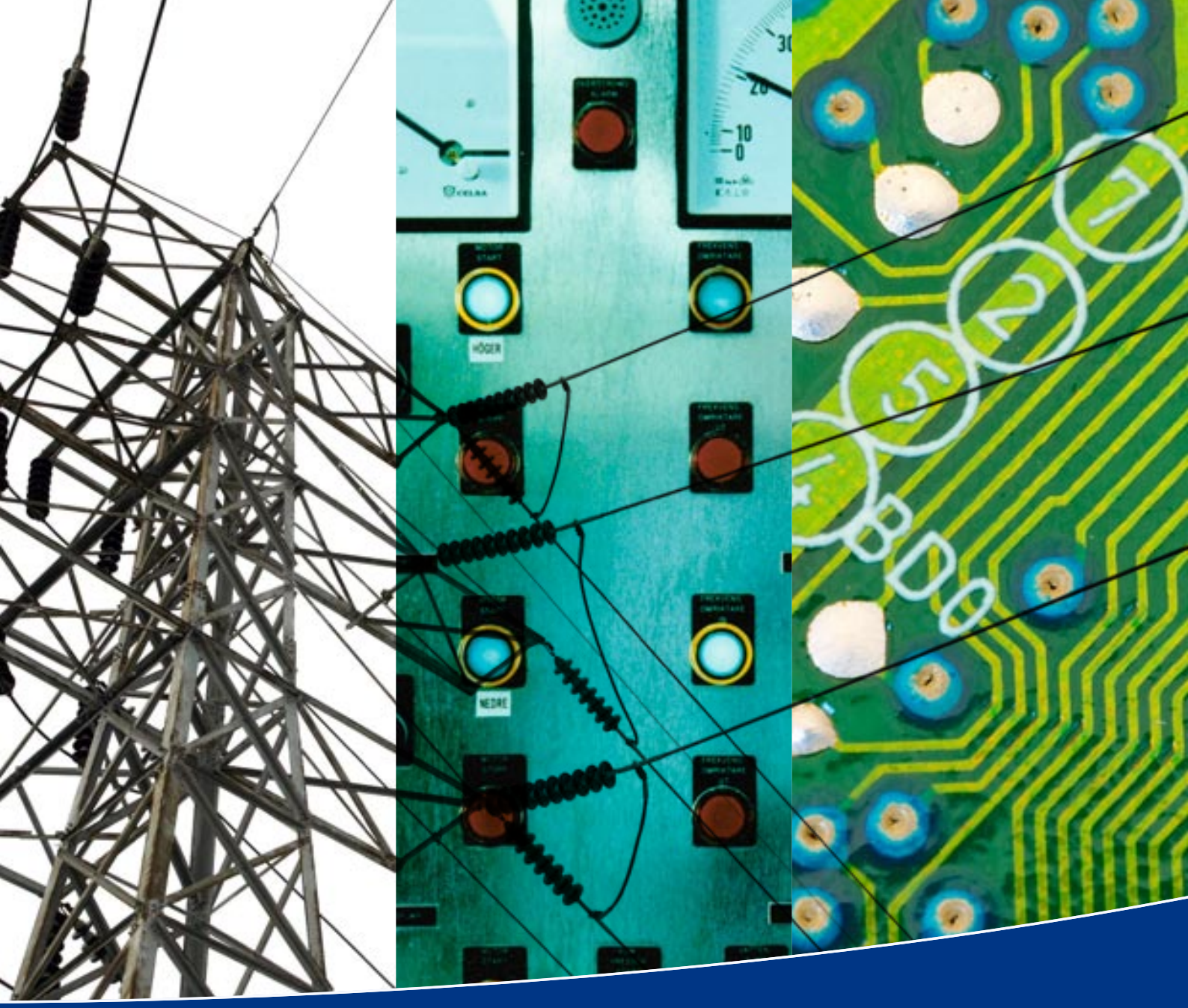


Guide to Increased Security in Process Control Systems for Critical Societal Functions

The Swedish forum for information sharing concerning information security – SCADA and process control systems (FIDI-SC)

SWEDISH EMERGENCY MANAGEMENT AGENCY

Guide to Increased Security in Process Control Systems for Critical Societal Functions

Title: Guide to Increased Security in Process Control Systems for Critical Societal Functions

Published by SEMA
Coverphoto: Ablestock, Mikael Bertmar/Nordic Photos, Ablestock
Photo: s. 7 och 39 Ablestock, s. 19 Mikael Bertmar/Nordic Photos, s. 13 Alessandro Della Bella/Keystone/Scanpix, Thomas Hernikssson/Scanpix, Kaspel Dudzik/Scanpis, Malin Hoelstad/SvD/Scanpix, Thomas Henriksson/Scanpix samt Cornelius Poppe/Scanpix
Number of copies: 300 ex

ISBN: 978-91-85797-23-3
SEMA:s dnr: 0451/2008
Design: AB Typoform

The publication can be downloaded from SEMA's web site:
www.krisberedskapsmyndigheten.se

Contents

Preface for English version

This is a direct translation of a Swedish document that is intended to create awareness of security in process control systems.

There is currently a large volume of recommendations for how security can be increased in process control systems. There are also several standardisation initiatives underway.

The reason for the Swedish Emergency Management Agency (SEMA) nonetheless choosing to produce a guide for increased security in process control systems is that information is lacking in Swedish. This has been especially desired by small and medium-sized operators of the critical infrastructure.

SEMA has directly translated the document so that it can be distributed to international collaborative partners, primarily the European SCADA and Control Systems Information Exchange (E-SCSIE).

E-SCSIE aims for European industry, government and research to benefit from the ability to collaborate on a range of common issues, and to focus efforts and share resources where appropriate. The outcome is a raised level of protection, adopted across Europe's SCADA and process control systems.

Moreover, several of the organisations in the Swedish information exchange forum FIDI-SC (see the next section), are active in various parts of Europe and can therefore benefit from an English version of the document.

This document refers to a number of established recommendations and standards. The authors want to acknowledge the important work done by all of the organisations listed on the reference list of this document. For more information, the reader is strongly encouraged to consult these sources for a more complete treatment of the subject.

Preface

Process control systems constitute a critical component of the systems that provide us with electricity, heating, drinking water, fuel and transports of persons and goods. In contrast to administrative IT systems, in which information processing in itself is often the final goal, disturbances in process control systems can entail direct disturbances in the underlying physical processes. This can ultimately lead to interruptions in the supply of critical societal services.

Today's process control systems are being made available via public networks such as the Internet to a progressively higher degree. They are increasingly based on the same technology used in common IT systems and are being integrated with administrative IT systems. Consequently, this trend entails a radically altered risk situation.

The Swedish Emergency Management Agency (SEMA) has conducted the FIDI-SC forum for increased security in digital control systems since 2005. The group's work is based on a model for trust-based information sharing developed by the British authority CPNI (Centre for the Protection of National Infrastructure).

Representatives for several sectors that use process control systems meet regularly to share information and exchange experiences. The following organisations presently participate in FIDI-SC: Banverket (Swedish Rail Administration), E.ON AB, Fortum AB, SEMA, Norrvatten, Preem Petroleum AB, Stockholm Transport (SL), Stockholm Vatten AB, Affärsverket Svenska Kraftnät (SvK), the Swedish Security Service and Vattenfall AB.

The purpose of this document is to increase awareness of the need for increased security in process control systems. The recommendations provided here are supported by the members of FIDI-SC, and work with the document has been significantly facilitated by the generous assistance obtained from the forum's members.

Guide to Increased Security in Process Control Systems for Critical Societal Functions has been prepared by Åke J. Holmgren (Information Assurance Department, SEMA), Erik Johansson (Industrial Information and Control Systems, Royal Institute of Technology) and Robert Malmgren (Robert Malmgren AB). The authors are responsible for the final content.

STOCKHOLM, OCTOBER 01, 2008

Arvid Kjell

HEAD OF THE INFORMATION ASSURANCE DEPARTMENT

SWEDISH EMERGENCY MANAGEMENT AGENCY (SEMA)

Purpose

The purpose of this document is to provide support in efforts to increase security in process control systems. Control systems are normally found in, for example, electrical and drinking water supply, the petroleum industry and rail traffic.

Security in process control systems have received considerable attention during recent years and there are now many international recommendations and practices.

This document provides fundamental recommendations for security in process control systems. The document also provides tips on obtaining additional information. The recommendations we provide are strongly affiliated with recognised recommendations, practices and standard ways of working.

The introductory portion of the document is oriented to those of you who work with security matters on the management level. This is followed by somewhat more detailed sections that are primarily oriented to those of you who work with the practical matters of security in process controls systems.

Scope and selection of references

This document addresses electronic security in process control systems and does not intend to provide generic advice on IT security matters.

We primarily refer to standards, guidelines and recommendations that can be generally implemented to create increased security in process control systems. We have given preference to references that we have assessed as not being sector-specific. The selection of reference documents is also limited to Swedish and English documents that as much as possible, are freely available via the Internet.

The document consists of three parts:

Part A

Prerequisites and general recommendations

Part B

Detailed guidance concerning recommendations and established guidelines

Part C

Reference list with comments

Additional information

The document will be periodically revised and comments regarding the content are welcome.

Contact FIDI-SC and the Swedish Emergency Management Agency at the following e-mail address:
`scada@kbm-sema.se`

Part A

Prerequisites and general recommendations

Process control systems

Critical societal functions, such as the distribution of electricity and drinking water, district heating and rail traffic, are dependent on computer-based systems for supervision, regulation and monitoring of the central physical processes.

There are a number of more or less overlapping designations for these computer-based supervision and control systems. Here we use the designation process control systems, but the systems are also referred to as SCADA (Supervisory, Control and Data Acquisition), digital control systems, industrial information and control systems, process IT, technical IT systems, distributed control systems, real-time embedded systems (RTE) and so forth. In certain respects, there are technical differences, but we do not always emphasise these.

Figure 1 shows the principle structure of a control system. The underlying physical process can contain a very large number of measuring points that can be dispersed over large geographical areas. The process interface, meaning the method of communicating reality, is primarily constituted by sensors for monitoring and actuators for control (control equipment).

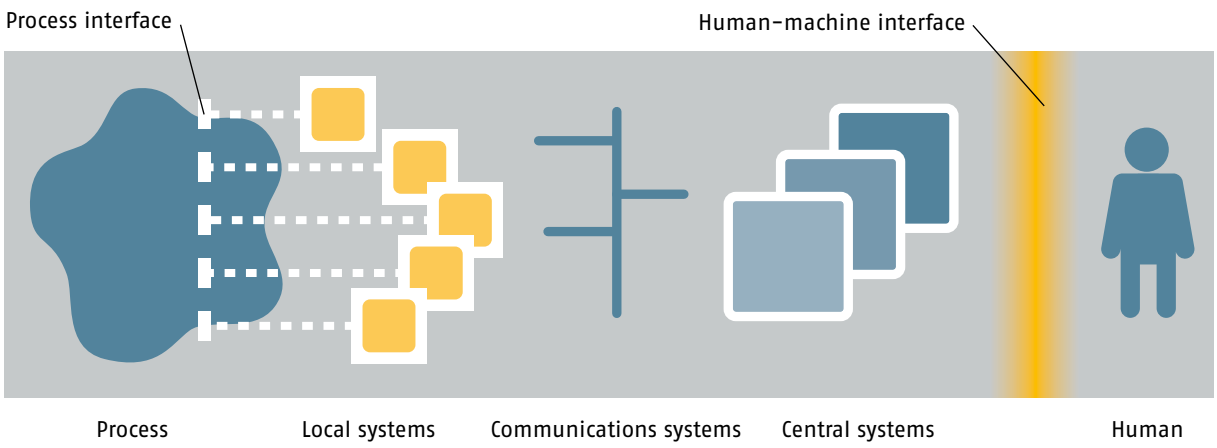
The local system that gathers signals from sensors and transmits control signals to the control equipment contains increasing numbers of functions and can often even seem independent during, for example, interruptions to communications with the central system. The local units often have both analogue and digital inputs and outputs, and the distinctions between various types of units – such as IEDs (Intelligent Electronic Devices), PLCs (Programmable Logic Controllers) and RTUs (Remote Terminal Units) – are becoming increasingly vague.

Important functions, for example, those that require substantial computational capacity and data from many different parts of the process, can be realised in one or more central systems. Data can also be stored here, and during peak loads, central units determine which system functions will be prioritised.

Communications between the various parts of a control system can be conducted in many different ways, via both unbound media (such as wireless networks) and bound media (such as fiber optics and telecom networks).

To present data and interact with a system, a human-machine interface is required. Some of the most important application areas for these system components are commissioning of the system (defining process data and functions), operation of the process (con-

Figure 1: Schematic structure of a digital control system [the figure is modified from Cegrell and Sandberg (1994)].



trolling and monitoring) and maintenance of the control system (changing and updating the system).

We can summarise the most important functions of digital control systems with the following points:

- **Data collection** (data storage, conversion and scaling, time stamping, feasibility assessment and so on)
- **Monitoring** (status monitoring, trend monitoring, limit value monitoring, performance monitoring, event and alarm management, and so on)
- **Control** (direct control, set point control, sequence control and so on)
- **Planning and follow-up** (non-real-time-critical functionality; planning, logging and history, follow-up and analysis, and so on)
- **Maintenance and change** (putting in and removing from service, upgrading, management of development environments and so on)

MORE INFORMATION

Boyer, S. A. (2004) *SCADA: Supervisory control and data acquisition.* The Instrumentation, systems, and automation society (ISA), Research Triangle Park, N.C.

Cegrell, T. & Sandberg, U. (1994) *Industriella styrsystem.* SIFU förlag, Borås.

Why is security in process control systems important?

Below are a number of observations that all point to the need for increased attention to security in process control systems. The observations are not listed in any order of priority and they overlap one another to a certain extent.

Critical societal functions are dependent on process control systems

Process control systems constitute a critical component of the systems that provide us with electricity, heating, drinking water, fuel and transports of persons and goods. In contrast to administrative IT systems, in which information processing in itself is often the final goal, disturbances to communications, computers systems or applications in process control systems can entail direct disturbances in the underlying physical processes. This can ultimately lead to interruptions in the supply of critical societal utilities.

Integration between process control systems and administrative information systems is dramatically increasing

Process control systems may previously have satisfied high security demands through isolation from the surroundings and good physical security. Today's demands on process orientation from a business perspective are leading to increased integration between process control systems and administrative IT systems, such as systems for asset management and billing. To achieve high flexibility and efficiency, process control systems are increasingly being made accessible via the Internet and other public networks. This integration is exposing the process control systems' vulnerabilities to the threats that exist, for example, on the Internet.

Process control systems are modernised slowly and entire systems are seldom replaced at the same time

Process control systems are included in system solutions with long service lives and can contain technical solutions from several generations of control systems (so-called legacy systems). Once installed, the intention is that a control system will maintain high availability and a good level of functionality for many years. In many organisations, there is therefore reluctance to change system settings, system components and similar items in commissioned equipment, in other words, after a system has been put into daily operation. This can lead to them not eliminating known IT security holes or it taking a very long time for this to be done.

Use of standard components are changing vendors' roles and increasing demands on users

The vendors of process control systems have traditionally most often functioned as comprehensive vendors, meaning that they have both designed and built the systems they have provided. These days, increasingly standardised technologies and components from the traditional IT world (often referred to as COTS, Commercial-Off-The-Shelf) are used in process control systems. A few examples of COTS products used are the operating systems from Microsoft, IP-based communications technology and database solutions from Oracle. Due to the switchover to standard components, the vendors' role is shifting from system vendors to system integrators. This in turn can lead to them attaining less insight and control of important components in the integrated systems. Subsequently, increased knowledge is needed of security in the digital control systems utilised by end-users of the systems.

Cyber-attacks against process control systems constitute a credible threat

Electronic security has not been a determining factor in development of process control systems. Security awareness on the part of both vendors of equipment, systems and software, and buyers is often weak. This entails that requirement specifications can be deficient and that security systems are not designed to handle security in a suitable manner. There are presently sophisticated tools for launching IT attacks freely available via the Internet. Now that process control systems are being connected together into networks to an escalating degree and are increasingly built with standard

IT components, there is a progressively greater risk for being subjected to cyber-attacks.

Process control systems have good availability – standard IT security problems can lead to operational disturbances

Because process control systems are used to monitor and control physical processes in real-time, the systems have been developed to maintain very high availability. Traditionally, IT security problems such as malicious code or computer intrusion in a process control context can entail impact on the control systems' availability and their operational security aspects. For example, a virus-inflicted system can have unacceptable response times. This in turn can lead to gathered values, alarms or commands not being received in the way intended by the original designer.

Work with security in process control systems leads to cultural conflicts in security organisations

To achieve high security in process control systems, it is necessary to have both knowledge of traditional IT security as well as knowledge of process control systems and the underlying physical processes. Proactive security work therefore requires collaboration between persons from different cultures, with different security traditions and organisational domiciles. Traditional IT security knowledge cannot be directly transferred to process control systems. Many newly produced documents with security tips express themselves in terms, or provide recommendations, that can be difficult to apply directly to control equipment. To harden a system – meaning the removal of unnecessary, unknown or unused software, and improving the configuration of used software – is a very difficult task in a control system used in production. It is often impossible to achieve – for both technical and legal reasons – other than by the system vendor, after careful evaluation, making these changes.

Attention to security in process control systems is constantly increasing and this is leading to external security requirements

Several international initiatives are now underway to develop standards and recommendations for how security is to be established in process control systems. The field has even received considerable attention from many government entities. By conducting proactive security work now, users and vendors of process control systems can actively influence which security requirements will be placed on these systems in the future. It can even be a competitive advantage to implement systematic security work. In certain branches, there are already established security requirements. In the US, for example, power utilities are expected to comply with the NERC CIP standard.

Security in process control systems is profitable, but it requires a good security culture and a long-term commitment

Security in process control systems is not primarily a technical problem. It chiefly concerns attaining a good balance between risks and costs in an organisation. Building up a security culture adapted to handle present-day IT related threats is a long-term transitional process that organisations must conduct with the support of top management. There are, however, major benefits with handling security issues in advance. Just as for traditional IT systems, it is much more expensive to correct security problems in process control systems after the systems have been delivered. The increased integration between administrative IT systems and control systems, however, does not just entail increased security problems. Increased integration can also provide higher efficiency and improved profitability, thanks to better-optimised production processes.

MORE INFORMATION

Johansson, E., Christiansson, H., Andersson, R., Björkman, G. & Vidström, A. (2007) *Aspekter på antagonistiska hot mot SCADA-system i samhällsviktiga verksamheter.* (in Swedish). Swedish Emergency Management Agency, Stockholm. The report can be downloaded from: `www.krisberedskapsmyndigheten.se/upload/SCADA_studie%20_070903.pdf`

Shaw, W. T. (2006) *Cybersecurity for SCADA systems.* PennWell Corp., Tulsa.


SJ
1348
1348


BIOGAS

Difference between administrative IT systems and process control systems

Despite increasing convergence between administrative IT systems and process control systems, there are still many significant differences. Some of the most important are summarised in Table 1. Compare these with the observations we presented in the previous section.

To create security in process control systems, good knowledge of their respective characteristics is required. It is, however, very important to keep in mind that many well-known IT attacks, conceptual attack methods and various alternatives for misusing IT systems – that are classic or standard in administrative IT environments – also work in digital control systems.

MORE INFORMATION

NIST (2007) *Guide to Industrial Control Systems (ICS) Security.* SP 800-82, National Institute of Standards and Technology (NIST), Gaithersburg. The report can be downloaded from:
`http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf`

Table 1: Significant differences between administrative IT systems and process control systems [table modified by the authors from NIST (2007)]

Categories	Administrative IT systems	Process control systems
Performance requirements	Not real-time	Real-time
	Response must be consistent	Response is time-critical
	Stringent demands on throughput speed	Moderate throughput speed acceptable
	Delay and jitter can be acceptable	Delay and jitter are serious problems
Availability requirements	Response in form of restart is acceptable	Response in form of restart can be unacceptable due to availability requirements in industrial processes
	Availability deviations can often be tolerated, depending on the system's operational requirements	Disturbances must be planned and scheduled days/weeks in advance
Risk management requirements	Data secrecy (confidentiality) and correctness (integrity) are most important	Safety is most important, both in regard to people and production systems
	Fault tolerance is less important – temporary shutdown is usually not a serious risk	Fault tolerance is very important; even shorter shutdowns are unacceptable
	The greatest risk is in disturbances to business operations	Greatest risks involve loss of life, process equipment or production capacity
Security architecture	Primary focus is on protecting computer-related assets and information that is stored or transmitted	Primary focus is on protecting terminal equipment (such as control equipment and PLCs)
	Central servers may require extra security	Protection of central servers is still important
Security solutions	Security solutions are designed for typical IT systems	Security tools must be tested to guarantee that they do not jeopardise the control system's normal operations

Categories	Administrative IT systems	Process control systems
Time-critical interaction	Less critical with interaction during emergencies	Response to human or other interaction during emergencies is critical
	Access to system resources can be limited and controlled to the desired degree	Access to control systems should be strictly regulated – may not disturb human-machine interaction (especially important during emergencies)
System operation and change management	The systems are designed to use standard operating systems	Specific and specially adapted operating systems and standard operating systems
	Upgrading is simple and is performed in accordance with security policies and routines – automatic tools are available	Upgrading of software should be conducted in steps and often requires participation by system vendors, for example, due to modified hardware and software
Resource limitations	Sufficient system resources are available for supporting addition of third-party applications (security solutions)	The systems are designed specifically for industrial processes – memory capacity and computational resources can limit security solutions
Communications	Communications protocols of standard types	Many proprietary communications protocols (commercial), but also standard protocols
	Primarily landline networks and local wireless networks	Many different types of media for communications, such as fiber optics, radio links, satellites (even private networks)
	Communications networks are built on typical IT network practices	Communications networks are complex and demand technical knowledge of control systems
Support	Many different variants and vendors	Usually only a few vendors
Service life	Components and systems have short service lives (typically 3–5 years)	Components and systems have long service lives (typically 15–20 years)
Physical access	Components are usually locally installed and easy to access	Components can be isolated, geographically distant and difficult to access

Good security culture – a basic requirement

To establish smoothly functioning activities for security in process control systems, an organisation requires a good security culture, meaning functioning general risk management and work with systematic information security. Figure 2 below illustrates the relationships between the activities that should be included in systematic risk management.

The recommendations that we provide in this document comply with ISO's information security standards (27000 series), such as the management model for information security presented in ISO/IEC 27001 (ISO, 2005).

There are very many analysis methods for risk analyses of IT systems. The Swedish Emergency Management Agency has issued BITS, for a basic level of information security, and an associated tool for information security analysis (BITS Plus). BITS and BITS Plus make it easier to initiate information security work in organisations and subsequently implementing, for example, the ISO standards above. Another example is the American agency NIST's report SP 800-30, which describes a general model for risk analysis of IT systems (NIST, 2002a). Furthermore, NIST's report SP 800-34 gives special attention to contingency planning in IT systems (NIST, 2002b).

At present, there are no established risk analysis methods that the authors are aware of that specifically address IT security in process control systems.

MORE INFORMATION

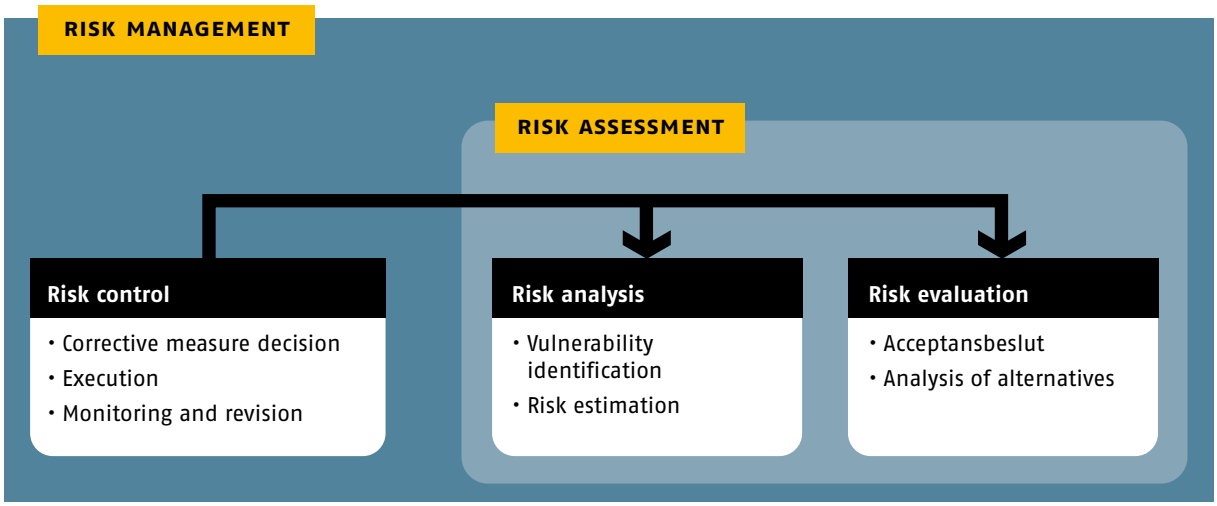
IEC (1995) *Dependability Management – Part 3: Application Guide – Section 9: Risk Analysis of Technological Systems.* International Electrotechnical Commission (IEC), Geneva.

ISO (2005) *Information technology – Security techniques – Information security management systems – Requirements.* ISO/IEC 27001:2005, International Organization for Standardization (ISO), Geneva.

NIST (2002a) *Risk Management Guide for Information Technology Systems.* SP 800-30, National Institute of Standards and Technology (NIST), Gaithersburg. The report can be downloaded from:
`http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf`

NIST (2002b) *Contingency Planning Guide for Information Technology Systems.* SP 800-34, National Institute of Standards and Technology (NIST), Gaithersburg.The report can be downloaded from:
`http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf`

Figure 2: Risk management [the figure has been modified by the authors from IEC (1995)]



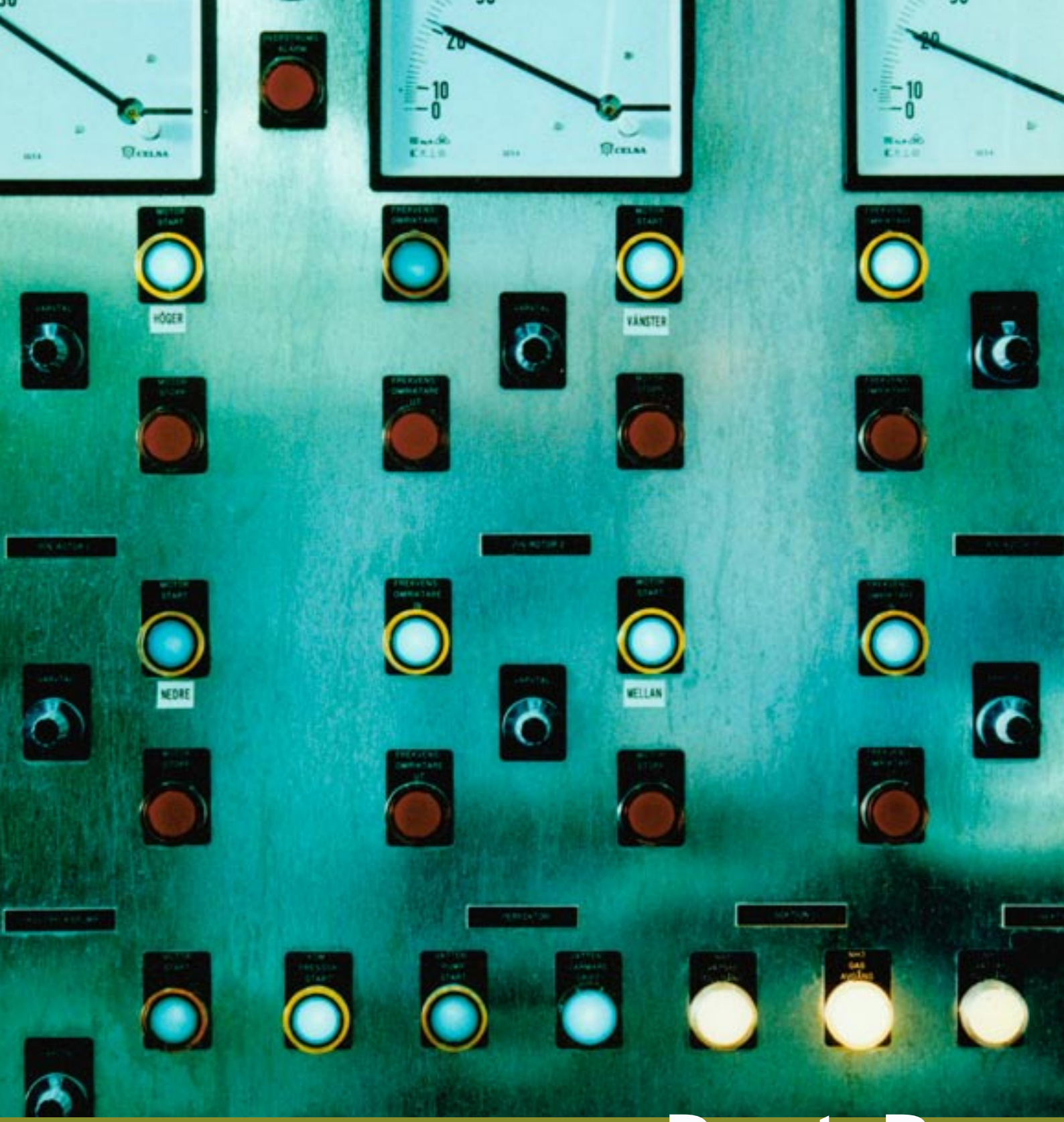
Summary of recommendations for increased security in process control systems

In Part B, we provide more detailed guidance regarding recommendations and established guidelines. Here in Part A, we summarise the most important recommendations.

The selection is based on discussions within FIDIS-SC and experiences from practical projects in which the authors have participated. It also has support in international recommendations and in well-known practices.

The following recommendations constitute the first step in work to increase security in process control systems.

1. **Increase awareness throughout the organisation of the need for security in process control systems.**
   This is a mission-critical matter and top management should therefore become involved at an early stage.
2. **Conduct fundamental training concerning security in process control systems.**
   Operators of control systems need to increase their knowledge of traditional IT security. IT personnel need more knowledge of process control systems and underlying physical processes. Persons who are involved in procurement and operational planning also require training in these matters.
3. **Keep process control systems separated from administrative IT systems as much as possible.**
   Survey existing process control systems and identify external connections to them. Process control systems should only be integrated with administrative IT systems in exceptional cases. Very advanced logic separation of the systems is required.
4. **Place security requirements in all procurements of process control systems and in service agreements.**
   There are major benefits to be gained by handling security matters in advance. Just as for traditional IT systems, it is much more expensive to correct security problems in process control systems after the systems have been delivered.



Part B

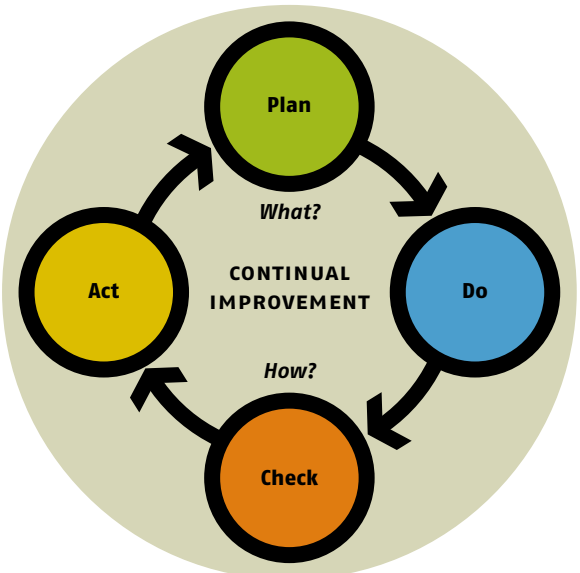
Detailed guidance concerning recommendations and established guidelines

Basis for recommendations

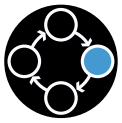
In this section, we provide recommendations for increasing security in process control systems. The selection of recommendations is based on discussions within FIDI-SC and experiences from practical projects in which the authors have participated. They also have support in international reports and in well-known practices. The recommendations are not listed in any order of priority, and in certain respects, they overlap one another.

The activities that we suggest in the following recommendations are a part of routine work with quality. To clarify the importance of the activities being a part of continual work with improvements we relate them to the well-known Deming Cycle (Figure 3), also referred to as the PDCA model (plan, do, check, act). The PDCA model is applied in several international standards, such as the ISO/IEC 27000 series on management systems for information security. The goal is that an organisation's work with security in process control systems will in this way be able to attain a natural connection to other work with information, security and quality.

Figure 3: We use the PDCA model (Deming Cycle) in this document, both to emphasise the importance of work leading to continual improvements, and to structure the recommendations.



The plan phase
concerns establishing policies, goals, processes and routines.



The do phase
concerns implementing and carrying out policies, measures, processes and routines.

The check phase
concerns monitoring and auditing by assessing, measuring and reporting.

The act phase
concerns maintaining and improving – in other words, taking corrective measures for improvements.

In the following section, we provide tips on where more information can be found. The established guidelines and standards that we refer to are described in more detail in **Part C**. They are briefly described below as follows:

NERC CIP	Cyber security standard CIP-002-1 – 009-1
NIST 800-82	Guide to industrial control systems (ICS) security
CPNI GPG	Good practice guide process control and SCADA security
DOE 21 Steps	21 steps to improve cyber security of SCADA networks
OLF 104	Information security baseline requirements for process control, safety, and support ICT systems
PL	Cyber security procurement language for control systems

Recommendations for increased security in process control systems

01 Clarify roles and responsibilities for security in process control systems.

02 Establish a process for surveying process control systems and for conducting risk analyses.

03 Establish a process for change management in process control systems.

04 Establish a process for contingency planning and incident management in process control systems.

05 Include security requirements for process control systems in all planning and procurement from the start.

06 Create a good security culture and heighten awareness of the need for security in process control systems.

07 Create a multilayer defence (defence-in-depth) in process control systems.

08 Implement around-the-clock internal and external intrusion detection and incident monitoring in process control systems.

09 Conduct risk analyses of process control systems.

10 Conduct periodic technical security audits of process control systems and connected networks.

11 Constantly evaluate physical security of process control systems.

12 Ensure that only secure and relevant connections to process control systems exist.

13 Harden and upgrade process control systems in collaboration with system vendors.

14 Follow up incidents in process control systems and monitor external security problems.

15 Collaborate in user groups, standardisation organs and other networks so as to increase security in process control systems.

01 Clarify roles and responsibilities for security in process control systems

NERC CIP (003-1) **NIST SP 800-82** (Kap. 4.2, 6.1, 6.2) **CPNI GPG** (GPG 4, GPG 7)
DOE 21 Steps (No. 12, 16, 20) **OLF 104** (No. 1, 3)

In many organisations, process-oriented control is common when it comes to administrative information systems. In this management model, there are often designated system owners, information owners, administrative managers, operations managers, system administrators or similar positions.

For control systems, this allocation of roles and responsibilities is often nonexistent, meaning that both areas of responsibility and management models are lacking. In the absence of IT technicians and system administrators, vendor representatives sometimes constitute the sole source of technical support. Moreover, systems may be administered by process engineers who have no knowledge of electronic security in control systems. This leads to an organisation having little or no knowledge of the IT technical properties of its process control systems. Subsequently, there will be reduced control and ability to manage the technology and its usage.

The allocation of responsibility for these security matters are most easily clarified by creating a *security policy for process control systems*. This policy can be in the form of a separate document, either which in such case must be related to the organisation's other policy documents, or as supplements to the organisation's information security policy.

Role and responsibility allocation for the administrative information systems and control systems should be coordinated. There should be clarification of which systems the organisation's central IT support administers and of which systems are administered locally by production. How this is accomplished on a purely practical level is related to how the organisation chooses to implement protection and layers of protective barriers in its overall IT environment. Even if a large portion of the systems closely related to processes are administered locally, the organisation's central IT support must be responsible for overall integration and establishment of a uniform approach to security matters. An important reason for a *uniform approach to the organisation's information security* being required is that it is becoming increasingly common with extensive data exchange between control systems and administrative systems.

Example of risks and problems

If no one is appointed as the system owner, system coordinator or system administrator for a control system, it is unlikely that routine security tasks – such as software updates or blocking of accounts of former contractors – will be conducted, or if they are conducted, that they will be performed punctually.

If a system is infected by malicious code, for example, no one feels responsible or knows which authorisation they have in dealing with the incident. This can delay efforts to limit the damage and result in operations being affected more than necessary.

02 Establish a process for surveying process control systems and for conducting risk analyses

NERC CIP (002-1) **DOE 21 Steps** (No.13) **OLF 104** (No. 2, 3, 11)

To create security in process control systems, it is important that there is an established process for surveying and understanding an organisation's information flows and system dependencies, meaning the existing connections between the various types of systems and operations.

It is crucial that an organisation's processes, systems and information analyses are based on an understanding of the consequences that a faulty or disrupted function can entail, both for processes and the organisation. This is an important prerequisite for creating a relevant risk evaluation and a classification of the systems and information that are most critical.

An organisational and system survey should result in lists of access and connection possibilities, system classifications and operational prioritisation categorisations. There should be diagrams available of the process controls systems with a sufficient degree of detail to enable identification of critical components and systems. Examples of information that should be included in system diagrams are information about operating systems of computer resources, IP addresses, communications protocols, technical information about local units such as PLCs and so forth. To be able to establish an electronic security perimeter, all connections to process control systems must be identified. Included here, besides intranets, are remote connections to collaborative partners, vendors and to the Internet, for example. Note that all wireless connections should be treated as remote connection points. Connections to the organisation's administrative information systems (intranets) should be considered as external connections.

The organisation's critical assets should be identified by applying a risk-based approach. Based on this analysis, critical cyber-based assets are identified. This requires that there is a documented process for how risk analyses are to be conducted and under which conditions they shall be updated. The choice of risk analysis method should be adapted to the purpose of the analysis and the available information. To make it easier to update a risk analyses, do not choose an unnecessarily advanced risk analysis method.

Example of risks or problems

If an organisation lacks a standardised process for risk analysis and surveys of process control systems, it will be more difficult to compare and monitor how the organisation's risks change with time.

If an organisation also lacks an adapted risk assessment, this can entail that important process control systems are unprotected. Unnecessarily larger resources will then be put into protecting other information resources that are not critical to the organisation's continued existence.

03 Establish a process for change management in process control systems

NERC CIP (003-1) **DOE 21 Steps** (No. 17) **OLF 104** (No. 10, 15)

Controlled management of changes and versions of parameter configurations, settings and data files or programs is important for avoiding disruptions, unnecessary troubleshooting or serious problems in digital control systems. Systems and applications that organisations will use for a longer period in industrial processes, for example, entail special requirements for strict control of change management.

Upgrading of software should be conducted in steps and often requires the participation of system vendors, due to both legal and technical stipulations. In process control environments, it is important that all involved parties – vendors, system managers and users – have a correct and common understanding of the system's current configuration and operational status. Separate testing, development and operating environments are common for administrative IT systems. Unfortunately, this does not apply to process control systems. Additional financial resources can therefore be needed to create the conditions for good change management in these systems.

There should be a formal process that specifies how authorisation to make changes in process control systems is to be granted. No changes should be permitted without formal authorisation. This should even apply to temporary changes and changes to support equipment. To maintain good security in critical systems, in principle, everything that is not explicitly permitted should be forbidden.

The formal process for change management should at least include a procedure for granting authorisation to make changes, a description of how tests before and after a change are to be conducted (including a description of the changes that require testing in separate test environments), requirements for how documentation is to be updated after changes, as well as requirements for how personnel are to be informed of changes (for example, in cases that require special operator training).

Examples of risks or problems

A vendor verifies changes in a test system that differs from a customer's actual system in respect to installation. When the changes are later implemented in the system used in production, unexpected system events occur and the process control system becomes unstable.

The vendor has not been notified of local changes in a control system. After the next program update, functionality is lost, corrections to security problems disappear and parameters revert to the default factory settings.

Process control systems often have a more static software status than information systems, and periodic backups are therefore not conducted as often. Backups are sometimes only made during system commissioning or upon larger changes. There is therefore the risk that changes will be lost and re-implementation overlooked in conjunction with any reinstallations from a backup copy.

04 Establish processes for contingency planning and incident management in process control systems

NERC CIP (008-1, 009-1) **NIST 800-82** (Kap. 6.2.3) **CPNI GPG** (GPG 3)
DOE 21 Steps (No. 19) **OLF 104** (No. 7, 16)

To ensure an organisation's continued existence in the event of serious disturbances, contingency planning is necessary that includes clear descriptions of roles and responsibilities during emergencies. Examples of such disturbances are blackouts, control system failures, illnesses to key operative personnel and so forth.

Besides continually following up and updating contingency plans, it is important that personnel have the opportunity to take part in preparedness training exercises and that tests are regularly conducted to ensure that operations can function satisfactorily in the event of an emergency. For process control systems, it is especially important to ensure that backups are made and can be used to restore the systems. A few important points that should be included in contingency planning are:

- Routines for handling operations manually (conducting processes without computer support)
- Routines for restoring data and configuration settings, and the restarting process
- Contact information for operators, service technicians, other personnel, vendors and support
- Description of how central components in control systems can be replaced
- Description of how and from where, emergency operations are to be conducted if the disturbance is serious

All unexpected events that lead to disturbances occurring in process control systems, such as a service becoming unavailable or having reduced functionality, must be documented for later analysis. One of the difficulties of incident management is in determining a balanced structure for how incidents are to be reported without this being perceived as obstructive to the normal work process. Furthermore, it is important to motivate the organisation by communicating the purpose of reporting incidents and to inform of the results of incident management. Without this communication, it can be difficult to maintain motivation for reporting incidents and weaknesses.

Examples of risks or problems

An organisation is affected by a major disturbance and forced to completely restore a mission-critical process control system. Regular backups have been made of the system, but the backup tapes have not been handled in an appropriate manner. They have thus aged to the point that restoration is impossible.

The person responsible for the process control systems in an organisation passes away while on vacation. The chief problem is that no one in the organisation can assume his duties. It is later discovered that he was also the only one who knew the most important passwords for certain system change capabilities, and how some of the central systems were configured.

05 Include security requirements for process control systems in all planning and procurement from the start

NIST 800-82 (Kap. 6.1.3) **CPNI GPG** (GPG 6) **OLF 104** (No. 8, 9) **PL** (Alla kapitel)

It is very important that an organisation's security matters are included in planning as early as possible.

It is difficult and expensive to achieve an acceptable level of security in process control systems after implementation. Security requirements should be included from the very beginning in system specifications and need analyses. Because many system solutions are fully or partially procured from external parties, special attention to security is necessary during procurement.

Security in process control systems should be expressly addressed in procurement documentation, testing and transfer management, contracts, and steering documents for maintenance or service undertakings. Procurement can encompass both new installations and full or partial modernisation of existing solutions. Security requirements should therefore be incorporated as an important element in all vendor agreements, including service and maintenance agreements. A good technical aid in all control system procurements is the Cyber Security Procurement Language for Control Systems (PL).

In conjunction with modernisation of process control systems, special consideration is required to IT security matters. This is because the changes will most likely affect existing control systems in a way that the original designers had not considered. For example, it was often assumed in older control systems that access to equipment would only be possible via local physical presence. Today, however, physical separation is no longer possible in many situations. It is instead a matter of creating logic separation between various parts of the process control systems.

Requirements gathering should be conducted in the form of various surveys, and threat and risk analyses. Besides complying with detailed requirements for security and protective functions in systems and applications, vendors should be able to present their methods and processes (such as in internal developer handbooks) used to guarantee the quality of their work with security.

Examples of risks or problems

Neglected security requirements during procurement lead to expensive supplemental orders, and poorly designed and overly complex security solutions after implementation.

Overlooked security requirements during procurement can entail that a process control system is unnecessarily vulnerable throughout its entire life cycle.

06 Create a good security culture and heighten awareness of the need for security in process control systems

NERC CIP (004-1) **DOE 21 Steps** (No. 21) **OLF 104** (No. 5)

It is important to establish an understanding that security in process control systems is a mission-critical issue. Understanding and influencing attitudes requires long-term effort, and top management's engagement is, as always when it comes to security matters, very important. This is due both to security in process control systems requiring increased resources, and to collaboration being necessary between parts of the organisation that do not normally collaborate.

To achieve high security in process control systems, it is necessary to have both knowledge of traditional IT security and of process control systems, as well as the underlying physical processes. Proactive security work therefore requires collaboration and trust between persons from different cultures, with different security traditions and organisational domiciles. This demands periodic instruction and training, both of IT personnel and of control system operators.

Process control systems are incorporated in system solutions with very long service lives. It is especially important to try to imagine how the systems will be used, or misused, in the future. Due to ignorance or unclear routines, many normal activities can lead to potential security problems.

Organisations should establish administrative security programs to create a general approach to IT. This provides good security awareness, encourages critical thought and creates a positive attitude to work with matters that improve security.

Examples of risks or problems

During a low-activity period in a routine operational situation, an operator is using an operator's computer to watch a sporting event via the Internet (streaming audio and video broadcasts). At the same time, he is chatting with a friend via IRC. This leads to the operator's computer being infected by spyware, which subsequently renders the computer unusable.

A few service technicians are working with a vendor's field personnel at a facility in the production system and unexpectedly need to transfer software and data between two different IT environments. Data is normally moved between these networks via a special removable hard disk. To avoid having to go for the hard disk, they run a network cable between the two computers in the otherwise separated networks. At the end of the working day, they forget to remove the network cable and the operator who normally uses the computer thinks that the cable is to be left in place. The process control system is now no longer physically separated, but is instead directly connected to the company's intranet. Because the control system has always been physically separated, the organisation has not found it necessary to install any IT security mechanisms.

07 Create a multilayer defence (defence-in-depth) in process control systems

NERC CIP (005-1, 007-1) **CPNI GPG** (GPG Firewall Deployment) **DOE 21 Steps** (No. 5, 15)
OLF 104 (No. 4, 13) **PL** (Alla kapitel)

A fundamental principle for protecting modern IT systems is to configure defence-in-depth, meaning the use of multiple layers of security and overlapping security mechanisms. The security mechanisms can be of the same type, such as multiple firewalls. They can also consist of various types of complementing security mechanisms, such as a firewall as network security protection, combined with strong authentication for access to the IT system.

A strong force in all types of organisations is the push to attain increasingly efficient information handling. This entails, among other things, connecting together information systems in such a way that duplication of work is avoided – it should not be necessary to manually enter information in an IT system in another system. Older process control systems, or digital components that are in process environments, have often been developed in a time when physical security was all that was needed. Electronic security was unheard of. Known deficiencies and vulnerabilities that were corrected in administrative IT environments several years ago, usually remain in process control systems. Interconnecting various networks can therefore expose process control systems to threats for which they lack protection, and all external connections to these systems entail substantial risks. A basic risk analysis should therefore precede integration of control systems and administrative IT systems. Interconnection of systems requires IT security of extremely good quality.

A task that must be conducted sooner or later is the creation of an electronic security perimeter around process control and operational systems. On a conceptual level, it is important to be able to differentiate between that which digitally constitutes a system landscape and the other systems within an organisation.

Process control systems should be divided into several different zones with security levels that are adapted to how critical the various systems are. This means that the network architecture should be segmented with overlapping security mechanisms, and non-secure services and connections should be placed in a so-call demilitarised zone (DMZ).

Data exchange between digital control systems via a DMZ to other external systems, such as business systems, should be conducted in a limited and controlled manner. Outgoing communications from control systems to business systems should be limited in regard to services and ports. It can even be appropriate to use different communications protocols for communications between different parts of a network. If a protocol is used for communications between the control system and a DMZ, another protocol should be used for further communications between the DMZ and the organisation's administrative IT systems.

Communications within a control system may also require protection. Communications between field equipment, such as PLCs, and local systems are usually based on industrial protocols with low or non-existent security.

Examples of risks or problems

Because it has been realised that "security by obscurity" (security through misrepresentation or concealment) is not a viable security solution, an organisation implements an electronic security perimeter that is believed to be strong and all-embracing. An employee connects a workstation to the Internet via a non-secure connection and thus creates a hole in the perimeter security. Once into the system, there are no security mechanisms (no defence-in-depth) that can prevent malicious code, or a hacker, from causing extensive damage.

It is important to attain a balance between how much work and resources that are expended on physical and electronic security. It is easy to opt for physical security – such as backups of computers or a steel door – at the expense of electronic security, which is much more abstract. A mental error in physical security can lead to both primary and secondary systems being affected by digital problems, such as a broadcast storm on the network, or a physical problem, such as hardware failure in a central network component.

08 Implement around-the-clock internal and external intrusion detection and incident monitoring in process control systems

NERC CIP (005-1) **DOE 21** Steps (No. 8)

In contrast to incident follow-up (open source intelligence) and updating of risk analyses, intrusion detection and security monitoring are intended to analyse attack attempts against one's own organisation. Open source intelligence combined with good monitoring of own systems and their communications provide a good overall understanding of threat assessments, such as altered attack trends and current malicious code.

There are two types of intrusion detection systems (IDS). There are systems that recognise attack attempts via analysis of communications flows (network-based intrusion detection systems, NIDS), and there are systems that monitor events in a computer system or pattern of use in an application (host-based intrusion detection system, HIDS). An advanced variant of these systems is the so-called intrusion preventing system (IPS), which not only detects attack attempts but also actively works to deflect them.

Note that installation of IPS in process control systems can lead to legitimate traffic being blocked (so-called false positives) if classification is faulty. A security system that unpredictably blocks control commands or result codes is unacceptable in process control systems.

So-called honey pots can also be used to indicate ongoing attack attempts. A simple solution that can be suitable in control systems is to install a computer in the network that does not normally receive traffic and that triggers an alarm if this occurs (such honey pots are sometimes called canaries or honey traps). Even an attempt to communicate with this computer can be reason to suspect an ongoing attack or that an antagonist is attempting to prepare an attack by inventorying the network.

It is important that logs and tracing data from intrusion detection systems are saved for a sufficiently long period so that they are available if further investigation is initiated. In many cases, months can pass after the initial problem.

Examples of risks or problems

An IDS misses attacks and attack attempts because it is not designed to understand the special communications protocols that are used in process control systems.

A network-based IPS reacts incorrectly to communications and blocks legitimate traffic, which leads to operational disturbances.

09 Conduct risk analyses of process control systems

NERC CIP (002-1) **NIST SP 800-82** (Kap. 3.2-3.6) **DOE 21** Steps (No. 14, 18) **OLF 104** (No. 2)

One of a security organisation's most important activities is to regularly update and evaluate conducted risk analyses. A risk analysis is the most important input for making decisions about which measures should be taken to avoid operational disturbances, production losses, or in the worst case, human injury or environmental damage.

The basic point of departure that should apply for all risk assessment of IT systems is that "the enemy knows the system" (Shannon's maxim). When it comes to process control systems, many unfortunately assume the opposite – that no external party knows the details of vendor-specific solutions. This is sometimes referred to as security by concealment or security by obscurity, which seldom succeeds due to the antagonist having a very wide range of choices when it comes to, for example, method of attack and point of attack. Vendor-specific communications protocols, encryption solutions or operating systems therefore do not in any way constitute security guarantees. The results are more often the opposite – that they cannot stand up to open examination by researchers or technical specialists.

A risk analysis can be conducted for a defined subsystem or for a more general operation. Organisations must update risk analyses in accordance with the methods that have been previously established and documented. Which risk analysis method that is used in a specific case depends on the purpose of the analysis, and which information is available concerning the pertinent system, including threats against the system. Updating a risk analysis can require an updating of the system survey, but the goal is that system diagrams and similar documentation are always up to date. Based on the operational analysis that the organisation has previously conducted, one should also have defined which systems and which information resources are mission-critical.

The risk analysis shall be documented in a predefined manner. Such documentation should at least cover discovered vulnerabilities and an assessment of risks, as well as a description and prioritisation of possible counter measures. To conduct a risk analysis, the following information may be needed: incident and interference data (logs and material from open source intelligence), results from conducted security audits (security tests and administrative assessments) and checklists.

Example of problems and risks

Because a risk analysis is not updated more than once each year, it does not take consideration to the extensive system changes that have recently been made in one of the organisation's production systems. This results in the authorisation requirements for a currently mission-critical control system being too low. For example, administrative personnel can log into the system and affect sensitive parts of a facility, and system vendors can access and change more than their own system via a service account.

10 Conduct periodic technical security audits of process control systems and connected networks

DOE 21 Steps (No. 9, 11)

By conducting practical security audits and technical checks, a more realistic picture can be created of security in systems and installed functions.

There are certain very important differences between practical security tests of administrative IT systems and the IT equipment that is used in process control systems. A large portion of the equipment that is used in control systems (for example, field equipment such as PLCs and RTUs) has poor security characteristics. The equipment can often be disrupted or attacked due to trivial programming errors. A resulting crash, restart or faulty behaviour of a test unit as a response to a simpler security tests is unfortunately not uncommon. In certain cases, the only existing installation is the one in production, and there is no testing or development environment that can be used for practical security tests.

Careful planning should precede a practical security test of process control systems, including a run-through of how any disturbances resulting from testing are to be handled. The organisation's management should approve the test plan. The basic principle is to rely on simple basic methods and interviews rather than automated tools for penetration testing of administrative IT systems. Few IT consultants have sufficient knowledge of how process control systems are tested. Many production environments are highly specialised, which requires an understanding of other technologies than those that exist in IP-based networks. For this reason, it can also be a good idea to notify system vendors prior to a security test.

When it comes to surveying process control systems to identify host computers, nodes and networks, traditional methods such as ping sweep can interfere with the systems. An inventory of a control system, however, is a very important step in the test process. Instead of using automated tools, it is often a matter of carefully examining the documentation and even visiting the actual site of a process and studying the physical connections and computers. When it comes to inventorying services and vulnerabilities of various services, active scanning methods (such as port scanning and vulnerability scanning with tools such as Nmap and Nessus) should be avoided in a production system that is in operation. Instead, use passive methods and investigate, for example, manually how routers are configured. Conduct active tests in a separate test system or in a control system that is not in operation.

Example of risks or problems

A test of a PLC is conducted in an operating production environment. The test method disrupts the operational status of the equipment, which subsequently misses important control commands or locks up.

11 Constantly evaluate physical security of process control systems

NERC CIP (006-1) **NIST 800-82** (Kap. 6.2.2) **DOE 21 Steps** (No. 10) **PL** (Kap. 9, 11)

Process control systems, especially central facilities, have historically had substantial physical security and in many sectors, there are established requirements for how important facilities are to be physically protected.

Process control systems are often geographically dispersed (decentralised), which makes it more difficult to establish good physical security at the remote facilities. Attacks against control systems can be conducted from equipment in the field. Local units such as PLCs and RTUs can be very sophisticated. For example, a modern RTU includes a web server and an Ethernet port (or Bluetooth) and it should therefore have sufficient physical security. Cables should be run so that unauthorised persons are prevented from physically accessing them and connecting into the networks.

Physical access to a system component makes it much easier to gain electronic access to process control systems. Electronic and physical security parameters must therefore be checked.

Physical security should be conducted in several ways – the principle of defence-in-depth also applies here – and it should include, among other things:

- Protection of sensitive premises (physical security perimeter, protection against unauthorised entrance, burglar alarms, camera surveillance and monitoring, fire protection and so forth)
- Authorisation control (ensure that only authorised persons have access to sensitive information and important operational areas)
- Traceability that applies to persons and assets (ensure that both persons and equipment stay in appropriate areas – for example, mobile equipment such as laptops for programming of PLCs should not be left unsupervised)
- Checks of environmental factors (such as ventilation and power supply)

Note that even persons with security clearances should be continuously monitored. They should also be subject to entry control if they want access to control facilities.

Example of risks or problems

An employee takes his laptop home. One of his children uses it for online gaming and the computer becomes infected by malicious code. Back at work, the employee connects the computer to the process network and the code executes. This results in an antagonist operating within the electronic security perimeter.

12 Ensure that only secure and relevant connections to process control systems exist

CPNI GPG (GPG 2, GPG Firewall Deployment) **DOE 21 Steps** (No. 1, 2, 3, 7) **OLF 104** (No. 10, 12) **PL** (Kap. 10, 11)

Process control systems have traditionally been physically isolated and few or no communications connections to the outside world have been incorporated. Efficiency measures and integration needs have resulted in more connections between administrative IT systems and process control systems. All types of connections are to be identified and equipped with security mechanisms that are adapted to each organisation's security requirements and to the operational requirements that are placed on the various control systems.

The connections to control systems can consist of dial-up, ISDN, landline and wireless network connections, or Internet-based connections. Examples of network connections are:

- Service inputs for vendor representatives
- Connection capabilities for on-call personnel who need quick access to process control equipment
- Connection capabilities for remote operation of facilities
- Connection capabilities for remote reading of sensors in facilities
- Connection capabilities for access to supplementary functionality or peripheral systems in facilities, such as camera surveillance, alarm installations, card and access security, fire alarms and so forth

Organisations should regularly conduct practical checks that only relevant connections to the process control systems exist, and that these are as secure as possible. One of the most important security-improving measures is to eliminate unnecessary connections.

Remote access for vendors or access for on-call personnel requires special consideration. To establish acceptable security, combinations of the various methods should be used, such as callback, limitation of connection times, strengthened authentication as well as restrictions to communications methods that can be used and the computers that can use them.

Example of risks or problems

There is an unknown connection between a control system in the process environment and an administrative computer system (intranet). A computer worm from the Internet infects a computer at the marketing department. It subsequently spreads and causes extensive operational disturbances in the production environment.

13 Harden and upgrade process control systems in collaboration with system vendors

CPNI GPG (GPG 5) **DOE 21 Steps** (No. 4, 6) **OLF 104** (No. 6, 10, 12, 13) **PL** (Kap. 2)

Hardening of computer solutions, system components and applications entails the removal of unused, unnecessary or unknown components of software and configurations, as well as installation of security upgrades (patches). This creates a limited attack surface and reduced exposure to risks. Hardening is a standard measure when it comes to improving security in administrative IT systems. The goal is to always use the most secure variant of system configurations and settings. It is important that hardening be conducted according to the process that is established for change management. A system's attack surface can be reduced by, for example:

- Changing factory settings, such as replacement of default passwords
- Choosing more secure alternatives and settings in applications, network functions or operating systems
- Turning off unused functions in applications, networks or operating systems
- Blocking login capabilities for users who are to no longer have access to systems, or limiting users' login capabilities and rights
- Correcting known security problems by upgrading (patching)

Hardening and manually closing security holes for system equipment, applications and operating systems – which security documents for process control systems sometimes mention – cannot normally be conducted without strong support from vendors. Changing equipment or software settings (including patching) without collaborating with system and application vendors can lead to operational disturbances, create instabilities in control systems and produce contractual consequences.

Examples of risks or problems

A system vendor has based functions in a process control system on non-secure network services and system components. Several of the non-secure functions used in the system cannot therefore be deactivated and the system cannot be hardened to the desired degree.

If persons without deeper knowledge of a control system conduct system hardening, the system can become instable. They inadvertently remove components that are seldom used by the system, but that nonetheless fill a function.

A false sense of security can arise if system hardening is conducted, but it is not as complete as those who conducted it believe; vulnerable parts of the system are still active.

14 Follow up incidents in process control systems and monitor external security problems

NERC CIP (008-1, 009-1) **NIST 800-82** (Kap. 6.2.3) **CPNI GPG** (GPG 3)
DOE 21 Steps (No. 19) **OLF 104** (No. 16)

An important prerequisite for all improvement work is that organisations report, document and learn from past incidents and security experiences – both those that occur in their own organisations and in others.

Documentation of experience and incidents should form the basis for risk assessment updates (risk analyses). It should also be able to lead to corrective measures and to the distribution of resources being reprioritised.

To discover incidents, it is necessary with continual follow-up and monitoring of an organisation's security routines and their statuses. By monitoring and following these up, an organisation can better deal with threats and discover new security deficiencies – both from its own organisation those of others. Attention should also be given to external incidents and events that can affect the organisation. Physical incidents can be related to IT incidents. For example, a burglary in which a laptop has been stolen can be a part of the information gathering that precedes a digital attack.

By keeping the organisation updated in regard to the incidents and security problems that have been discovered outside the organisation, it is easier to maintain good preparedness against new threats and vulnerabilities in process control systems.

A problem related to knowledge and analysis is that there is very little open information about past disruptions in process control systems. At present, there are few forums and communications channels where information is easily accessible to system and facility owners.

As an aspect of open source intelligence, each organisation should establish a group that gathers to discuss incidents and risk problems, and analyse how these can affect security in their process control systems. The group should meet regularly and must consist of representatives from both process control and IT.

Examples of risks or problems

If incidents are not reported, it is difficult to discover deficiencies in existing security routines, such as improperly configured firewalls or faulty units.

If minor incidents are not addressed, they can lead to damage and critical disturbances in process operations.

15 Collaborate in user groups, standardisation organs and other networks so as to increase security in process control systems

Several international initiatives are now underway to develop standards and recommendations for creating security in process control systems. Many government entities in Europe, North America and Asia are highly prioritising the area. By actively participating in this security work, users and vendors of process control systems can influence which security requirements will be placed on these systems in the future.

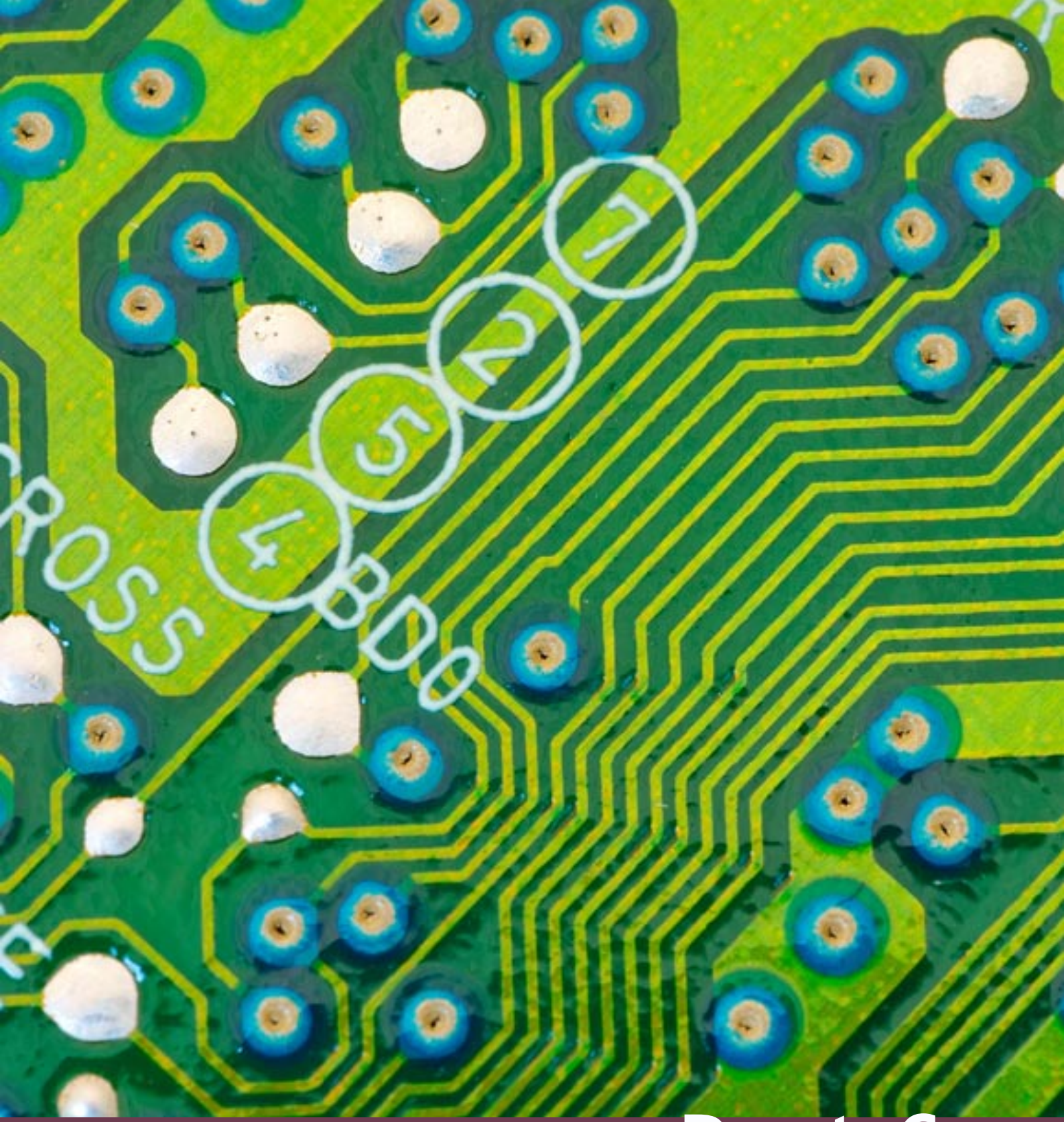
By users of process control systems working through various national and international organisations and interest groups, higher, clearer and more cohesive security demands can be placed on vendors, system integrators and application developers.

By vendors of process control systems, applications or other equipment participating in security work, competitive advantages can be created. In certain sectors, there are already established security requirements. In the US, for example, power utilities are expected to comply with the NERC CIP standard. In the future, this will likely be a requirement for the delivery of both hardware and software.

Collaborating through user groups, standardisation organs and other networks is an economically realistic alternative for many small and medium-sized users and vendors.

Example of risks or problems

If participation in standardisation and security work is weak – on the part of either vendors or users – unbalanced security requirements or technically inept requirements are developed.



Part C

Reference list with comments

NERC CIP-002-1 to CIP-009-1

Type of document: Standard
Publisher: North American Reliability Council (NERC), U.S.A.
Version: Final version (applicable as of June 1, 2006)
Scope: 53 pages (total)

`http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html`

The standards in NERC CIP (CIP 002-1 to 009-1) are generally formulated and can be used in operational areas other than electric power (authors' summary below).

NERC CIP 002-1 requires that the responsible organisation identifies critical assets by applying a risk-based approach. Based on this analysis, critical cyber-based assets are identified.

NERC CIP 003-1 requires that the responsible organisation establishes some form of administrative security program (minimum security management controls) to protect critical cyber-based assets.

NERC CIP 004-1 requires that the responsible organisation ensures that personnel (including extra personnel of various types) that are given electronic access, or unmonitored physical access, to critical cyber-based assets have the necessary training and security awareness.

NERC CIP 005-1 requires that the responsible organisation identities and protects so-called electronic security perimeters that enclose the critical cyber-based assets, and identify and protect all access points in these perimeters.

NERC CIP 006-1 requires that the responsible organisation implements a program for physically protecting critical cyber-based assets.

NERC CIP 007-1 requires that the responsible organisation defines methods, processes and procedures to secure the systems they have determined to be critical cyber-based assets. This also applies to non-critical cyber-based assets that are within any of the so-called electronic security perimeters.

NERC CIP 008-1 requires that the responsible organisation ensures that it identifies, classifies, responds to and reports security incidents related to critical cyber-based assets.

NERC CIP 009-1 requires that the responsible organisation establishes recovery plans for critical cyber-based assets and that these plans follow established practices and techniques for preparedness and contingency planning.

NIST SP 800-82 – Guide to Industrial Control Systems (ICS) Security

Type of document: Rekommendation
Publisher: National Institute for Standards and Technology (NIST), U.S.A.
Version: Second Public Draft (September 2007)
Scope: 157 pages (including appendices)

`http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf`

NIST SP 800-82 is generally formulated and can be applied in areas in which process control systems are used. The document consists of six main sections:

Sektion 1: The section presents the purpose, scope and target group of the recommendations.

Sektion 2: The section provides a general description of process control systems and explains the importance of these systems.

Sektion 3: The section contains a discussion on the differences between process control systems and administrative IT systems, and provides a description of threats, vulnerabilities and past incidents.

Sektion 4: The section provides a general description of security programs for reducing the risks of vulnerabilities that have been identified in Section 3.

Sektion 5: The section provides recommendations for how security can be integrated in traditional network architectures of process control systems. It emphasises practices for segmentation of networks.

Sektion 6: The section provides recommendations on how the various forms of control (management, operational and technical control), which have been identified in NIST SP 800-53 (Recommended Security Controls for Federal Information Systems) can be applied for process control systems.

The document also includes six appendices (A to F) that supply references, list abbreviations, provide a glossary, describe various activities in the US that are intended to increase security in process control systems and so forth.

CPNI Good Practice Guide Process Control and SCADA Security

Type of document: Recommendations
Publisher: Centre for the Protection of National Infrastructure (CPNI), U.K.
Version: Final version (different dates)
Scope: 14–42 pages (depending on the document)

http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

The documents are generally formulated and can be used in all areas in which process control systems are used. The series presently consists of a summarising guide and eight specific documents:

- Good Practice Guide Process Control and SCADA Security
- Good Practice Guide Process Control and SCADA Security. Guide 1. Understand the business risk
- Good Practice Guide Process Control and SCADA Security. Guide 2. Implement secure architecture
- Good Practice Guide Process Control and SCADA Security. Guide 3. Establish response capabilities
- Good Practice Guide Process Control and SCADA Security. Guide 4. Improve awareness and skills
- Good Practice Guide Process Control and SCADA Security. Guide 5. Manage third party risk
- Good Practice Guide Process Control and SCADA Security. Guide 6. Engage projects
- Good Practice Guide Process Control and SCADA Security. Guide 7. Establish ongoing governance
- Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks

21 Steps to Improve Cyber Security of SCADA Networks

Type of document: Recommendation
Publisher: Department of Energy (DOE), U.S.A.
Version: Final version (September 2002)
Scope: 10 pages

`http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf`

This document very briefly discusses the following recommendations:

1. "Identify all connections to SCADA networks.
2. Disconnect unnecessary connections to the SCADA network.
3. Evaluate and strengthen the security of any remaining connections to the SCADA network.
4. Harden SCADA networks by removing or disabling unnecessary services.
5. Do not rely on proprietary protocols to protect your system.
6. Implement the security features provided by device and system vendors.
7. Establish strong controls over any medium that is used as a backdoor into the SCADA network.
8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.
9. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11. Establish SCADA "Red Teams" to identify and evaluate possible attack scenarios.
12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.
13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14. Establish a rigorous, ongoing risk management process.
15. Establish a network protection strategy based on the principle of defence-in-depth.
16. Clearly identify cyber security requirements.
17. Establish effective configuration management processes.
18. Conduct routine self-assessments.
19. Establish system backups and disaster recovery plans.
20. Senior organisational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.
21. Establish policies and conduct training to minimise the likelihood that organisational personnel will inadvertently disclose sensitive information regarding SCADA system design, operations, or security controls."

Information Security Baseline Requirements for Process Control, Safety, and Support ICT Systems

Type of document: Recommendation (Guideline no. 104)
Publisher: OLF
Version: Revision no.: 01 Date written: January 4, 2007
Scope: 6 pages (Norwegian version), 32 pages (English version)

http://www.olf.no/hms/retningslinjer/?50I82.pdf

The English document discusses the following recommendations:

1. "An Information Security Policy for process control, safety, and support ICT systems environments shall be documented.
2. Risk assessments shall be performed for process control, safety, and support ICT systems and networks.
3. Process control, safety, and support ICT systems shall have designated system and data owners.
4. The infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled.
5. Users of process control, safety, and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
6. Process control, safety, and support ICT systems shall be used for designated purposes only.
7. Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems.
8. Information security requirements for ICT components shall be integrated in the engineering, procurement, and commissioning processes.
9. Critical process control, safety, and support ICT systems shall have defined and documented service and support levels.
10. Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety, and support ICT systems and networks.
11. An updated network topology diagram including all system components and interfaces to other systems shall be available.
12. ICT systems shall be kept updated when connected to process control, safety, and support networks.
13. Process control, safety, and support ICT systems shall have adequate, updated, and active protection against malicious software.
14. All access requests shall be denied unless explicitly granted.
15. Required operational and maintenance procedures shall be documented and kept current.
16. Procedures for reporting of security events and incidents shall be documented and implemented in the organisation."

Cyber Security Procurement Language for Control Systems

Type of document: Recommendation
Publisher: Idaho National Laboratory and U.S. Department of Homeland Security
Version: August 2008
Scope: 111 pages (total)

http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-I9-08.pdf

This document is intended for use in setting security requirements in the procurement of process control systems. For each main area, examples are provided of the requirement specifications, including testing measures. The document is being constantly expanded and currently includes the following sections:

Hardening of systems: The section addresses, for example, requirements for removal of unnecessary programs, configuration of hardware and updating of operating systems.

Perimeter security: The section addresses, for example, demands on firewalls and network IDSs.

Accounts and passwords: The section addresses, for example, demands on guest accounts, passwords and authentication, logging and role-based access control.

Programming practices: The section addresses demands on documentation of vendor-developed code.

Fault management: The section addresses, for example, demands on messages and documentation from the vendor and problem reporting.

Malicious code: The section addresses, for example, demands on detection and protection against malicious code.

Network addressing: The section addresses demands on addressing in networks and configuration of DNS servers.

Local units: The section addresses security in IED, PLC, RTU and so forth.

Remote access: The section addresses demands on various connections to control systems.

Physical security: The section addresses physical security demands, for example, concerning availability of digital components.

Network partitioning: The section addresses demands on network units and architecture.

Information resources (selection)

Extensive international initiatives are underway in regard to security in process control systems. A good way of staying up to date is to regularly follow what is written at some of the established websites. The following sites are a good start:

Centre for the Protection of National Infrastructure (CPNI), U.K.
`http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx`

Department of Homeland Security, US-CERT, Control Systems Security Program, U.S.A.
`http://www.us-cert.gov/control_systems/`

Process Control Systems Forum (PCSF), U.S.A.
`https://www.pcsforum.org/`

SCADA Blog (Digital Bond), U.S.A.
`http://www.digitalbond.com/`

ISBN 978-91-85797-23-3

Swedish Emergency Management Agency

P.O. Box 599
SE-101 31 Stockholm

Tel +46 8-593 710 00
Fax +46 8-593 710 01

kbm@kbm-sema.se

www.krisberedskapsmyndigheten.se