TECHNICAL STUDIES

Cyber Security of Industrial Control Systems:

How to get started?

An overview of existing documents, standards, guidelines and best practices

September 2014

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11 rue de Mogador - 75009 Paris
Tel : +33 1 53 25 08 80 – Fax : +33 1 53 25 08 88
clusif@clusif.fr – www.clusif.fr

The French law of March 11, 1957, specifically Sections 2 and 3 of Article 41 on one hand, authorizes only "copies or reproductions strictly reserved for the private use of the copyist and not intended for a collective use" and, on the other hand, “analysis and short quotations for the purpose of example and illustration ". Any representation or complete or partial reproduction, made without the approval of the author or the entitled parties or the legal successors is unlawful " (Section 1 of Article 40).

This representation or reproduction with whatever process, would thus constitute a forgery punishable under Section 425 of the French Penal Code

Contents

ACKNOWLEDGMENTS

The CLUSIF wishes to recognize all those who have contributed to this document, especially:

The heads of the workgroup:

Gérôme	**BILLOIS**	*Solucom*
Hervé	**SCHAUER**	*HSC*

The contributors:

Patrice	**BOCK**	*ISA France, Sogeti France*
Jean	**CAIRE**	*RATP*
Emmanuel	**DE LANGLE**	*Solucom*
Loïc	**DIVAN**	*Andra Cigéo*
Anthony	**DI PRIMA**	*Solucom*
Loïc	**GUEZO**	*Trend Micro*
Philippe	**JEANNIN**	*RTE*
Thierry	**PERTUS**	*Conix*
Orion	**RAGOZIN**	
Éric	**SAVIGNAC**	*Airbus Defence and Space*

The **CLUSIF** also thanks all members who have reviewed and edited this document.

For any comment, please contact the CLUSIF at scada@clusif.fr.

I. Introduction

This document is the outcome of a large-scale consolidation of feedbacks from contributors and of existing resources and literature, with the aim to support the information security community in charge of cyber security of industrial control systems.

An overview of existing reference documents, along with explanatory notes, is made available to provide decision-making guidance to users willing to set up a cybersecurity framework, or identify appropriate resources to read.

Based on this overview, this document also offers a staged, progressive approach in 5 key steps, to help those unfamiliar with industrial environments get a better grasp of this topic and help their respective organization adopt a continuous improvement approach.

This resource is targeted primarily at CISO (Chief Information Security Officers) who are in charge of industrial control systems cyber security. Yet, any profile involved in the cyber security of industrial systems will benefit from this resource.

Please note that the set of reference documents listed herein is a snapshot of existing supporting literature as of March 31, 2014.

II. Definition, Constituents and Challenges

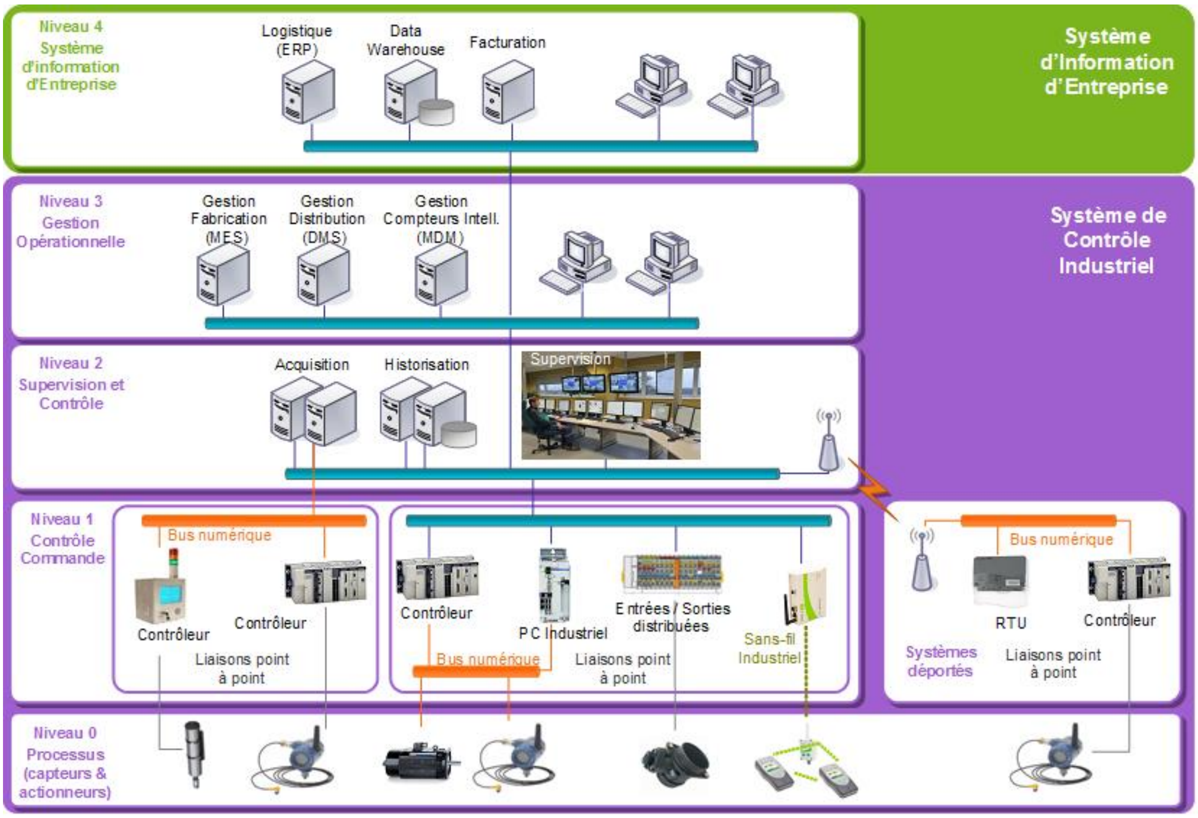
Industrial Control Systems (ICS) or Industrial Automation and Controls Systems (IACS) is a broad concept that encompasses all digital systems that directly interact with the “Physical World”. This concept also includes contiguous areas such as BMS (Building Management Systems).

Such systems are classified under 4 key categories of components as described in the CIM pyramid (Computer Integrated Manufacturing):

- Components that help interact with the physical world. These are sensors (temperature, open/close sensors, humidity, light…) and actuators (pumps, cylinders, valves, indicator lights…). They are often connected to each other over a specific network called a fieldbus. Proprietary protocols are commonplace, but the use of IP technologies is on the rise. Some smart models come with an IED (Intelligent Electronic Device). These components form the level 0 of the CIM pyramid.
- Industrial control components are those that manage the actuators with regards to information delivered by sensors and embedded software. Such components can be distributed (DCS: Distributed Control System) or autonomous; in the form of PLCs (Programmable Logical Controller) deployed at the local level, or RTUs (Remote Terminal Unit). Today, this difference tends to fade in the field. The next-generation components (PAC: Programmable Automation Controller) provide more features than traditional components and are connected through IP links to production control IT networks. This is the first level of the CIM pyramid.
- Process monitoring and control components constitute the level 2 of the pyramid. Through a Human-Machine Interface (HMI), those components provide visibility throughout the process, and manage the process according to instructions. Acronyms, such as SCADA (Supervisory Control And Data Acquisition) or MTU (Master Terminal Unit) are often used. These components are linked to the production management systems (level 3 of the pyramid) where they get their instructions. They often comprise traditional IT modules, such as servers and clients running operating systems like Windows.

The three categories of components can be assembled, shared, or used distinctly, depending on the supported process and, together, they constitute the Industrial Information System.

Industrial systems are increasingly leveraging IT features, and are linked to the Office Information Systems, the level 4 of the CIM pyramid. The scope of ICS has, therefore, expanded to include remote management (remote maintenance via the Internet or the MIS, for example). Consequently, IIS has become more exposed to cyber risks.



The CIM pyramid (source: Thierry Cornu)

There are three main categories of ICS:

- **Systems located at a specific site**. This is the most common case, and refers to digital systems located at a specific physical site or just a short distance away (a few kilometers at the most). These systems are, for example, part of a production chain in the automobile, food, or pharmaceutical industries, and can also be found in an extraction and/or transformation infrastructure in the nuclear, gas and oil industries. It is quite common to have one or more industrial systems on site, thus defining a comprehensive infrastructure. These systems also include Building Management Systems, as well as safety processes that protect manufacturing environments. They are clearly identified and their location is known, while there is often a human presence nearby.
- **Distributed systems**. These systems are scattered throughout a country or region, and support different applications: transportation, utility networks, tracking of distributed systems on remote industrial sites (management of liquid levels in tanks…). These require telecommunication networks over long distances, often subcontracted to a third-party service provider. Note that there may be no staff available at such physical sites. In most cases, remote access is an essential requirement for performing daily tasks, such as maintenance.
- **Stand-alone/mobile/embedded systems**. There are different meanings ascribed to these terms. In this document, such systems are defined as systems with a smaller footprint of less than 10 meters. They include, for example, medical systems, such as

scanners, MRIs (Magnetic Resonance Imaging), as well as pacemakers and such stand-alone healthcare systems. Systems from the transportation industry (vehicles, planes…) are also included in this category. Overall, these systems are usually part of a wider system.

Those systems can of course be combined and made available in different formats. Regardless, this categorization scheme makes it possible to identify requirements in cyber security and limitations specific to the considered context.

In the industrial environments, operational safety (system availability and integrity) is prioritized above privacy and tracking. Yet, this may be different for selected business processes, or determined by regulatory requirements.

Industrial control systems have specific features that impact risk management and information security processes:

- Their lifespan is long, often spanning dozens of years between one generation of a product and the next.
- They are deployed in harsh environments (dust, humidity, electromagnetism, extremes of temperature, corrosion…).
- They can be deployed over an isolated and segregated information system, and this may add to the complex task of ensuring their security.
- Disruptions in service must be as few and far between as possible, and this requires serious planning efforts. An industrial process or equipment can be brought to a standstill due to physical limitations (i.e., the duration required to initiate an industrial process, or the timeframe necessary for safe intervention further to the disruption of a process). Note that cyber security tasks may conveniently be scheduled during planned maintenance shutdowns.
- Interventions on such systems may be conducted in environments with low accessibility and under certain conditions. This may require specific expertise and compliance with stringent physical safety guidelines.
- In most industries, IIS depends on their vendors. These vendors usually supply a turnkey system, with a maintenance contract running over several years, while evolutions and reversibility is limited, and sometimes not possible due to the specific features and proprietary technologies used.
- The configuration of the components that make the IIS must be certified by a supervisory authority, which may require undergoing certification after each modification. This can prove time consuming, and may bring the production process to a halt until the certification is granted.

III. Security Guidelines for ICS

There are many security guidelines and standards related to IIS, and these multiple resources make it sometimes difficult to understand all aspects of this topic.

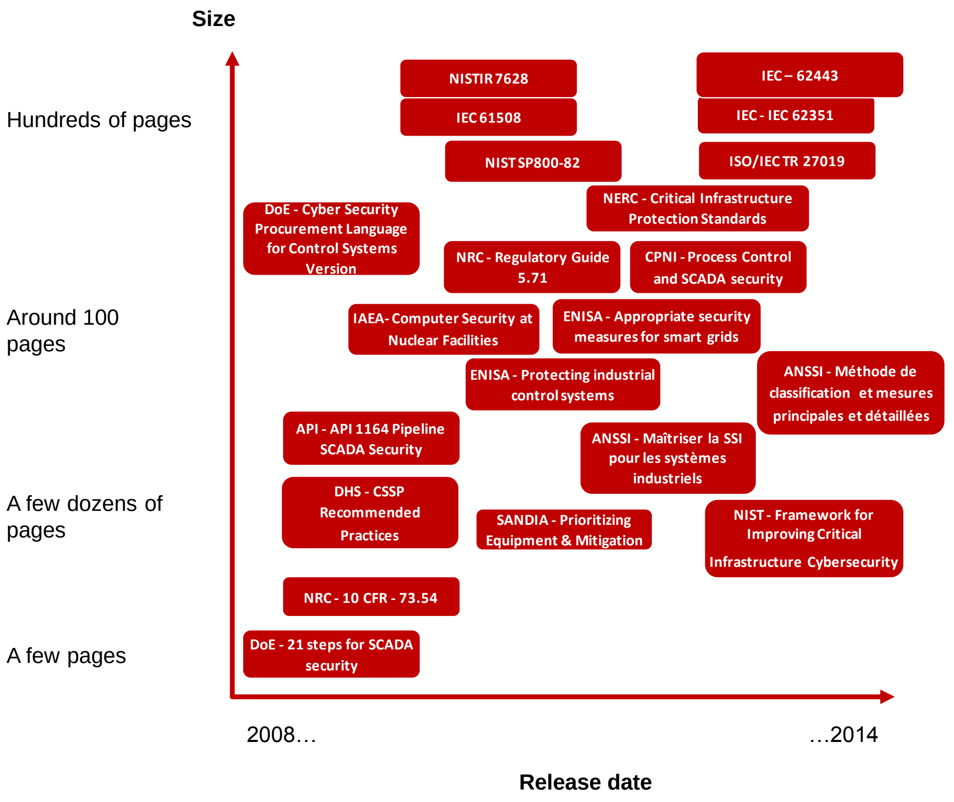
Therefore, it seemed wise to build a landscape of reference documents and resources dealing with the issue, with the goal to identify most of the existing documents and spot the most relevant ones. This chapter provides the tools to identify the guidelines and reference documents that are of most value to those willing to initiate an IIS information security project. This subject will be covered in the final section.

As highlighted in the news, IIS security is a priority for many organizations. More than 50 reference documents were identified by the workgroup; and 30 of them were picked as the most relevant publications. This selection was performed after readings and analysis performed by all workgroup members who shared their insights. These documents were read and screened once again, and a final selection of 20 publications was found to be the most relevant, legible and practical to use.

Please refer to the Appendix for the list of all documents screened by the workgroup members.

III.1. A rich and diverse literature

The figure below outlines the documents that were eventually selected for reading, and these are classified according to their release date and their size. This illustration evidences the crop-full of content from multiple documents released over the past recent years, as well as the diversity of such publications when it comes to their volume: from a few pages to thousands of pages.



A rich and diverse literature

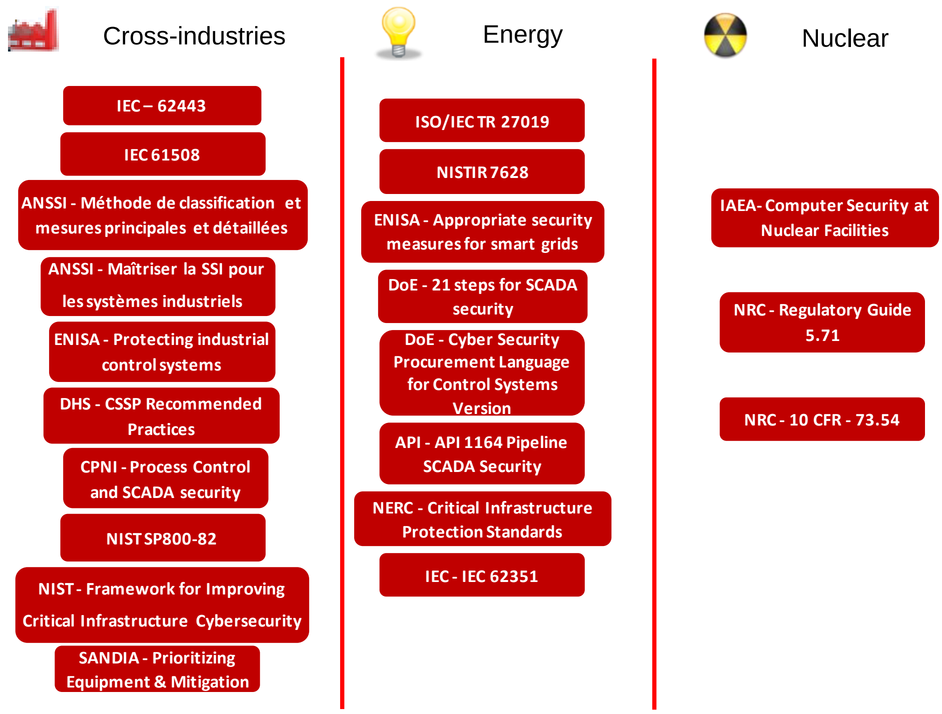
III.2. Significant presence of different industries

The documents studied deal with IIS security relevant to specific industries, while some of them are cross-industry. The screening of these resources made it possible to highlight several findings.

Yet, it is interesting to note that resources are rather abundant for the energy industry, as many organizations, including international organizations, such as ISO and ENISA, as well as the US Department of Energy and the IAEA, have focused on this industry. Many other documents, such as the IEC 62645 standard for the nuclear sector, are still in the draft stage.

There are very few documents specific to the healthcare and transportation industries, and such publications are rather old or fail to be comprehensive.

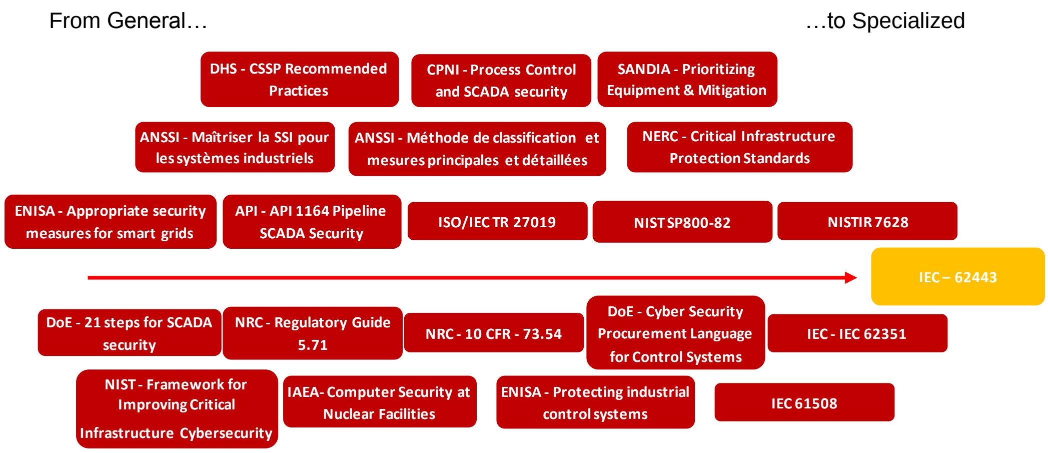
Meanwhile, the documents that are specific to an industry may also consist of documents, most of which will be relevant to other industries, simply by adapting selected concepts or switching to appropriate terminology. Therefore, the focus of a publication on a specific industry should not be seen as a limiting criterion, and there are no reasons to set the sole focus on documents that are industry-specific.


Cross-industries
IEC – 62443
IEC 61508
ANSSI - Méthode de classification et mesures principales et détaillées
ANSSI - Maîtriser la SSI pour les systèmes industriels
ENISA - Protecting industrial control systems
DHS - CSSP Recommended Practices
CPNI - Process Control and SCADA security
NIST SP800-82
NIST - Framework for Improving Critical Infrastructure Cybersecurity
SANDIA - Prioritizing Equipment & Mitigation
Energy
ISO/IEC TR 27019
NISTIR 7628
ENISA - Appropriate security measures for smart grids
DoE - 21 steps for SCADA security
DoE - Cyber Security Procurement Language for Control Systems Version
API - API 1164 Pipeline SCADA Security
NERC - Critical Infrastructure Protection Standards
IEC - IEC 62351
Nuclear
IAEA- Computer Security at Nuclear Facilities
NRC - Regulatory Guide 5.71
NRC - 10 CFR - 73.54

Origin of documents

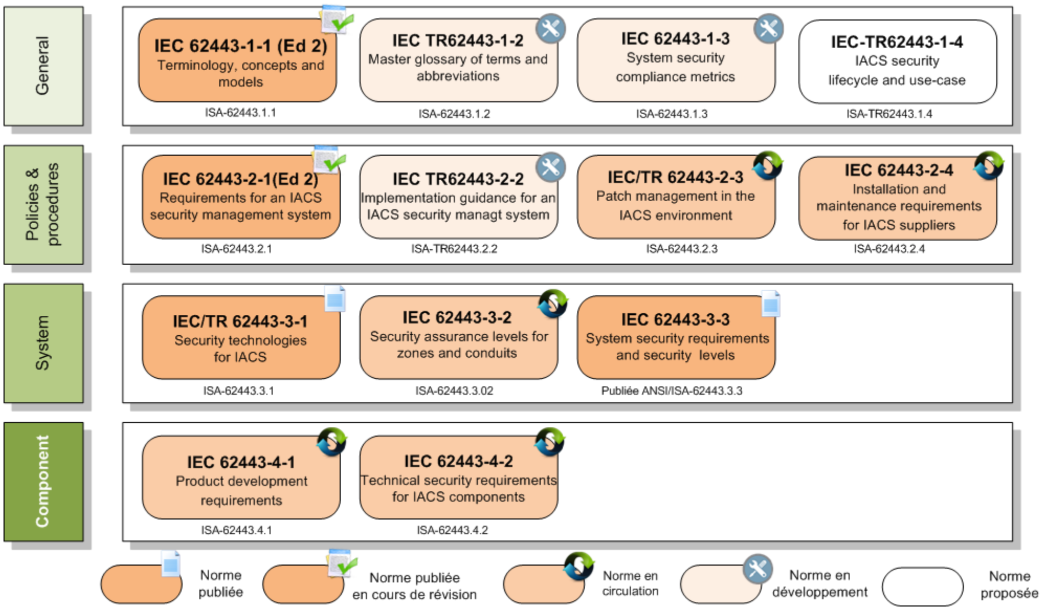
III.3. Multiple document profiles

The documents released officially have different goals: some of them provide an overview of key concepts, while others are highly granular and far-reaching in the principles they cover.


From General…
…to Specialized
DHS - CSSP Recommended Practices
CPNI - Process Control and SCADA security
SANDIA - Prioritizing Equipment & Mitigation
ANSSI - Maîtriser la SSI pour les systèmes industriels
ANSSI - Méthode de classification et mesures principales et détaillées
NERC - Critical Infrastructure Protection Standards
ENISA - Appropriate security measures for smart grids
API - API 1164 Pipeline SCADA Security
ISO/IEC TR 27019
NIST SP800-82
NISTIR 7628
IEC – 62443
DoE - 21 steps for SCADA security
NRC - Regulatory Guide 5.71
NRC - 10 CFR - 73.54
DoE - Cyber Security Procurement Language for Control Systems
IEC - IEC 62351
NIST - Framework for Improving Critical Infrastructure Cybersecurity
IAEA- Computer Security at Nuclear Facilities
ENISA - Protecting industrial control systems
IEC 61508

A diversity of document profiles

Note that the IEC – 62443 standard (formerly ISA 99) is a family of standards with a large scope of use: some guidelines are rather general, while others are precise, specific and focused. Many of those guidelines are still in the process of being defined or upgraded, which makes them rather difficult to comprehend. The documents are categorized as follows, depending on their level of precision and their targets:


General
IEC 62443-1-1 (Ed 2)
Terminology, concepts and models
ISA-62443.1.1
IEC TR62443-1-2
Master glossary of terms and abbreviations
ISA-62443.1.2
IEC 62443-1-3
System security compliance metrics
ISA-62443.1.3
IEC-TR62443-1-4
IACS security lifecycle and use-case
ISA-TR62443.1.4
Policies & procedures
IEC 62443-2-1(Ed 2)
Requirements for an IACS security management system
ISA-62443.2.1
IEC TR62443-2-2
Implementation guidance for an IACS security managt system
ISA-TR62443.2.2
IEC/TR 62443-2-3
Patch management in the IACS environment
ISA-62443.2.3
IEC 62443-2-4
Installation and maintenance requirements for IACS suppliers
ISA-62443.2.4
System
IEC/TR 62443-3-1
Security technologies for IACS
ISA-62443.3.1
IEC 62443-3-2
Security assurance levels for zones and conduits
ISA-62443.3.02
IEC 62443-3-3
System security requirements and security levels
Publiée ANSI/ISA-62443.3.3
Component
IEC 62443-4-1
Product development requirements
ISA-62443.4.1
IEC 62443-4-2
Technical security requirements for IACS components
ISA-62443.4.2
Norme publiée
Norme publiée en cours de révision
Norme en circulation
Norme en développement
Norme proposée

Structure of the IEC – 62443 standard (December 2013 – source: ISA France)

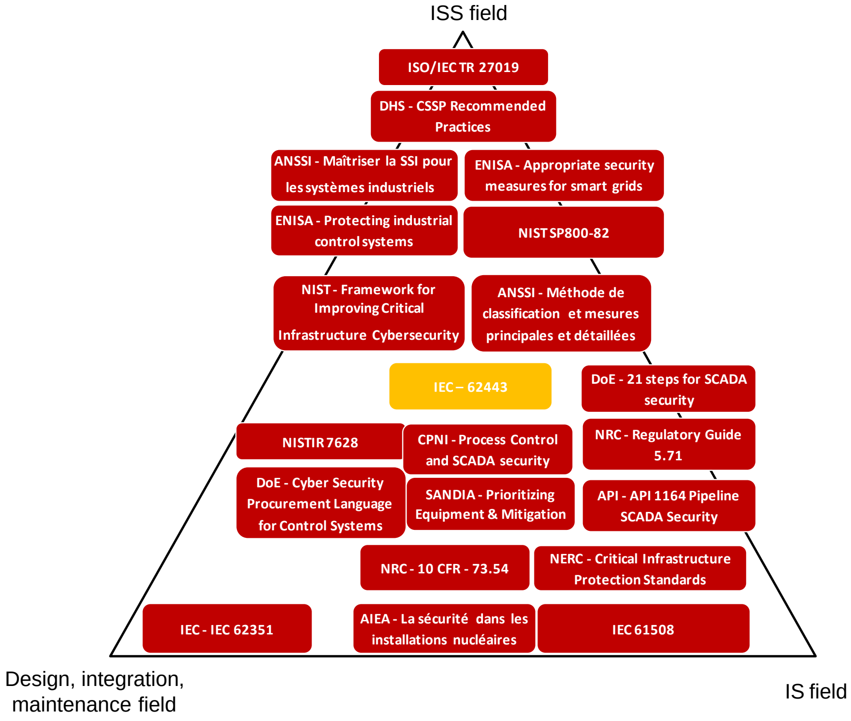
III.4. Documents for different readers' profiles

Knowing that publications do not always target the same profile, it is interesting to identify those that are the most useful for each of such profiles dealing with IIS. Three key profiles (or fields) can be identified: Information Security (IS) linked to the Management Information System, the field of IIS, and the design, integration and maintenance field that may include vendors.

Several observations have been noted: first, each field could draw benefit from using documents relating to other fields. Yet, selected guidelines are more targeted than others, as they relate for instance to protocol specification and, therefore, are more focused on the design, integration and maintenance fields (IEC – 62351, for example). Others are more useful to the information security field, such as the ISO/IEC TR 27019 document that provides advice and visibility into the practices of the ISO 27002 standard, and how to adapt then to IIS. These documents will, therefore, be more relevant to people dealing with the Management Information Systems, as the differences to account for in this document are rather seldom. There are also publications that are very business oriented and more relevant to the IIS field (e.g., IEC – 61508).

Another noteworthy finding is that selected documents are not focused on a specific field, but aim at being open to all. This is the case of the IEC –

62443 standard, which provides several documents that can be adapted to different reader profiles.


ISS field
ISO/IEC TR 27019
DHS - CSSP Recommended Practices
ANSSI - Maîtriser la SSI pour les systèmes industriels
ENISA - Appropriate security measures for smart grids
ENISA - Protecting industrial control systems
NIST SP800-82
NIST - Framework for Improving Critical Infrastructure Cybersecurity
ANSSI - Méthode de classification et mesures principales et détaillées
IEC – 62443
DoE - 21 steps for SCADA security
NISTIR 7628
CPNI - Process Control and SCADA security
NRC - Regulatory Guide 5.71
DoE - Cyber Security Procurement Language for Control Systems
SANDIA - Prioritizing Equipment & Mitigation
API - API 1164 Pipeline SCADA Security
NRC - 10 CFR - 73.54
NERC - Critical Infrastructure Protection Standards
IEC - IEC 62351
AIEA - La sécurité dans les installations nucléaires
IEC 61508
Design, integration, maintenance field
IS field

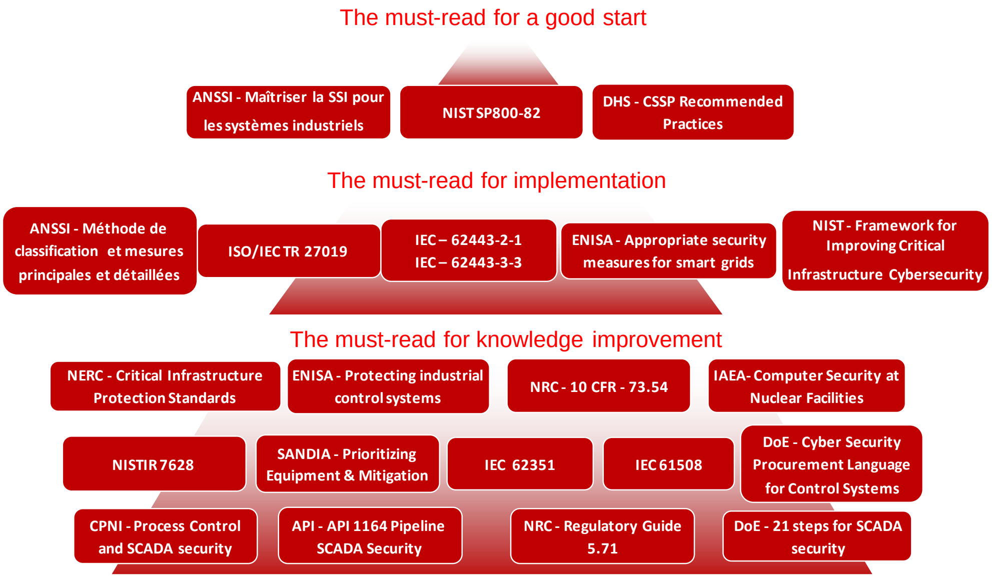
Documents targeting different populations

III.5. Must-read documents

The study made it possible to select documents that would be essential to readers, according to their needs.

Three categories of documents identified can be outlined:

- **Must-read to start**: these are documents that anyone dealing with information system or information security should read. Information is provided in a simple and legible way, along with real-world examples to deal with issues around IIS. Such readings are imperative for a start, but they are high-level educational resources. Yet, they remain quite comprehensive and instructive for execution.
- **The must-read for implementation**: these are documents that help evaluate, guide and implement projects in details.
- **The must-read for knowledge improvement**: such documents help to further explore a specific topic or industry.


The must-read for a good start
ANSSI - Maîtriser la SSI pour les systèmes industriels
NIST SP800-82
DHS - CSSP Recommended Practices
The must-read for implementation
ANSSI - Méthode de classification et mesures principales et détaillées
ISO/IEC TR 27019
IEC – 62443-2-1
IEC – 62443-3-3
ENISA - Appropriate security measures for smart grids
NIST - Framework for Improving Critical Infrastructure Cybersecurity
The must-read for knowledge improvement
NERC - Critical Infrastructure Protection Standards
ENISA - Protecting industrial control systems
NRC - 10 CFR - 73.54
IAEA- Computer Security at Nuclear Facilities
NISTIR 7628
SANDIA - Prioritizing Equipment & Mitigation
IEC 62351
IEC 61508
DoE - Cyber Security Procurement Language for Control Systems
CPNI - Process Control and SCADA security
API - API 1164 Pipeline SCADA Security
NRC - Regulatory Guide 5.71
DoE - 21 steps for SCADA security

The must-reads

III.6. Improving consistency

There are multiple existing guidelines, and there are others in the process of being drafted. Yet, our study does not help spot a specific set of guidelines that would be superior and preferred to others.

The *IEC – 62443* standard holds a central position, and offers the only guidelines with an international and cross-industry scope; but the standard hosts a number of resources that are still in their design or review stage, and cannot easily be used in their current format. Two documents of this standard (the 2-1, under review as of May 2014), and the 3-3 (released version), can be considered to design a cyber security set of guidelines. Meanwhile, it is preferable to simplify such resources and extract the key ideas, rather than implement them as is. The pitfalls are well identified by the related standardization committee and improvements are expected in the upcoming years.

A certain level of inconsistency is present because of the variety of guidelines: topics are sometimes described in different ways, while terminology is not consistent. This highlights the need to add more maturity on all subjects related to IIS security, in the same way as when the initial works on information security were published.

Meanwhile, the representatives of the organizations in charge of such guidelines are aware of these limits, and we can expect standardization across those guidelines in the upcoming year.

We can also note that business specific expectations are high in the industrial domain, and this explains why resources are so abundant and diversified. This is a key difference with regards to regular information security, which is usually implemented universally, across various industries.

IV. The 5 Key Steps in Securing IIS

Experience earned from the workgroup members in their daily practice, along with the analysis of the different guidelines and reference documents, have made it possible to outline key steps towards securing the industrial IS.

IV.1. Stage 1: integrate the industrial nature of the business, and conduct an inventory of security issues

The implementation of a IIS-focused cyber security project requires precise knowledge of the company's industrial environment, so as to better evaluate the impact of cyber risks related to humans, the environment and operations, and to prioritize countermeasures.

This first stage is twofold:

1. **Define a representative sample of the facilities to be audited, based on the industrial business activities.** A company may have one or more lines of business (chemicals, metal-working, mechanical, manufacturing…), depending on the type of products (final or intermediate goods). This sample can be defined in collaboration with safety managers, and/or production site managers.
2. **Map the audit's scope, and assess the level of exposure to cyber risks.** Once the sample is defined, an audit is necessary to assess the exposure to cyber risks in three areas:
   - **Technical environment:** facilities may host a diversity of technologies that are, for some of them, obsolete, or not based on IT (e.g., analog and non-IP technologies). If dealing only with old technologies, exposure to cyber attacks may be quite limited. External interfaces (in particular, with the corporate IS) must be audited.
   - **Industrial safety:** the safety status and the results of hazard analysis are required to assess the impact of cyber risk scenarios. Actually, safety processes (safety-oriented Programmable Logic Controller, wired security, Safety Instrumented Systems (SIS)), may be implemented to stop industrial processes in a safe way.

When assessing the impact of cyber risks, safety measure may be taken into account to lower their impact.

Meanwhile, this is feasible only if safety is provided through processes that are not automated, or by an autonomous industrial system (physically independent). Furthermore, note that safety mechanisms may be used against the facilities themselves through a denial of service (triggering of safety measures to disrupt the production process).

- **Cyber security**: a gap analysis may be carried out with regards to best practices in securing traditional IT[1], or industry-focused/specific[2] guidelines.

During this stage, it is urgent to meet up with key stakeholders to educate them to the project, raise their awareness and earn their approval to carry on with the security project. Such stakeholders include:

- The **Site Director**: he/she will provide visibility into business risks, production goals and related requirements (e.g. the necessity for reduced maintenance downtime to achieve production targets).
- The **Safety/Quality/Environment Manager,** who can indicate requirements for controlling and tracking physical accesses to the site, as well as interventions on IT and business systems. He/she may also provide insights into the applicable regulations.
- The **Risk Manager**. Allow him/her to take into account the cyber risks, especially safety risks, in addition to organizational risks.

It is important to identify the applicable regulations, as they may require the implementation of specific security measures (e.g., NERC, NRC and FDA).

- Industrial floor staff: **Maintenance Manager, Industrial IT Manager, MIS Manager, Supervisors, Automation Technicians, Operators, etc.** They can help identify existing

[1] Using the ISO 27002 standard for example

[2] ANSSI, IAEA, NIST, FDA

security measures, as well as the safety processes already implemented.

IV.2. Stage 2: Educate the management board on the issue of vulnerabilities and related industrial risks

Support from top executives is required for the success of the project. The security of industrial environment requires supporting the transformation process through investments and resources. Such investments are made by each industrial site, and these sites must mediate between production goals, cost containment and investments in cyber security. Top executives must, therefore, support the project to make it successful.

Several topics must be covered by the executives:

1. **Identify all impacts: human, environmental, operational, financial, reputation and non-compliance with regulations**[3]. The different risk profiles must be identified in order to prioritize the action plan, especially for organizations that deal with multiple industrial lines of business. Risk Managers must be part of the project to incorporate IIS risks, and build up a consistent approach to risk management across their organization.
2. **Provide examples** of ICS vulnerabilities through audits and penetration testing.
3. **Design an actions plan that** includes Quick Wins to reduce quickly the risk exposure. Here are a few actions that may be part of this plan:
    - Appoint a sponsor among top executives;
    - Appoint a manager in charge of ICS security (CIISO), as well as correspondents on sites;
    - Design a cyber security framework;
    - Design a formal strategic document to manage risk and circulate it internally (blueprint, guidelines, umbrella policy, etc.).

[3] Failure to comply with selected requirements may bring production to a halt, with an adverse impact on relationship with customers or on the corporate share price.

IV.3. Stage 3: Design an industrial control system cybersecurity policy (I-ISSP)

Besides educating top executives to the security issues, it is wise to design a specific security policy. To encourage its acceptance and implementation at the operational level[4], it is strongly recommended to involve operational staff dealing with IIS.

> The validation of the document by the appropriate operational staff is a good way to have local staff treats it as critical document.

This stage covers three key areas:

1. **The setting up of a workgroup that includes the key operations profiles** (operations and maintenance manager, automation technicians, ICS architects, etc.), in order to:
   - List the difficulties in implementation: operations that require controllers to reboot, regulatory requirements, costly upgrade of obsolete machines…
   - Identify security measures and emphasize Quick Wins[5]. Such measures must prove effective so that they can be implemented.
2. **Structure the output of the workgroup by adopting an approach** based on the levels of risks, similarly to what is performed by the IEC, the IAEA[6] or the ANSSI[7] (France). Security measures will then be allocated, based on their robustness or intrinsic efficiency, to each level of cyber risk. The higher the level of risk, the tighter the security measures, and the most urgent it is to separate the target zones from the Internet and office networks, using multiple layers of physical and logical security barriers.
3. **Design implementation guidelines for the I-ISSP.** These guidelines (directive, guide) will introduce an implementation methodology. Here are some of the topics that can be dealt with:
   - Split the ICS into relevant areas (or sub-systems) that host one or many autonomous business processes;
   - Evaluate the level, or class, of cyber security for each of those areas;
   - Implement security measure in line with the level of cyber security. Obviously, these measures should be consistent with the level of

[4] Please refer to the final section of this document for the resources that help implement this approach.

[5] These are measures with a low technical, human and financial impact, and that does not require the process to be stopped.

[6] ; International Agency for Atomic Energy

[7] Resources are stated at the end of this document.

maturity of the organization, and the amount of investment scheduled. An idealist outlook may have a negative impact on motivation, while a minimal vision may not cover all risks.

IV.4. Stage 4: Implement the I-ISSP at the operational level

Once the framework is defined and support received from top management, an implementation plan must be drafted, approved by decision makers, and translated into accurate and operational measures, in compliance with the following advices:

- Define a time frame of 2 to 3 years max.
- Define the investment budget required to implement this strategy.
- Adopt a project-focused methodology.
- Get approval from the highest decision-making level, to ensure support from all stakeholders.

This stage includes three key actions:

1. **Define the functional cyber security chain, and set up a governing committee for this project**
   It is essential to identify all stakeholders, centrally and on each site, before the project kicks off. A central governance body can be set up to manage all stakeholders, coordinate actions, encourage the sharing of experiences, and identify practices and solutions that could be standardized across all sites.

   > For the project to be legitimate at the local level, it is advised to appoint a local security officer chosen from among the operations team and not the IT team (e.g. an Industrial IT Manager.)

2. **Implement « Quick Wins »** at the site level, within a short timeframe: less than 6 months (e.g. review of open flows, guidelines for using a USB dongle and other such mobile drives, education regarding security practices, change management, etc.).

3. **Start the project by prioritizing critical sites.** Critical sites should be identified according to two criteria: the risk profile of each company's business and the analysis of various criteria: human, environmental, operational, financial, reputation and regulatory compliance.

IV.5. Stage 5: Keep cyber risks under control

To manage cyber risks, governance is required to ensure a level of security in line with the evolution of the malware landscape. The implementation should leverage international standards that promote continuous improvement and a PDCA model (Plan – Do – Check – Act).

> When industrial sites are run independently (budget, resources, etc.), it is suggested that governance is managed at the local level and linked to the local management information system. This helps customize the security policy to the specifics of each site and encourages acceptance at the local level.

The key governance processes to implement are the following:

- **Manage cyber risks** and ensure continuous monitoring to define the fundamentals of IIS security against cyber attacks, and to support vulnerabilities and emerging threats. This monitoring can be centralized.
- **Train/educate** all staff members to increase their awareness on cyber risks, and as to their responsibility when it comes to containing such risks.
- **Make security an integral part of new and ongoing projects**, to identify business projects with features that may increase exposure to cyber risks: mobility, smart sensors, remote maintenance, etc. Projects that are the most prone to risks may be considered on top priority.
- **Manage security incidents** to detect and analyze such incidents, and implement appropriate remediation.
- **Audit and internal control** to ensure compliance of the ICS with the I-ISSP.
- **Implement and manage appropriate plans of action**, in line with the audit findings, or to block new threats and vulnerabilities as identified.
- **Conduct regular management reviews** to assess the situation, fine-tune the project, or give new orientation to improve the containment of cyber risks.

V. Appendix

V.1. Reviewed reference documents

Reference documents	Publisher	Publication	Pages
A Framework for Aviation Cyber security	AIAA	2013	16
Computer Security at Nuclear Facilities	IAEA	2013	91
La sécurité des SII - Méthode de classification et mesures principales et détaillées	ANSSI	2014	164
Maîtriser la SSI pour les systèmes industriels	ANSSI	2012	40
API 1164, Pipeline SCADA Security	API	2009	64
Securing Control and Communications Systems in Transit Environments - Part II : Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones	APTA	2013	78
Securing Control and Communications Systems in Transit Environments - Part 1 : Elements, Organization and Risk Assessment / Management	APTA	2010	29
Informationstechnik in Prozessüberwachung und -steuerung	BSI	2008	5
Good Practice Guide "Process Control and SCADA security"	CPNI	2008 – 2011	215
Cyber Security Assessments of Industrial Control Systems - A Good Practice Guide	CPNI	2011	66
Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security	CSWG	2010	597
21 Steps to Improve Cyber Security of SCADA Networks	DoE	2002	10
Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies	DoH	2009	44
Can we learn from SCADA security incidents	ENISA	2013	10
Window of exposure ... a real problem for SCADA systems? - Recommendations for Europe on SCADA patching	ENSIA	2013	19
Appropriate security measures for Smart Grids	ENISA	2012	84
Protecting industrial control systems - Recommendations for Europe and member states	ENISA	2011	81

IEC 62443 – Security for industrial Automation and Control Systems	IEC	2013 - 2016	1010
IEC 62351 – Technical specifications – Power system management and associated information exchange technique – Data and communications security	IEC	2013	500
IEC 61508 : Standard for Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems	IEC	2010	400
TR IEC 62210 – Power system control and associated communications - Data and communication security	IEC	2003	52
ISO/IEC TR 27019	ISO/IEC	2013	320
Cyber Security Procurement Language for Control Systems	INL	2008	120
Critical Infrastructure Protection Standards	NERC	2012	320
Framework for Improving Critical Infrastructure Cybersecurity	NIST	2014	41
Guide to Industrial Control Systems (ICS) Security	NIST	2011 – 2013	155
Regulatory Guide 5.71 – Cyber security programs for nuclear facilities	NRC	2010	105
Protection of digital computer and communication systems and networks	NRC	2009	2
Cybersecurity Through Real-Time Distributed Control Systems (RTDCS)	OAK Ridge / DoE	2010	30
Methodology for Prioritizing Cyber-vulnerable Critical Infrastructure Equipment and Mitigation Strategies	Sandia	2010	42
Control System Devices : Architectures and supply Channels Overview	Sandia	2010	70
Security Framework for control System Data classification and Protection	Sandia	2007	33
Framework for SCADA Security Policy	Sandia	2005	6
Guide to CIP Cyber Vulnerability Assessment	Sandia	2008	19
SCADA and Process Control Survey	SANS	2013	18
Attack Methodology Analysis: Emerging Trends in Computer-Based Attack Methodologies and Their Applicability to Control System Networks	US – CERT	2005	30
Process Control Domain – Security Requirements for vendors	WIB	2010	52

CLUSIF

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11 rue de Mogador
75009 Paris
France
☎ +33 1 53 25 08 80

Download all publications of the CLUSIF from
www.clusif.fr