Swedish Civil Contingencies Agency

Guide to Increased Security in Industrial Information and Control Systems

Guide to Increased Security in Industrial Information and Control Systems

Guide to Increased Security in Industrial Information and Control Systems

Also available in Swedish, July 2014:
Vägledning till ökad säkerhet i industriella informations- och styrsystem

Swedish Civil Contingencies Agency (MSB)

Layout: Advant Produktionsbyrå
Print: DanagårdLiTHO

Order No: MSB766 - November 2014
ISBN: 978-91-7383-500-8

Contents

Foreword **5**

Summary **7**

Introduction **11**

Guide to Increased Security in Industrial Information and Control Systems 11

Part A – A summary overview **13**

Industrial information and control systems 14

Developments and trends within industrial information and control systems 19

Security in industrial information and control systems is important! 23

Good security culture – a basic requirement 27

Part B – Recommendations and objectives **29**

Recommendations for increased security in industrial information and control systems 31

1. Secure management's commitment and responsibility for security in industrial information and control systems 32
2. Clarify roles and responsibilities for security in industrial information and control systems 34
3. Maintain processes for system surveys and risk management in industrial information and control systems 36
4. Ensure systematic change management in industrial information and control systems 38
5. Ensure systematic contingency planning and incident management in industrial information and control systems 40
6. Introduce security requirements in industrial information and control systems right from the start in all planning and procurement 42
7. Create a good security culture and heighten awareness of the need for security in industrial information and control systems 44
8. Work with a security architecture in the industrial information and control systems 46
9. Continuously monitor connections and systems in order to detect intrusion attempts in industrial information and control systems 48
10. Conduct regular risk analyses of industrial information and control systems 50
11. Conduct periodic technical security audits of industrial information and control systems 52
12. Continually evaluate the physical security of industrial information and control systems 54
13. Regularly ensure that any and all connections to industrial information and control systems are secure and relevant 56
14. Harden and upgrade industrial information and control systems in collaboration with system vendors 58
15. Conduct training and practice regarding IT incidents in industrial information and control systems 60
16. Follow up incidents in industrial information and control systems and monitor external security problems 62
17. Participate in user associations, standardisation bodies and other networks for security in industrial information and control systems 64

Part C – Reference list with comments **67**

Glossary **82**

Checklists **84**

Information resources (selection) **86**

Foreword

Electricity supply, water supply and transportation are examples of critical societal functions. In order to control and monitor this infrastructure and the processes necessary for these functions to run smoothly, *industrial information and control systems* are used. Interruptions to these control systems can lead to the disruption of critical societal functions, which can in turn lead to serious consequences for society.

The purpose of this guide is to increase awareness of the need for high security in industrial information and control systems. The guide shall also serve as a concrete support for those working within critical infrastructure.

The first edition of this guide was published in 2008 and has received a wide distribution, both nationally and internationally. It has also become standard in many sectors. With this third edition, the document's name has been changed to *Guide to Increased Security in Industrial Information and Control Systems*. Through this name change, we would like to emphasise the increasing dependency between process IT and administration IT.

With this revision, we have also supplemented the recommendations with a number of objectives for the security work in order to make it easier for the reader to link the recommendations to their own organisation.

The recommendations provided in the guide are supported by the members of the Swedish forum for information sharing[1] concerning industrial information and control systems, and the work on this document has been significantly facilitated by the generous help we received from both the forum's representatives and the authorities that have been involved in the work.

Stockholm, November 2014

Richard Oehme
Director, Office of Information Assurance and Cybersecurity
Swedish Civil Contingencies Agency (MSB)

1. Since 2005, the Swedish Civil Contingencies Agency (MSB) has conducted the FIDI-SC forum for increased security in industrial information and control systems, where the group's work is based on a model for trust-based information sharing developed in the UK by CPNI (Centre for the Protection of National Infrastructure). Representatives from several industries that use industrial information and control systems meet regularly to share information and exchange experiences.

Summary

Summary

Computerisation of the systems that supply society with fuel, electricity, heating, water and transportation is happening at a rapid rate. Several modernisation projects are being initiated in order to replace older technology with newer IP-based technology, and various IT systems are being integrated to make operations more efficient.

Industrial information and 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 traditional/administrative IT systems and industrial information and control systems are becoming blurred as integration between these different systems increases. In order to achieve a high level of flexibility and efficiency, industrial information and control systems are also becoming increasingly available via the Internet and other public networks. Today's industrial information and control systems are also to a greater degree built on the same technology as standard IT systems and are therefore subject to the same security problems.

This development results in an increased attack surface and a radical change to the risk picture.

Disruptions in industrial information and control systems can lead not only to the destruction of expensive equipment, but also to the 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 information and control systems is to follow these basic recommendations:

Increase awareness of the need for security in industrial information and control systems throughout the entire organisation.
This is a business-critical matter and therefore executive management should be involved at an early stage. This also includes the clarification of roles and responsibilities within the organisation and the facilitation of a good security culture.

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 business planning also need training in these subjects.

Work actively with a security architecture within industrial information and control systems and any connected IT systems.
Survey and identify the existing industrial information and control systems. It is especially important to identify external connections. Then create a zone model where the defence-in-depth concept is implemented. A part of the defence-in-depth concept is to implement the monitoring and detection


STANGD
ÖPPEN
0.0
0.00
9.9

of intrusion attempts in the zone boundaries. The administrative IT systems should only in exceptional cases be integrated with the industrial information and control systems and, if this is done, these shall be placed in one or several defined parts of the zone model.

Set security requirements in all industrial information and 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 information and control systems after the systems have been delivered.

This document also offers detailed guidance in the form of 17 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.

Introduction

Introduction

Guide to Increased Security in Industrial Information and Control Systems

Many critical societal functions are based on functional information flows. Electricity supply, water supply and transportation are some examples. In order to control and monitor this type of operation, industrial information and control systems are used. As systems have a direct impact on physical processes, short interruptions can also have serious consequences for society. This necessitates high security requirements in industrial information and control systems. The main responsibility for establishing a high level of security rests on the provider of the public service. Since there are strong dependencies between different critical societal functions, it is important that organisations work together and share information, both within their sector and with other relevant sectors.

Working for increased security in industrial information and control systems is challenging as technological developments and changes in society are constantly altering the array of problems.

Structure

With this edition, the name of the guide is being changed to *Guide to Increased Security in Industrial Information and Control Systems* in order to reflect developments within the field. The guide provides 17 basic recommendations for increasing security and, through its widespread distribution, has achieved its status as a Swedish industry standard.

Purpose

The guide shall provide support in efforts to increase security in industrial information and control systems. The recommendations provided are based on internationally recognised recommendations, practices and working methods. It is however important to remember that there are sector-specific requirements that require additional security measures.

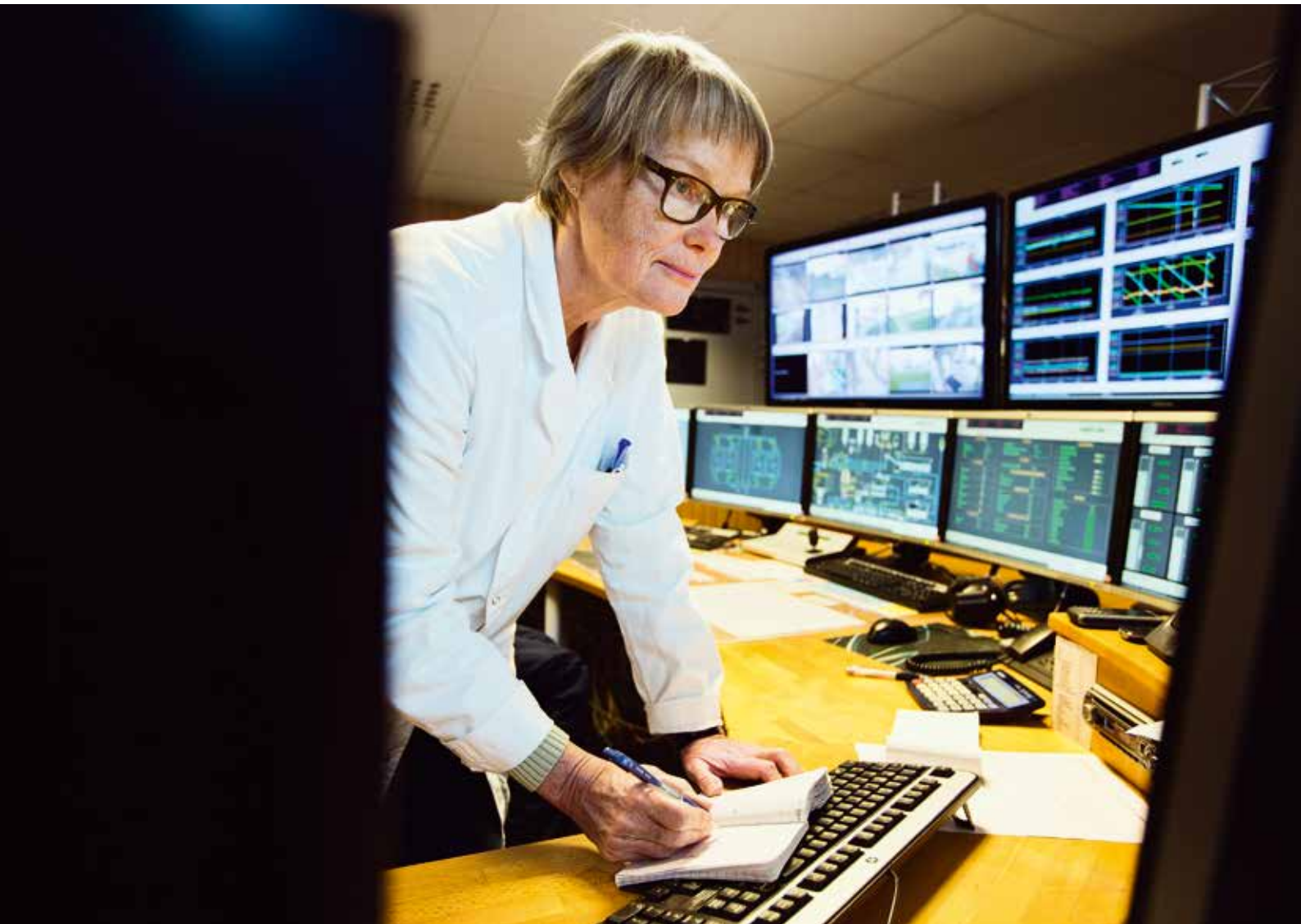
Scope and selection of references

In addition to an introduction to the subject area and basic recommendations, a selection of references are presented along with tips on where to find more information. The document primarily refers to standards, guidelines and recommendations that can be generally applied to increase the security in industrial information and control systems. Certain preference has been given to references that are not industry specific, that are in Swedish or English, and where possible are freely available.

Part A

Part A – A summary overview

It is important for IT systems that control critical societal functions to meet the security requirements. Unfortunately, this is not always the case. The fact is that security is often higher in administrative IT systems than in industrial information and control systems. In an office environment, it almost goes without saying that the operating system is updated several times a year, but in a deployed control system this is seldom the case since it can be highly dangerous to make changes without rigorous consequence analyses. How this has come to be and how we can deal with the situation is comprehensively described in this chapter.



Industrial information and control systems

Historically, physical industrial processes have been supervised by mechanical or electromechanical machines controlled and monitored by human operators. Nowadays, most vital societal functions, such as electricity production, drinking water production and transportation, are more or less controlled autonomously with the help of so-called *industrial information and control systems*. These are systems that not only store and process information but also control physical processes. The systems can for example turn on and off motors that open a sluice gate, shift the gears on the railway lines or change the load in a substation. It has also become common for these systems to be connected to the organisation's administrative systems. Since the administrative systems often have connections to the Internet, it is possible to use these systems to access the industrial information and control systems - maybe from the other side of the world. Figure 1 shows the basic design of an industrial information and control system.

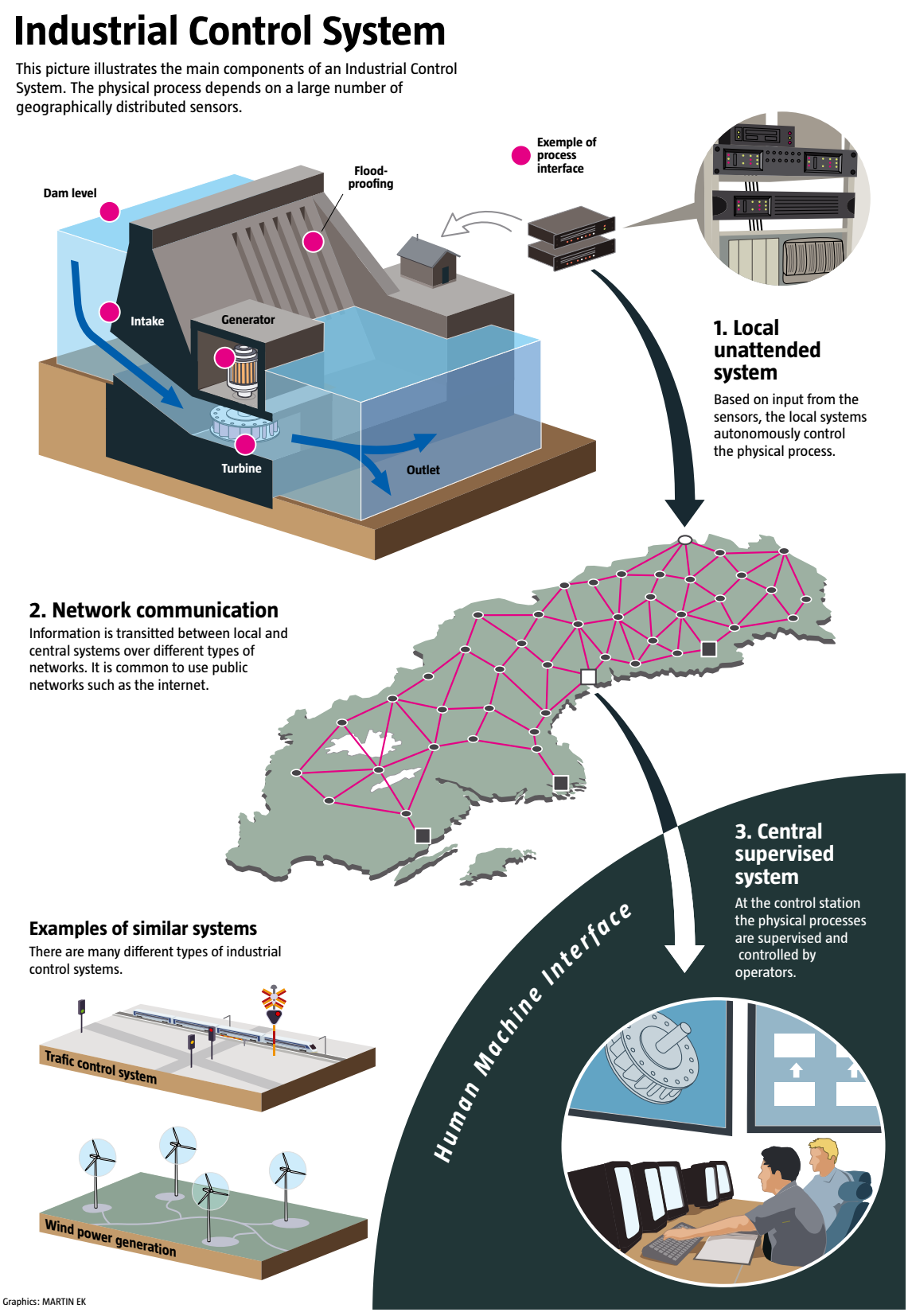


Figure 1. *Schematic structure of an industrial information and control system.*

The underlying *physical process* can contain a very large number of measurement points that can be spread over large geographic areas, sometimes across an entire country. The process interface is the point where the control system is connected to the physical process. It is primarily made up of sensors for monitoring and actuators for control.

The *local systems* that collect signals from sensors and transmit control signals to the physical process 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.

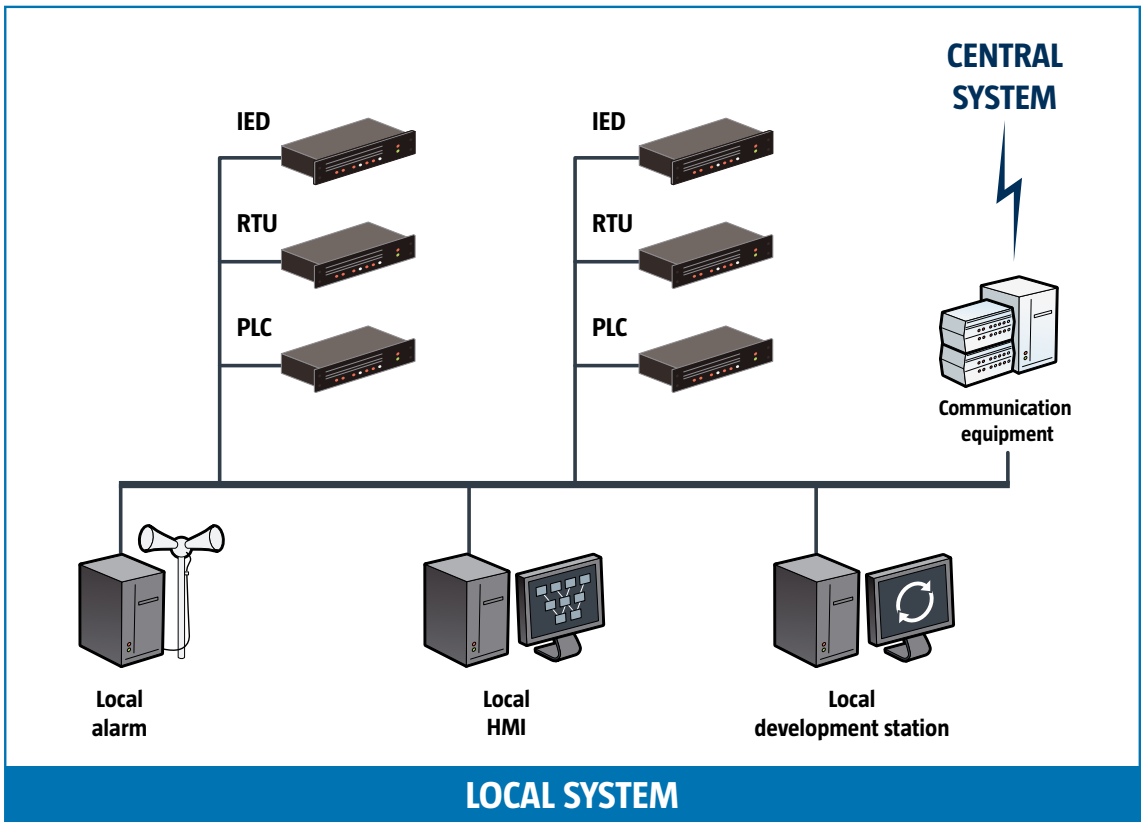


Figure 2. *The local systems receive signals from sensors and control physical processes via control computers. PLC – Programmable Logic Controller, RTU – Remote Terminal Unit, IED – Intelligent Electronic Device, HMI - Human Machine Interface. Local systems often communicate with a central system.*

Important functions that require data from many different parts of the physical process are run 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.

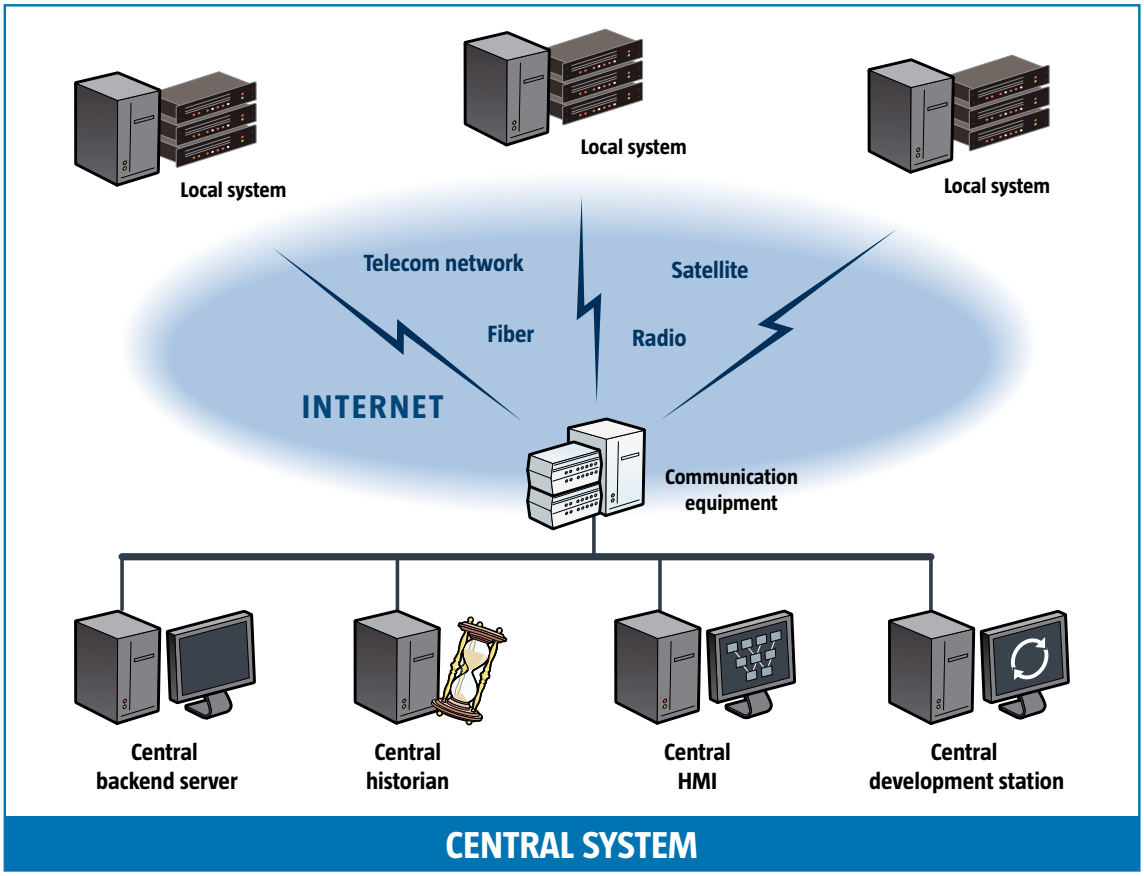


Figure 3. *The central systems receive information from the local systems and present the state of the processes in graphical interfaces. Through the interfaces, the operators can alter parameters and thus affect the local systems.*

The infrastructure between the different components of an industrial information and control system consists of *electronic communication and data transfer*. The communication can occur with a variety of communications protocols and across many different carrier services, for example via radio technology and wireless networks, or via fibre, copper cable and telephone networks. The long term trend has been to move away from vendor-specific solutions towards open standards and technology solutions that are used in everyday IT management. Thus, TCP/IP as the communications protocol and PC platforms have, in different ways and to varying degrees, made inroads in the industrial automation world. Security functions are often found within process automation that are capable of functioning as an emergency stop or in some other way temporarily able to take over the process control in the event of serious malfunctions or disasters. These are critical components that cannot be knocked out or break down. Here too, the evolution moves from simple mechanical components to solutions which are fully or partly digital and IT-based. In addition to the strict control and monitoring of the physical industrial process, the process networks often communicate with the administrative systems to increase operational efficiency. These systems can include quality systems, drawing/blueprint archives, spare parts inventory, diagnostics and statistics functions.

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).

THE PRINCIPAL FUNCTIONS OF INDUSTRIAL CONTROL SYSTEMS CAN BE EXPRESSED AS:

- 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

Other names for industrial information and control systems

There are a number of more or less overlapping designations for industrial information and control systems. Common designations include SCADA systems (Supervisory, Control and Data Acquisition), process control systems, process automation, process IT, technical IT systems, facilities IT, distributed control systems, real-time embedded systems (RTE) and so forth. Sometimes there are also industry-specific solutions or designations. In certain respects, there are technical differences, but we do not always emphasise these in this text. Instead we view all these variations from the perspective of automation controlled or supported by information technology.

Developments and trends within industrial information and control systems

The prerequisites for working with security in industrial information and control systems are changing. This section gives some examples of developments and trends that may affect the security challenges an organisation may face. Since the development is driven primarily to increase efficiency and profitability, it is important to constantly analyse the impact development has on security.

Responsible authority, modes of operation and deregulation

Previously, the state and municipalities often owned almost all critical infrastructure. This is no longer the case. Nowadays, many operations are being run by private and sometimes multinational corporations. Even within operations that perhaps are still publicly run, such as public transport and drinking water production, it happens that *parts* of the operation are farmed out to external actors. This kind of deregulation often leads to rationalisations and increased efficiency, but is not always optimal from a IT security standpoint. The fact that many operations are also multinational can in addition make it more difficult for local operators to receive support with regard to national requirements and standards. This can also mean that sensitive information on and in the industrial processes is stored in another country.

Organisational structure and culture

In recent years, process and operational areas have often become more significant than function and geography in terms of organisation, which in its turn affects the industrial information and control systems. A process-controlled operation can reduce the incentive for individual employees to be attentive to security problems. The fact that large parts are often farmed out on contract means that it also becomes more difficult to institute effective incident reporting. A cultural aspect of industrial information and control systems is that a form of "*industrial culture*" persists in certain organisations. In large production plants, the plant manager often has a prominent role, and it is harder for central functions to take over duties and responsibilities or affect internal plant processes. With regard to security, industrial culture can be both good and bad. For example, it often leads to long employment periods and with that, employees with a great sense of responsibility and a deep knowledge of the plant. But it can also lead to not regarding control systems as IT systems and, in doing so, current threats and vulnerabilities are disregarded.

Vendors and procurement

The vendors develop and provide what the market demands, which places high demands on the *purchasing and procurement processes*. As industrial information and control systems are often expensive and associated with legal requirements, the procurements have become more *centralised*. A centralised procurement process in which security issues are given significant attention can in many ways lead to increasingly secure and more uniform systems. One clear trend is that the vendors are represented by a number of specialists. Previously, one representative could describe an entire system. Nowadays, the organisations always encounter several representatives with different specialities, making it difficult to obtain a comprehensive picture of the industrial information and control systems. As modern information and control systems often consist of standard components, purchases are often coordinated with the purchase of administrative IT systems. This means that parts of the industrial information and control systems sometimes end up in the mainstream IT operational organisations and thereby, for example, risk being updated in the same way as the administrative systems. This can lead to security risks, as the industrial information and control systems often require extra precautionary measures when being updated.

Technology and service development

Industrial information and control systems are increasingly being built with standard components and it is therefore becoming more common to have PC platforms and communications solutions built on standard protocols (TCP/IP). The result is that more IT components are being introduced into many functions, which increases the number of communication paths into the industrial information and control systems. One example is monitoring functions that automatically contact the vendor for preventive maintenance or in connection with a malfunction in the equipment. This type of component with the capability to communicate electronically with other equipment can affect the operation of the industrial information and control systems or lead to unknown paths into the infrastructure.

Virtualisation and cloud services

The reason why *virtualisation* has become popular is mainly because it can lower costs and increase availability; for example through redundancy. It is also a method which enables the installation of old software on modern hardware, which is popular in the case of industrial information and control systems as a lot of the hardware is outdated. Unfortunately, virtualisation means that the real-time control is compromised and the systems are no longer isolated in the same way as before. Virtualisation also means that there is another layer of software that must be maintained and secured. At the same time, virtualisation can be an asset to those systems that, for example, do not have hard real-time requirements. However, before a virtualisation solution is introduced, thorough consequence analyses must be performed.

Similarly, cloud services have become popular, which requires technical, security-related, commercial and legal considerations. In industrial information and control systems, cloud services involves a higher degree of interconnectivity and increased exposure of the systems that control physical processes. Although cloud services may be appealing from a purely commercial point of view, costly customisations are often required to ensure their secure operation in industrial information and control systems.

SUMMARY CHARACTERISTICS OF INDUSTRIAL INFORMATION AND CONTROL SYSTEMS:

Investments
Industrial information and control systems often require large investments, leading to lengthy system service lives and depreciation periods. With the organisation introducing new work methods over time, there is a risk that the original security architecture will be undermined. As threats and risks change over time, in tandem with industrial information and control systems being rarely replaced, it is important that security issues are handled thoroughly in connection with investment decisions, procurement and implementation projects.

Customised installations and custom hardware
Industrial information and control systems are often customised for a specific industrial process. It is therefore difficult to achieve the uniformity or scalability pursued within traditional IT. The solutions often contain a mixture of standard components, embedded systems and vendor-specific hardware solutions. Security solutions and procedures for change must therefore be adapted to this heterogeneous system landscape.

Performance and availability
Industrial information and control systems must generally deliver precise response times in order for the physical process to be controlled properly. Availability requirements are therefore high and delays, such as those due to signal interference or insufficient bandwidth, are unacceptable.

Change management
The high availability requirements make it difficult to update the hardware and software in industrial information and control systems. Updates, system changes or maintenance of components and systems that affect the process must be planned well in advance.

Security in industrial information and control systems is important!

Security

Industrial information and control systems has the primary task of controlling and monitoring a physical process. At the same time, they also protect personnel, the environment, third parties and the physical equipment should an accident occur. Within critical operations, there is knowledge and awareness regarding operational security, availability, correctness and protective functions.

Historically, industrial information and control systems have been physically isolated and separated from other systems, which has meant that threats from the outside world have not been classed as a high priority. However, in the last decade, this physical isolation has more or less been erased for very many installations.

Integration with administrative information systems provides increased exposure to the Internet

To become more flexible and efficient, industrial information and control systems are increasingly connected to external public networks like the Internet. When the separation between different networks disappears, old and vulnerable systems are increasingly exposed to various threats that they have not been designed for. It is therefore important to raise awareness in the organisation with regard to the growing need for information and IT security.

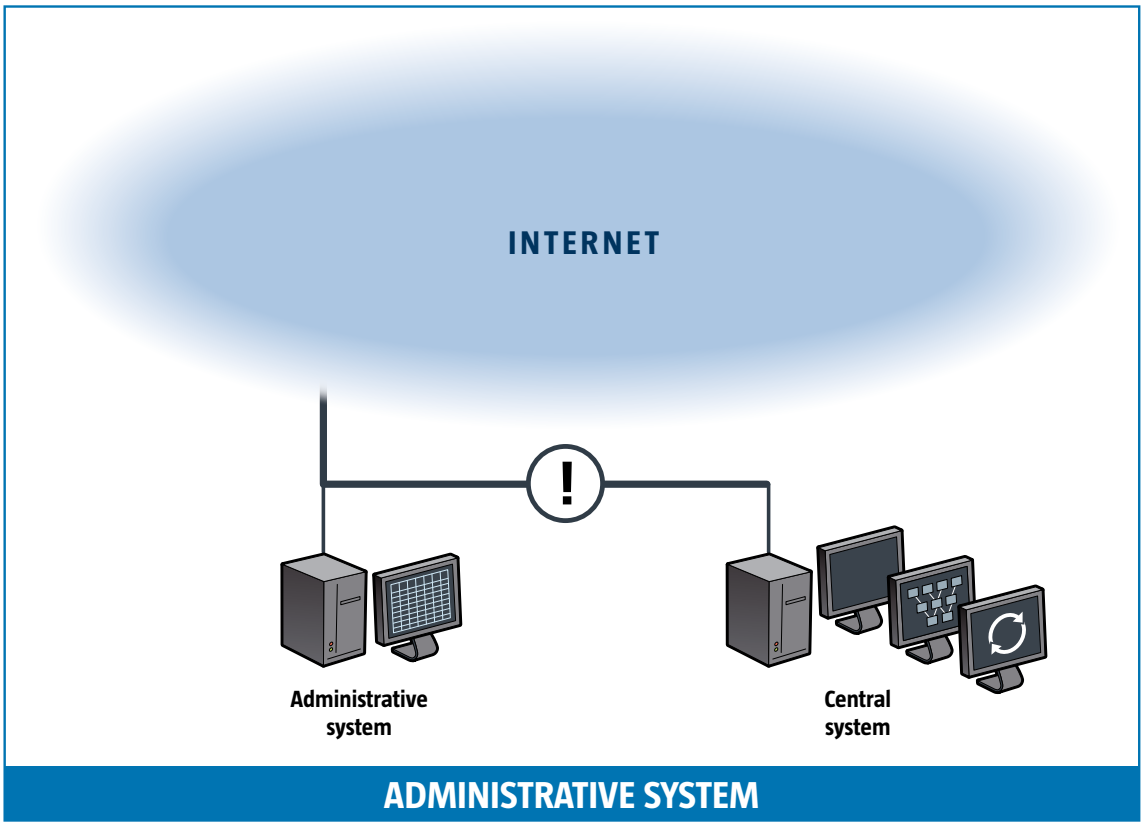


Figure 5. *When those systems used to control physical processes are connected to the administrative systems, the threat level rises significantly. Suddenly there is a path from the Internet into the sensitive control systems.*

In system solutions with a long service life, IT security holes often go unpatched

Industrial information and control systems are included in system solutions with a long service life, and can contain technical solutions from several generations. Correctly installed, these systems maintain a high degree 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 after the system has been put into daily operation. Since modern industrial information and control systems are often based on general IT systems, this often leads to a tendency within the organisation not to remedy newly discovered or known IT security vulnerabilities. Alternatively, it takes a very long time before updates are introduced. This means that industrial information and control systems are often very vulnerable to malicious attacks.

System integrators shall handle higher complexity

Vendors of industrial information and control systems have traditionally developed comprehensive solutions where they have both designed and built the systems they have provided. Nowadays, standardised technologies and components from the traditional IT world (often referred to as "Commercial-Off-The-Shelf" COTS) are also increasingly used in industrial information and control systems. Some examples of COTS-based products used include operating systems, IP-based communication technology and database solutions. Due to the conversion to standard components, the role of vendors is changing from system vendors to system integrators. This in turn can lead to them possessing a lower level of detailed knowledge with regard to vital parts of the integrated system. By extension, this requires increased knowledge of security in industrial information and control systems on the part of the end-users of the systems.

Attacks on control systems pose a real threat

Security has not been a priority issue in the development of industrial information and control systems. Security awareness on the part of equipment, system and program vendors as well as procurement officers and buyers is often weak. This often leads to unclear requirement specifications and the system not being designed to handle IT-related security in a suitable manner. These problems are compounded by the fact that nowadays there are a wide variety of tool boxes for cyber attacks available on the Internet. There are also descriptions of vulnerabilities in industrial information and control systems as well as instructions for how malicious code can be created.

In July 2010, *Stuxnet* was discovered, an advanced form of malicious code that attacked industrial information and control systems. Stuxnet used several different mechanisms to spread itself (including via USB memory sticks) in order to finally reach the industrial information and control systems. By manipulating basic programming blocks, Stuxnet could thus change the *physical process* without the process operators being able to see that something was wrong. According to most analysts, Stuxnet was tailored to attack and knock out a specific target – a uranium enrichment facility in Iran – without destroying anything else. There are already successors to Stuxnet that have been used in cyber attacks, such as Duqu and Flame (flamer, Skywiper)[2].

It is therefore not unlikely that, in the future, we will see direct successors of the above attacks that may not always be as well made, in the sense of being well-targeted. The successors may therefore represent a more serious threat to our relatively unprotected industrial information and control systems.

IT security problems can lead to operational disturbances

Because industrial information and control systems are used to monitor and control physical processes in real time, they have been developed with a specific focus on high availability. The current trend towards general data communication via TCP/IP-based networks guarantees no real time communication, but since they are built with excess capacity, it often works nonetheless. Unfortunately, this means that the systems become very sensitive to various disturbances. Malicious code can, for example, cause a system's response times to becomes unacceptable, or cause an alarm or commands to not be received in the manner intended. This can result in incorrect behaviour of the systems or the systems simply stop working.

2. Duqu and Flame are collections of computer malware with a modular design. This means that functions can be easily modified, added or removed in order to customise these attack frameworks for one or more specific targets or new attack vectors.

Good security culture – a basic requirement

To develop and manage secure industrial information and control systems requires not only technical solutions but, to a similarly high degree, a systematic way to work with information security regarding the systems and a good security culture in the organisation. MSB recommends that organisations implement an information security management system (ISMS) designed in accordance with the principles contained in ISO's information security standards (ISO/IEC 27001 and 27002), and also apply this management system to the industrial information and control systems. A well-developed management system provides a systematic way to work with information security based on general risk management that can be used, for example, in development projects and procurements. Those security solutions that are implemented thus become adapted to the organisation's need for protection regarding their information systems.

A systematic way to work with information security also leads to a good security culture, where management and employees have a common view of the risks and are motivated to implement and adhere to the necessary security rules. An additional benefit of a management system is that it leads to continuous security efforts that also support the operation and management of, for example, industrial control systems.

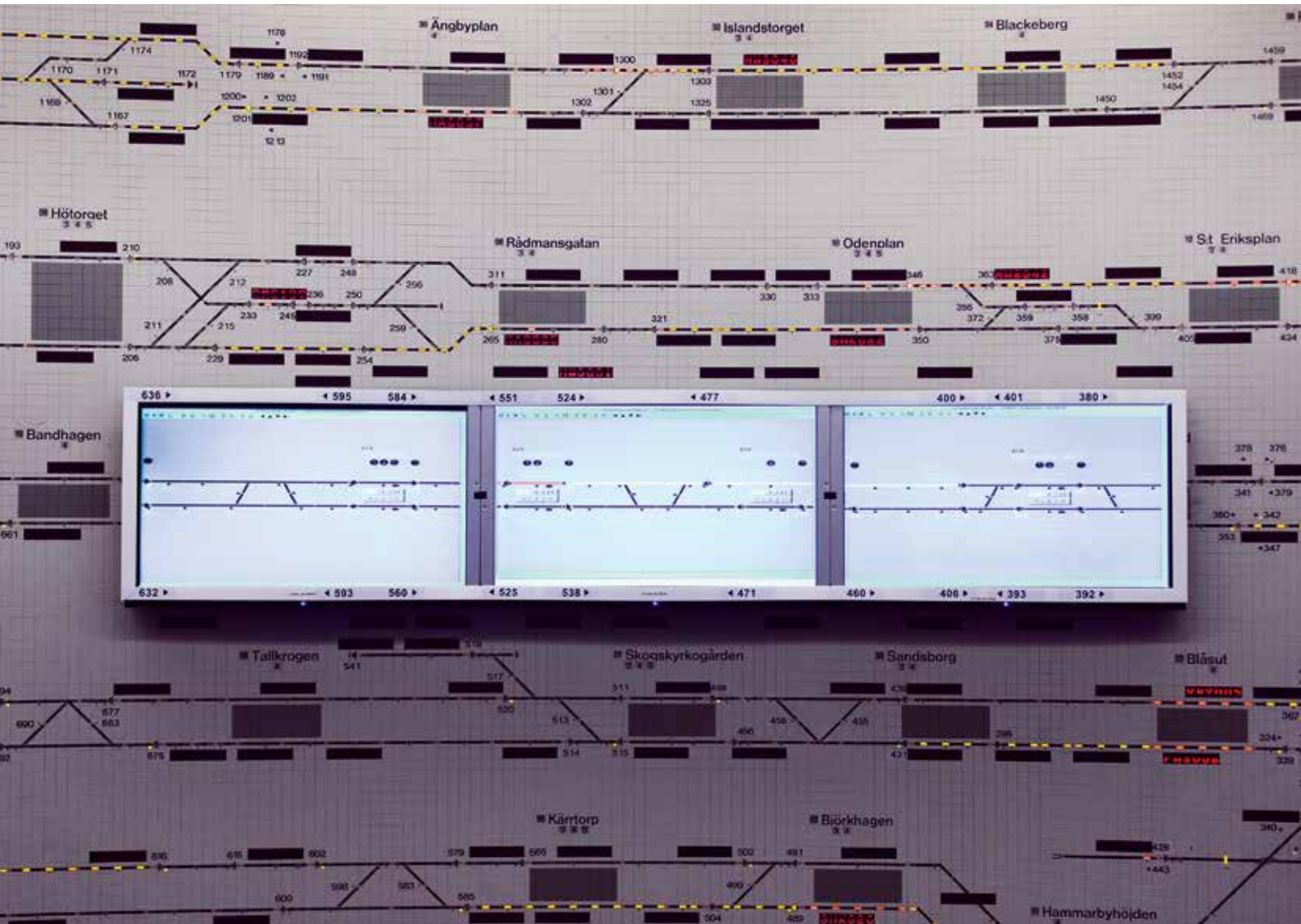
In order to provide support, MSB has developed a[3] methodological support that organisations can use in order to implement information security management systems. Our recommendation is to ensure that the management system is also applied in the case of industrial control systems.

3. www.informationssakerhet.se

Part B

Part B – Recommendations and objectives

There is no established recipe for how the work with security in industrial information and control systems shall be designed, but there are a number of accepted work practices that every organisation should implement. In this chapter, we have compiled 17 recommendations that will be helpful in achieving a good security culture and systematic security work with the industrial information and control systems. Some recommendations are technical in nature and others focus more on methodology.



Objectives for the security work

Each recommendation concludes with a number of objectives for the security work. The purpose of the objectives is for an organisation to roughly be able to appreciate how their own operations currently relate to each recommendation.

References and further information

For each recommendation, advice is provided on where to find more information. The established checklists and standards we refer to are described in more detail in Part C.

These are referred to as follows:

NERC CIP	NERC CIP-002-4 to CIP-009-4
NIST 800-82	Guide to Industrial Control Systems (ICS) Security
CPNI	Good Practice Guide Process Control and SCADA Security
DOE 21 Steps	21 Steps to Improve Cyber Security of SCADA Networks
OLF	Information security baseline requirements for process control, safety and support ICT systems
PL	Cyber Security Procurement Language for Control Systems
IAEA	Nuclear security series #17 (Computer Security at Nuclear Facilities)
2700[X]	SS-ISO/IEC 27000 series
ISA95	Manufacturing Enterprise Systems Standards and User Resources
IEC 62443[X-X]	Security Guidelines and User Resources for Industrial Automation and Control Systems

Recommendations for increased security in industrial information and control systems

1. Secure management's commitment and responsibility for security in industrial information and control systems.
2. Clarify roles and responsibilities for security in industrial information and control systems.
3. Maintain processes for system surveys and risk management in industrial information and control systems.
4. Ensure systematic change management in industrial information and control systems.
5. Ensure systematic contingency planning and incident management in industrial information and control systems.
6. Introduce security requirements in industrial information and control systems right from the start in all planning and procurement.
7. Create a good security culture and heighten awareness of the need for security in industrial information and control systems.
8. Work with a security architecture in the industrial information and control systems.
9. Continuously monitor connections and systems in order to detect intrusion attempts in industrial information and control systems.
10. Conduct regular risk analyses of industrial information and control systems.
11. Conduct periodic technical security audits of industrial information and control systems.
12. Continually evaluate the physical security of industrial information and control systems.
13. Regularly ensure that any and all connections to industrial information and control systems are secure and relevant.
14. Harden and upgrade industrial information and control systems in collaboration with system vendors.
15. Conduct training and practice regarding IT incidents in industrial information and control systems.
16. Follow up incidents in industrial information and control systems and monitor external security problems.
17. Participate in user associations, standardisation bodies and other networks for security in industrial information and control systems.

1 Secure management's commitment and responsibility for security in industrial information and control systems.

27001
27002 (Chapter 5, 6.1.1)
CPNI (GPG 7)
OLF (No. 1)
IEC 62443-1-1 (Chapter 5.8.2)

Management is responsible for running the company's operations in a business-like manner and it is not always certain that the security of industrial information and control systems receives the attention it requires. One reason could be difficulties in seeing how security investments in the short-term contribute to business performance. It can be especially difficult to address those specific information security-related aspects prevalent in the industrial information and control systems. For many, information security only relates to the administrative systems.

In order to motivate management to understand and highlight these issues, a sustained educational initiative is required. It is important to respect the fact that security work is often perceived as something boring and tedious. It is therefore important to explain how a heightened level of information security in the industrial information and control systems improves the business.

A first step can be to try to make time for a short presentation during a management team meeting. It is important to be well prepared before such a meeting. Avoid scaremongering. Instead describe the way in which the business can become more efficient by managing risks at an early stage. When you discuss risks, try to make the risks concrete and describe how they can be remedied and thus improve the business. Also prepare a tangible and relatively simple proposal for what the next step might be – for example, a risk analysis of a defined part of the industrial information and control systems.

An important goal is to ensure that the industrial information and control systems are taken into consideration in the organisation's information security management system (ISMS). If there is no ISMS in the operations, the first step is then to have management assign someone the task of developing such a system.

Other recommendations in this guide contain proposals for elements that should be considered in the organisation's systematic information security work in respect of the industrial information and control systems.

Recommendations

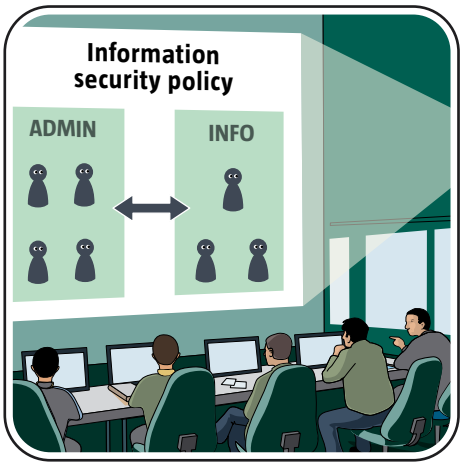
- Work with long-term objectives and try to get management themselves to show an interest in security work and the benefits it can yield for the business.
- Try to describe what different measures cost – both in investment and in working hours. Relate the cost to the benefit that the measures yield for the business.
- Propose tangible changes in the organisation's steering documents with the goal of having the industrial information and control systems considered in the systematic information security work.
- Avoid talking about technology and instead focus on how long-term efficiency can be improved concurrently with increased security work in the industrial information and control systems.
- Use specific examples applicable to the operations in question in order to explain what IT security in the industrial information and control systems entails.

Example of risks and problems

In an organisation, there are general rules for how employees should act with regard to security. After an incident where a USB memory stick had infected a computer in the production environment, it was found that management had failed to update the steering documents for over four years. There was no designated person responsible for the ongoing implementation of relevant risk analyses and the updating of guidelines in the governing document for the business. The management team had not formally signed the steering document which led to some doubts regarding the validity of the guidelines. Therefore the prevailing culture within the organisation was one where the steering documents did not need to be adhered to, since no one at the executive level seemed to care about or even be aware of the rules. For example, many managers themselves used USB memory sticks to share files with each other without reflecting on the guidelines that were laid down specifically regarding risks with USB memory sticks.

OBJECTIVES FOR THE SECURITY WORK
There is an information security policy that includes industrial information and control systems.
Management actively highlights the importance of following the information security policy.
Management is informed about and approves regularly updated risk analyses and action plans for the industrial information and control systems.
All members of the management team have a basic understanding of the differences in security and functional requirements between the administrative systems and the industrial information and control systems.

2 Clarify roles and responsibilities for security in industrial information and control systems.



NERC CIP (003-4)
NIST 800-82 (Chapter 4.2, 6.1, 6.2)
CPNI (GPG 4, GPG 7)
DOE 21 Steps (No. 12, 16, 20)
OLF (No. 1, 3)
27002 (Chapter 6, 8)
IAEA (Chapter 4, 5.1)

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 information and control systems, this allocation of roles and responsibilities is often non-existent. 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, whose main area of expertise lies outside of logical security in information and control systems. This leads to an organisation having insufficient or no knowledge of the IT properties of the industrial information and control systems. Subsequently, there is reduced control and ability to manage how the technology is used.

Recommendations

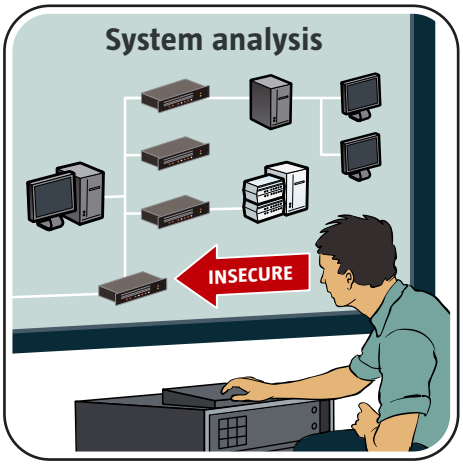
- Create an information security policy for industrial information and control systems. The allocation of responsibilities for security issues is most easily clarified in this way. The policy can either be a separate document, which must then be related to the organisation's other steering documents, or the issue may be resolved through supplements to the organisation's information security policy.
- Coordinate the allocation of roles and responsibilities in respect of the administrative information systems and the industrial information and control systems. It should be clear which systems are managed by the organisation's central IT support and which systems are managed locally at the production location.
- Let the organisation's central IT support be responsible for the overall integration and create a coherent approach to the security issues even though some systems are managed locally.
- Clearly document the requirements imposed on a system owner.

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 the culprit 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.

OBJECTIVES FOR THE SECURITY WORK
There is one person in charge of the overall security of the industrial information and control systems.
For each mission critical system, there is one person appointed as system owner.
The system owners' duties, responsibilities, resources and mandates are clearly documented.
All system owners are aware of their responsibilities.
There are documented requirements for a system owner, such as expertise, training, security classification, etc.

3 Maintain processes for system surveys and risk management in industrial information and control systems.



NERC CIP (002-4)
DOE 21 Steps (No. 13)
OLF (No. 2, 3, 11)
27002 (Chapter 4)
27005
IAEA (Chapter 5)
EC 62443-1-1 (5.6)
IEC 62443-2-1 (4.2, 4.3)

To maintain proper security in industrial information and control systems, it is important that there is a process to survey and understand the operation's information flows, information assets and system dependencies. That is, the relationship that exists between the activities and the different types of systems.

Analysing the operation's processes, systems and information requires a deep understanding of the consequences that a faulty or disrupted function may involve, both for the physical process and for the organisation. This is an important prerequisite for creating a relevant risk evaluation and a classification of which systems are most critical and which information is most critical.

An organisational and system survey should result in lists of access and connection possibilities, system classifications and operational priority classifications. There should be diagrams of the industrial information and control systems which are detailed enough to make critical components and systems identifiable. A system diagram shall, for example, contain IP addresses, communications protocol, version number, information on the operating system of computer resources, technical information about local devices such as PLCs, and so on. It is also helpful if each component in the system diagram has a unique serial number that points to an entry in a configuration database. In order to establish the electronic security perimeter, all connections to industrial information and control systems must be identified. In addition to the Intranet, this includes, for example, remote connections to business partners, vendors and the Internet. Note that all wireless connections should be treated as remote points. Connections to the organisation's administrative information system (Intranet) should be considered external connections.

Recommendations

- Take an inventory of the organisation's assets and identify those that are critical by applying a risk-based approach. Then identify the critical cyber assets.
- Establish a documented process for how risk analyses are carried out and the conditions under which they are updated. Select a risk analysis method based on purpose of the analysis and the information available. The choice of method should take into account the ability to easily update the risk analysis.
- Maintain a configuration database to facilitate the search for various components and parameters in a complicated network topology.

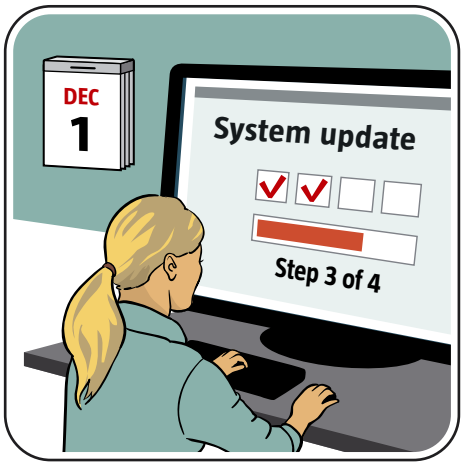
Example of risks and problems

The industrial information and control systems of an organisation were regarded as separate from other computer networks, and it was therefore not considered necessary to provide them with protection against malicious code. But when the organisation's administrative office network was infected by malicious code, several of the control systems were also knocked out. A closer examination of the activities identified several previously unknown connections between different computer networks. As these had not been documented, they had never been taken into account during previous security analyses. Consequently, the organisation was of the belief that their system was far more secure than it actually was.

One of the reasons these vulnerabilities had not been identified was that the organisation lacked a well thought-out process for how and when the system survey and risk analyses would be performed. It thereby lacked data to compare and monitor operational risks and how these had changed over time. The consequence was that important parts of the control system remained unprotected year after year while considerable resources were expended to protect other information assets, which however were not as critical to the company's survival.

OBJECTIVES FOR THE SECURITY WORK
There is clear and updated documentation on the operation's systems, information flows and system dependencies.
The systems are classified in order to identify which of them are critical to the organisation.
There is clear and updated documentation on all communication paths to and from the industrial information and control systems.
There are clear guidelines as to how, and how often, classification and risk analyses should be performed in order to identify critical information assets.
All mission-critical systems and components can be quickly identified with the help of system diagrams, configuration databases, network maps and similar.

4 Ensure systematic change management in industrial information and control systems.



NERC CIP (003-4)
DOE 21 Steps (No. 17)
OLF (No. 10, 15)
27002 (Chapter 12.5.1, 10.1.2)

Systematic 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 information and 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.

In the industrial information and control systems, it is important that all involved parties – vendors, system administrators and users – have a correct and common understanding of the system's current configuration and operational status. Separate testing, development and operating environments are common for administrative information systems. Unfortunately, this is not the case for industrial information and control systems, which makes it even more important to allocate sufficient resources to systematic change management in these systems. There should be a formal process that specifies how to obtain authorisation to make changes in industrial information and control systems. This should also apply to temporary changes and changes to support equipment. Everything that is not explicitly authorised should be forbidden.

Recommendations

- Upgrade software incrementally. Preferably in consultation with system vendors, due to legal and technical requirements.
- Ensure that the formal process for change management includes:
  1. a description of what is subject to authorisation requirements,
  2. a procedure for obtaining authorisation to make changes,
  3. a description of how tests before and after a change are to be conducted (including a description of the changes that require testing in a separate test environment),
  4. requirements for how documentation shall be updated after changes
  5. and requirements for how personnel shall be informed of changes (for example, in which cases special operator training is required).

- Ensure that rules and procedures related to changes in the industrial information and control systems are in keeping with existing change rules in physical processes or facilities.
- Inspect tools (computers/laptops) used for updates of settings and programs.
- Check the management of the hardware and software tools, such as compilers and file transfer methods, used in the change process.
- Check devices so that only known and verified system software (firmware) is used.
- Perform differential checks against previous versions before and after all updates.

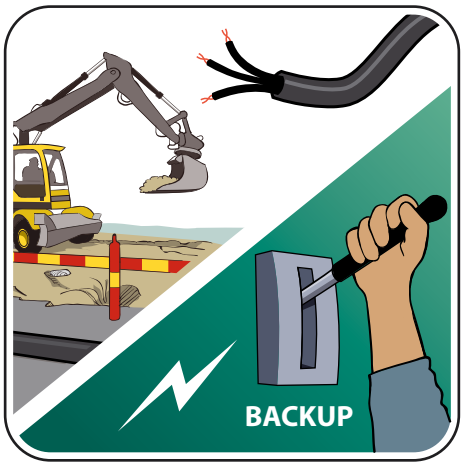
Example of risks and problems

The industrial information and control system of an organisation became increasingly unstable over time, which resulted in unanticipated system events. Some functionality disappeared and all parameters reverted to their default factory settings. During a later investigation it was 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 had, due to the unplanned and unexplainable stop in production, an impact on the confidence in the organisation. 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.

OBJECTIVES FOR THE SECURITY WORK
There are documented procedures in place for how often all the different systems are to be updated or checked.
It is possible to deduce which hardware and software (version and "patching") that has been in operation, and how it has been configured, at a given time.
There are clear procedures for how faulty system components are replaced.
There are rules for how external consultants and vendors can connect equipment to the industrial information and control systems.
Before and after changes in the industrial information and control systems, affected parties are always informed of the change.
Changes (configurations, "patching", etc.) are always tested in a separate test environment before being installed in daily operation.

5 Ensure systematic contingency planning and incident management in industrial information and control systems.



NERC CIP (008-4, 009-4)
NIST 800-82 (Chapter 6.2.3)
CPNI (GPG 3)
DOE 21 Steps (No. 19)
OLF (No. 7, 16)
27002 (Chapter 13, 14)
27035
IEC 62443-1-1 (Chapter 4.3.2.5)
IEC 62443-2-1 (Chapter 4.3.4.5, A.3.4.5, 4.3.2.5, A.3.2.5)

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 information and control systems, it is often the case that the restoration of the system must happen quickly, and tolerance for error is minimal. It is therefore particularly important to ensure backups for these systems.

All unexpected events (incidents) that lead to a disturbance in the industrial information and 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.

Recommendations

- Establish and maintain incident management procedures and contingency plans for the industrial information and control systems.
- Analyse incidents to determine and understand the problem of origin, the extent (spread), and the direct and indirect consequences. Check, for example, if it is a case of simple errors and whether they occurred due to intentional or unintentional events.
- Ensure that the following items are included in the contingency planning:
  - 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 system owners, operators, service technicians, other personnel, vendors and support
  - description of support agreements and suspension times
  - 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.

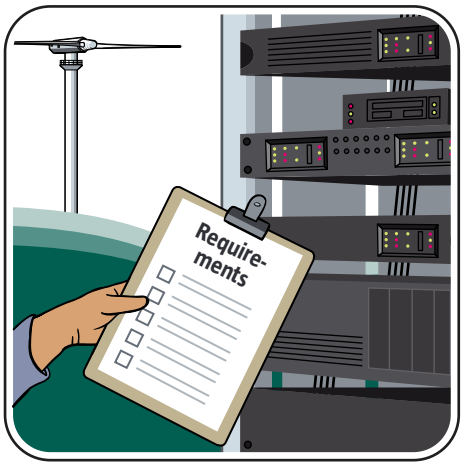
Example of risks and problems

An organisation ran into trouble when a key individual who served as system administrator of a critical information and 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 duties.

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.

OBJECTIVES FOR THE SECURITY WORK
The contingency plans cover critical information assets in the industrial information and control systems.
There is a documented process for the development and maintenance of contingency plans.
There are clear definitions of what constitutes an incident and how different types of incidents should be handled.
All employees, including management, encourage co-workers to notify a relevant part of the organisation, for example system owners, in the event of discovered weaknesses or vulnerabilities in the system, organisation, documentation, etc.
Reported incidents are immediately analysed and reported to executive management according to fixed intervals.

6 Introduce security requirements in industrial information and control systems right from the start in all planning and procurement.



NIST 800-82 (Chapter 6.1.3)
CPNI (GPG 6)
OLF (No. 8, 9)
PL (all chapters)
27002 (Chapter 6.2, 10.2)
IEC 62443-2-1 (4.3.4.3, A.3.4.3.4)

Since it is difficult and expensive to achieve an acceptable level of security in industrial information and 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 information and 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 industrial information and control systems, special consideration must be given to IT security matters since the changes will most likely affect the existing information and control system in a manner that the original designers had not considered. For example, in older information and control systems there was often a presumption that access to equipment would only be possible via local physical presence. Nowadays, physical separation is no longer always possible which places high demands on a logical separation between different parts of the industrial information and control systems.

Recommendations

- Use threat and risk analyses as well as various surveys to gather requirements.
- Follow up that vendors satisfy detailed requirements for security and protective functions in systems and applications.
- Require the vendors to present their methods and processes (such as internal developer handbooks) used to guarantee the quality of their own security work.
- Be sure that vendors receiving information on the industrial information and control systems sign non-disclosure and security agreements.
- Include requirements for deployed equipment to be tested in a secure manner. A control computer, for example, must be able to cope with the volume of traffic that occurs during a penetration test.
- Ensure that there are documented procedures for how security aspects should be taken into account during procurement.
- Conduct regular audits to ensure compliance.

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. They would likely also have obtained a better planned and better adapted security system.

OBJECTIVES FOR THE SECURITY WORK
There are documented procedures for how information security issues shall be handled during all procurement of goods and services.
Regular audits are conducted to ensure that procurement procedures are followed.
Security considerations are always documented for products or services supplied by external parties.
All external vendors receiving information on the industrial information and control systems always sign non-disclosure and security agreements.
All equipment and associated operational processes related to the industrial information and control systems are tested before they are deployed.
Management always ensures that managers from the process side are involved in IT procurements that have a bearing on the industrial information and control systems.

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

NERC CIP (004-4)

DOE 21 Steps (No. 21)

OLF (No. 5)

IAEA (Chapter 4.2)

27002 (Chapter 6.1.2)

It is important to establish the understanding that security in industrial information and control systems is a mission-critical issue. It takes long-term efforts to influence understanding and attitudes and the commitment of executive management is extremely important, as always when it comes to security matters. The importance of this commitment is in part because security in industrial information and control systems requires increased resources 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 information and control systems, it is necessary to have knowledge of traditional IT security, control systems and the underlying 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. It is also important to allocate time and resources so that different parts of the organisation can meet and exchange experiences.

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

Recommendations

- Establish an administrative security program to create a general approach to IT. This provides a good level of security awareness, encourages critical thinking and creates a positive attitude towards working with issues that improve security.
- Before a person is allowed access to the industrial information and control systems, he or she must undergo appropriate training. It is important that management understands the importance of training, allocates sufficient resources and continually revises the organisation's program for in-service training.

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. She 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 industrial information and 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.

OBJECTIVES FOR THE SECURITY WORK
There is a clear plan for the security training required of personnel who work with the industrial information and control systems, or have physical or logical access to them.
Executive management understands and approves the training plan at least once a year.
There is a unit within the organisation that regularly evaluates the approach to information security and reports to management.
At least one activity is organised every year during which process technicians and IT personnel meet and discuss security issues.
New employees and external consultants always receive basic security training before they are given physical or logical access to the industrial information and control systems.

8 Work with a security architecture in the industrial information and control systems.

NERC CIP (005-4, 007-4)
CPNI (GPG FirewallDeployment)
DOE 21 Steps (No. 5, 15)
OLF (No. 4, 13)
PL (all chapters)
IAEA (Chapter 5.5, 2.3.3)
27002 (Chapter 10, 11)
ISA-95
IEC 62443-3-3 (Chapter 9.4)

Working with a security architecture implies a structured and systematic approach to organising the protection and defence mechanisms of the organisation. The security architecture is based on a number of governing security principles with the aim of protecting information with regard to confidentiality, correctness, availability, and traceability. An important part of the security architecture is to maintain "defence in depth". Defence in depth consists of overlapping security mechanisms installed at several different levels in the network or in different systems and applications. The security mechanisms are sometimes redundant, e.g. multiple firewalls, and sometimes complementary, e.g. combinations of intrusion detection systems, firewalls, encryption of network traffic and data, authentication mechanisms and the logging of use and abuse.

Different security mechanisms can constitute boundaries in a zone model, where different zones represent groupings of components and systems with different security or functional criteria. In zone boundaries, a data diode, for example, can function as adequate protection in the event information is only permitted to be transported in one direction. A file gateway s another mechanism that can be used in a zone boundary. A data lock performs a more detailed and controlled examination of the data to be passed. The communication within an information and control system may also need to be protected. Communication between field equipment such as PLCs and local systems is usually based on industrial protocols with little or no security. Zone models should also be considered at this level.

Recommendations

- Design security architectures for industrial information and control systems that include principles and security concepts for
  - network security
  - system security
  - application security
  - operational security issues.
- Divide the industrial information and control systems into different zones with security levels adapted to how critical the systems are. Depending on system and information classification, among other things, so-called sub-zones may also need to be created.

- Divide up the network based on functional classification.
- Data traffic across zone boundaries should be handled with additional restriction and should also be monitored and logged. For certain types of IT environments, it may be useful to use data diodes and file gateways.
- Introduce functions for monitoring, alarming, traceability logs, network recording and analysis in zone boundaries.
- Avoid connecting IT systems and their support functions (e.g. data storage) to multiple zones in parallel (so-called multihoming), as this short-circuits the zone division and actively counteracts the zone model as a security concept.
- Place insecure services and other external connections in the demilitarised zone (DMZ).
- Create an electronic security perimeter (logical perimeter) around the industrial information and control systems. Note that the administrative systems are outside this security perimeter.
- The network architecture should be segmented with overlapping security mechanisms.
- Feel free to use different communications protocols between different parts of the network. If one protocol is used between the control system and a DMZ, another protocol should then be used for further communication between the DMZ and the organisation's administrative information systems.

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 could log in to all IT systems using a single password, a so-called Single-Sign-On (SSO). The operator could also remotely control the facility via the Internet over a virtual private network (VPN).

After a period of time, the organisation suffered operational disturbances which stemmed from an operator's computer becoming infected with malicious code at their 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.

OBJECTIVES FOR THE SECURITY WORK
The operation's constituent parts are divided into different zones. The division is documented.
No IT systems are connected to more than one zone.
The security architecture includes concepts for traceability and the logging of violations, errors and attack attempts.
The architecture has security mechanisms for confidentiality, correctness and availability.
Traffic going between two different zones is always logged.
The boundaries between two zones are equipped with alarm and monitoring functions.
If the administrative systems are interconnected with the industrial information and control systems, they are separated by a demilitarised zone.

9 Continuously monitor connections and systems in order to detect intrusion attempts in industrial information and control systems.

NERC CIP (005-4)
DOE 21 Steps (No. 8)
PL (Chapter 2.2, 3.2, 3.3, 4.4)
27002 (Chapter 10)
IEC 62443-3-1 (Chapter 8.4)
IEC 62443-3-3 (Chapter 10.4)

In addition to horizon scanning, monitoring of incidents and updating of risk analyses, the organisation needs to continuously monitor and detect intrusion attempts. Monitoring of own systems and their communications, combined with horizon scanning, provides a better understanding of current threats, changing attack trends and current malicious code. This monitoring should be performed both internally, within the organisation's own systems, and externally to monitor attacks against external connections.

There are primarily two types of intrusion detection systems (IDS). Some systems recognise attack attempts via analysis of communication flows – so-called network-based intrusion detection systems (NIDS). Others monitor events in a computer system or usage patterns in an application – so-called host-based intrusion detection system (HIDS).

An advanced variant of these systems are so-called intrusion prevention systems (IPS), which can also work to deflect attacks. Note that use of IPS in industrial information and 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 information and control systems.

So-called honey pots can also be used as a complement to indicate attack attempts in progress. Honey pots are often targeted to also collect information about an attacker or intruder. A simple solution that can be suitable in industrial information and 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 attacker is attempting to prepare for an attack by surveying the network.

Recommendations

- Continuously monitor external connections and internal systems to detect all forms of intrusion attempts.
- Continuously analyse logs and tracing data from intrusion detection systems.
- Establish long-term storage for logs and tracing data from intrusion detection systems. This data is needed if further investigation is initiated, which can occur long after the initial problem surfaced.
- There should be a role responsible for honing in on any warnings from the technical systems.

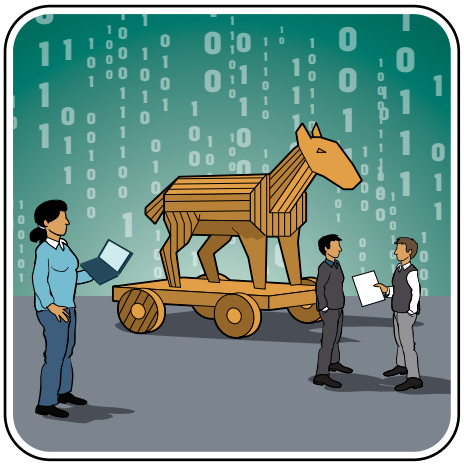
Example of risks and problems

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 and the industrial information and control systems, which severely increased the exposure of the control systems to malicious code and attacks.

Another organisation had procured intrusion detection service from an IT security company, but to save money it entered into an agreement that only 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.

OBJECTIVES FOR THE SECURITY WORK
All subsystems are monitored around the clock for suspicious activity.
There is always at least one person on duty that is immediately informed about suspected intrusion attempts.
If intrusion prevention protection is used, there is always a documented risk analysis which ensures that the system is not knocked out due to the erroneous refusal of traffic.
Log events and alarms from all intrusion detection systems are logged and stored in a secure place for at least six months.
The logs from the intrusion detection and incident management systems are analysed regularly.

10 Conduct regular risk analyses of industrial information and control systems.



NERC CIP (002-4)
NIST 800-82 (Chapter 3.2 – 3.6)
DOE 21 Steps (No. 14, 18)
OLF 104 (No. 2)
27002 (Chapter 4)
27005
IAEA (Chapter 6)
IEC 62443-1-1 (Chapter 5.6)
IEC 62443-2-1 (Chapter 4.2, 4.3)

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 is familiar with the system. When it comes to information and 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.

It is also important that risk analyses are carried out before introducing changes in an organisation. Since industrial information and control systems may have internal dependencies that are not always obvious, one should critically analyse the potential indirect effects of changes.

There are also risks that come to light without a formal risk analysis having been performed. It is important that there are processes to capture these risks and manage them according to their assessed level of seriousness.

Recommendations

- Conduct risk analyses of industrial information and control systems. A risk analysis can be conducted for a defined subsystem, or for a more general operation.
- Update the risk analyses in accordance with the methods that have been previously established and documented. The choice of risk analysis method to be used in the particular case depends on the purpose of the analysis and the information that is available on the system in question and its potential threats.
- Remember to update the system survey (system diagrams, configuration databases and the like) while updating the risk analysis, where necessary.
- Based on the operational analysis, there should be defined which systems and information resources that are mission-critical.
- The risk analysis shall be documented in a pre-defined manner and approved by management. The documentation should, at a minimum, include detected vulnerabilities and 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 industrial information and control systems as it considered them to be difficult to access and secure due to their unique nature. Thus, they had not identified critical vulnerabilities in existing systems, 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 gain access to and change more than their own system via their service accounts.

OBJECTIVES FOR THE SECURITY WORK
Management has determined how often risk analyses are to be performed on each critical information asset.
There is a documented method description for risk analyses performed on information assets connected to the industrial information and control systems.
Management always makes the formal decision on what risks are unacceptable.
There is an effective system for registering and managing discovered risks.
Suddenly revealed risks with major consequences are always handled immediately.

11 Conduct periodic technical security audits of industrial information and control systems.

DOE 21 Steps (No. 9, 11)

27002 (Chapter 15.2.2)

IEC 62443-2-1 (Chapter 3.4.3.5, A.3.4.2.4.2, A.3.4.2.4.3)

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 important differences between practical security tests on administrative IT systems and the IT equipment used in industrial information and control systems which often have poor security qualities (for example, field equipment such as PLCs and RTUs). 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 information and 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 of relevant personnel rather than automatic tools for penetration testing of traditional IT systems. Few IT consultants have sufficient knowledge of how to test industrial information and 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 have a discussion with system vendors prior to a security test.

When it comes to surveying information and 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.

Recommendations

- Conduct periodic technical security audits of industrial information and control systems and connected networks.
- Practical tests can negatively impact control systems and processes. These should therefore only be performed after careful preparation and once the possible consequences of the tests are understood. Instead, use passive methods and manually examine, for example, how routers are configured.
- If active tests are to be performed, then conduct these in a separate test system or in a control system that is not in operation.
- Continuous intelligence analysis should be carried out in order to acquire knowledge on discovered vulnerabilities that could affect the organisation's information and control systems.

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, one of which 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.

OBJECTIVES FOR THE SECURITY WORK
There are established procedures and intervals for the implementation of technical security audits.
A security audit never takes place without the approval of the relevant authorised manager.
All surveying of operational information and control systems is performed using only passive methods.
There is a person in charge of intelligence analysis for gathering knowledge on discovered vulnerabilities in products. This responsibility includes regular contacts with vendors.

12 Continually evaluate the physical security of industrial information and control systems.

NERC CIP (006-4)
NIST 800-82 (Chapter 6.2.2)
DOE 21 Steps (No. 10)
PL (Chapter 9, 11)
27002 (Chapter 9)
IAEA (Chapter 5.2.1)
IEC 62443-1-1 (Chapter 5.9)
IEC 62443-2-1 (Chapter A.3.3.3, A.2.3.3.8.9)
IEC 62443-3-1 (Chapter 10)

Industrial information and control systems, particularly central facilities, have historically had substantial physical protection and in many sectors there are established requirements for how important facilities are to be classified and physically protected.

Industrial information and control systems are often geographically dispersed (decentralised), which makes it more difficult to maintain good physical protection at the remote facilities. Attacks on industrial information and 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 protection. Cables and cross-connection spaces should be located in a manner that prevents unauthorised individuals from physically accessing them and connecting to the network.

Physical access to a system component makes it much easier to gain logical access to industrial information and control systems. Logical and physical security perimeters must therefore be strictly followed. Keep in mind that certain industries may have their own rules and requirements.

Recommendations

- Physical protection 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
  - cables for communication – minimise the risk of cables and cross-connection spaces being subjected to interception or manipulation
  - checks of environmental factors – such as ventilation and power supply.
- Establish a good level of physical protection in all facilities and spaces. Balance the physical and logical protections so that they are harmonised. Good physical security without corresponding efforts made with logical security, or vice versa, can undermine the work that has been done.

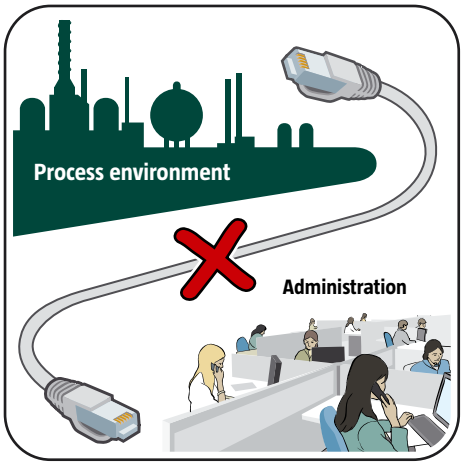
Example of risks and problems

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. Nor was a more extensive analysis of the equipment conducted on site.

One week later, unexplainable operational disturbances began to occur. Much later, 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.

OBJECTIVES FOR THE SECURITY WORK
Physical locations of the critical information assets are continuously documented and the documentation for this is also classed as a critical information asset.
Fire protection and building management systems are reviewed according to established procedures.
Cables and cross-connection spaces for communication between field equipment and other systems are carefully surveyed and protected from interception, manipulation and damage.
There are clear procedures for access control to all locations where critical information assets are found.
All physical perimeter protection of premises that harbour critical information assets is reviewed at regular intervals.

13 Regularly ensure that any and all connections to industrial information and control systems are secure and relevant.



CPNI (GPG 2, GPG Firewall Deployment)
DOE 21 Steps (No. 1, 2, 3, 7)
OLF (No. 4, 10, 12)
PL (Chapter 10, 11)
27002 (Chapter 10.6, 11.4)
27033

Industrial information and control systems have traditionally been physically isolated with few or no communications connections to the outside world. New business needs and efficiency improvement measures have resulted in streamlining solutions with integration between the information and control systems and the administrative 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 industrial information and 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 information and 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, fire alarms, etc.

Recommendations

- Regularly ensure that only relevant connections to the industrial information and control systems exist, and that these are sufficiently secure.
- Eliminate unnecessary connections. All existing connections are to be formally sanctioned by an authorised manager.
- 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.
- All user and system accounts should only have necessary authorisations. Access to files, applications and system resources should be denied if they are not explicitly permitted. All accounts should be equipped with fortified authentication.

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.

OBJECTIVES FOR THE SECURITY WORK
All ports and network services that are not needed are disabled. All active services are documented.
Modems (or other mechanisms for remote access) provided for vendors and consultants may be used only during specific times and under specific circumstances.
All connections between the administrative systems and the industrial information and control systems are sanctioned by an authorised manager.
Connections to physical security (e.g. alarms, building management systems, video surveillance, etc.) are physically separated from other equipment.

14 Harden and upgrade industrial information and control systems in collaboration with system vendors.

CPNI (GPG 5)
DOE 21 Steps (No. 4, 6)
OLF (No. 6, 10, 12, 13)
PL (Chapter 2)
27002 (Chapter 12.1.1, 12.4.1)

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 information and 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.

Recommendations

- Harden and upgrade industrial information and control systems so that they are as secure as possible.
- Maintain system security over time by continuing with the installation of patches, upgrades or similar.
- Make sure to document all changes that are made. It is advisable to log this in a configuration database. These recommendations also apply to all peripheral systems and aids – such as laptops used by support technicians – that are used to maintain and run the function.
- When replacing equipment or subcomponents, all new components should be hardened during installation. All hardening and upgrading should be handled according to procedures for change management (see Recommendation 4).

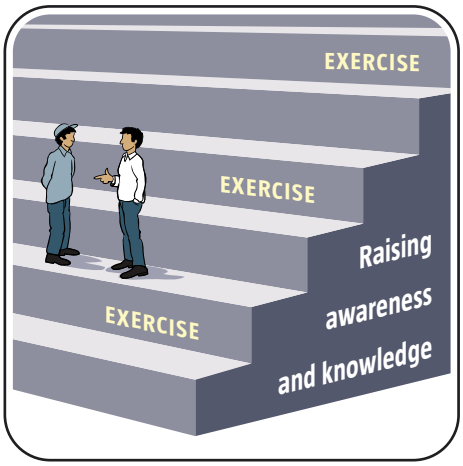
Example of risks and problems

A system vendor based several central information and 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.

OBJECTIVES FOR THE SECURITY WORK
There is clear documentation on how and when system hardening is to be performed or has been performed.
All upgrades, reconfigurations and "patches" are documented.
Default passwords for all functions in all equipment are replaced with advanced passwords.
All users' access rights are reviewed at fixed intervals.
All access to files and applications in the industrial information and control systems are denied unless rights are explicitly given. Minimal rights and the distinguishing and division of responsibilities prevails ("Separation/segregation of duties").

15 Conduct training and practice regarding IT incidents in industrial information and control systems.



IAEA (Chapter 4.2.1)

OLF (No. 5)

27002 (Chapter 8.2.2)

27035

IEC 62443-2-1 (Chapter 4.3.2.4)

Developments within IT have meant that many organisations have been able to develop new business models and have found new ways to make work more efficient. Unfortunately, this development also involves new security deficiencies which in turn lead to IT vendors being forced to develop new protection and so on. These constant changes make it important to engage in *ongoing in-service training*.

IT can constitute both the means and the target of different types of attacks. Industrial information and control systems are no exception. One problem is that many who work with these systems have a lack of experience with regard to IT-related attack scenarios. It is therefore important that the skills, procedures and processes that have been developed are practiced regularly. This applies mainly to the IT-related procedures, processes or process steps that rarely or never occur under normal conditions. With the help of exercises, the skills and experiences needed to be mentally and practically prepared for an incident when it actually occurs can be acquired. To implement a completely untested procedure in critical situations often involves great risks.

Exercises also lead to the improvement of methods, procedures and tools.

Recommendations

- Ensure that all who have responsibilities within the area have built up a good level of expertise and that, through in-service training, they maintain this level of expertise within their respective subject areas.
- Plan and carry out different types of exercises within the area of IT-related incidents within industrial information and control systems. As an initial step, exercises can be used as a learning element within incident management where IT is a key feature. When procedures, process steps and expertise are in place, the exercises can instead aim to maintain their skills but also to evaluate and fine-tune procedures, methods, tools and working methods.
- Have a documented strategy for exercise and training activities which is regularly reviewed by management. There should be a role with the responsibility for updating the exercise and training strategy.

Example of risks and problems

When a key server in a hydroelectric power plant had to be rebooted, not all device drivers were properly loaded. This caused repercussions down in the process network and a control computer that regulated the voltage to a transformer stopped working. No one working that day was prepared for such an eventuality and had never considered what the effects would be or what measures could be taken in such a situation. A long time was spent searching through documentation and calling employees who were off that day to ask for advice. Since no one was mentally prepared for such a situation, an environment of panic was created that further hampered the efforts.

OBJECTIVES FOR THE SECURITY WORK
There is a training package that everyone must undergo before they are granted access to the industrial information and control systems.
All employees in roles that concern the security of the industrial information and control systems participate in a seminar class or simulation exercise at least every two years.
All employees who work with industrial information and control systems can account for the most common attack types that a malicious intruder can use.
There is a role within the organisation responsible for the in-house training of personnel on the subject of information security in the industrial information and control systems.
Management annually approves the in-house training and exercise plan.

16 Follow up incidents in industrial information and control systems and monitor external security problems.

NERC CIP (008-4, 009-4)
NIST 800-82 (Chapter 6.2.3)
CPNI (GPG 3)
DOE 21 Steps (No. 19)
OLF (No. 16)
27002 (Chapter 13)
IEC 62443-2-1 (Chapter 4.3.4.5)

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 externally, it is easier to maintain good preparedness for fighting new threats and vulnerabilities in industrial information and control systems.

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

Recommendations

- Put together a group that regularly meets to discuss incidents and risk problems, and analyses how these might impact the security of the organisation's information and control systems.
- The group should consist of representatives from management as well as from both the process control and IT side. It is important to create a culture where employees are confident to inform about incidents and security deficiencies without being fingered as "scapegoats".
- In addition, monitor security problems in standard IT security components, as these are often the core or subcomponents of the IT solutions that control the industrial information and control systems. A Cisco bug or a Windows bug can be just as serious as a security bug in the software that controls the industrial information and control systems.

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 procedures, 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.

OBJECTIVES FOR THE SECURITY WORK
There is a group that meets at regular intervals to survey new threats with respect to external events.
There is a group that meets at regular intervals to analyse incidents in their own operations.
Employees working with industrial information and control systems can account for incidents in their own operations within the past six months.
Employees working with industrial information and control systems can account for external information security incidents during the past six months which are relevant to the operations.
Analyses of incidents are always reported back to the employees concerned.

17 Participate in user associations, standardisation bodies and other networks for security in industrial information and control systems.

27002 (Chapter 6.1.2)

27010

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

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

By participating in security work it is possible for vendors of industrial information and control systems, applications or other control equipment, to create a competitive advantage. Certain branches already have established security requirements. Power companies in the USA, for example, 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. In Sweden, for example, there is *Elbranschens informations- och it-säkerhetsforum (The electricity industry's information and IT security forum)* (EBITS), which is a network for the coordination of Svensk Energi (Swedish energy), the Swedish District Heating Association, the Swedish Water & Wastewater Association and Svenska Kraftnät (Swedish national grid) regarding issues associated with information and IT security.

Recommendations

- Collaborate in user associations, social networks and organisations that develop expertise and support the members in their daily security work.
- Ensure that the representation is documented and that activities undertaken in each network are continuously reported to the employees concerned.
- Ensure management's familiarity with the representation and justify the way in which participation in the networks strengthens the security in the operations.

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.

OBJECTIVES FOR THE SECURITY WORK
The organisation is represented in at least one active national network with a focus on information security in industrial information and control systems.
There is clear documentation on which people are involved in which networks.
Employees participating in a network continuously report back to other employees and to management.
All concerned employees are aware of the networks in which the organisation is participating.
The extent of participation in networks and standardisation bodies is reported annually to management.

Part C

Part C – Reference list with comments

In this section you will find some well-established international guidelines, standards and checklists that can be useful to know in security work. Some of the references are specific to certain industries, but the content is usually sufficiently generic to be applicable in most organisations. The URLs listed only go to the main page of the respective publisher. From there it is usually easy to seek out the specific documents.

NERC CIP-002-4 to 009-4

Type of document:	Standard
Publisher:	North American Electric Reliability Council (NERC), USA
Version:	Version 4, published 24/01/2011
Scope:	43 pages (total)
URL:	www.nerc.com

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 002-4 requires that the responsible organisation identifies the critical assets. In previous versions of the standard, organisations have used their own risk analyses to determine what is critical. In the latest version, the organisation shall instead use a number of established criteria. Based on this analysis, the organisation then identifies the critical cyber assets.

NERC CIP 003-4 requires that the responsible organisation establishes some form of administrative security program (minimum security management controls) to protect critical cyber assets.

NERC CIP 004-4 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 005-4 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 006-4 requires that the responsible organisation implements a program for physically protecting critical cyber assets.

NERC CIP 007-4 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 008-4 requires that the responsible organisation identifies, classifies, responds to and reports security incidents related to critical cyber assets.

NERC CIP 009-4 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), USA
Version:	07/06/2011
Scope:	155 pages including appendices
URL:	www.nist.gov

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

Section 1: This section presents the purpose, scope and target group of the recommendation.

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

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

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

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

Section 6: This 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 information and 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 information and control systems and so forth.

CPNI Good Practice Guide Process Control and SCADA Security

Type of document:	Recommendations
Publisher:	Centre for the Protection of National Infrastructure (CPNI), Great Britain
Version:	Published 2008
Scope:	18–67 pages depending on document
URL:	www.cpni.gov.uk

”Good Practice Guide” from CPNI consists of seven documents (and an overview document) dealing with various aspects of security in industrial information and control systems. The documents are generally formulated and can be used in all areas where industrial information and control systems are used.

Good Practice Guide – Process Control and SCADA Security. This document provides an introduction to the field and briefly describes what the other documents are about.

***Guide 1* – Understand the business risk.** This document describes how business risks can be linked to threats and risks in the industrial information and control systems with the aim of all information assets being accorded the right level of security.

***Guide 2* – Implement secure architecture.** This document provides recommendations for how to choose an appropriate security architecture, based on identified risks.

***Guide 3* – Establish response capabilities.** This document describes how an organisation should prepare for an IT-related attack.

***Guide 4* – Improve awareness and skills.** This document discusses how to raise security awareness and the ability to manage IT-related incidents in an organisation.

***Guide 5* – Manage third party risks.** This document describes how an organisation can manage the risks involved in working with external vendors.

***Guide 6* – Engage projects.** This document discusses the importance of considering security aspects early on in all implementation projects.

***Guide 7* – Establish ongoing governance.** This document discusses the steps an organisation should take to have continuous control over security work.

Firewall deployment for SCADA and process control networks (2005). A guide to how firewalls should be used to protect industrial information and control systems.

21 Steps to Improve Cyber Security of SCADA Networks

Type of document:	Recommendation
Publisher:	Department of Energy (DOE), USA
Version:	September 2002
Scope:	10 pages
URL:	www.energy.gov

This document is from 2002 but the recommendations discussed are still highly relevant. The 21 recommendations contained in the document have the following headings:

1. Identify all connections to SCADA networks.
2. Disconnect unnecessary connections to the SCADA network.
3. Evaluate and strengthen the security of any remaining connections to the SCADA network.
4. Harden SCADA networks by removing or disabling unnecessary services.
5. Do not rely on proprietary protocols to protect your system.
6. Implement the security features provided by device and system vendors.
7. Establish strong controls over any medium that is used as a backdoor into the SCADA network.
8. Implement internal and external intrusion detection systems and establish 24-hour-a-day incident monitoring.
9. Perform technical audits of SCADA devices and networks, and any other connected networks, to identify security concerns.
10. Conduct physical security surveys and assess all remote sites connected to the SCADA network to evaluate their security.
11. Establish SCADA “Red Teams” to identify and evaluate possible attack scenarios.
12. Clearly define cyber security roles, responsibilities, and authorities for managers, system administrators, and users.
13. Document network architecture and identify systems that serve critical functions or contain sensitive information that require additional levels of protection.
14. Establish a rigorous, ongoing risk management process.
15. Establish a network protection strategy based on the principle of defence in depth.

16. Clearly identify cyber security requirements.
17. Establish effective configuration management processes.
18. Conduct routine self-assessments.
19. Establish system backups and disaster recovery plans.
20. Senior 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
Publisher:	Oljeindustrins Landsförening (OLF)
Version:	Revision 05, published 15/01/2009
Scope:	37 pages
URL:	www.norskoljeoggass.no

The document is based on 16 basic recommendations which are summarised below. There is also a self-measurement tool linked to this document which can be used by an organisation to roughly survey the security situation in their own operations. The recommendations are written for the oil industry but are relatively general and applicable within several sectors:

1. An Information Security Policy for process control, safety, and support ICT systems environments shall be documented.
2. Risk assessments shall be performed for process control, safety, and support ICT systems and networks.
3. Process control, safety, and support ICT systems shall have designated system and data owners.
4. The infrastructure shall be able to provide segregated networks, and all communication paths shall be controlled.
5. Users of process control, safety, and support ICT systems shall be educated in the information security requirements and acceptable use of the ICT systems.
6. Process control, safety, and support ICT systems shall be used for designated purposes only.
7. Disaster recovery plans shall be documented and tested for critical process control, safety, and support ICT systems.
8. Information security requirements for ICT components shall be integrated in the engineering, procurement, and commissioning processes.
9. Critical process control, safety, and support ICT systems shall have defined and documented service and support levels.
10. Change management and work permit procedures shall be followed for all connections to and changes in the process control, safety, and support ICT systems and networks.

11. An updated network topology diagram including all system components and interfaces to other systems shall be available.
12. ICT systems shall be kept updated when connected to process control, safety, and support networks.
13. Process control, safety, and support ICT systems shall have adequate, updated, and active protection against malicious software.
14. All access requests shall be denied unless explicitly granted.
15. Required operational and maintenance procedures shall be documented and kept current.
16. Procedures for reporting of security events and incidents shall be documented and implemented in the organisation.

Cyber Security Procurement Language for Control Systems

Type of document:	Recommendation
Publisher:	Idaho National Laboratory and the Department of Homeland Security (USA)
Published:	September 2009
Scope:	145 pages (total)
URL:	www.us-cert.gov/control_systems

This document is intended for use in setting security requirements in the procurement of industrial information and 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: This section addresses e.g., requirements for removal of unnecessary programs, hardware confirmation and operating system updating.

Perimeter security: This section addresses e.g., requirements for firewalls and network IDSs.

Accounts and passwords: This section addresses e.g., 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 e.g., requirements for messages and documentation from the vendor and problem reporting.

Malicious code: The section addresses e.g., 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.

IAEA Nuclear security series #17 (Computer Security at Nuclear Facilities)

Type of document:	Technical guide
Publisher:	International Atomic Energy Agency (IAEA)
Published:	December 2011
Scope:	82 pages
URL:	www.iaea.org

This document is a technical guide on how to achieve a good level of security at nuclear facilities. With the exception of chapter seven, however, the content is applicable within several industries. The document emphasises the importance of management systems, responsibilities and the organisation of operations. The document is divided into seven chapters:

1. **Introduction.**
2. **Regulatory framework and responsibilities:** This section discusses how different legal regulations should be considered by management and constitute the basis for a security policy.
3. **Management systems:** This section briefly describes how security issues should be included in a management system. Although the concept of an ISMS (Information Security Management System) is not addressed, the principles are very similar to those that permeate the 27000 series.
4. **Organisational issues:** This section provides recommendations on how an operation should be organised to ensure a good security culture.
5. **Implementation of data security:** This section provides a number of tips on how to incorporate information security in operations. It specifically discusses how a zone defence can be built up.
6. **Threats, vulnerabilities and risk management:** This section describes how an organisation can systematically work to constantly reassess risks and identify vulnerabilities.
7. **Security aspects for nuclear power plants.**


auma
SPOLLUFT

SS-ISO/IEC 27000 series

Type of document:	Standard
Publisher:	(SS-)ISO/IEC
Published:	2006 and onwards
Scope:	Under development. There are currently 18 established standards.
URL:	www.sis.se

The ISO 27000 series provides a structured and effective work approach for organisations that strive for improved internal control over information security. SS-ISO/IEC 27000 provides an overview of associated standards, defines relevant terms and introduces the PDCA (Plan-Do-Check-Act) cycle. The standard series is extensive and many new documents are being drawn up. Although many of the standards are useful for enhancing security in industrial information and control systems, the following documents are most relevant to this guide.

SS-ISO/IEC 27000: Information security management system – Overview and vocabulary

SS-ISO/IEC 27001: Information Security Management System – Requirements

SS-ISO/IEC 27002: Code of practice for information security management

SS-ISO/IEC 27005: Information security risk management

SS-ISO/IEC 27010: Information security management for intersector and inter-organizational communications

SS-ISO/IEC 27033: Information technology – Security techniques – Network security (the standard consists of six parts)

SS-ISO/IEC 27035: Information security incident management

IEC 62264 (ANSI/ISA-95) – Manufacturing Enterprise Systems Standards and User Resources

Type of document:	Standard
Publisher:	International Electrotechnical Commission (IEC)
Published:	2005-2012 depending on document
Scope:	977 pages (total)
URL:	webstore.iec.ch

IEC 62264 is a standard that describes how information should be exchanged between systems that are located at different logical distances from the industrial process. The systems are divided into four levels with pure enterprise/business systems at the top and control systems at the bottom. The five sections of the standard are:

IEC 62264-1: Enterprise-control system integration – Part 1: Models and terminology

IEC 62264-2: Enterprise-control system integration – Part 2: Objects and attributes for enterprise-control system integration

IEC 62264-3: Enterprise-control system integration – Part 3: Activity models of manufacturing operations management

EC 62264-5: Enterprise-control system integration – Part 5: Business to manufacturing transactions

ISO/IEC 62443 (ISA-99) – Industrial Communication Networks – Network and system security

Type of document:	Standard
Publisher:	International Electrotechnical Commission (IEC)
Published:	2008 and onwards
Scope:	395 pages in total (additional documents on the way)
URL:	webstore.iec.ch (www.sis.se)

This standard generally addresses information security in industrial information and control systems, and is still under development. It is largely based on ISA99, and those parts that are currently completed primarily describe the various components of a management system for security in industrial information and control systems, as well as different security measures that are appropriate to implement. At present, the following four parts are published:

IEC/TS 62443-1-1: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models

IEC 62443-2-1: Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

IEC/TR 62443-3-1: Industrial communication network – Network and system security – Part 3-1: Security technologies for industrial automation and control systems

IEC 62443-3-3: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

IEC/PAS 62443-3: Security for industrial process measurement and control – Network and system

Glossary

Administrative systems	IT systems used for administrative data processing, office automation or business systems.
Central system	System that makes it possible to log, monitor and control various local processes.
COTS	*Commercial off-the-shelf*. Finished standard components as opposed to custom-made products or vendor-unique solutions.
DMZ	*DeMilitarized Zone*. An isolated subnet placed outside the administrative network which only contains systems that needs to be exposed to the outside world.
FIDI-SC	FIDI SCADA, Information sharing forum for SCADA. Network operated by MSB for information sharing on security in industrial information and control systems.
Physical protection	Protection which includes stopping attackers from physically accessing information or information assets. Physical protection can also protect information assets from fire, floods, earthquakes, etc.
HMI	*Human Machine Interface*. See Operator Station.
Hardening	(Within IT) Processes and procedures designed to reduce the system's attack surface and thus better resist attacks and attack attempts.
ICS	*Industrial Control Systems*. A common abbreviation sometimes used synonymously with industrial information and control systems.
IED	*Intelligent Electronic Device*. Term found within the electricity industry to describe microprocessor-based systems for controlling the power system's various parts, such as isolators.
Embedded systems	Computers or computer-like systems included in devices that have one or a few specific functions, often with some form of real-time requirements. The software in an embedded system is usually stored in a ROM or flash memory. Embedded systems are often part of a device or machine including hardware and mechanical parts. Embedded systems are often found in industrial information and control systems.
Industrial information and control systems	Industrial information and control systems control, check and monitor a physical process. The systems also have the ultimate responsibility of protecting the physical equipment in the process, the operating personnel, the environment and third parties in the case of deviations from the normal operation. The information system part is IT systems within the automation IT that are not directly involved in the control of industrial processes, but which are important support systems with ties to the automation part.

Local system	System that controls a physical process, such as a sluice gate, level-crossing gate or water pump.
Logical protection	Protection of logical infrastructure such as system functions or network functionality. Logical protection exists in parallel with physical protection.
Worm	Malicious code that spreads itself through, for example, networks or portable devices.
Operator station	Computer used by operators in data centres or in control rooms to control and monitor the physical process.
PLC	*Programmable Logic Controller*. Dedicated digital computer used for automation. Often a sophisticated unit that can be expanded or programmed to perform new tasks.
Process automation	Automatic systems that control and monitor industrial processes.
RTE	*Real Time and Embedded*. Embedded systems with a strong focus on real-time applications (cf. *embedded systems)*.
RTU	*Remote Terminal Unit*. Digital control system component that interacts with the physical process by reading or controlling it. It exchanges telemetry data with overlying control systems, often a SCADA system.
SCADA	*Supervisory, Control and Data Acquisition*. A comprehensive, often geographically distributed, industrial control system for monitoring and controlling processes for industrial use.
Vulnerability	Critically dependent on an information asset, latent deficiency in an information asset. The vulnerability exposes the information asset to different types of misuse, such as hacking or the unauthorised escalation of access privileges.
TCP/IP	*Transmission Control Protocol/Internet Protocol*. Standardised data communication protocol that is used as carrier services both on the Internet and within industrial solutions.
VPN	*Virtual Private Network*. Technology used to create overlay connections, called tunnels, between two points in a data network. The tunnel often includes protection and security mechanisms when set up over an insecure carrier network.

Checklists

There is at present a growing number of checklists that can be used to more or less concisely measure the security in one's organisation. The list below is to be considered as an example only and does not claim to be complete. Many organisations are also developing their own checklists.

"The Blue List" – Swedish Water & Wastewater Association's checklist for SCADA security

Publisher:	Swedish Water & Wastewater Association
Published:	2012
Scope:	2 pages (64 questions)
URL:	www.svensktvatten.se

"The Blue List" is developed by the Swedish Water & Wastewater Association and is based on a survey of the security in Swedish drinking water production, and was presented in 2010. The checklist consists of 64 questions where the user takes a position on whether a security measure is implemented, partially implemented, or not implemented at all. At the end, the user receives an overall result and an indication of whether or not the security work is satisfactory.

Checklist security of ICS/SCADA systems

Publisher:	National Cyber Security Centre, the Netherlands
Published:	February 2012
Scope:	15 questions
URL:	www.ncsl.nl

A checklist of fifteen controls that focus on how the most common vulnerabilities with industrial information and control systems can be managed. Five controls deal with organisation and ten are technical in nature.

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

Publisher:	Oljeindustrins Landsförening (OLF)
Version:	Version 1.2 – 2007
Scope:	117 questions
URL:	www.norskoljeoggass.no

A self-measurement tool that is closely linked to the recommendation of the same name (see previous reference). The user assesses the degree to which each of the 117 security measures are met. The user then receives an evaluation of the overall security level.

Information resources (selection)

Extensive international work is underway with regard to security in industrial information and control systems. A great way to keep up to date is to regularly follow what is posted on some of the established websites. The following pages are a good start:

SWEDISH AUTHORITIES	
www.msb.se/scada/	MSB's page with SCADA information.
www.cert.se	Sweden's national CSIRT (Computer Security Incident Response Team) is found at MSB and has been tasked with supporting society in efforts to manage and prevent IT incidents.

INTERNATIONAL AUTHORITIES	
www.cpni.gov.uk	Centre for the Protection of National Infrastructure, Great Britain.
www.inl.gov	Idaho National Laboratory (INL).
https://ics-cert.us-cert.gov/	DHS (Department of Homeland Security) CERT with a focus on SCADA.
www.sandia.gov/scada	Sandia National Laboratories.
www.enisa.europa.eu	European Union Agency for Network and Information Security.

COMPANIES AND INDEPENDENT RESEARCHERS	
www.digitalbond.com	American company that actively blogs about SCADA security.
www.scadahacker.com	Active blog about security in industrial information and control systems.
www.shodanhq.com	Search engine for devices that are connected on the Internet.
www.tofinosecurity.com	Canadian company that publishes a lot of news about SCADA security.

Swedish Civil Contingencies Agency (MSB)
SE-651 81 Karlstad Phone +46 (0)771-240 240 www.msb.se
Order No. MSB766 - November 2014 ISBN 978-91-7383-500-8