



# Industrial information system security <sup>Part 3</sup>

Standards for securing industrial automation systems

Martin Naedele, Dick Oyen

Part 2 of this three-part tutorial on information system security in industrial networks explained the different types of malware and suggested how an automation system could be defended against them.

This final installment looks at various initiatives that have been started over the last couple of years by different groups to create standards and other forms of guidance to secure industrial automation systems. An overview of a number of those initiatives and their work products is presented, and the approach taken by IEC TC65 WG10 to produce technical blueprints for securing certain control system scenarios is explained.

## Tutorial

Currently there is a flood of information available on information system security in general. On top of this, there are some automation vendor white papers that explain certain aspects of locking down their systems. However, there is a serious lack of impartial and easily accessible guidance on how to systematically secure automation and control systems against electronic attacks.

There is no doubt that standards in this area would be very beneficial for both automation users and automation vendors, thus enabling them to:

- Estimate the effort required to implement, maintain, and operate security mechanisms and processes.
- Specify the security objectives for their plant and the security functionalities and measures that have to be provided by vendors and system integrators.
- Compare the threat coverage and cost of offered security solutions.
- Implement and operate cost efficient security mechanisms across multiple plants and locations in the enterprise.
- Be sure that their defense against IT-based threats corresponds to state-of-the-art solutions.

Vendors and system integrators will be able to:

- Anticipate security requirements and develop corresponding functionality.
- Create security architectures that may be reused across multiple projects and customers. This reduces costs in proposal writing, engineering, and the purchasing of third party security devices and applications.

#### Major standardization initiatives

The following survey of industrial security standardization initiatives is adapted from [1] and [2].

#### ISA S99

The intention of the ISA (Instrumentation, Systems, and Automation Society) Committee SP99, "Manufacturing and Control Systems Security"<sup>1)</sup> is to create guidance documents and a standard (S99) on introducing IT security to existing industrial control and automation systems.

ISA is entitled to produce standards for the process industry with national validity in the US. Many ISA standards are used internationally as best practices or, such as S88 and S95, adopted as international standards.

### Standards outlining how to systematically secure automation and control systems against electronic attacks would be very beneficial for both automation users and automation vendors.

SP99 started its work in 2002. As a first step, it produced two technical reports that were published in spring 2004. The first report "Security Technologies for Manufacturing and Control Systems" [3] is a comprehensive survey of what is state-of-the-art in security technologies and mechanisms, with comments on their applicability for the plant floor. It covers: authentication and authorization; filtering/blocking/access control; encryption and data validation; audit, measurement, monitoring, and detection; operating systems and software; and physical security. Each technology is evaluated with regard to the following questions: Addressed security vulnerabilities; typical deployment; known weaknesses; use in an automation environment; future directions; recommendations; and references.

The second report "Integrating Electronic Security into the Manufacturing and Control Systems Environment" [4] presents recommendations for a security architecture and describes the administrative issues and processes for introducing a security management system in industrial plants. The approach in this report is inspired by ISO/IEC 17799 [5]. It contains sections on developing a security program, policies, risk assessment, audits and testing, developing, selecting, and procuring, countermeasures, as well as examples for policies and forms.

Since the summer of 2004 SP99 has been working on the S99 standard. S99 focuses on:

- Retrofitting security mechanisms in existing plants with commercially available components without actually prescribing a specific architecture.
- The processes to operate the underlying management system and administrative processes.

The actual security architecture and processes will likely be customized for specific plants.

#### IAONA

The Industrial Automation Open Networking Alliance (IAONA) is an interest group of industrial communication system users and manufacturers. Its Joint Technical Working Group Security<sup>2)</sup> has developed a Security Data Sheet which is intended to serve as a template for automation system and

Table 1 Security initiatives

**CIDX** (<http://www.cidx.org/CyberSecurity/>) creates procedural security guidance for the chemical industry. Its work is aligned with ISA SP99. CIDX is mostly active in North America.

**NAMUR** (<http://www.namur.de/en/694.php>) provides guidance on secure usage of networking technology for the process industry. NAMUR is mostly active in Germany/Europe.

**NERC** (<http://www.nerc.com/>) is the North American self-regulation authority for power utilities. Compliance with NERC 1200 and successor CIP 002...009 standards on security management with their strong focus on processes and documentation is compulsory for North American power utilities.

**CIGRE** (<http://www.cigre.org>), the International Council on Large Electric Systems addresses IT security considerations in a number of its working groups.

**PCSRF** (<http://www.isd.mel.nist.gov/projects/processcontrol/>), the Process Control Security Requirements Forum, promotes security certification of future control system components according to ISO/IEC 15408 ("Common Criteria"). It is driven by the US National Institute of Standards and Technology, the US national ISO/IEC 15408 certification authority.

**PCSF** (<http://www.pcsforum.org/>), the Process Control System Forum, was established 2004 as a meta-initiative to promote information sharing between all the other initiatives on the topic.



device vendors to document the security and communication related features and requirements of their individual products. This information can serve as valuable input for the automation security architect as he designs and configures the necessary security mechanisms for the plant. The benefit of such a Security Data Sheet is that it collects, at a single location, concise security relevant information that is otherwise often hard to obtain from vendor literature.

### IEC

In early 2004 the IEC Technical Subcommittee 65C (Digital Communications), through its working group WG13 (Cyber Security), started to address security issues - within the IEC 61784 standard – for field buses and other industrial communication networks. These issues are outlined in a new part 4 entitled “Digital data communications for measurement and control – Profiles for secure communications in industrial networks”.

What became evident during this work was that security issues in the automation system cannot be solved by protecting communication alone and by looking only at the field level. Instead, the working group started to specify state-of-the-art secure realizations of certain common automation networking scenarios, such as dial-up remote access. These descriptions, called requirement sets, contain a product independent specification of technical mechanisms in the context of a best-practice security architecture, as well as guidance on the configuration and operation of these mechanisms. The approach is described in greater detail below.

Consequently, the work of the group was moved to TC65 WG10 to align the actual and necessary work with the IEC committee mandate. The completed standard IEC 62443, entitled “Security for industrial process measurement and control – Network and system security” is expected in 2006. The final voting for international validity will take place during the first half of 2007.

Some other security initiatives are briefly described in [Table 1](#).

### Security management on the plant floor according to ISA S99

The ISA SP99 technical report TR99.00.01 [3], “Security Technologies for Manufacturing and Control Systems” provides guidance on the applicability of a broad and inclusive range of security technologies. Its advice comes from the combined experience of security experts from automation system vendors and users. As the information presented is analytical in

nature, it is not a normative standard against which compliance can be measured. The reader determines the applicability of the information to the specific case. It is an excellent document for those starting to determine security measures and those with experience. TR99.00.01 continues to be updated but its content will not be covered by the S99 standards.

As of October of this year, drafts of two of the four parts of the S99 standard are almost ready for public review.

Part 1 defines terms and describes the models used in discussing security in automation systems. Part 2 advises how a cyber-security management system (CSMS) can be established. There are 18 key elements in a CSMS which are structured in a life cycle that is constantly repeated through four phases: Plan, Do, Check, and Act. The CSMS is provided by the Chemical Industry Data Exchange (CiDX) [7], which adapts the four phases of the British Standard BS 7799-2:2002 [6] to automation systems and defines the 18 key elements. The CSMS and its elements are shown in [1](#). Its cyclic nature is implicit in step 18 in which the security program itself is modified according to lessons learned in the course of the preceding elements.

#### Plan phase:

Security planning begins with making a business case so that top management can set a clear top-level policy that mandates the security program.

Organizational Security is planned and this takes into account all of the departments and people that are involved with the control system. It identifies roles and establishes responsibilities relative to security.

Security relates to people: those who have assets to protect, those who are expected to protect them, and those who might compromise those assets. Personnel Security defines personnel policies to estimate and maintain the trustworthiness of those who are given greater access to the assets. Physical and Environmental Security must also be planned. Cyber security is

**1** Cyber Security Management System.



## Tutorial

based on an assumption that there are substantial (not absolute) barriers against physical attack.

Security risks are identified, classified, and assessed in the planning phase. Detailed instructions about how to do this is provided in S99 and the material that it references.

### Do phase

Risk assessment leads directly into the Do Phase. Using the risk assessment, security resources can be efficiently applied to real vulnerabilities.

Procedures are established that plan the response to potential incidents. Response planning must include when it becomes necessary to notify government officials of a significant threat to the community.

Overall management policies and procedures are established to cover com-

munications, system operations, and change management.

Access control defines the privileges that accompany specific roles. It also defines the procedures that limit people's access to activities and information to which they are privileged. Authentication means are determined which will ensure that a particular user (person or software) has the necessary access authorization.

Information and Document Management identifies the security classification of data and specifies safeguards. Security issues of developing and maintaining the system are also handled by policies and procedures.

Staff must be trained in the relevant security procedures and all personnel should undertake regular refresher courses on general security precautions. Compliance of departments and person-

nel to the security policies and procedures must be measured through continuous monitoring, and periodically, through audits. Compliance must also take into account external requirements such as those of customers, contractual partners, and regulatory agencies.

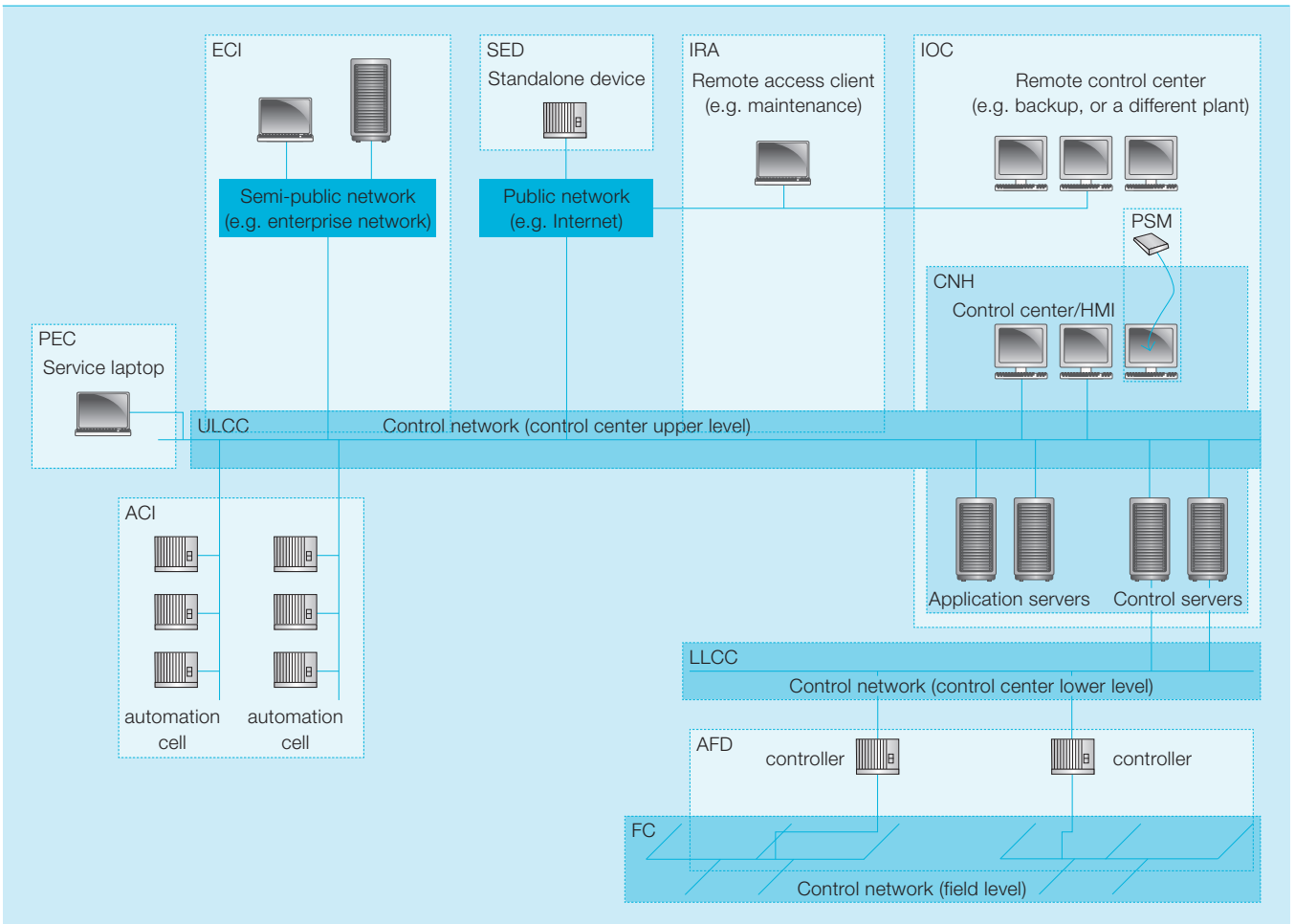
### Check phase

The Check Phase includes developing a Business Continuity Plan and following it. This plan establishes how the company will operate through incidents that result in serious damage, plant outage, and possibly community catastrophe. The lessons learned from the CSMS activities are reviewed in the Check Phase.

### Act phase

As the CSMS is a cyclic process, the security program is revised according to the review in the Check Phase. S99 Part 2 provides more details as well as 19 steps for establishing a

2 Modular security architecture. Each can be mapped to certain components of the automation system and its network.




CSMS. Part 3 aims at providing guidance on how to operate the CSMS.

#### Technical security architecture based on IEC 62443

IEC 62443 mainly addresses – on a system level – technical aspects of the security architecture, and thus complements product oriented initiatives like IAONA, and process guidance provided by SP99 and NERC.

With the ongoing standardization efforts for Industrial IT security processes and architectures, plant managers have a real chance to implement state-of-the-art and cost-efficient information system security.

The basic idea of the IEC approach is that of a modular security architecture. Each module corresponds to a certain usage or communication scenario and can be mapped to certain components of the automation system and its network . Each module is represented by a requirement set specified in the standard. Some of the requirements, as well as the physical or logical components they refer to, are common to multiple modules. Security architecture modules can and should be combined to suit the specific usage and threat situation of an automation system. The standard will provide guidance on the priority of modules for situations where a complete implementation of the standard is not possible due to budget limitations for initial implementation and ongoing maintenance.

The requirements will be formulated in a way that can be used as the basis for Requests for Proposals (RFPs) for data communication standards, and offers, as well as security audits. They

should, at the same time, allow for different technical solutions. One goal is that it will be possible to meet the requirements of the standard using products and technologies that are commercially available today. The requirements can also be applied to current and legacy systems and they can be scaled down for systems where an analysis has indicated they represent a low risk for both the enterprise and society.

The working group foresees the following modules:

**Enterprise – control net interconnect (ECI):** ECI defines the security architecture for non-real-time dataflow between a control network and an enterprise network, preferably unidirectional out of the control network.

**Interactive remote access (IRA):** IRA details the security architecture needed so that parts of the control system can be accessed remotely (ie, via telephone dialup or Internet) for perhaps engineering or expert diagnosis.

**Inter control center connect (ICC):** ICC describes how communications between fixed control centers over public networks can be secured.

**Stand-alone embedded device (SED):** SED outlines the security requirements for an automation device that is not contained in a security zone and for which a full-blown security perimeter would not be cost efficient, eg, a pole-top Intelligent Electronic Device (IED).

**Portable engineering computer (PEC):** PEC details how a control system can be protected against threats originating from portable computers that may be moved back and forth between public networks and the control system

**Portable storage media (PSM):** An automation system may be exposed to malware infections through storage media like memory sticks or CDs. PSM explains how this can be prevented.

**Automation cell interconnect (ACI):** ACI outlines the security architecture required for protected communication between automation cells within a control network.

**Upper Level Control center (ULCC):** Part of a control network is connected to operator workstations, “historians”, application servers and connectivity

servers. ULCC details network oriented security mechanisms specific to this part.

**Lower Level Control center (LLCC):** LLCC outlines network oriented security mechanisms in the part of the control network connected to controllers and PLCs.

**Field Control (FC):** FC outlines network oriented security mechanisms in the part of the control network connected to field devices.

**Control network host (CNH):** CNH explains how automation workstations and servers for operations and engineering can be secured against attacks from insiders and malware, for example.

**Automation field device (AFD):** AFD explains how field devices and embedded controllers can be secured.

Each module describes: a use case to which it applies; threats that are addressed or not addressed; the underlying assumptions; the requirements; and the party (automation vendor, system integrator, or plant owner) responsible for meeting each of the requirements. The core part of each module is the requirement set and it contains between 20 and 50 requirements, depending on the module.

Each requirement consists of a normative statement, optionally including scale-down alternatives, a rationale, and in many cases one or more application notes. The rationale is an essential element, as it enables the reader to make an informed decision about the importance and applicability of the requirement. The application notes provide technical guidance on how the requirement could be realized.

The IEC 62443 standard describes the “what” and “why” of the security architecture, but the “how” is specific to an individual site and system and is therefore left to the engineering judgment of the plant experts and the automation/IT integrator.

#### Summary

With the ongoing standardization efforts for Industrial IT security processes and architectures, specific to control and automation systems, plants managers now have a real chance to

#### Footnotes

<sup>1)</sup> <http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821>

<sup>2)</sup> <http://www.iaona.org/home/jtwg-se.php>

Tutorial

implement state-of-the-art and cost-efficient information system security.

The standardization initiatives described above have so far been characterized by a general recognition that pragmatic solutions are needed to serve the industry, as well as very constructive collaboration among automation vendors and end users so that this objective is achieved.

ABB is a major contributor to various security standardization initiatives. The company offers products and solutions that are compliant to evolving standards, and provides assistance to its customers in applying these standards to specific plants and sites.

**Martin Naedele**

ABB Switzerland, Corporate Research  
martin.naedele@ch.abb.com

**Dick Oyen**

ABB US, Corporate Research  
dick.oyen@us.abb.com

**References**

[1] Naedele, M.: Standardizing Industrial IT Security – A First Look at the IEC approach, 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 05), Catania, September 2005

[2] Dzung, D., Naedele, M., von Hoff, T., Crevatin, M.: Security for industrial communication systems, Proceedings of the IEEE, Vol. 93 (6), June 2005, pp 1152–1177

[3] ISA SP99: Security Technologies for Manufacturing and Control Systems, Instrumentation, Systems, and Automation Society, ISA-TR99.00.01-2004, March 2004,





[4] ISA SP99: Integrating Electronic Security into the Manufacturing and Control Systems Environment, Instrumentation, Systems, and Automation Society, ISA-TR99.00.02-2004, April 2004,

[5] ISO: Information technology – Code of practice for information security management, ISO/IEC 17799:2000, December 2000,

[6] British Standards Organization: Information security management systems – Specification with guidance for use, BS 7799-2:2002, September 2002

[7] Chemical Industry Data Exchange (CIDX): Guidance for Addressing Cybersecurity in the Chemical Sector, Version 2.0, December 2004.

INDEX 2005

 <p><b>1/2005: Pioneering spirits</b></p>		 <p><b>3/2005: Sustainability</b></p>	
A revolution in high dc current measurement	6	Sustainability in ABB	6
Form and Function	11	Healthy, safe and productive	10
The perfect cast	14	Emissions trading	14
DryQ – Dry and silent	17	SF <sub>6</sub> technology	20
PSGuard contributes to UCTE grid reconnection	22	Energy efficiency	22
Team-mates	26	Networking	28
Instant comfort	30	Not on my watch	31
Satisfaction guaranteed	33	Leaner, fitter, smarter	36
Panoramic projection	37	HVDC	42
Digging into the archives	40	Safety management in process industries:	
Best innovations 2004	43	Part 1	47
Don't touch: ABB's new passive voltage indicator	52	Part 2	51
Wireless Ad-hoc networks	54	Energy efficiency	
Autonomic computing	55	Green shipping	54
		The ABB turbocharger	58
		Boosting supply	63
		Cut and dry	66
		Unplugged but connected – Part 1.	70
		Industrial information system security – Part 2	74
 <p><b>2/2005: University and industry cooperation</b></p>		 <p><b>4/2005: Innovation – The DNA of business</b></p>	
Closing the gap	6	Looking back to look forward	6
Welcome to our world	10	Fruits of innovation	9
The MIT experience	14	Best innovations 2005	15
Leaders of tomorrow	18	Grid flexibility	21
University co-operation	22	Light and invisible	25
City of learning	29	Convergence in the control room	30
Let's work together	32	Powerful and stable	33
Looking ahead	35	High voltage assembly	36
Value for money	39	Breaking to the front	39
Root cause	44	Ironing out resonances	42
Predictable assembly	49	Age is no issue	47
Hot stuff	55	The process “copper”	51
Grids united	59	Control loops: pleasure or plague?	55
Simulated reality	62	Stabilizing influence	60
Industrial information system security –Part 1	66	Live(ly) neighbours	64
		Unplugged but connected Part 2	65
		Industrial information system security – Part 3	69