

Standardizing Industrial IT Security - A First Look at the IEC approach

Martin Naedele
ABB Corporate Research
CH-5405 Baden-Dättwil
Switzerland

Abstract

Information system security for industrial plants is a topic of increasing importance. Effective and cost-efficient security solutions require some kind of industry consensus or standardization. This paper examines the interests of the various stakeholders in the industrial security field (e.g. society, plant owners, service providers, automation vendors, and consultants) and evaluates some of the more visible industrial security initiatives (ISA, NERC, IEC) with regard to stakeholder benefits and requirements. The paper then proceeds to give some details on the approach and current draft of the industrial control system security working group within IEC TC65.

1 Introduction

Automation systems are no longer isolated information systems, limited to islands on the shop floor of an industrial plant. Instead, state-of-the-art automation systems are today part of a vertically integrated production information management infrastructure that connects the shop floor information system with business systems like enterprise resource planning (ERP), manufacturing execution systems (MES), and supply chain management (SCM). Remote access via public networks such as the Internet or the telephone network is also essential for timely and cost efficient plant maintenance and optimization.

Any system connected to a public network is exposed to the potential threat of an attack through that network. Common types of attackers and attacks today are worms, leisure hackers using openly accessible tools and canned exploits, insiders abusing their knowledge and privileges, as well as criminals abusing the specific weaknesses of a target system.

To protect against attacks and to prevent the resulting damages and liabilities, security measures are thus needed in networked industrial plants. While the necessity for security measures is the same as in office environments, the actual mechanisms have to be adapted to the particular situation on the plant floor [2, 9, 10, 3].

In recognition of this need for dedicated guidance on security for industrial automation systems, several activities and initiatives were started over the last few years, covering different industries, geographic areas, and approaches to security.

This paper will investigate the different requirements and expectations of the various stakeholders involved in the process of standardizing automation system security, compare these requirements with the actual approaches of several of the more significant security initiatives, and then look in detail into one specific activity, the standard to be produced by the industrial control system security working group within IEC TC65.

2 Benefits and requirements

This section discusses the potential benefits and resulting requirements and expectations of different stakeholders in the automation system security field.

2.1 Society

Society expects that enterprises take the necessary precautions to avoid that a network based attack endangers the financial viability of the enterprise or the safe operation of the plant. The former would have a negative impact on employment, for example, while the latter could harm humans or the environment.

Society is most concerned with the effectiveness of security measures and that they are generally implemented.

Society is unlikely to provide direct financial subsidies or other incentives to enterprises for securing their plants. If at all, it exerts its influence via legislation, regulations, and lawsuits.

2.2 Regulatory authority

The regulatory authority is tasked to achieve the highest reasonable level of security to avert harm to society. It also has to be aware of the fact that the enterprises it regulates will often try to implement the lowest cost measures that they can legally claim to be compliant with regulations. Regulations thus have to cope with the tension that they should provide an objective benefit, but that compli-

ance can be effectively measured and non-compliance be proven in court, if necessary.

Due to these goals, regulations tend to lag behind the state of technology or concentrate on easily measurable performance criteria like usage of certified products [7] and regular submission of certain documentation [12]. These performance criteria do not necessarily reflect the true security posture of the regulated enterprise.

2.3 Plant operating enterprise

The enterprise that operates industrial plants requires security mechanisms that protect against direct and indirect financial damages resulting from attacks.

The biggest concern of the enterprise is cost. The desire to avoid certain costs, together with a lack of good theoretical foundations on security risk estimates and return on security investment (ROSI) calculations, may induce enterprises to accept (too) high risks with regard to their security posture and the effectiveness of their security architecture. The enterprise also tries to avoid security measures that limit its business functions.

A security architecture is more cost efficient for the plant owner

- the more it uses commodity products,
- the more it can be implemented and maintained in a similar fashion across multiple plants,
- the more it can be applied to automation systems of different generations (legacy systems) and vendors,
- the less it requires maintenance and updates,
- the better it is aligned with other processes and procedures in the plant,
- the more it is able to be adapted to evolving threats and business scenarios, and
- the less it requires specialist knowledge to operate.

2.4 Service provider

The providers of non-security-related services to the plant, such as engineering, maintenance, and optimization, are mostly concerned that the security mechanisms do not get in the way of their activities. Such service providers, relying for cost reasons on remote access instead of physical presence in the plant, may be part of the plant owning enterprise or external companies. Especially for external companies it is important that the security rules and procedures they have to follow, and the mechanisms and products they have to employ, can be reused across a large part of their customer base. The need for compliance with customer specific, significantly different security architectures would create cost hurdles that could force many such service companies either out of business or induce them to neglect or circumvent security precautions.

2.5 System integrator

The system integrator has to combine the control system components and the networking equipment, both potentially from a number of multiple vendors, into a consistent plant automation system according to the specification of the plant owner and in compliance with applicable regulations.

In order to reduce its own cost and improve its competitiveness, the system integrator is interested in security architectures that work with control system and networking equipment from as many vendors as possible, do not interfere with the functionality of the automation system, and can be adapted with little effort to evolving threats and business scenarios, regulations, and automation system generations. The system integrator will likely use remote access for engineering and optimization at least during the initial operation time. There is thus an overlap with the interests of the service provider.

2.6 Automation system vendor

The control system vendor wants to satisfy security requirements from plant owners and system integrators using its products with as little additional cost as possible. The control system vendor would like to avoid being forced to become a security specialist.

In order to keep its cost related to providing security mechanisms low the control system vendor would like to

- get security requirements from its customers that are similar among different projects, customers, industries, and geographic locations,
- receive internally consistent security requirements from even its less security-savvy customers,
- fulfill the requirements using technology that is commercially available, off-the-shelf, from multiple sources,
- reuse the same solutions throughout its own various business units,
- apply the same security architecture to secure future automation systems as well as systems that are already in place, and
- provide solutions that are easily understood by its own sales staff and customer purchasing representatives.

Regulations or customer expectations and requirements should not cause recurring costs that are not part of a service contract with the customer (plant owner).

2.7 Security product vendor

The security product vendor would like the automation system security standard to be compatible with its products, ideally mirroring their feature set as closely as possible. The perspective on security of the security product vendor is often focussed on the specific part of the security problem its product solves, e.g. virus protection.

stakeholder	ISA	NERC	IEC
society	+	+	++
regulator	o	++	o
plant	++	+	++
service	o	-	++
integrator	o	+	++
control vendor	o	-	++
security vendor	+	++	o
consultant	+	++	o

Table 1. Match between automation system security initiatives and stakeholder expectations/interests/benefits (" - " against the interests of the stakeholder, "++" perfect match with stakeholder interests).

2.8 Security consultant

For the security consultant, as for the security product vendor, the automation system security standard is mainly a source of business opportunities. In contrast to the vendor of predefined security products, he is more interested in providing security solutions that are customized for specific plants.

The security consultant derives continuous revenue from recurring activities like security audits, or (re)certifications of products and product versions.

3 Standardization approaches

A number of different initiatives world-wide are currently working on different types of guidance documents, standards, and regulations to improve the security of networked automation systems. The initiatives differ with respect to the involved parties and their goals, as well as geographic and industry scope.

This section surveys the more visible ones among those initiatives and evaluates their approach with respect to the interests of the different stakeholders outlined in the previous section (See also Table 1 for a summary).

3.1 ISA S99

The ISA Committee SP99 "Manufacturing and Control Systems Security" intends to create guidance documents and a standard (S99) on introducing IT security to existing industrial control and automation systems [13]. ISA, the Instrumentation, Systems, and Automation Society, is entitled to produce standards for the process industry with national validity in the US. Many ISA standards are also used as best practices internationally .

SP99 started its work in 2002. In a first step, SP99 produced two technical reports that were published in spring 2004:

The first report "Security Technologies for Manufacturing and Control Systems" [6] is a comprehensive survey of the 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, detection; operating systems, 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" [5] 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 [8]. 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 summer 2004 SP99 has been working on the standard S99 itself. S99 is envisioned to consist of four major parts: Introduction and terminology, implementing a security management system, operating a security management system, and requirements on automation system products and vendors. It is planned to develop and publish those four parts sequentially. The first part is close to completion, the scope and content of the fourth part are still rather vague.

Among the active members of SP99, plant owning enterprises are strongly represented. Other significant groups are consultants and control system vendors.

S99 focusses on retrofitting security mechanisms on existing plants using COTS technology components without actually prescribing a certain architecture, and on the processes to operate the underlying management system and administrative processes. The actual security architecture and processes will likely be customized for a specific plants and thus vary between plants. Implementation of S99 will certainly improve security of a plant. While a plant can be audited with regard to the content of S99, the standard so far is not focussed on providing metrics for schematic measurement of compliance.

3.2 NERC1300 / CIP 002-009

The North-American Electric Reliability Council (NERC) passed in August 2003 its Urgent Action Standard 1200 "Cyber Security" [11]. This Urgent Action Standard NERC 1200 has been extended for one year in August 2004, while work on its permanent successor CIP-002-1 through 009-1 (formerly called NERC 1300) is under way. A second draft of CIP-002-1...009-1 has become available in January 2005 [12]. The CIP-002-1 through 009-1 implementation plan calls for the standard to become effective October 1, 2005 and to begin to require compliance in the first quarter of 2006. Compliance with NERC standards is compulsory for US power utilities.

NERC 1200 requires US transmission and distribution utilities to create and maintain documentation of about 16

different aspects of IT security, such as access control, physical security, incident handling, training, and policy. The CIP-002-1 through 009-1 series appears to be rather similar in character and content of its prescriptions, but it will extend the scope to power generation companies and also impose penalties for non-compliance.

The working group that produces the NERC security standards consists of representatives of several utilities subject to NERC regulation. In contrast to ISA SP99 and PCSRF, participation is open only to employees of member companies, which must be electric utilities.

By imposing metrics based on processes, procedures, and documentation CIP-002...009 is clearly focussed towards enforceable regulation, while still leaving some room for customization to the plant owning utilities. Implementing the NERC requirements will certainly have a positive effect on the security of many utilities, compared to practices before the NERC standard. Building, maintaining, and auditing NERC-compliant security architectures creates business opportunities for consultants and, to a lesser degree, system integrators. Control system vendors and service providers will have to adapt certain aspects of their systems and practices.

3.3 IEC

The IEC Technical Sub-Committee 65C "Digital Communications" started in early 2004 to address security issues for field buses and other industrial communication networks in a new part 4 "Digital data communications for measurement and control - Profiles for secure communications in industrial networks" of the IEC 61784 standard in its working group WG13 (Cyber Security). As it was recognized that security has to be addressed on the system level, not on the communication link alone, the working group decided in May 2005 to propose to move the activity into a new working group (WG10) at the level of TC65. At the time this paper was finalized, the voting of the IEC national committees on this proposal was still ongoing. The first committee draft [4] produced by WG13 was sent out for comments together with this restructuring proposal as base for the work of the new working group. If the formation of a new working group and of a new work item with a more comprehensive charter is approved, the IEC security work in industrial control will be split. IEC 61784-4 will then deal only with those issues that are concerned with (Ethernet) field bus communication security, while the system-level work that has been done so far will become part of a new standard.

The objective for this IEC standard is to describe 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 further guidance on configuration and operation of these mechanisms. With this standard, it should be possible in future to replace dozens of pages of project

specific security specifications by a reference to one or more of the requirement sets of the IEC standard. Completion of the standard is expected in 2006 with the final voting for international validity in the first half of 2007.

Implementing the industry best practices captured in the prescriptions of the IEC requirement sets will in many cases considerably improve the current state of plant security. The firewall architecture in the Enterprise / Control network Interconnect (ECI) requirement set, for example, gets one of the highest rankings in the NISCC firewall guide [1]. Standardized technical security architectures will reduce the cost for control system vendors, system integrators, and service providers. It is possible to audit compliance with the standard in a certain plant, but this will likely require an inspection of the actual site.

4 Details on the IEC approach

The following description reflects the current thinking of WG13 as captured in [4]. Based on feedback from the IEC national committees, the standard may still change considerably in structure and content until it is officially passed.

4.1 Area of concern

As explained in section 3.3 it became clear during the initial analysis of the task for WG13 that field communication, as was originally targeted, is not the area with the most pressing demand for security solutions in the industrial environment. More urgently, security solutions are needed for the control center level in the automation hierarchy, and especially for connections to or from outside systems in the enterprise or beyond. In addition, considering realistic threats and threat agents in that environment, including worms, disgruntled insiders, and criminal attackers from the outside, such security solutions have to cover not only the communication system in a narrow sense (bits on the wire), but also the various communication endpoints, that is, the hosts and devices in the automation system. This is reflected by the reference model in Fig. 1 which schematically shows how the proposed requirement sets cover the whole automation system and its external connections.

4.2 Stakeholders

The work in IEC SC65/WG13 is based on an explicit statement on the target audience and its expected benefits from using the standard:

Plant designer (owner / consultant) The standard helps to capture requirements, to identify constraints and to define a technical security architecture.

System integrator The standard supports component selection, implementation, configuration and evaluation/acceptance testing of the technical security architecture.

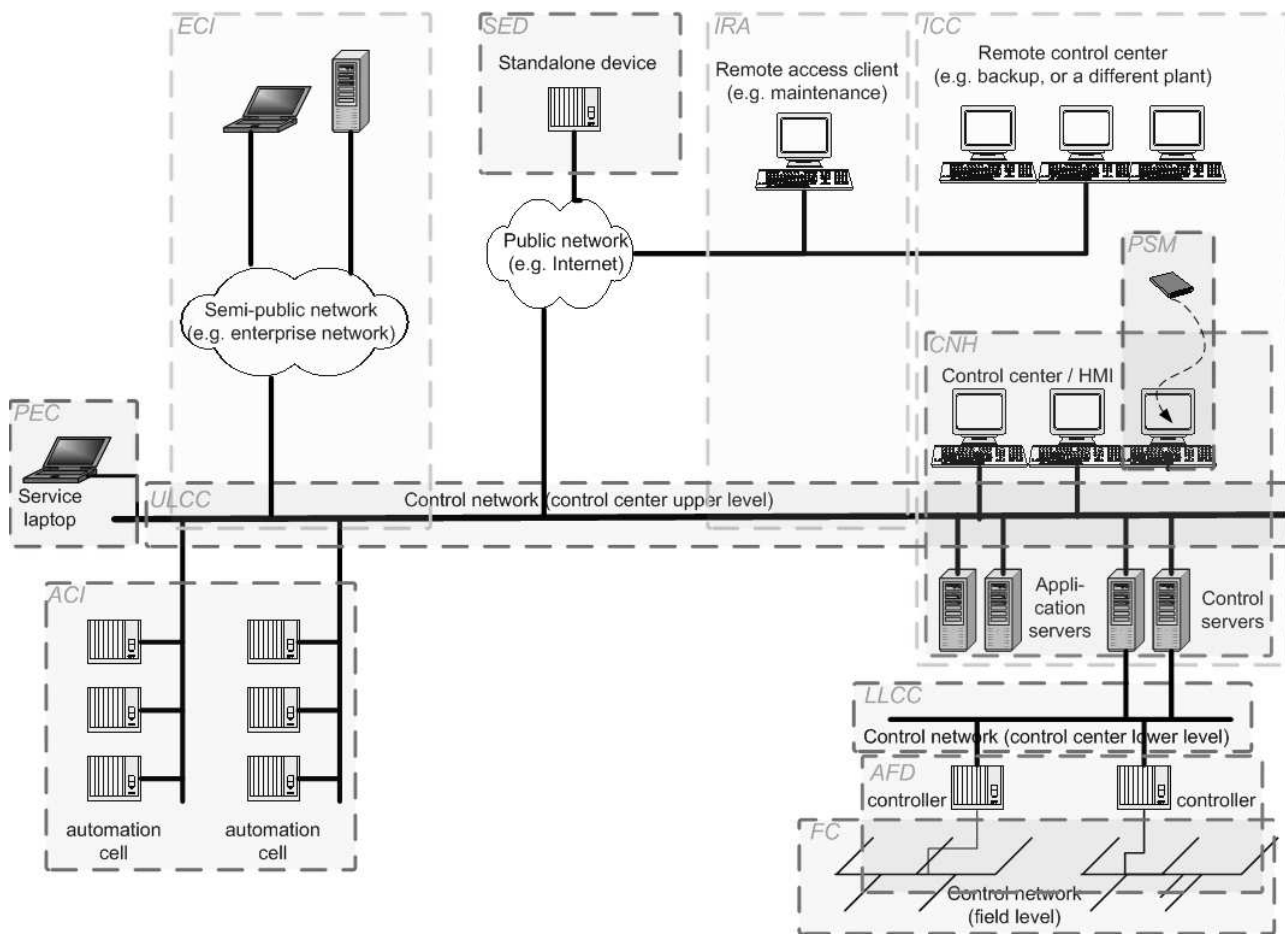


Figure 1. IEC requirement sets in [4] and their coverage of components in an exemplary networked automation systems.

Plant owning enterprise (operating role) The standard provides guidance for operation and evaluation of the technical security architecture.

Automation system vendor The standard advises on necessary capabilities and guides their testing and evaluation.

4.3 Basic philosophy

The work on the standard is governed by a number of guiding principles that are derived from the target audience and their interests as stated above:

- It addresses mainly technical aspects of the security architecture on the system level and is thus complementary to initiatives like SP99 and NERC.
- Its requirements are realizable today with commercially available technology, but it is, of course, product independent, and it allows for technology evolution.
- It captures state-of-the-art security best practices that correspond with the needs for high security. Options

for scaling the requirements down to reduced security architectures are indicated for plants where the additional risk inherent to such scale-down can be justified. The standard is open to future improvements in security technology.

- Its requirements are applicable to current as well as legacy systems.
- The measures in the standard are compatible with safety requirements. Security, safety, and automation requirements and system components are decoupled to the largest extent possible to facilitate independent evolution.

4.4 Requirement sets

The IEC approach addresses certain common communication or security scenarios in an industrial network by a collection of requirement sets:

4.4.1 External connectivity

These requirement sets deal with scenarios where a dataflow crosses the control system perimeter, either by means of a network connection or by means of a physical storage device or host that may be used alternately inside and outside the control network.

Enterprise - control net interconnect (ECI) Describes 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) Describes the security architecture for interactive remote access, e.g. for diagnosis or engineering, to parts of the control system via telephone dialup or Internet.

Inter control center connect (ICC) Describes how to secure communications over public networks between fixed control centers.

Stand-alone embedded device (SED) Describes how to secure a device that is not contained in a security zone.

Portable engineering computer (PEC) Describes how to secure portable computers that are brought into the plant and connected to the control network.

Portable storage media (PSM) Describes how to deal with threats arising out of memory sticks etc.

4.4.2 Control system internal networking

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

Upper Level Control center (ULCC) Describes network based security mechanisms in the part of the control network connected to operator workstations.

Lower Level Control center (LLCC) Describes network based security mechanisms in the part of the control network connected to controllers and SPSs.

Field Control (FC) Describes network based security mechanisms in the part of the control network connected to field devices.

4.4.3 Control system internal hosts

Control network host (CNH) Describes how to secure automation servers and workstations for operations and engineering, e.g. against attacks from insiders and malware.

Automation field device (AFD) Describes how to secure field devices and embedded controllers.

Note that this list may still change depending on both the feedback the national committees provide and the progress within the working group. The current draft contains the requirement sets ECI, IRA, and ACI.

The requirement sets are designed to be compatible and even composable both on a conceptual level as indicated in Fig. 1, and also on a technical level, e.g. by sharing parts of the architecture such as IDS or firewall devices between requirement sets.

4.5 Requirement set structure

Each requirement set contains an explanation of usage scenarios for the requirement set, a list of the threats that are addressed or are explicitly not addressed by the requirement set, a description of the network topology that the requirement set is based on, as well as the set of assumptions that are the foundation for the rationales behind each requirement. It is assumed, for example, that all networks outside the control network are untrusted, that the security architecture of the requirement sets is not bypassed, and that in addition to the technical means described in the requirement sets an administrative security management framework is in place.

The core part of each requirement set is a list of requirements. Some requirements are shared between requirement sets, others are valid only for a specific requirement set. Requirements are categorized as relating to network topology, data flows, protection of security functions, operations, and policy. There is also an indication which stakeholder(s) is/are responsible for meeting a specific requirement.

In order to allow for some scalability of the effort needed to implement a security architecture according to the standard, corresponding to different threat and risk assessments, the standard introduces the concept of Security Requirements Levels (SRLs). They indicate whether the security architecture implemented for a certain plant realizes the FULL defensive potential of the standard, a REDUCED set of mechanisms, or only LOW security efforts. Due to the fact that the capabilities of attackers are continuously increasing, it is recommended to consider the FULL SRL first and only scale down if a risk analysis, for which guidance is given in the Annex of the standard, indicates clearly that a FULL effort is not needed.

4.6 Examples for requirement clauses

The following two examples for clauses common to the external connectivity requirements sets ECI and IRA demonstrate the way how requirements are formulated and explained in [4]¹:

7.1.2.1 The firewall functions (firewall 1 between the enterprise network (EN) and the DMZ network (DN), and firewall 2 between DN and

¹The text here is slightly reformulated to provide context and expansion of acronyms that are given at separate locations in the original.

the control network (CN)) [shall; low protection: should] be deployed on different hosts or dedicated appliances.

Rationale: This requirement reduces the possibility that a vulnerability in a single host system design, e.g., on the operating system or network stack level, can be used to disable both firewalls at the same time. Also, with two firewalls it is not possible for a single configuration mistake to permit direct EN to CN forwarding and leave the CN completely unprotected.

NOTE: In addition to being more secure, a configuration with two firewalls with two network interfaces each may often be more cost efficient than a single firewall with three network interfaces needed to create the screened subnet variant of a DN, as multiple network interfaces are often only available with high-end (e.g., high throughput) firewall products.

[...]

7.1.5.5 There shall be no shared user accounts on hosts, devices, and applications that make up the DMZ, except where technically unavoidable. All such exceptions shall have a documented business justification with risk analysis and a responsible person. For all such cases procedural or technical means shall be implemented to ensure that an individual user can be proven to be accountable for any action executed under the shared account.

Rationale: Ensuring non-repudiable accountability is one of the most important measures against insider attacks. Also outside intrusions on shared accounts are less likely to be detected, as legitimate users often assume that changes that they encounter must have been created by one of the other legitimate account users.

For every requirement a rationale is provided to enable the reader to make informed trade-off decisions, and in many cases additional application notes clarify and guide implementation considerations.

5 Conclusions

This paper pointed out the expectations that various stakeholders have with regard to initiatives to standardize information system security for industrial plants. The ISA SP99, NERC CIP, and IEC TC65 activities were investigated closer as to their match with stakeholder expectations. It turns out that each of these best matches a subset of stakeholders. ISA and IEC are in their current state largely complimentary

The paper then provides more details on the IEC approach, which has a technical, scenario-oriented focus.

This approach and content has been welcomed by security experts as well as representatives from both the plant owner / end user and automation vendor communities.

References

- [1] BCIT. NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control networks, v1.4. <http://www.niscc.gov.uk/niscc/bestPractice-en.html>, Feb 2005.
- [2] E. Byres, J. Carter, A. Elramly, and D. Hoffman. Worlds in collision: Ethernet on the plant floor. In *ISA Emerging Technologies Conference, Instrumentation Systems and Automation Society, Chicago*, October 2002.
- [3] D. Dzung, M. Naedele, T. von Hoff, and M. Crevatin. Security for industrial communication systems. *Proceedings of the IEEE*, 93(6):1152–1177, June 2005.
- [4] IEC SC65c WG13. Digital data communications for measurement and control - Part 4: Profiles for secure communications in industrial networks (1st CD), April 2005.
- [5] ISA SP99. Integrating electronic security into the manufacturing and control systems environment. Technical Report ISA-TR99.00.02-2004, Instrumentation, Systems, and Automation Society, April 2004.
- [6] ISA SP99. Security technologies for manufacturing and control systems. Technical Report ISA-TR99.00.01-2004, Instrumentation, Systems, and Automation Society, March 2004.
- [7] ISO/IEC. Evaluation Criteria for Information Technology Security, version 2.1. Standard ISO/IEC 15408, December 1999.
- [8] ISO/IEC. ISO/IEC 17799, Code of Practice for Information Security Management, December 2000.
- [9] M. Naedele. Herausforderungen bei der Sicherung von Automatisierungssystemen.
- [10] M. Naedele. *IT Security for Automation Systems, in: Industrial IT Handbook*. CRC Press, 2005.
- [11] NERC. Urgent Action Standard 1200 - Cyber Security. <http://www.nerc.com/~filez/standards-cyber.html>, 2003.
- [12] NERC. Standard series CIP 002-1 to 009-1 - Cyber Security, draft 2, January 2005.
- [13] R. Oyen. Making sense of the myriad of manufacturing and control system security standards. In *ISA Expo 2005*, Oct 2005.