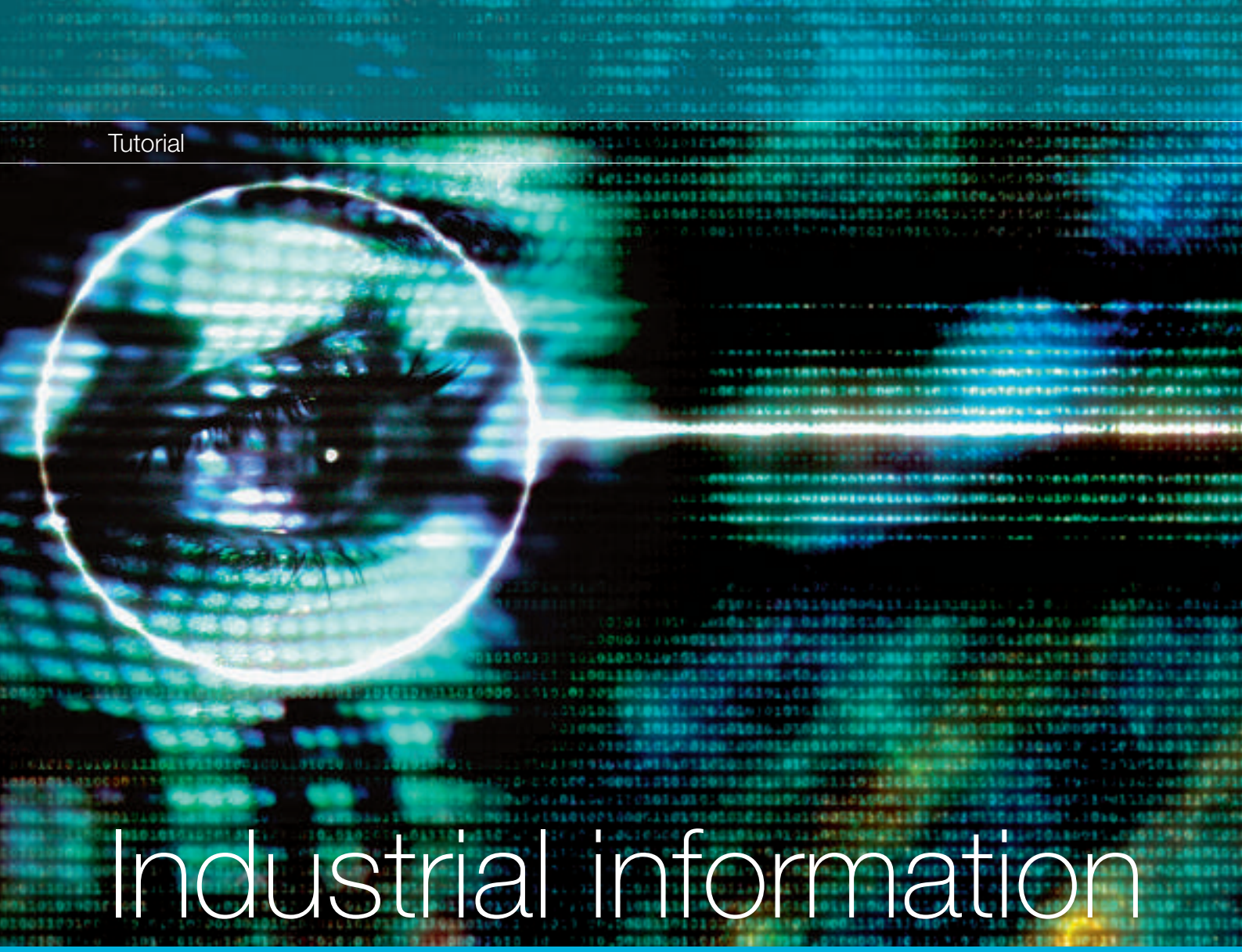


Industrial information system security Part 1

IT security in industrial plants - an introduction

Martin Naedele, Dacfey Dzung

The topic of IT security is becoming increasingly relevant in modern automated industrial plants. Modern automation systems provide high levels of inter-connectivity. Implementations are based on commercial IT platforms, many of which are known to be vulnerable to electronic attacks. This article is part 1 of a three part tutorial on IT security for industrial systems.

Security objectives are explained, attack types are illustrated, and available and suggested countermeasures and general good practices are briefly described. Part 2 of this series will address best practices in protecting against certain types of attacks, and Part 3 will survey emerging standards for automation system security.

In the past, industrial automation systems were not linked to each other and were not connected to public networks like the Internet. Today, the situation is somewhat different: because the market puts pressure on companies to make fast and cost efficient decisions, accurate and up-to-date information about the plant and the process status must be available not only on the plant floor, but also at the management level and even for supply chain partners [1]. This results in greater inter-connectivity between different automation systems and between automation and office systems. Modern industrial automation systems are, to a large extent, based on commercial operating systems, protocol implementations, and communication applications originally developed for the office IT environment. Many of these systems and implementations are known to be vulnerable to attacks, and with open and standardized Internet-technologies, expertise and knowledge of such vulnerabilities is easily available to potential attackers. By connecting industrial plants to the Internet or to other public networks these vulnerabilities are exposed. Thus, IT security issues must also be addressed in industrial automation systems.

What is IT security?

For many people, IT security is considered a synonym for encryption and for others, the foremost IT security issue concerns protection against computer viruses. In reality however, IT security has a much wider scope. The following eight *security objectives* are a suitable framework for structuring security requirements and properties of a system:

Confidentiality: The confidentiality objective deals with preventing the disclosure of information to unauthorized persons or systems. For automation systems, this is relevant both with respect to process specific information, such as product recipes or plant performance and planning data, and to the secrets specific to the security mechanisms themselves, such as passwords and encryption keys.

Integrity: The integrity objective deals with ensuring that modifications made by unauthorized persons or systems to specific information are detected. For automation systems, this applies to information such as product recipes, sensor values or control commands. Violation of integrity may cause safety issues, ie, equipment, the environment, or even people may be harmed.

Modern industrial automation systems are, to a large extent, based on commercial operating systems, protocol implementations, and communication applications originally developed for the office IT environment.

Availability: Availability means ensuring unauthorized persons or systems cannot deny access/use to authorized users. For automation systems, this refers to all elements of the plant like: control systems; safety systems; operator workstations; engineering workstations; manufacturing execution systems; and the communication systems between these elements and to the outside world. Violation of availability, also known as denial-of-service (DoS), may not only cause economic damages but also safety issues as operators may lose the ability to monitor and control the process.

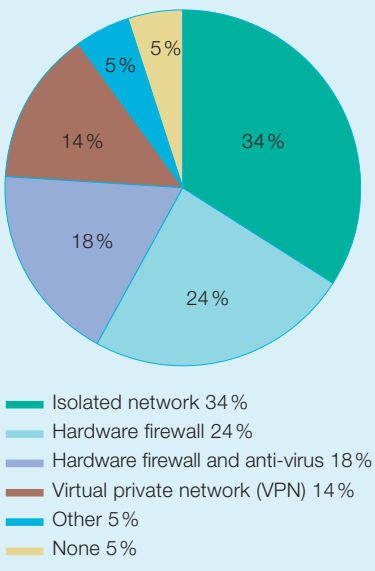
Authentication: Authentication is concerned with determining the true identity of a system user and mapping this identity to a system-internal principal (eg, valid user account) under which this user is known to the system. Most other security objectives, most notably authorization, distinguish between legitimate and illegitimate users based on authentication.

Authorization: The authorization objective – also known as access control – is concerned with preventing people (or systems) who do not have permission from accessing the system. In the wider sense, authorization refers to the mechanism that distinguishes between legitimate and illegitimate users for all other security objectives, eg, confidentiality, integrity, etc. In the narrower sense of access control, it refers to restricting the ability to issue different types of commands to the plant control system. Violation of authorization may create safety issues.

Auditability: Auditability is concerned with being able to reconstruct the complete system behavior history from records of all (relevant) actions executed on it. This security objective is mostly concerned with discovering and finding reasons for malfunctions in the system and to establish the scope of the malfunction or the consequences a security incident. Note that auditability without authentication may serve diagnostic purposes, but does not provide accountability.

Non-repudiability: The non-repudiability objective means being able to provide irrefutable proof to a third-party of who initiated a certain action in the system, even if this actor is not cooperating. This security objective is relevant in establishing accountability and liability. In the context of automation systems, this is most important with regard to regulatory requirements, eg, US Food and Drug Administration (FDA) approval. Violation of this security objective may have legal

1 Security mechanisms used between control system and external networks as reported in [3]. Note that 5 % of systems are not secured in any war.



and commercial consequences, but no safety implications.

Third party protection: A successfully attacked and subverted automation system could be used for various attacks on the IT systems, data or users of external third parties using, for example, distributed denial-of-service (DDoS) or worm attacks. The third party protection objective deals with preventing this type of damage from occurring.

The importance of each security objective depends on the system, specifically its purpose and its assets. In automation systems, for example, confidentiality is important for production and performance data, while integrity and authorization is most relevant for operator commands, parameters, and control functions. For each system and installation, a *security policy*, stating the security objectives and specific system constraints must be in place before the security architecture for any system can be designed.

At this point it may be worth pointing out the difference between the concepts of *security* and *safety* as applied to an automation system or plant. Although no undisputed definitions for these terms exist, they tend to be used in the following way: security is concerned with the prevention of intentional malicious attacks whereas safety is concerned with the prevention of damage caused by a predominantly unintentional or random loss of integrity and availability of plant components, or by user error.

What types of attacks are there?

An *attack* is a violation of one or more security objectives and can be initiated either inside or outside the plant. Attacks may target a specific system or type of system, or they may, for example, in the form of viruses and worms simply victimize any vunerable system they encounter.

For each system and installation, a security policy, stating the security objectives and specific system constraints must be in place before the security architecture for any system can be designed.

A computer may be attacked for example to: obtain specific data stored on the computer (eg, production data); to abuse the processing or storage resources of this computer (eg, to store and distribute pirated software); to use applications installed on the computer to manipulate data or other systems (eg, a production plant controlled by the computer); or to prevent usage of this computer for its intended purpose.

A data transmission link is another possible target and may be attacked: to eavesdrop on transmitted information; to falsify the information sent to the recipient of the transmission; or to prevent the legitimate use of the transmission link by, for example, flooding it with messages.

Do such attacks really happen?

January 1998: External attackers took over the central control center for the Gazprom pipeline system. For an unknown period of time they were able to control the flow in the whole Gazprom pipeline network[1)].

March 2000: A disgruntled former contractor gained access to the control system of a sewage treatment plant in Maroochy Shire in Queensland/Australia. He flooded the surrounding environment with millions of litres of untreated sewage[2)].

December 2000: Attackers compromised the computer network of an unnamed power utility in the US via an unsecured data exchange protocol. They used the compromised hosts to play networked computer games. Their usage of computing resources and network bandwidth severely impedeed the utility's electricity trading[3)].

January 2003: The safety monitoring system of the Davis-Besse nuclear power plant in the US was infected with the "Slammer" worm. The worm bypassed the plant's firewalls via a contractor's laptop - which was connected to the power plant network at the same time - and via a modem to the infected enterprise network of the contractor company[4)].

August 2003: At CSX Transportation, a US railway company, a worm infected the communication network used for signalling, bringing all trains to a halt for half a day[5)].

Table 1: Which security mechanism for which security objective?

Security objective	Security mechanisms
Confidentiality	Encryption, Virtual Private Network (VPN), Secure Socket Layer (SSL)
Integrity	Cryptographic checksums, malware scanners
Availability	Redundancy, diversity, malware scanners
Authentication	Pass phrases, certificates, tokens/smartcards, biometrics, challenge-response protocols
Authorization	Hardened operating systems (no insecure or unused services, user accounts; tightly defines access control lists (ACLs) on resources, etc.), firewalls, personal firewalls, application level message filters, Virtual LAN (VLAN)
Auditability	Intrusion Detection System (IDS), logs
Non-repudiation	Digital signature
3rd party protection	Firewall (egress filtering), malware scanner (for outgoing data)

Footnotes:

1) http://www.gtiservices.org/security/riskassess/gazprom_attack_04261999.doc
2) http://www.theregister.co.uk/content/4/22579.html
3) http://zdnet.com.com/2100-11-526431.html?legacy=zdnn
4) http://www.theregister.co.uk/content/56/32425.html
5) http://www.csx.com/?fuseaction=company.news_detail&i=45722&news_year=-1

May 2004: The "Sasser" worm infected the signalling and control system of the Australian railway company, RailCorp. 300,000 commuters in and around Sydney had no transportation on this day[6].

These examples show that electronic attacks on industrial control systems really do happen. In addition, it can be safely assumed that a large number of attacks have not been reported in the press. Canadian researchers maintaining a confidential database of IT security incidents in industrial installations have observed an increase in incidents and a shift from internal to external attacks [2]. It is worth mentioning, however, as far as details about the above mentioned incidents are known, they were all possible only because suggested practices were disregarded. A survey conducted by ARC in 2004 indicates that a significant number of control systems connected to external networks have no security mechanisms 1.

Which security mechanisms should be used?

A risk of an attack exists if there is an exposed *vulnerability and a threat.* The *vulnerability* of an information system may be caused by a logical design flaw (eg, a wrongly designed protocol), an implementation mistake (eg, allowing a buffer overflow), or a fundamental weakness (eg, passwords and cryptographic keys that are guessable by trying out all possible permutations).

Threats to a system are the potential goals of attackers, for example, to disrupt production for a certain period of time. Threats may also be realized by an incidental, non-intentional exploitation of a vulnerability.

The *risk* of a given attack is determined by the *likelihood* of a successful attack and the *severity* of the damage it may cause. For a given system, a *threat analysis* must be performed during which risks are evaluated and ranked in importance. This analysis forms the basis for the security policy, where the relevant security objectives are specified. This finally determines the *security mechanisms* to be deployed. Security mechanisms reduce the risk to a system by making the exploitation of vulnerabilities less likely or by limiting the damage. 2 illustrates the interrelations between the IT security terms used in threat and vulnerability analysis.

Table 1 shows which security mechanisms are commonly used to reduce the risk of certain types of security objective violations:

Suggested best practices

Securing a system is difficult as it is necessary to spread effort and budget to efficiently and effectively prevent a wide variety of attacks. Based on experiences that have been made in this field over the last few decades, the following best practices should be taken into account when deploying technical security measures or implementing procedural controls:

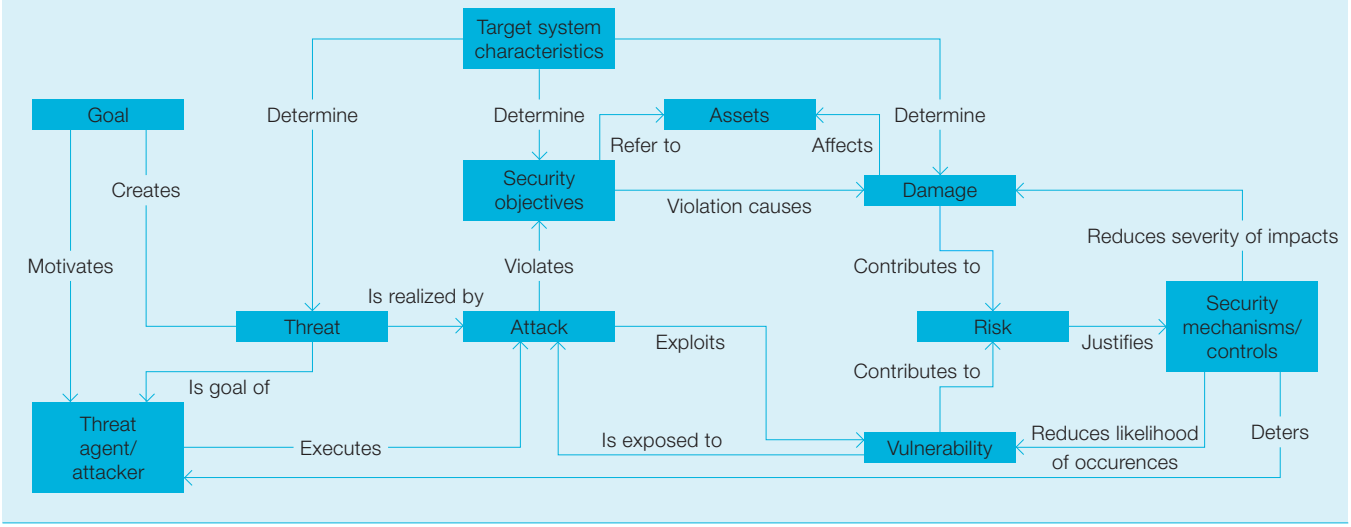
Avoid a weak link: The effort spent on protecting the various interdependent security objectives required for a system has to be distributed so that all mechanisms facing an attacker are of comparable strength. Otherwise, an attacker could bypass a strong mechanism by breaking a weak one. In security systems humans are often the weakest link, the effect of which places greater importance on procedures and training.

There is no "security by obscurity": It used to be argued that automation systems were secure because very few people had sufficient detailed knowledge about their operations and protocols to attack them. Unfortunately this is no longer the case. Many automation experts exist in all parts of the world, and automation systems are largely based on well-documented open standards.

Least privilege: By only giving users the minimum permission necessary to

Footnotes:
6) http://news.com.au/common/story_page/0,4057,9455677%255E15306,00.html

2 IT security threat analysis terms and their interrelations.



do their job, the risk of insider attacks or the abuse of compromised user identities is reduced.

Important secure system design principles

Two design principles should be considered when architecting a secure system:

Defense-in-depth: There are two commonly used basic approaches for securing physical and information systems: *hard perimeter* and *defense-in-depth*. The idea behind the hard perimeter approach is to put a single impenetrable wall around the system and to disregard all security issues inside. In the defense-in-depth approach several zones are placed around the object to be protected. Different types of mechanisms for detecting and delaying an attacker are used concurrently inside and around each zone. The outer zones contain less valuable targets. Properly implemented defense-in-depth security architectures are more resistant to attacks than hard perimeter architectures.

Security is a process, not a product: Due to changes in the operating environment and the availability of new attacks, no security system even if it is implemented flawlessly, will be able to fulfill its purpose forever without maintenance. Maintenance includes reviewing access control rules and updating installed software. These reviews compare actual state with the defined state of the system. In addition, they assess whether the defined state is still appropriate in the face of a changing business and risk environment. The need for maintenance means that continuous financial and staffing resources are needed to keep a system secure.

Where do we stand?

Even though reports about spreading worms and a general increase in network based attacks seem to dominate the news in IT related publications, this is not really a reason to forego the enormous benefits that full vertical and horizontal integration based on network interconnections can bring to an enterprise. As long as well-known good practices are respected in implementing and operating network connectivity between the control system and other networks, an adequate level of security can be achieved for any application. That security level then represents the residual risk that is regarded as acceptable after a thorough threat and risk analysis for the particular installation.

Part 2 of this tutorial will explain how an automation system may be protected against damages from worms and viruses. Part 3 will show what industry standards are emerging in the field and how they can be used to reduce the effort to secure a plant against targeted and untargeted attacks.

"Security" is not a fixed target. Continuous efforts are necessary to keep any system secure. In the case of control systems, both the plant operating enterprise and the automation vendor have to be involved in these efforts.

Glossary

Cryptographic Checksum	Check-bits calculated from the content of a document or message and a secret key, such that any unauthorized changes in the document can be detected.
Challenge-Response	A sends a challenge to B: a question whose answer can only be given if a common secret (password) is known. If B responds correctly, it has proven its identity to A, without having sent a password. (Sending a password is vulnerable to eavesdropping.)
Public Key Cryptography	Encryption method using a pair of keys: Encryption with the public key results in data which can only be decrypted by the receiver using the matching private key. The private key must be kept secret.
Digital Signature	Check-bits appended to a document or message, calculated from the document and a secret known only by the sender. Used to prove that the document originates from the claimed sender.
Digital Certificate	Digital "passport", attests that a public key belongs to the claimed owner. Issued (signed) by a trusted certification authority.
Virtual Private Network (VPN)	Private network running over encrypted tunnels through the public Internet.
Firewall	Device or program which inspects all incoming (ingress) or outgoing (egress) messages. Messages are filtered (blocked or forwarded) based on source/destination addresses or application level contents.
Intrusion Detection System (IDS)	Devices observing traffic in a network, in order to detect electronic intrusions and raise alarms. Detection is based on attack signatures or anomalies in the traffic patterns.
Secure Socket Layer (SSL)	Security protocol widely used to authenticate Web servers and to establish encrypted communication between Web browsers and servers. Uses digital certificates.

Dr. Martin Naedele
Dr. Dacfey Dzung
ABB Switzerland, Corporate Research
martin.naedele@ch.abb.com
dacfey.dzung@ch.abb.com

References:

[1] **Leffler, N. , Terwiesch, P.:** Aspects of Productivity, ABB Review 2/2004.

[2] **Byres, E. , Lowe, J.:** The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, VDE Kongress 2004.

[3] **Forbes, H.:** Plant Floor Network Practices in Today's Factories and Plants, ARC insight 2004-53EMHLP, December 2004.

Further reading:

M. Naedele: IT Security for Automation Systems, in: **R. Zurawski** [Editor]: Industrial Information Technology Handbook. CRC Press, January 2005, ISBN 0-8493-1985-4.

M. Naedele: IT Security for Automation Systems - Motivations and Mechanisms, atp international, Vol 1 (1), 11/2003, and atp, Vol 45 (5), 5/2003.

R. Anderson: Security Engineering, Wiley, 2001.