant with existing software, might interfere with the control processes, or render existing licenses invalid. Finally, in the meanwhile notebooks, emails and web-servers have become integral part of a control system — including all their inherent risks.

In addition, there are operators and system experts, who do not necessarily assign highest priority to cyber-security or ignore cyber-security to a large part. Passwords are freely communicated to third parties, written on a sticker and fixed directly onto a terminal or not configured at all. Infected notebooks are carried on site and connected to the controls network. Personnel open infected emails or download malicious code. People are also susceptible to „Social Engineering“, i.e. the direct — but stealthy — spying of security-relevant information like passwords.

The “vulnerability” factor can be reduced by immediately fixing known and published security holes. Additional measures should be able to protect unknown or potential areas of lower security.

1.1.3 The Consequences: No Light!

The consequences from suffering a security incident are inherent to the design of the control system, the control processes and its area of deployment. Consequences cover the loss of control or safety, reduction or loss of production, damage or destruction of equipment, injuries or even deaths, and bad publicity and loss of customer confidence.

A series of documented incidents can be found in [3]. One spectacular incident was the destruction of a power generator during a cyber-attack exercise of the U.S. Idaho National Laboratories [4].

2 Towards Cyber-Security

Driven by the fear of further terrorist attacks after September 11th 2001, the U.S. authorities, in particular the Department of Homeland Security (DHS), have begun to analyse, minimize, and even prevent the consequences of cyber-attacks to their national critical infrastructure (e.g. the national power grids, water distribution & sewage, oil and gas production, chemical plants). European countries have been following with a delay of a couple of years.

The growing demand for “Critical Infrastructure Protection” (CIP) and “Critical Information Infrastructure Protection” (CIIP) has led to a consolidation in the area of control system cyber-security. A significant series of new initiatives, standards, guidelines and laws have been started or produced. These will be discussed in more detail in the following sections.

2.1 (Too many?) Standards and Guidelines

Sponsored by the DHS, many private or commercial organizations in the U.S. (e.g. CIDX, ISPE, NERC) have begun to develop and publish a large number of guidelines or standards. It is questionable, whether this cacophony is justified, or whether a smaller set of detailed and complete in-depth documents would be sufficient.

A wide-ranging set of guidelines has been produced by the British CPNI (”Centre for the Protection of the National Infrastructure“) [5]. These guidelines cover the basic aspects of cyber-security and provide initial mitigation strategies. The SP99 series of the U.S. Instrumentation, Systems, and Automation Society (ISA) is more detailed and covers the whole production cycle starting with the project definition, the control system commissioning and deployment, and its operation [6]. The U.S. National Institute for Standards and Technology (NIST) also produced wide-ranging guidelines (SP800-53, -53A, and -82) [7]. These are in direct competition with the “CIP” Standards (NERC CIP-002 to -009) [8] of the U.S. Federal Energy Regulatory Commission (FERC), which just recently became mandatory. Finally, also the International Standardization Organization (ISO) has begun to extend its guidelines on management of information security (ISO 27001 et sqq.) [9].

2.2 “Defence-In-Depth”

Following the CPNI or ISA SP99 guidelines, a common and general approach is that of “Defence-In-Depth“, which suggests the application of cyber-security protection on *each* layer of the control system:

- the security of the device itself, including its firmware and its operating system,
- the security of the network, its protocols and remote access,
- the security of software applications, including the software of third parties,
- the security of user accounts and the accounts for remote access as well as their access rights.

Such a “Defence-In-Depth” approach must jointly be implemented by the operators, system experts, developers, users, manufacturers and system integrators. Focusing on single aspects corresponding to an “M&M“-principle (“hard on the outside, soft in the inside“) has to be avoided: protective measures following “Network security that’s it!”, “Firewall protection is sufficient”, “…we’re deploying only Linux” or “Our control systems and network protocols are proprietary” shall be put in the realm of myths. It is the general approach of “Defence-In-Depth”, which ensures that vulner-

abilities are protected by multiple means. These additional layers offer the flexibility not necessarily needing to act immediately to (new) security risks — which does not mean ignoring them.

With the adaptation of the “interesting” IT-technologies (like TPC/IP, HTTP, Microsoft Windows, USB) to the level of control systems, also the corresponding security technologies have to be inherited:

The network has to be segmented into smaller and separately protected network cells. All incoming and outgoing traffic must be filtered (e.g. using professionally configured firewalls) such that only authorized traffic can pass. A direct connection to the Internet must be avoided by all means. Remote access from outside must be carefully controlled (e.g. using “Application Gateways“). Sensitive devices like PLCs have to be protected separately, or have to be replaced by security-tested and certified devices. “Intrusion Detection Systems” (IDS) might be advantageous to detect the usual viruses and worms, but are currently only capable of analyzing a small fraction of controls-specific network traffic. In particular because of this, “Intrusion Prevention Systems” (IPS) have to be deployed with care, since misidentified network traffic can lead in rare cases to production stoppage.

Operating systems of control PCs should be patched regularly, regardless whether the operating system is based on Microsoft’s Windows or on Unix/Linux. The control systems itself must be laid-out such that a restart of a control PC does not affect the overall availability and functionality. This is also advisable with respect to the short life-cycles of PCs. Dedicated test procedures have to validate the compliancy of this patch with the existing controls applications, before the patch is widely deployed. In the long-term, also the development, deployment, and operation of (more complex) controls applications might benefit from established IT-technologies. Here methodologies for software management exist since years, and today’s controls applications should be able to easily adapt to this, too.

Sufficiently separated rights must handle restrictively the access to the operating system and to the controls application. Only those users should be authorized, who have a professional need for access. The access rights have to be adapted accordingly (e.g. operators must be allowed to make general settings; system experts need access to more specialized settings; guest access must be restricted to “read-only”— if at all). Hidden accounts (e.g. installed by third party software) must be identified and disabled. All access must be logged. Modern IT-technologies like magnetic strip readers or RFIDs allow the inconvenient and multiple keying of passwords to be avoided. Access rights for remote maintenance especially that of third parties, must be handled even more restric-

tively. In parallel to these software-based access protection, sufficient physical access protection must be deployed.

On the human side, one finds the operators, the system experts, and the developers, who have an in-depth knowledge of their control system, but might lack deep IT-knowledge. Vice versa, it is not granted that an IT department is sufficiently trained to handle control system specific aspects. Therefore, dedicated seminars and training sessions on the cyber-security of control systems have to raise the awareness of the control system experts *and* the IT-experts. A tight collaboration of both sides avoids future misunderstandings and increases mutual trust.

With respect to security, improving security and addressing new security issues as they arise is the goal. Therefore, the overall cycle of “planning”, “implementing”, “checking”, “acting” must be integrated on the management level. This has to be preceded by a written security policy, the documentation of the Status Quo, as well as a risk assessment, in order to be able to focus on the real security issues, and to avoid the deployment of expensive and useless security protections. Regular, independent, and unrestricted audits by external, specialized companies, which compare the reality (the Status Quo) with the security policy, are recommended.

3 International Risk — International Collaboration

The aforementioned factors of the risk-equation are global: viruses, worms, and attacker do not stop at the border; control devices are sold world-wide — including their security holes — and also the consequences are international, as several power outages in the U.S. and in Europe have shown. Furthermore, there are no reasons to believe that mitigations and solutions concern one nation alone. User and manufacturer act globally, products are sold globally. And this should also apply for solutions and standards.

3.1 Information Exchange of Users and Authorities

In Europe, British, Dutch, German, Norwegian, Suisse, and Swedish users and governmental bodies have joined together in an information exchange group, the EuroSCSIE (European SCADA and Control System Information Exchange). Partially, these members already represent national information exchange groups with additional members. Non-disclosure agreements allow exchanging confidential information on threats and security holes, (successful) security-attacks, as well as discussing mitigations and solutions.

On the commercial side the ISA Compliance Institute offers an in-depth collaboration between users, manufactures and other parties. The focus in the coming years will be security testing and certification of devices and the development of new standards.

The risk is global — so are the solutions and collaborations.

3.2 Involvement of Manufacturers and Suppliers

Manufacturers, suppliers, and system integrators are part of the solution. Unfortunately, there is a lack of for demand them to take control system cyber-security seriously. CERN has discussed the results of its “TOCSSiC” tests with the corresponding manufacturers, and explained its view of the situation. However, their response was rather discouraging: “There is no market demand for having security in PLCs!“.

Therefore, the EuroSCSIE has begun to address the problem of the lack of security to European manufacturers. In particular the long list of members from users and governments should provide the manufacturers with a good reason to start acting. Furthermore, an international collaboration lead by the U.S. Idaho National Laboratory has produced the “Cyber Security Procurement Language for Control Systems” [10]. This document allows users to formulate dedicated requirements on cyber-security, and to demand these from the manufacturers.

3.3 Certification: A Basic Level of Cyber-Security

Being proactive, manufacturers have the chance to act, too. However, it is not sufficient to refer to obscure — often internal — results of penetration and robustness tests. CERNs published procedures for the “TOCSSiC” tests [11] provide a first means in order to reach a basic level of cyber-security. Other third parties like the ISA Security Compliance Institute, the U.S. Idaho und Sandia National Laboratories, Wurldtech or Digital Bond already offer the certification of devices, if these devices withstand their test methods.

With this, a first step towards secure control systems would have been done by the manufacturers, even if such a certificate has a limited validity since it cannot provide any security guarantees for the future. Also, this should not motivate users to reject further security protections according to the “Defence-In-Depth” approach. Security measures must be deployed on *every* level of the control system.

4 Summary

Modern Information Technologies like Ethernet, TCP/IP, web server or FTP are nowadays increasingly used in distributed control and automation systems. While this offers a direct communication channel with higher-level management systems, also viruses, worms, and attacker can now gain the possibility of accessing the controls system. However, contrary to office PCs, control systems usually lack the standard protective measures…

In order to address this problem, leading organizations in the field of control system cyber-security recommend inheriting also the corresponding IT-technologies for their protection. A useful approach is based on a „Defence-In-Depth“, which protects vulnerabilities on several layers and with different means: on the network layer, on the layer of the control PC, on the software layer, and in the area of access control. Of course, this is a collaborative effort between operators, system experts, developers, users, manufacturers, and system integrators.

External international forums like the EuroSCSIE or the ISA Compliance Institute provide the forum for an information exchange between users, agencies, and manufacturers. Non-disclosure agreements allow for the exchange of confidential information on threats and security holes, (successful) security-attacks, as well as discussing mitigations and solutions. Requirement catalogues offer the user the means to demand more secure products and certificates allow manufacturers to prove the cyber-security of their products.

Nevertheless: “Security” is an iterative process. Continually improving security and addressing new security issues as they arise is the goal; ultimate security will remain utopia.

5 References

[1] S. Lüders, “Control Systems Under Attack?”, 2005, CERN EDMS 867444

[2] Sandia National Laboratories, “Penetration Testing of Industrial Control Systems”, 2005, SAND2005-2846P

[3] The Register, 2000, http://www.theregister.co.uk/2000/04/27russia_welcomes_hack_attacks; Computer Crime Research Centre, 2005, http://www.crime-research.org/analytics/1718; Security Focus, 2005, http://www.securityfocus.com/news/6767; eWeek.com, 2005, http://www.eweek.com/article2/0,1759,1849914,00.asp; Security Focus, 2006, http://www.securityfocus.com/news/11465; CSO online, 2007, http://www2.csoonline.com/exclusives/column.html?CID=32893

[4] CNN online, 2007, http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html

[5] Centre for the Protection of the National Infrastructure (CPNI), “Good Practice Guidelines Parts 1-7”, 2006, http://www.cpni.gov.uk/Products/guidelines.aspx

[6] ISA, “Scope, Concepts, Models and Terminology”, 2007, ISA 99.00.01; ISA, “Establishing a Manufacturing and Control Systems Security Program”, 2007, ISA 99.00.02; ISA, “Operating a Manufacturing and Control Systems Security Program”, 2007, ISA 99.00.03; ISA, “Specific Security Requirements for Manufacturing and Control Systems”, 2007, ISA 99.00.04, http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

[7] NIST, “Recommended Security Controls for Federal Information Systems“, 2007, NIST SP800-53; “Guide for Assessing the Security Controls in Federal Information Systems”, 2007, NIST SP800-53A Draft; “Guide to Industrial Control Systems (ICS) Security”, 2007, NIST SP800-82 Draft, http://csrc.nist.gov/publications/PubsSPs.html

[8] FERC / NERC, “Cyber Security Standards”, 2008, CIP-002 bis 009, http://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp
http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection

[9] ISO, “Information Technology — Security Techniques — Specification for an Information Security Management System”, ISO 27001 et sqq., http://www.iso27001security.com/html/iso27000.html

[10] Idaho National Labs, “Cyber Security Procurement Language for Control Systems”, 2007, http://www.msisac.org/scada

[11] S. Lüders, “The TOCSSiC Procedures”, 2007, CERN EDMS 573062