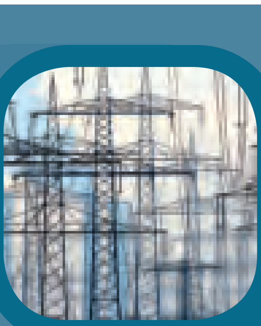
Swedish Civil
Contingencies
Agency

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

Guide to Increased Security in Industrial Control Systems



Title: Guide to Increased Security in Industrial Control Systems
Published by the Swedish Civil Contingencies Agency (MSB)
Photo: Z1025 Gambarini Federico, Dan Hansson/Scanpix, Malin Hoelstad/SvD/
Scanpix, Elvig Hansen, Bertil Ericson/Scanpix, Alexander Farnsworth, Thomas
Henriksson/Scanpix, Anders Wiklund/Scanpix, Fredrik Sandberg/Scanpix,
Pär Eliasson, Scott Paulson
Number of copies: 1500

ISBN: 978-91-7383-089-8
Publ. no: MSB 0184-10

Copies can be downloaded from the Swedish Civil Contingencies
Agency’s website, www.msb.se

Summary

Computerisation of the systems that supply society with fuel, electricity, heating, water and transportation is happening at a rapid rate. Various IT systems are being integrated to make operations more efficient. Digitalisation also facilitates communication between systems and users.

Industrial control systems, also known as Supervisory Control and Data Acquisition (SCADA) systems, have traditionally been physically isolated and based on specially developed technology. The boundaries between administrative IT systems and industrial control systems are becoming blurred as integration between these different systems increases. In order to achieve a high level of flexibility and efficiency, industrial control systems are also becoming increasingly available via Internet and other public networks. Today's industrial control systems are also built to a greater and greater degree on the same technology as standard IT systems and are therefore subject to the same security problems.

This development results in a radical change to the risk picture.

Disruptions in industrial control systems can lead not only to the destruction of expensive equipment, but also interruption of critical operations. This, in turn, can result in extensive costs and lost confidence for both the individual company and society at large.

A first step in the work to increase security in industrial control systems is to follow these *basic recommendations:*

Increase awareness throughout the entire organisation of the need for security in industrial control systems. This is a business-critical matter. Thus, executive management should be involved at an early stage.

Conduct basic training on security in industrial control systems. Control system operators need to expand their knowledge of traditional IT security. IT personnel need more knowledge on industrial control systems and the underlying physical process. Individuals involved in procurement and activity planning also need training in these subjects.

Keep industrial control systems separated from administrative IT systems to the highest degree possible. Survey existing industrial control systems and identify external connections to them. Industrial control systems should only be integrated with administrative IT systems as an exception.

Set security requirements in all industrial control system procurement and in service agreements.
There are great gains to be made by handling security matters before they become a problem. Just as with traditional IT systems, it is much more expensive to remedy security problems in industrial control systems after the systems have been delivered.

This document also offers detailed guidance in the form of 15 specific recommendations. These are based on experiences in the industry as well as practices and standardised work methods. The document also makes reference to other relevant publications in the field.

Contents

Part A Prerequisites and general recommendations

Part B Recommendations and guidelines

Part C Reference list with comments

Preface

Industrial control systems constitute a critical part of the systems that supply society with electricity, heating, drinking water, fuel and transportation for people and goods. Disruptions in industrial control systems can have serious consequences for society. Increasing security in these systems is therefore an important goal of the Swedish Civil Contingencies Agency's (MSB) work with cybersecurity.

The purpose of this document is to provide support and increase awareness of the need for increased security in industrial control systems. The first edition of the document was published in October 2008 and was well received both nationally and internationally.

The recommendations given here are supported by the members of FIDI-SC[1] and work with the document has been significantly facilitated by the generous help received from representatives of the forum.

Stockholm, May 2010

Richard Oehme
Department for Information Assurance
MSB

[1] MSB, formerly the Swedish Emergency Management Agency, has conducted the FIDI-SC forum for increased security in industrial control systems since 2005. The group's work is based on a model of trust-based information sharing developed by the British authority CPNI (Centre for the Protection of National Infrastructure). Representatives of several sectors that use industrial control systems meet regularly to share information and exchange experiences. The following organisations currently participate in FIDI-SC: E.ON AB, Fortum AB, MSB, Norrvatten, Preem Petroleum AB, AB Storstockholms Lokaltrafik (SL), Stockholm Vatten AB, Svenska Kraftnät (SvK), the Swedish Security Service, VA SYD AB and Vattenfall AB

Guide to Increased Security in Industrial Control Systems

Purpose

The purpose of this guide is to provide support in efforts to increase security in industrial control systems. Control systems are normally found in electricity and drinking water supply, the petrochemical industry and rail traffic, for example.

Security in industrial control systems has received considerable attention in recent years and there are now many international recommendations and practices.

This guide provides fundamental recommendations on security in industrial control systems. The document also provides tips on where additional information can be found. The recommendations we provide are affiliated with internationally recognised recommendations, practices and standard work methods.

Scope and selection of references

This document addresses electronic security in industrial control systems and does not provide specific advice on IT security matters.

We primarily refer to standards, guidelines and recommendations that can be generally applied to increase the security in industrial control systems. We have given preference to references that we have assessed as not being sector-specific. The selection is also limited to Swedish and English documents that are freely available via the Internet to the greatest possible extent.

This guide has been drafted by Dr. Åke J. Holmgren (Department for Information Assurance, MSB), Erik Johansson (Industrial Information and Control Systems, KTH) and Robert Malmgren (Robert Malmgren AB).

The document consists of three parts:

Part A

Prerequisites and general recommendations.

Intended for those who work with security issues at the management level.

Part B

Recommendations and guidelines.

Intended for those who work with security in industrial control systems in practice.

Part C

Reference list with comments.

ADDITIONAL INFORMATION

This guide will be periodically revised and comments regarding its content are welcome.

Please contact FIDI-SC and MSB at the following e-mail address: scada@msb.se

Part A

Prerequisites and general recommendations

Industrial control systems

Nowadays, 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. In this document, we use the designation *industrial control systems*, but the systems are also referred to as SCADA systems (Supervisory, Control and Data Acquisition), process 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 measurement points that can be spread over large geographical areas. *The process interface, meaning the method of communicating reality, is primarily made up of sensors for monitoring and actuators for control (control equipment).*

The *local systems* that collect signals from sensors and transmit control signals to control equipment contain an increasing number of functions and can often even seem to work independently during, for example, the interruption of communication with the central system. The local units often have both analogue and industrial inputs and outputs and the distinctions between different types of units – such as IEDs (Intelligent Electronic Devices), PLCs (Programmable Logic Controllers) and RTUs (Remote Terminal Units) – are becoming increasingly vague.

Important functions, such as those requiring 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 can determine which system functions will be prioritised.

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

To present data and interact with the 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 (controlling and monitoring) and maintenance of the control system (changing and updating the system).

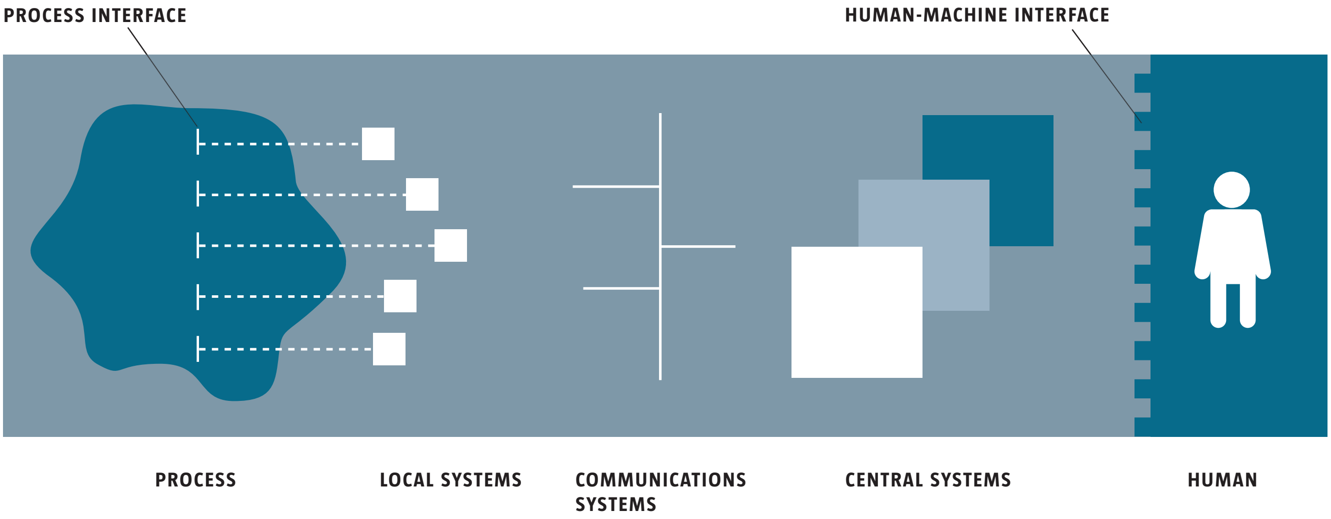


Figure 1: Schematic structure of a industrial control system [figure modified from Cegrell and Sandberg (1994)].

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

Data collection (e.g. data storage, conversion and scaling, time stamping, feasibility assessment).

Monitoring (e.g. status monitoring, trend monitoring, limit value monitoring, performance monitoring, event and alarm management).

Control (e.g. direct control, set point control, sequence control).

Planning and follow-up (e.g. non-real-time-critical functionality, planning, logging and history, follow-up and analysis).

Maintenance and change (e.g. putting in and removing from service, upgrading, management of development environments).

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.

Security in industrial control systems is important!

Below are a number of observations that all point to the need for increased attention to security in industrial 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 industrial control systems

Industrial control systems constitute a critical part of the systems that supply society with electricity, heating, drinking water, fuel and transportation for people and goods. Unlike administrative IT systems, where information processing itself often is the end goal, disturbances to communication, computer systems or applications in industrial control systems can lead to direct disturbances in the underlying physical process. This can ultimately lead to an interruption in the supply of critical societal utilities.

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

Industrial control systems previously 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 industrial control systems and administrative information systems, such as systems for logistics and asset management. In order to achieve a high level of flexibility and efficiency, industrial control systems are also becoming increasingly accessible via Internet and other public networks. This integration is exposing the industrial control systems' vulnerabilities to threats that exist, for example, on the Internet.

Industrial control systems are modernised slowly and entire systems are rarely replaced at the same time

Industrial control systems are part of system solutions with long service lives and can include technical solutions from several generations of control systems (so-called legacy systems). Once installed, the intention is for the control system to maintain a high level of availability and a good level of functionality for many years. In many organisations, there is therefore reluctance to change system settings, system components and the like in commissioned equipment, in other words after the system has been put into daily operation. This often leads to them not eliminating known IT security holes are taking a very long time before doing so.

Use of standard components changes the role of the vendor and increases demands on the user

Industrial control system vendors have traditionally functioned most often as comprehensive vendors, meaning that they have both designed and built the systems they supplied. These days, increasingly standardised technologies and components from the traditional IT world (often referred to as Commercial-Off-The-Shelf, COTS) are being used in industrial control systems. Some examples of COTS products used are Microsoft operating systems, IP-based communication technology and Oracle database solutions. This shift to standard components is changing the role of the vendor from system supplier to system integrator. This, in turn, can lead to a reduction in vendor insight and control of important components of the integrated system. Subsequently, increased knowledge of security in industrial control systems is needed by end users of the systems.

Cyber attacks on industrial control systems are a real threat

Security from an antagonist perspective (attacker perspective) has not been a crucial factor in the development of industrial control systems. Security awareness on the part of equipment, system and program vendors as well as procurement officers and buyers is often weak. This means that requirement specifications could be deficient and that systems are not designed to handle security in a suitable manner. Nowadays, sophisticated tools for launching IT attacks are freely available via the Internet. As industrial control systems are connected together into networks to an escalating degree and are increasingly built with standard IT components, there is a progressively greater risk that they will be subjected to cyber attacks.

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

Because industrial control systems are used to monitor and control physical processes in real time, the systems have been designed to maintain a very high level of availability. In a process-control context, traditional IT security problems, such as malicious code or computer intrusion, could affect the availability of the control systems and their operational security aspects. For example, a system infected with a virus could have unacceptable response times. This, in turn, could lead to collected values, alarms or commands not being received in the manner intended by the original designer.

Work with security in industrial control systems leads to culture conflicts in the security organisation

In order to achieve a high level of security in industrial control systems, it is necessary to have knowledge of traditional IT security, industrial control systems and the underlying physical process. Security work therefore requires collaboration between individuals from different cultures with different security traditions and organisational seats. Traditional IT security knowledge cannot be directly applied to industrial control systems. Many recently produced documents with security tips are expressed in terms or give recommendations that can be difficult to apply directly to control equipment. For example, hardening a system – in other words removing unnecessary, unknown or unused software and improving the configuration of the software that is used – is an extremely 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 industrial control systems is constantly increasing, leading to external security requirements

Several international initiatives are now underway to develop standards and recommendations for establishing security in industrial control systems. The field has even received considerable attention from many government bodies. By conducting proactive security work now, users and vendors of industrial control systems can actively influence which security requirements will be placed on these systems in the future. It could even be a competitive advantage to implement systematic security work. Certain branches already have established security requirements. For example, power companies in the USA are expected to follow the NERC CIP standard.

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

Security in industrial control systems is not primarily a technical problem. It chiefly concerns finding a good balance between risks and costs in the organisation. Building up a security culture adapted to handle present-day IT-related vulnerabilities is a long-term process of adjustment that the organisation must carry out with the support of executive management. There are great gains to be made by handling security matters before they become a problem. Just as with traditional IT systems, it is much more expensive to remedy security problems in industrial control systems after the systems have been delivered. The increased integration between administrative information systems and control systems brings with it more than just increased security problems. Increased integration can also increase efficiency and improve 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*. Swedish Emergency Management Agency, Stockholm. The report can be downloaded from: www.msb.se/scada

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

Differences between administrative IT systems and industrial control systems

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

To create security in industrial control systems, good knowledge of their respective characteristics is required. It is, however, extremely important to bear in mind that many well-known IT attacks, conceptual attack methods and various alternatives for abusing IT systems – which are classic or standard in administrative IT environments – also work more and more often in industrial 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/nistpubs/

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

Categories	Administrative IT systems	Industrial 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
Time-critical	– Less critical with interaction during emergencies	– Response to human or other interaction during emergencies is critica
	– 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

In order to establish smoothly functioning activities for security in industrial control systems, the organisation must have a good security culture, meaning functioning general risk management and systematic information security work. Figure 2 below illustrates the relationships between the activities that should be included in systematic risk management.

The recommendations in this guide 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 many methods for performing risk analyses on IT systems.

The Swedish Emergency Management Agency 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 an organisation and subsequently implement, for example, the ISO standards above. Another example is the American agency NIST's report SP 800-30, which describes a general model for IT system risk analysis and SP 800-34, which addresses contingency planning in IT systems (NIST, 2002a; NIST, 2002b).

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

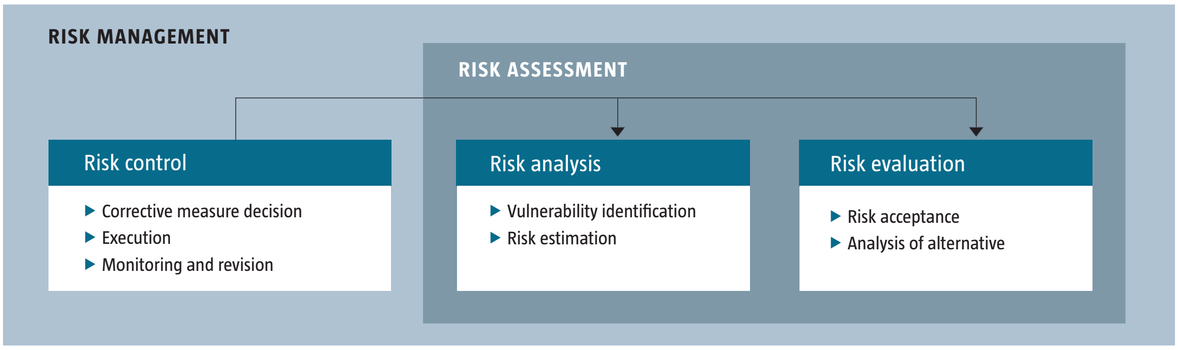


Figure 2: Risk management [figure modified by authors from IEC (1995)]

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 Techno-logy (NIST), Gaithersburg. The report can be downloaded from: http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf

Summary of recommendations for increased security in industrial 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 FIDI-SC and experiences from research and practical projects in which the authors have participated. It is also supported by international recommendations and well-known practices.

The following recommendations serve as the first step in work to increase security in industrial control systems.

→ **Increase awareness throughout the entire organisation of the need for security in industrial control systems.**

This is a business-critical matter. Thus, executive management should be involved at an early stage.

→ **Conduct basic training on security in industrial control systems.**

Control system operators need to expand their knowledge of traditional IT security. IT personnel need more knowledge on industrial control systems and the underlying physical process. Individuals involved in procurement and activity planning also need training in these subjects.

→ **Keep industrial control systems separated from administrative IT systems to the highest degree possible.**

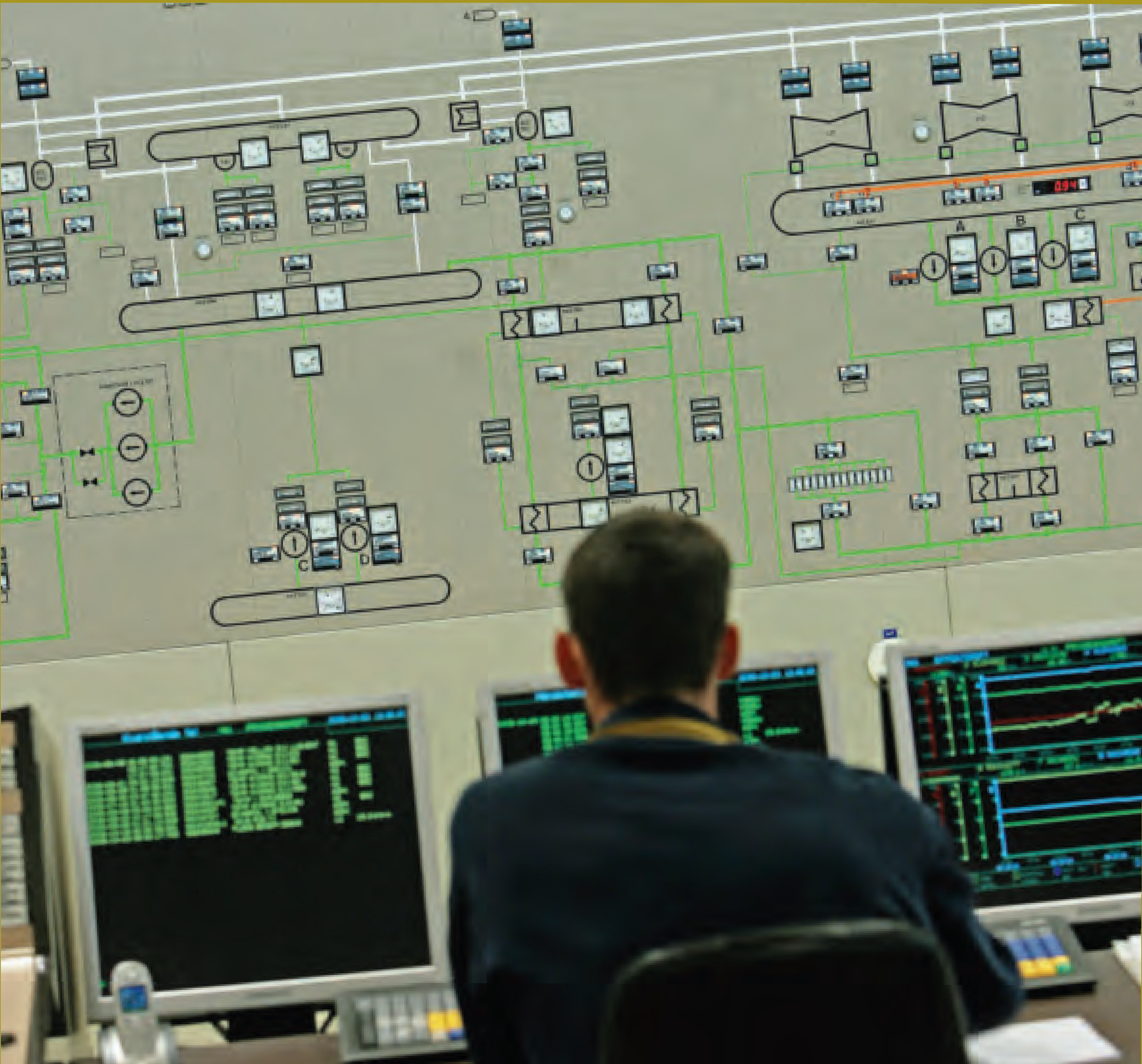
Survey existing industrial control systems and identify external connections to them. Industrial control systems should only be integrated with administrative IT systems as an exception. In cases where this is done, extremely advanced logic separation of the systems is required.

→ **Set security requirements in all industrial control system procurement and in service agreements.**

There are great gains to be made by handling security matters before they become a problem. Just as with traditional IT systems, it is much more expensive to remedy security problems in industrial control systems after the systems have been delivered.

Part B

Recommendations and guidelines



Basis for recommendations

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

Because the recommended activities are part of routine quality work, we relate them to the well-known Deming Cycle (Figure 3), also known as the PDCA model (Plan, Do, Check, Act). The PDCA model is applied in several international standards, such as the ISO/IEC 27 000 series on management systems for information security. The goal is for an organisation's work with security in industrial control systems to in this way have a natural connection to other work with information, security and quality.

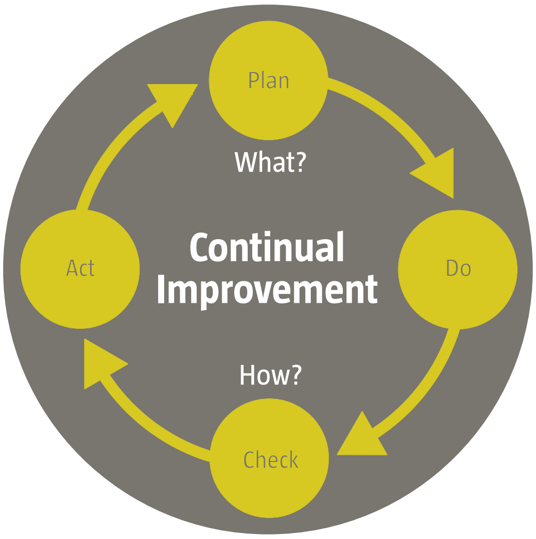
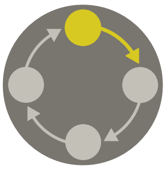
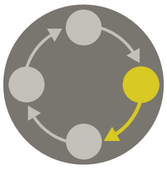


Figure 3: We use the PDCA model (Deming Cycle) in this document, both to emphasise the importance of work leading to continual improvements, and to structure the recommendations.



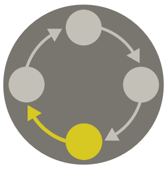
The plan phase

involves establishing policies, goals, processes and routines.



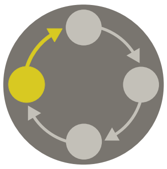
The do phase

involves implementing and enforcing policies, measures, processes and routines.



The check phase

involves monitoring and auditing by assessing, measuring and reporting.



The act phase

involves maintaining and improving – in other words, taking corrective measures for improvement.

In the following sections, we provide tips on where more information can be found. The established guidelines and standards that we make reference to are described in more detail in **Part C**. These have the following designations:

NERC CIP	Cyber security standard CIP-002-2 - 009-2
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	Krav til informasjonssikkerhetsnivå i IKT-baserte prosesskontroll-, sikkerhets- og støttesystemer
PL	Cyber security procurement language for control systems

Recommendations for increased security in industrial control systems

01 Clarify roles and responsibilities for security in industrial control systems

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

03 Establish a process for change management in industrial control systems

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

05 Introduce security requirements in industrial control systems right from the start in all planning and procurement

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

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

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

09 Conduct risk analyses of industrial control systems

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

11 Continually evaluate physical security of industrial control systems

12 Ensure that any and all connections to industrial control systems are secure and relevant

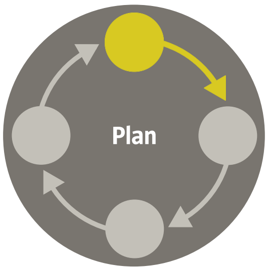
13 Harden and upgrade industrial control systems in collaboration with system vendors

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

15 Participate in user associations, standardisation bodies and other networks so as to increase security in industrial control systems

Ej ATC
30

0302CBL



01 Clarify roles and responsibilities for security in industrial control systems

▶ NERC CIP (003-2) ▶ NIST SP 800-82 (Chap. 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.

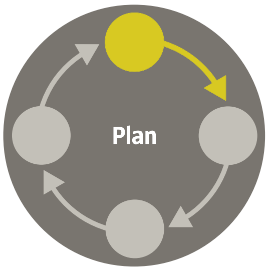
For control systems, this allocation of roles and responsibilities is often non-existent, meaning that there are neither areas of responsibility nor control models. At times, vendor representatives are the closest thing to an IT technician or system administrator available. Moreover, practical administration of the systems may be handled by process engineers, who have no knowledge of logical security in control systems. This leads to an organisation having little or no knowledge of the IT technical properties of the industrial control systems. Subsequently, there is reduced control and ability to manage the technology and its usage.

The allocation of responsibilities for these security matters are most easily clarified by creating a security policy for industrial control systems. This policy can either be a separate document, which must then be related to the organisation's other policy documents, or the matter can be resolved by adding to the organisation's information security policy.

Allocation of roles and responsibilities for the administrative information systems and control systems should be co-ordinated. There should be clarification of which systems are administrated by the organisation's central IT support and which systems are administrated locally out in production. How this is accomplished on a purely practical level is related to how the organisation chooses to implement protections and layers of protective barriers in its overall IT environment. Even if a large portion of the process-related systems are administrated locally, it the organisation's central IT support must be responsible for total integration and creates a uniform approach to security matters. An important reason for a uniform approach to the organisation's information security is that it is becoming increasingly common to have extensive data exchange between control systems and administrative systems.

Example of risks and problems

An organisation with no clear allocation of roles and responsibilities for daily security work did not perform the necessary application updates and had no processes in place to quickly delete obsolete accounts. A former employee who wanted to take revenge on his employer took advantage of this. The attack was possible because the culprit's user accounts and access rights were not blocked. The intrusion could be done from a distance and once in the SCADA system, the attacker could use existing group accounts whose password had not been changed since he left the organisation. The organisation suffered an extremely serious disruption when the SCADA system was attacked. Damages from the attack were much worse than necessary since incident management and damage limitation were delayed by a completely unprepared organisation that lacked knowledge of who was authorised to take necessary measures.



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

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

To create security in industrial control systems, it is important to establish a process for surveying and understanding the information flows and system dependencies of the organisation, in other words the connections between the various types of systems and operations.

It is crucial that the organisation's processes, systems and information analyses are based on an understanding of the consequences that a fault or disrupted function could have, both for the physical process and for the organisation. This is an important prerequisite for creating a relevant risk evaluation and for classifying which systems and which information are most critical.

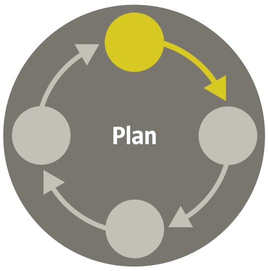
An organisational and system survey should result in lists of access and connection possibilities, system classifications and operational priority categories. Diagrams of the industrial control systems should be available and have a degree of detail sufficient to enable identification of critical components and systems. Examples of information that should be available in system diagrams are data on operating systems of computer resources, IP addresses, communications protocols and technical data on local units, such as PLCs. In order to be able to establish the electronic security perimeter, all connections to industrial control systems must be identified. In addition to intranets, this includes remote connections to collaborative partners, vendors and the Internet. Note that all wireless connections should be treated as remote connection points. Connections to the organisation's administrative information systems (intranet) should be considered external connections.

The organisation's critical assets should be identified by applying a risk-based approach. This analysis is then used to identify the critical cyber assets. This requires the existence of a documented process for how risk analyses are to be conducted and under what conditions they shall be updated. This choice of risk analysis method should be adapted to the purpose of the analysis and the information available. To make it easier to update the risk analyses, an unnecessarily advanced risk analysis method should be avoided.

Example of risks and problems

An organisation's control systems are considered to be separate from other computer networks, so it was deemed unnecessary to equip them with any type of protection against malicious code. When the organisation's administrative office network was struck by malicious code, several of the control systems were also struck down. Upon closer inspection of the organisation, several previously unidentified connections between different computer networks were discovered. Because these were not documented, they were never incorporated into previous security analyses. Consequently, the organisation held the misguided belief that there systems were significantly more secure than they actually were.

One of the reasons that these vulnerabilities had not been identified was that the organisation lacked a systematic process for how and when system surveying and risks analyses should be conducted. Thus, there was no basis for comparing and monitoring the organisation's risks and how they changed over time. As a result, important components of the control system remained unprotected year after year while considerable resources were invested into protecting other information resources, which were not as critical to the organisation's survival.



03 Establish a process for change management in industrial control systems

▶ NERC CIP (003-2) ▶ 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 in order to prevent disruptions, unnecessary troubleshooting or serious problems in industrial control systems. Systems and applications that organisations will use for a long period of time, such as in industrial processes, entail special requirements for strict control of change management.

Software upgrading should be done in stages and often requires the participation of system vendors due to both legal and technical requirements. In process control environments, it is important for all parties involved – vendors, system administrators and users – to 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 information systems. Unfortunately, this is not the case for industrial control systems. Extra financial resources may therefore be required to create the right conditions for good change management in these systems.

There should be a formal process that specifies how to obtain authorisation to make changes in industrial control systems. 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 authorised should be forbidden.

The formal change management process should, at a minimum, include a procedure for obtaining authorisation to make changes, a description of how tests before and after a change should be conducted (including a description of which changes require testing in a separate test environment), requirements for how documentation shall be updated after changes have been made and requirements for how personnel shall be informed of changes (for example, in which cases special operator training is required).

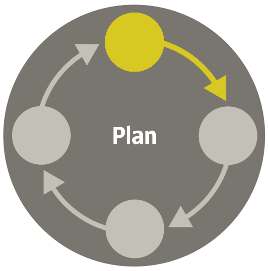
Example of risks and problems

The industrial control systems of an organisation have become increasingly unstable over time, resulting in unanticipated system events. Some functionality has disappeared and all parameters have reverted to their default factory settings. A later investigation determined that certain local changes that the organisation made to a control system were not reported to the system vendor. As a result, the vendor's running upgrades to control system software had not been correctly verified since the test system differed from the customer's actual system.

The consequences were made worse by the fact that there were no clear routines for handling change management and control system updates. The vendor's system updates eliminated local system changes, which unintentionally deactivated certain system functions.

These disruptions led to significant costs in the form of lost revenue and impacted confidence in the organisation due to the unplanned and unexplainable stop in production.

The organisation could not claim that it was the vendor who caused the disruptions since they had no clear process for their own system change management.



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

▶ NERC CIP (008-2, 009-2) ▶ NIST 800-82 (Chap. 6.2.3) ▶ CPNI GPG (GPG 3)
▶ DOE 21 Steps (No. 19) ▶ OLF 104 (No. 7, 16)

To ensure the organisation's ability to survive serious disturbances, there must be *contingency planning* that includes clear descriptions of routines, roles and responsibilities during emergencies. Examples of such disturbances are power outages, control system failures and key operating personnel out on sick leave.

In addition to continually following up and updating contingency plans, it is vital for personnel to participate in preparedness training exercises and for operations to be regularly tested to ensure satisfactory functionality in the event of an emergency. For industrial control systems, it is particularly 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:

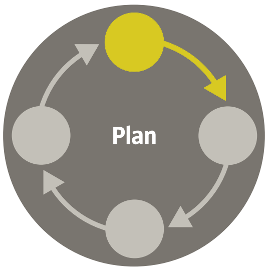
- routines for handling operations manually (run the process without computer support)
- routines for restoring both data and configuration settings as well as restarting the process
- contact details for operators, service technicians, other personnel, vendors and support
- description of how central control system components 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 a disturbance in the industrial control systems, such as a service becoming unavailable or having reduced functionality, must be documented for later analysis. One of the difficulties with incident management is finding a balanced structure for how incidents can be caught and reported without this being perceived as obstructive to the normal work process. It is also important to motivate the organisation by communicating the purpose behind reporting incidents and providing information on the results of incident management. Without this communication, it can be difficult to maintain motivation to report incidents and vulnerabilities.

Example of risks and problems

An organisation ran into trouble when a key individual who served as system administrator of a critical control system suddenly died in a motorcycle accident. He was the only one in the organisation who had complete knowledge of how the control system was configured. As the basic control system documentation was not updated, and in some cases was missing completely, no one in the organisation could easily step in and take over his work tasks.

The key individual had not shared more information than absolutely necessary to others in the organisation. This had made him indispensable within the organisation, which contributed to making the organisation extremely vulnerable.



05 Introduce security requirements in industrial control systems right from the start in all planning and procurement

▶ NIST 800-82 (Chap. 6.1.3) ▶ CPNI GPG (GPG 6) ▶ OLF 104 (No. 8, 9)
▶ PL (all chapters)

In an organisation, it is extremely important for security matters to be included in planning as early as possible.

Since it is difficult and expensive to achieve an acceptable level of security in control systems after implementation, security requirements should be included from the very beginning in system specifications and needs analyses. Because many system solutions are fully or partially procured from external parties, special attention must be given to security issues during procurement work.

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

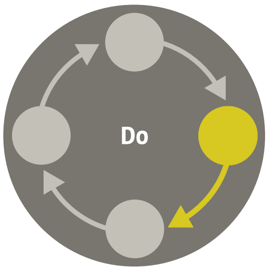
When modifying control systems, special consideration must be given to IT security matters since the changes will most likely affect the existing control system in a manner that the original designers had not considered. For example, in older control systems there was often a presumption that access to equipment would only be possible via local physical presence. Nowadays, however, physical separation is no longer possible in many situations. It is instead a manner of creating logic separation between the different parts of the industrial control systems.

Requirements gathering should be done in the form of different surveys and threat and risk analyses. In addition to comply with detailed requirements for security and protective functions in systems and applications, the vendor should also be able to present their methods and processes (such as internal developer handbooks) used to guarantee the quality of their own security work.

Example of risks and problems

After a couple of security-related incidents, an organisation is forced to supplement its control system with some complex, technical security solutions. Unfortunately, it became apparent that not enough thought was put into these supplementary orders. As a result, the system became unnecessarily vulnerable during its entire life cycle since, amongst other reasons, it became more difficult to implement updates. The organisation could not reach the level of security it desired.

If the organisation had not neglected security requirements during its original procurement, they would probably not been subjected to these extra costs and would likely have obtained a better planned and better adapted security.



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

▶ NERC CIP (004-2) ▶ DOE 21 Steps (No. 21) ▶ OLF 104 (No. 5)

It is important to establish the understanding that security in industrial control systems is a mission-critical issue. It takes long-term efforts to influence understanding and attitudes and – as always when it comes to security matters – the commitment of executive management is extremely important. The importance of this commitment is in part because security in industrial control systems requires increased reasons and because it requires collaboration between parts of the organisation that do not normally work together.

!

In order to achieve a high level of security in industrial control systems, it is necessary to have knowledge of traditional IT security, industrial control systems and the underlying physical process. Security work therefore requires collaboration and trust between individuals from different cultures with different security traditions and organisational seats. This requires regular education and training of both IT personnel and control system operators.

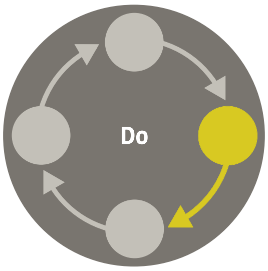
Industrial control systems are incorporated into system solutions is very long service lives. It is particularly important to try to imagine how the systems will be used or misused in the future. Ignorance or unclear routines can cause many normal activities to lead to potential security problems.

The organisation should establish an administrative security program to create a general approach to IT. This provides good security awareness, encourages critical thinking and creates a positive attitude towards working with matters that improve security.

Example of risks and problems

A technician working out in the field needed to transfer data between two different IT environments. The technician normally used a removable hard drive, but had forgotten it at the office. He instead connected a network cable between the two computers in the normally physically-separated networks. At the end of the work day, the technician forgot to remove the network cable. Now, instead of being physically separated, the control system was directly connected to the organisation's office network. Since the control system had previously been physically isolated, the organisation never saw a need to install any IT security mechanisms in its process-related network.

The organisation suffered several unexplainable operational disturbances. Because the organisation did not perform technical security reviews on a regular basis, it took a long time before the mistake was discovered.



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

▶ NERC CIP (005-2, 007-2) ▶ CPNI GPG (GPG Firewall Deployment)
▶ DOE 21 Steps (No. 5, 15) ▶ OLF 104 (No. 4, 13) ▶ PL (all chapters)

A fundamental principle of protecting critical systems is to configure defence-in-depth, by use of multiple layers of protection and overlapping security mechanisms. These security mechanisms may be of the same type, such as multiple firewalls, or of different, supplementary types, such as firewall as network security protection combined with a strong authentication for access to the IT system.

There are strong incentives in all types of organisations to increase information management efficiency, amongst other things by connecting information systems in a manner that avoids duplication of work. Older control systems or industrial components found in process environments were often developed during a time when physical separation was a given and logical security was unheard of. Known flaws and vulnerabilities remedied in the administrative IT environments many years ago can often still be found in industrial control systems. Interconnecting various networks could therefore entail considerable risk, as external connections to industrial control systems may expose them to threats for which they lack protection. A thorough risk analysis should therefore precede integration of control systems and administrative IT systems. IT security protection of extremely high quality is also required.

It is necessary to set up an electronic security perimeter (logical perimeter protection) around process control and operating systems. On a conceptual level, it is important to be able to differentiate between that which logically forms a system landscape and the other systems within the organisation.

Industrial 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 so-called demilitarised zones (DMZ).

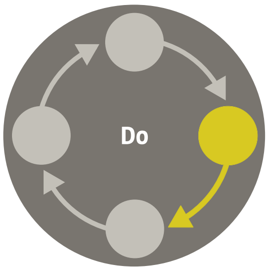
Data exchange between industrial control systems via one or more DMZs to other external systems, such as business systems, should be done in a limited and controlled manner. Outgoing communication from control systems to business systems must be limited in regard to services and ports. It may also be a good idea to use different communications protocols for communication between different parts of the network. If a protocol is used for communication between the control system and a DMZ, another protocol should be used for further communication between DMZ and the organisation's administrative information systems.

Communication within a control system may also require protection. In most systems, communication between field equipment, such as PLCs, and local systems is based on industrial protocols with low or non-existent security.

Example of risks and problems

An organisation implemented logical perimeter protection in the form of a firewall to protect against external IT attacks. Secure behind the new firewall, the organisation's operators can log in to all IT systems using a single password, a so-called Single-Sign-On (SSO). The operator could also remote control the facility via the Internet over a virtual private network (VPN).

After a period of time, the organisation suffers operational disturbances because an operator's computer was infected with malicious code at his home. Via the Internet, an attacker could gain control of the operator's computer and learn both the username and password. Because defence-in-depth was not implemented, i.e. authorisation was only linked to a username and a simple password, the attacker could connect to the organisation and access the process-related systems.



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

▶ NERC CIP (005-2) ▶ DOE 21 Steps (No. 8) ▶ PL (Kap. 2.2, 3.2, 3.3, 4.4)

Unlike incident follow-up (open source intelligence or horizon scanning) and risk analysis updating, intrusion detection and security monitoring are intended to analyse attack attempts and attacks against one's own organisation. Horizon scanning together with good monitoring of the organisation's own systems and their communication provides a good overall understanding of threat patterns, such as altered attach trends and current malicious code.

There are two types of intrusion detection systems (IDS). There are systems that recognise attack attempts via analysis of communication flows (network-based intrusion detection systems, NIDS) as well as systems that monitor events in a computer system or usage patterns in an application (host-based intrusion detection system, HIDS). An advanced variant of these systems are so-called intrusion prevention systems (IPS), which not only detect attack attempts but also actively work to deflect them.

! Note that use of IPS in control systems with incorrect attack classification can lead to legitimate traffic being blocked (so-called false positives). A security system that unpredictably blocks control commands or result codes is unacceptable in industrial control systems.

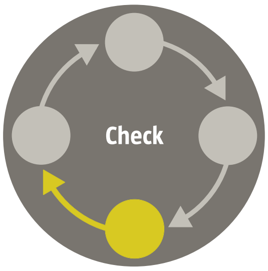
So-called honey pots can also be used to indicate attack attempts in progress. A simple solution that can be suitable in control systems is to install a computer in the network that does not normally receive any traffic and that triggers an alarm if this occurs (such honey pots are sometimes called canaries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

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

Example of risks and problems

An organisation lacked continual monitoring of which computers were connected to the network. Because of this, no one noticed that operating personnel had "accidentally" connected the administrative networks with the process-related networks, which increased the exposure of the vulnerable control systems.

Another organisation had procured intrusion detection service from an IT security company, but to save money only entered into an agreement that covered normal office hours. Because of this, no one detected the attacks and intrusion attempts that occurred after office hours. A few months later, the organisation was attacked at night and the systems were compromised.



09 Conduct risk analyses of industrial control systems

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

One of the security organisation's most important activities is to regularly update and evaluate the risk analyses that have been conducted. A risk analysis is the most important input for making decisions on which measures should be taken to prevent operational disturbances, loss of production or even human injury and environmental damage.

The basic presumption that should be applied to all IT system risk assessment is that the enemy knows the system (Shannon's maxim). When it comes to control systems, many unfortunately assume the opposite – that no outsider knows the details of the vendor-specific solutions. This is sometimes referred to as security by obscurity, which seldom succeeds since the attacker has a wealth of choices when it comes to factors such as method and time of attack. Vendor-specific communications protocols, encryption solutions or operating systems therefore do not in any way guarantee security. The results are more often the opposite – they cannot stand up to open examination by researchers or technical specialists.

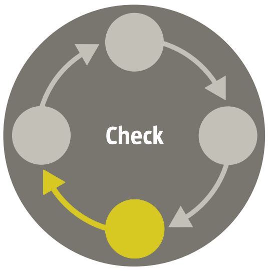
A risk analysis can be conducted for a defined subsystem or a more general operation. The organisation must update the risk analyses in accordance with the method that have been previously established and documented. Which risk analysis method is used in a specific case depends on the purpose of the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

The risk analysis shall be documented in a pre-defined manner. Such documentation should, at a minimum, include detected vulnerabilities, assessment of risks as well as descriptions and prioritisation of possible countermeasures. The following information may be required to perform a risk analysis: incident and interference data (logs and material from horizon scanning), results from conducted security audits (security tests and administrative audits) and checklists.

Example of risks and problems

An organisation did not prioritise risk analyses for its process IT environment because it considered the environment difficult to access and secure due to its unique nature. Because if this thinking, critical vulnerabilities in existing systems were not identified and relevant security requirements were not set when it was time for extensive system procurement. In this case, there was a system change that gave users access to systems which they should not have been authorised to access.

For example, administrative personnel could log into the system and affect sensitive parts of the facility. System vendors could also get access to and change more than their own system via their service accounts.



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

▶ DOE 21 Steps (No. 9, 11)

Conducting practical security audits and technical controls makes it possible to create a more realistic picture of security in systems and installed functions.

There are some extremely important differences between practical security tests on administrative IT systems and the IT equipment used in industrial control systems. A large proportion of the equipment used in control systems (for example, field equipment such as PLCs and RTUs) has poor security qualities. The equipment can often be disrupted or attacked due to trivial programming errors. Unfortunately, it is not uncommon for this to result in a crash, restart or faulty behaviour of the test unit in response to a simple security test.

> In some cases, the only installation that exists is the one in production and there is no test or development environment that can be used for practical security tests.

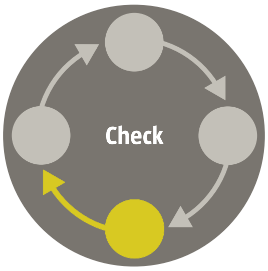
Careful planning should precede a practical security test of industrial control systems, including a run-through of how any disturbances resulting from the test are to be handled. The test plan should be approved by the organisation's management. The basic principle is to rely on simple basic methods and interviews rather than automatic tools for penetration testing of traditional IT systems. Few IT consultants have sufficient knowledge of how to test industrial control systems. Many production environments are highly specialised, which requires an understanding of technologies other 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 control systems to identify host computers, nodes and networks, traditional methods such as ping sweep could disrupt with the system. However, inventorying the control system is an extremely important step of the test process. Instead of using automatic tools, the process often involves carefully examining the documentation and even visiting the actual site of the process and studying physical connections and computers. When 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 manually investigate factors such as 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 and problems

A vendor holds a course on the power supply control system for a city's rail traffic. The course is held using the system in operation. The system is redundant with two standard servers, of which one is a "hot standby". There is also a reserve server in "cold standby". During the course, there is a demonstration on how to switch over to the reserve server, at which time there is unintentional emergency disconnection in all substations. All trains stop and a large number of passengers are delayed up to two hours.

The cause was determined to be that the configuration database in the cold standby server did not match the one in the regular operational database. Later investigation showed that the three-server concept did not have the right conditions to work.



11 Continually evaluate physical security of industrial control systems

▶ NERC CIP (006-2) ▶ NIST 800-82 (Chap. 6.2.2) ▶ DOE 21 Steps (No. 10) ▶ PL (Chap. 9, 11)

Industrial control systems, particularly 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.

Industrial control systems are often geographically dispersed (decentralised), which makes it more difficult to maintain good physical security at the remote facilities. Attacks on industrial control systems can be made from equipment in the field. Local units, such as PLCs and RTUs, can be very sophisticated. For example, a modern RTU can include a web server and more modern communication methods (Bluetooth, Ethernet port or WLAN) and should therefore have sufficient physical security. Cables should be routed in a manner that prevents unauthorised individuals from physically access them and connected to networks.

> Physical access to a system component makes it much easier to gain logical access to industrial control systems. Logical and physical security perimeters must therefore be strictly followed.

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

- protection of sensitive premises (physical perimeter protection, protection against unauthorised entrance, burglar alarm, camera surveillance and monitoring, fire protection and so on)
- authorisation control (ensure that only authorised individuals have access to sensitive information and important operating premises)
- traceability that applies to individuals and assets (ensure that both individuals and equipment remain in appropriate areas – for example, portable equipment such as laptops for PLC programming should not be left unsupervised)
- checks of environmental factors (such as ventilation and power supply)

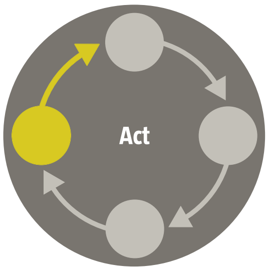
Note that even individuals with security clearance should be monitored continually. They should also be subject to physical access control if they want access to control facilities.

Establishing a good level of physical security in the geographically dispersed process network is becoming increasingly important. Since the tools used for attacks are growing in sophistication, it is only a matter of time before an attacker breaks through the logical security.

Example of risks and problems

An organisation's burglar alarm was triggered at a facility out in the field. Upon arrival, a monitor was found to be missing and the incident was considered simply a minor attempt at sabotage by a bunch of adolescents. There was no camera surveillance that could reveal what actually happened before security personnel arrived at the scene. Neither was more extensive analysis of the equipment conducted on site.

One week later, unexplainable operational disturbances began occurring. After a long time had passed, it was detected that a wireless access point had been installed during the break-in. The installation was done via one of the workstation's USB contacts – the theft of the monitor was probably just a diversion.



12 Ensure that any and all connections to industrial control systems are secure and relevant

▶ CPNI GPG (GPG 2, GPG Firewall Deployment) ▶ DOE 21 Steps (No. 1, 2, 3, 7)
▶ OLF 104 (No. 4, 10, 12) ▶ PL (Chap. 10, 11)

Control systems have traditionally been physically isolated with few or no communications connections to the outside world. Various types of new business needs and efficiency improvement decisions have resulted in streamlining solutions with integration between control systems and administrative information systems. All types of connections must be identified and equipped with security mechanisms that are adapted to the organisation's security requirements and to the operational requirements set for the various control systems.

Connections to control systems can consist of dial-up modems or 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 the industrial control system
- 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 systems, card and access security and fire alarms

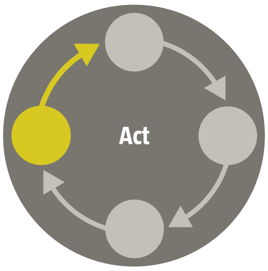
!

The organisation should regularly conduct practical checks to ensure that any and all connections to industrial control systems are relevant and as secure as possible. One of the most important security-improving measures is eliminating unnecessary connections.

Remote access for vendors or access for on-call personnel requires special supervision. To establish an acceptable level of security, combinations of various methods should be used, such as callback, limitation of connection time, stricter authentication and limitations on which communication methods can be used and which computers can use them.

Example of risks and problems

When conducting an audit of existing network connections, an organisation found, to its surprise, that there were a number of previously unknown connection points. For example, there were connections between a control system in the process environment and the administrative computer network. This enabled a computer worm that infected a computer in the Accounting department to spread and cause extensive disruption to production. Another connection possibility was the modems the vendors used during updates. Although these normally should be disconnected, this was not the case. All connections to networks must be routinely analysed and carefully evaluated.



13 Harden and upgrade industrial 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 (Chap. 2)

Hardening of computer solutions, system components and applications entails the removal of unused, unnecessary or unknown components of software and configuration and installation of security upgrades (patches). This limits the size of the attack surface and reduces risk exposure. Hardening is a standard measure when it comes to improving security in traditional IT systems. The goal is to always use the most secure variant of system configuration and settings. It is important for hardening to be done in accordance with the change management process that has been established. The attack surface of a system can be reduced by, for example:

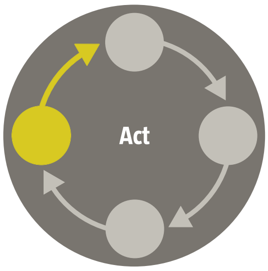
- changing factory settings, such as changing default passwords
- choosing more secure alternatives and settings in applications, network functions or operating systems
- deactivating unused functions in applications, network functions or operating systems
- blocking login capabilities for users who are no longer to have access to systems or limiting users' login capabilities and rights
- correcting known security problems through upgrades (patches)

! Hardening and manually closing security holes in system equipment, applications and operating systems – which security documents for industrial 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 even have contractual consequences.

Example of risks and problems

A system vendor based several central control system functions on open source code. This source code proved to have a number of vulnerabilities in the form of relatively non-secure net services and system components. Several of these non-secure functions were essential in the control system and could not be deactivated. As a result, the control system could not be hardened to the desired extent.

If individuals without advanced knowledge of the control system perform system hardening, the control system could become unstable. They could, for example, accidentally remove components that are used rarely by the system but nonetheless serve an important function. Thus, routines are required to specify how hardening is to be carried out and documented and that this is done in collaboration with the system vendor.



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

▶ NERC CIP (008-2, 009-2) ▶ NIST 800-82 (Chap. 6.2.3) ▶ CPNI GPG (GPG 3)
▶ DOE 21 Steps (No. 19) ▶ OLF 104 (No. 16)

An important prerequisite in all improvement work is that the organisation reports, documents and learns from past incidents and security experiences – both those that occur within the organisation and those that occur in other organisations.

Experience and incident reports should serve as the basis for risk assessment updates (risk analysis updates). They should also be able to lead to corrective measures and reprioritising of resource allocation.

In order to detect incidents, there must be continual follow-up and monitoring of the organisation's security routines and their status. With this monitoring and follow-up, the organisation can better handle threats and detect new security deficiencies – both from its own organisation and from others. Attention should also be given to external incidents and events that could impact the organisation. Physical incidents can be related to IT incidents. For example, a break-in resulting in a stolen laptop could be part of the information gathering that precedes a digital attack.

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

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

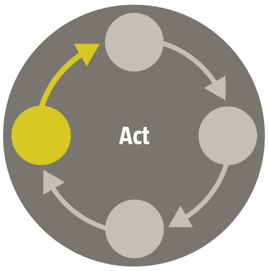
Monitoring of external security problems should also include standard IT security components, as these are often the core or subcomponents of process IT solutions. A Cisco bug or a Windows bug could just as serious as a security bug in the process IT software itself..

As part of its horizon scanning (Open source intelligence), the organisation should establish a group that meets to discuss incidents and risk problems and to analyse how they could impact security in the organisation's control systems. The group should meet regularly and must consist of representatives from management as well as process control and IT.

Example of risks and problems

An organisation maintained a culture in which detected security problems and deficiencies were kept quiet. This made it difficult to detect deficiencies in existing security routines, such as incorrectly configured firewalls and incorrect configuration in systems. Furthermore, security awareness was never fostered since incidents were never brought to light.

Several minor incidents that no one had called attention to eventually led to critical operational disturbances in the organisation.



15 Participate in user associations, standardisation bodies and other networks so as to increase security in industrial control systems

Many international initiatives are currently underway to develop standards and recommendations for creating security in industrial 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 industrial control systems can influence which security requirements will be placed on these systems in the future.

By industrial control system users working through various national and international organisations and interest groups, it becomes possible to set higher, clearer and more cohesive security requirements on vendors, system integrators and application developers.

By vendors of industrial control systems, applications or other control equipment participating in security work, it becomes possible to create a competitive advantage. Certain branches already have established security requirements. For example, power companies in the USA are expected to follow the NERC CIP standard. In the future, this will likely be a requirement in order to deliver both hardware and software.

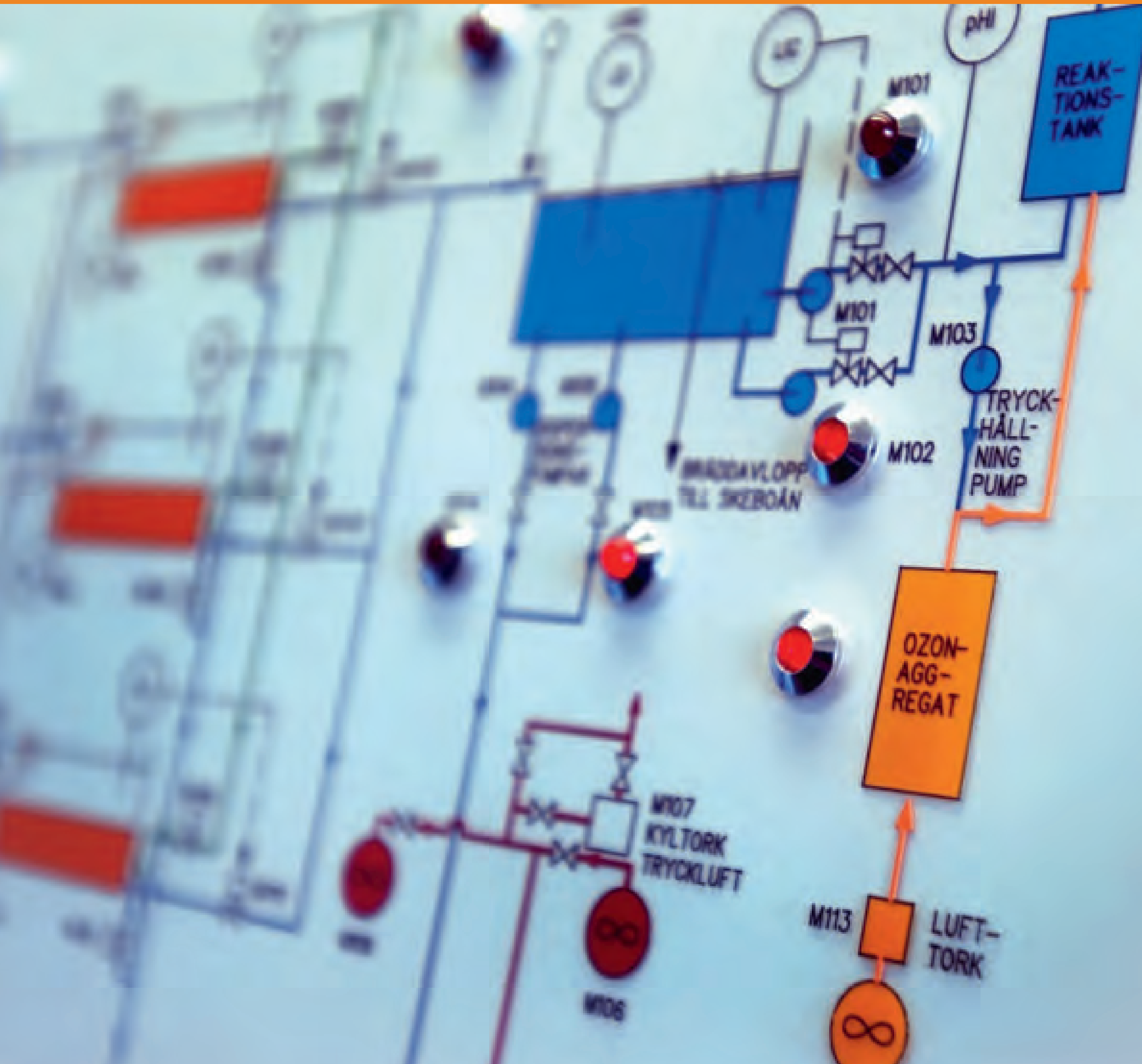
Collaborating through user associations, standardisation bodies and other networks is a financially realistic alternative for many small and medium-size users and vendors.

Example of risks and problems

If participation in standardisation and security work is weak on the part of either vendors or users, the security requirements that are developed are either unbalanced or based on an incorrect understanding of the technical systems.

Part C

Reference list with comments



NERC CIP-002-2 to CIP-009-2

Type of document	Standard
Publisher	North American Reliability Council (NERC), U.S.
Version	Final version (applicable as of May 6, 2009)
Scope	34 pages (total)
http://www.nerc.com/page.php?cid=2|20	

The standards in NERC CIP (CIP 002-2 to 009-2) are generally formulated and can be used in operational areas other than electrical power.

NERC CIP 002-2 requires that the responsible organisation identifies critical assets by applying a risk-based approach. The organisation then uses this analysis to identify critical cyber assets.

NERC CIP 003-2 requires that the responsible organisation establishes some form of administrative security program (minimum security management controls) to protect critical cyber assets.

NERC CIP 004-2 requires that the responsible organisation ensures that personnel (including external personnel of various types) that are given digital access or unmonitored physical access to critical cyber assets have the necessary training and security awareness.

NERC CIP 005-2 requires that the responsible organisation identifies and protects so-called electronic security perimeters that enclose the critical cyber assets and identifies and protects all access points in these perimeters.

NERC CIP 006-2 requires that the responsible organisation implements a program for physically protecting critical cyber assets.

NERC CIP 007-2 requires that the responsible organisation defines methods, processes and procedures to secure the systems that have been defined as critical cyber assets. This also applies to non-critical cyber assets that are within the so-called electronic security perimeters.

NERC CIP 008-2 requires that the responsible organisation identifies, classifies, responds to and reports security incidents related to critical cyber assets.

NERC CIP 009-2 requires that the responsible organisation establishes recovery plans for critical cyber assets and that these plans follow established practices and techniques for emergency preparedness and contingency planning.

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

Type of document	Recommendation
Publisher	National Institute for Standards and Technology (NIST), U.S.
Version	Final Draft (September 2007)
Scope	156 pages (including appendices)
http://csrc.nist.gov/publications/nistpubs/	

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

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

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

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

Section 4: The section provides a general description of security programs for reducing the risks associated with the vulnerabilities identified in section 3.

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

Section 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 to industrial control systems.

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

CPNI Good Practice Guide Process Control and SCADA Security

Type of document	Recommendation
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/Products/guidelines.aspx	

The documents are generally formulated and can be used in all areas in which process control systems are used.

- 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.
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 defense-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 organizational leadership should establish expectations for cyber security performance and hold individuals accountable for their performance.
21. Establish policies and conduct training to minimize the likelihood that organizational 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	Oljeindustrins Landsförening (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/category180.html	

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 och U.S. Department of Homeland Security
Version	February 2008
Scope	120 pages (total)
http://www.msisac.org/scada/	

This document is intended for use in setting security requirements in the procurement of industrial control systems. Examples of requirement specifications, including testing measures, are given for each main area. 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, hardware confirmation and operating system updating.

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

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

Programming practices: The section addresses requirements for documentation of vendor-developed code.

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

Malicious code: The section addresses, for example, requirements regarding detection and protection against malicious code.

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

Local units: The section addresses requirements for security in IED, PLC, RTU, etc.

Remote access: The section addresses requirements for various control system connections.

Physical security: The section addresses physical security requirements, such as those concerning availability of process components.

Network partitioning: The section addresses requirements for network units and architecture.

Information resources (selection)

Extensive international initiatives are underway regarding security in industrial control systems. A good way of staying up-to-date is to regularly follow what is written on 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.
http://www.us-cert.gov/control_systems/

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

Swedish IT Incident Centre (Sitic)
http://www.sitic.se

Swedish Civil Contingencies Agency (MSB)
http://www.msb.se/scada/

Collaboration between:

MSB Swedish Civil Contingencies Agency

SVENSKA KRAFTNÄT SWEDISH NATIONAL GRID

Säkerhetspolisen Swedish Security Service

LIVSMEDELS VERKET NATIONAL FOOD ADMINISTRATION

The purpose of this guide is to provide support in efforts to increase security in industrial control systems and to increase awareness of these issues.

Industrial control systems constitute a critical part of the systems that supply society with electricity, heating, drinking water, fuel and transportation for people and goods. Disruptions in industrial control systems can lead not only to the destruction of expensive equipment, but also interruption of critical operations. This, in turn, can result in extensive costs and lost confidence for both the individual company and society at large.

This document provides fundamental recommendations on security in industrial control systems. The document also provides tips on where additional information can be found.

Part A is intended for those who work with security issues at the management level.

Part B is intended for those who work with security in industrial control systems in practice.

MSB Swedish Civil Contingencies Agency
Norra Klaragatan 18   SE-651 81 Karlstad   Sweden   Tel +46 (0) 771-240 240   www.msb.se/en
Publ. no 0184-10   ISBN 978-91-7383-089-8