Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors and Contributors

Rossella Mattioli, ENISA
Konstantinos Moulinos, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

The study was conducted in cooperation with EY Business Advisory, and in particular with the experts:
Piotr Ciepiela, EY Business Advisory
Leszek Mróz, EY Business Advisory
Mirosław Ryba, EY Business Advisory
Tomasz Szałach, EY Business Advisory

We have received valuable input and feedback from
Jens Wiesner, German Federal Office for Information Security (BSI)
Mathieu Feuillet, French Network and Information Security Agency (ANSSI)
Stephane Meynet, French Network and Information Security Agency (ANSSI)
Yann Salamon, French Network and Information Security Agency (ANSSI)
Kristina Blomqvist, Swedish Civil Contingencies Agency (MSB)
Maciej Pyznar, Polish Government Centre for Security (RCB)
Adam Politowski, Polish Government Centre for Security (RCB)
Marit van Galen, Dutch National Cyber Security Centre (NCSC)
Arthur van der Weerd, Dutch National Cyber Security Centre (NCSC)
Enrique Redondo Martínez, Spanish National Cybersecurity Institute (INCIBE)
Vytatutas Butrimas, Cybersecurity and Information Technology Department, Ministry of Defence, Lithuania
Urmo Sutermae, Estonian Information System Authority (RIA)
Finally we thank the experts of ENISA ICS SCADA Stakeholder Group, EuroSCSIE and all participants to the validation workshops held in Luxembourg the 30th of September 2015 in providing us useful feedback during discussions and interviews.

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 526/2013. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Copyright Notice

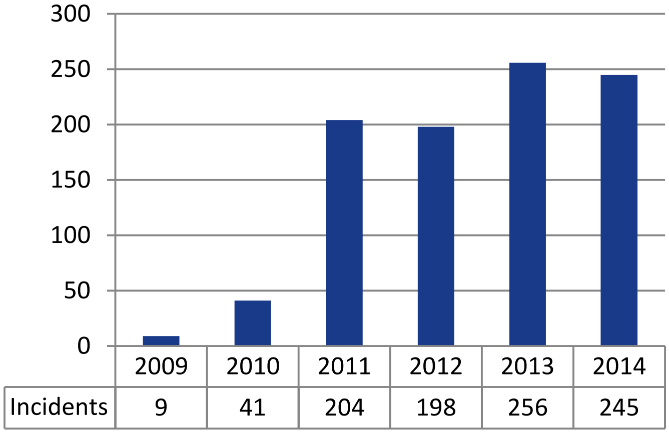
978-92-9204-135-9, 10.2824/835661

Table of Contents

Executive Summary

ICS (Industrial Control Systems) is a general term describing industrial automation systems responsible for data acquisition, visualization and control of industrial processes, often found in various industrial sectors and Critical Infrastructures. They play a critical role not only in maintaining the continuity of industrial processes but also to ensure functional and technical safety, preventing large industrial accidents and environmental disasters.

The criticality of control systems in vital sectors, and high impact in case of disruption, makes them a major target for malicious activities. Based on the ICS-CERT Monitor (part of U.S. Department of Homeland Security)[1], between 2009 and 2014 the number of reported cyber security incidents in the ICS-SCADA area increased more than 27 times. At the same time more than half of the incidents (59% in 2013) were aimed at the energy and critical manufacturing sectors and around 55% involved advanced persistent threats (APT). Still many ICS-SCADA cyber security incidents stay undetected or unreported.



	2009	2010	2011	2012	2013	2014
Incidents	9	41	204	198	256	245

Figure 1 ICS-SCADA cyber security incidents 2009-2014

This study reveals the current maturity level of ICS-SCADA cyber security in Europe and identifies good practices used by European Member States to improve this area.

The first and second part of this study introduces us to the ICS-SCADA cyber security topic, explains the role of ICS-SCADA in critical sectors and summarizes the methodology of this study.

During the desk research, current activities of different Member States in the area of ICS-SCADA cyber security were identified, including related activities, legislation status, existing cyber security strategies and the responsibility matrix of entities dedicated to improve the level of ICS-SCADA cyber security in each country.

Following the research, the ICS-SCADA Cyber Security Maturity Model was used while performing a series of interviews with designated officials from eight Member States. As a result, four Maturity Profiles were identified and described in the third part of this study:

- Leading - Member States with strong legislation and supporting mechanisms dedicated to ICS SCADA cyber security improvement
- Proactive Supporters - Member States focused on strong Critical Infrastructure operators support and driving the ICS SCADA cyber security improvement
- Reactive Supporters - Member States focused on lessons learned and reactive means of improving ICS SCADA cyber security
- Early Developers - Member States in the process of developing of legislation and supporting system to protect ICS SCADA in Critical Infrastructure

[1] https://ics-cert.us-cert.gov

The analysis of maturity level reveals areas for improvement which are concluded in the fifth and last part of this study. As a result, a set of high level and context specific future recommendations to policy and decision makers are issued that include, among others:

Recommendation 1: Align ICS-SCADA efforts with national cyber security strategies and CIIP effort. Currently ICS-SCADA cyber security is not aligned with National Cyber Security Strategies (NCSS) and Critical Information Infrastructure Protection (CIIP) efforts. National Cyber Security Strategies create a baseline for defining cyber space, cyber security objectives and areas of actions. As the ICS-SCADA area is an integral part of the National and EU cyberspace and Critical Infrastructures, it should be aligned with the NCSS as well as CIIP efforts.

Recommendation 2: Develop good practices specific to ICS-SCADA cyber security. Many Member States do not use industry good practices as a reference to set-up an ICS-SCADA cyber security baseline for Critical Sectors. Multiple guidelines, ICS-SCADA security standards and good practices are already developed in the ICS community as well as by individual Member States. It is recommended to leverage from this to develop a minimum security baseline and good practices for ICS-SCADA in Critical Sectors in EU.

Recommendation 3: Standardize information sharing among critical sectors and Member States. Information sharing on ICS-SCADA cyber security incidents and good practices are not communicated in a standardized and frequent manner. A special emphasis should be given on standardizing information sharing of good practices and known threats across critical sectors. A single platform and process (e.g. ICS CERT) to report cyber security incidents and good practices should be in place. Trust between Critical Information Infrastructure (CII) operators and the platform should be built to ensure effective communication from as well as towards the operators.

Recommendation 4: Build ICS-SCADA cyber security awareness. Special emphasis should be given on building awareness of ICS-SCADA cyber security aspects not only across CII operators, but also among decision and policy makers. Nowadays the awareness is built mainly on serious security breaches and incidents. This underlines the more reactive approach, which should be moved towards a continuous awareness growth. As a consequence the ICS-SCADA cyber security threats should be well understood and considered separate from Information Technology (IT) security. This could be achieved by organizing ICS-SCADA cyber security related events involving sector specific platforms to share current challenges and good practices. Knowledge sharing and awareness building should result directly from the ICS-SCADA cyber security strategies.

Recommendation 5: Foster expertise with ICS-SCADA cyber security trainings and educational programmes. Current ICS-SCADA cyber security threats multiply at a very rapid pace. Also several more robust and technology advanced attacks (e.g. Advanced Persistent Threat - APT) are aimed at ICS systems. Moreover a lot of ICS-SCADA cyber security aspects are considered the same as in IT. This basic misunderstanding very often leads to security flaws in ICS-SCADA environments. A deep understanding of the process as well as the technology is needed in order to perceive the real risk and focus area for improving ICS-SCADA cyber security. This is why it is so important to develop future experts and leaders in the area of ICS-SCADA cyber security. This could be done by setting up and supporting new study programs for ICS-SCADA security as well as organizing and promoting related trainings among public bodies.

Recommendation 6: Promote and support ICS-SCADA cyber security research and test beds. It is necessary to involve ICS-SCADA experts and system vendors in the process of addressing current and future cyber security related threats. Support in research programmes and creation of common test-beds can foster ICS-SCADA cyber security innovation and improve security-by-design concept.

The recommendations shall assist, both the European Commission and the Member States, in the process of building resilient ICS-SCADA environment in Europe.

Glossary

APT	Advanced Persistent Threat APT
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
DCS	Distributed Control System.
DHS	Department of Homeland Security
EPCIP	European Programme for Critical Infrastructure Protection
ICS	Industrial Control Systems
ICT	Information and Communication Technologies
ISA	International Society of Automation
IT	Information Technology
NCSS	National Cyber Security Strategies
OT	Operations Technology
PLC	Programmable Logic Controller
PMU	Phasor Measurement Units
REP	Retail Energy Providers
RTO	Regional Transmission Organizations
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition

1. Introduction

The security of ICS-SCADA (Industrial Control and Supervisory Control and Data Acquisition Systems) is increasingly recognized as a high priority area among European Critical Infrastructure operators due to its strategic impact on processes essential for uninterrupted functioning of the EU industries and economy. A rapidly increasing number of incidents in the ICS-SCADA domain, many of which are confirmed or believed to result from cyber-attacks, reveals the vulnerability and fragility of this area and highlights the importance of continuous improvement of ICS-SCADA security for critical service providers. Furthermore, dependencies of Critical Infrastructure across the EU increases the attack surface and potential impact of cyber incidents.

ENISA, as part of its activities, released a series of reports and documents tackling the topic of cyber security in industrial control systems[2]:

- Protecting Industrial Control Systems, Recommendations for Europe and Member States (2011)[3]
- Can we learn from SCADA security incidents? (2013)[4]
- Good practice guide for CERTs in the area of Industrial Control Systems (2013)[5]
- Window of exposure… a real problem for SCADA systems? (2013)[6]
- Good Practices for an EU ICS Testing Coordination Capability (2013)[7]
- Certification of Cyber Security skills of ICS/SCADA professionals (2015)[8]

Furthermore, ENISA has established in 2014 an ICS Stakeholder Group. The role of this group is to provide the opportunity for ICS/SCADA experts to address important issues to ENISA in its efforts to enhance ICS security in the EU. It creates a common platform to enable ENISA consult providers, gather requirements, concerns and share new ideas[9].

Along with the EICS, in 2015 ENISA took over the coordination of EuroSCSIE (European SCADA and Control Systems Information Exchange). This platform was created in June 2005 with the aim of sharing mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions; acting as cross-country facilitator for the exchange of good practices and information and supporting the EU-Countries policy makers on the matter of Critical Infrastructure Protection[10].

[2] Official ENISA Internet page - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems

[3] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

[4] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/can-we-learn-from-scada-security-incidents

[5] https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/ics-cerc/good-practice-guide-for-certs-in-the-area-of-industrial-control-systems

[6] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/window-of-exposure-a-real-problem-for-scada-systems

[7] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/good-practices-for-an-eu-ics-testing-coordination-capability

[8] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

[9] „Terms of reference for an ENISA ICS Security Stakeholder Group” - https://resilience.enisa.europa.eu/ics-security/EICSSGTermsofReference.pdf

[10] https://espace.cern.ch/EuroSCSIE/default.aspx

1.1 Role of the ICS solutions in Critical Infrastructure security

‘Critical Infrastructure’ means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions[11].

The ICS-SCADA environment is the fundamental component of European and national Critical Infrastructures. Most sectors rely on ICS-SCADA to ensure process control and safety which ensure continuity of national critical functions. Vital sectors such as energy, oil & gas, water or chemical, rely on industrial control systems to supervise and control their key processes. As industries lean towards pervasive process automation and maintenance-free operations, the role of ICS-SCADA in the business continuity aspect of those sectors is even greater.

The latest transformation changed the ICS-SCADA environment from proprietary, isolated systems to open architectures and standard technologies. Critical infrastructure operators demand high quality, real time information to make more accurate and justified business decisions. The technological agenda of tomorrow is focused among other things on the following topics: Internet of Things, smart infrastructures, E-Health, Connected retail and Industry 4.0. A good example is the Industry 4.0, which is a collective term for technologies and concepts of value chain organization' which draws together Cyber-Physical Systems, the Internet of Things and the Internet of Services.[12]. The term “Industry 4.0” refers to the idea of a fourth industrial revolution, and originates from the high-tech strategy of the German government, which promotes the computerization of critical manufacturing[13].

The move towards connecting ICS-SCADA and IT environments, however, results in an increased attack surface, thus exposing the critical functions to higher cyber security risks. The priority of ICS-SCADA security results from the great impact on national and European critical functions. The interdependencies of Critical Infrastructures across the EU, may result in a cascading effect in case of a successful cyber-attack.

ICS-SCADA cyber-attacks, on the other hand, are becoming more robust and aimed at specific control system technologies. The Aurora vulnerability[14] and Stuxnet[15] are examples of advanced and well prepared attacks, which were dedicated to exploit unknown vulnerabilities of particular control systems.

[11] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection.

[12] http://www.snom.mb.tu-dortmund.de/cms/de/forschung/Arbeitsberichte/Design-Principles-for-Industrie-4_0-Scenarios.pdf

[13] http://www.bmbf.de/en/19955.php

[14] http://www.powermag.com/what-you-need-to-know-and-dont-about-the-aurora-vulnerability

[15] http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf

1.2 Objective of the study

In order to align, properly address and pave the road for future efforts in ICS-SCADA security, ENISA has analysed the current maturity levels in ICS-SCADA across Europe and drawn conclusions on different national approaches. The aim is to present the current national ICS-SCADA security status and to provide the stakeholders with a set of recommendations on how they can improve their practices, especially regarding critical sectors.

The objective of this study is to:

- Address the current cyber security maturity levels as regards the ICS-SCADA protection in the European Member States;
- Identify, at European level, the thematic areas/indicators of maturity and lessons learnt from the ICS-SCADA security practices followed by Member States in critical sectors; and
- Issue a set of high level and context specific future recommendations to policy and decision makers that will assist, both the European Commission and the Member States, in the process of building resilient ICS-SCADA in Europe.

1.3 Target Audience

The goal of this paper is to inform policy makers and critical service providers on the current ICS-SCADA cyber security agenda in the EU Member States, and identify key areas for improvement. In particular the intended target audience is:

- Relevant national authorities
- The European Commission
- ICS- SCADA stakeholders
- The CIIP community at large

2. Methodology for the assessment of ICS Cyber Security maturity

The ICS-SCADA Cyber Security Maturity Analysis was conducted on the basis of publicly available information and interviews with relevant national authorities in various Member States. For the purpose of this assessment of maturity levels in each Member State, an ICS SCADA security maturity model was developed. The entire study was divided into three tasks:

Task 1 - Desk research

The desk research was conducted on publicly available information which covered both Europe-wide and Member State activities as well as legislation in the area of ICS-SCADA cyber security. Information was collected on existing governance models, practices, policies and critical sectors activities followed by Member States.

Task 2 - Series of interviews

Interviews were held with relevant experts about ICS-SCADA security practices and policies in eight selected Member States. The interviews were conducted on government level with representatives responsible for cyber security of Critical Infrastructure assets. Interviews were based on a questionnaire developed together with an ICS-SCADA Cyber Security Maturity Model. For one Member State, the relevant authority submitted the questionnaire without interview. The questionnaire was used to validate desk research, assess the maturity level of the Member States and identify possible gaps and underline good practices. Thematic areas used within the questionnaire were consistent with ICS-SCADA Cyber Security Maturity Model and covered:

- Legislation in the area of obligations of CI operators concerning ICS SCADA security,
- Support provided by Member State administration to the Critical Infrastructure operators,
- Local conditions of the ICS-SCADA security improvement process (progress, restraints, objectives).

Task 3 - Summary list of all security requirements

Development of an aggregated list of key findings and lessons learnt in the process of securing resilient ICS-SCADA for Europe’s critical sectors. Preparation of this report, which interprets and presents aggregated results from the ICS-SCADA Cyber Security Maturity Model.

In order to facilitate the work 8 Member States were involved in this study:

- Estonia (RIA – Estonian Information System Authority)
- France (ANSSI - French Network and Information Security Agency)
- Germany (BSI – German Federal Office for Information Security)
- Lithuania (Ministry of National Defence)
- Netherlands (NCSC – Dutch National Cyber Security Centrum)
- Poland (RCB – Polish Government Centre for Security)
- Spain (INCIBE – Spanish National Cybersecurity Institute)
- Sweden (MSB – Swedish Civil Contingencies Agency)

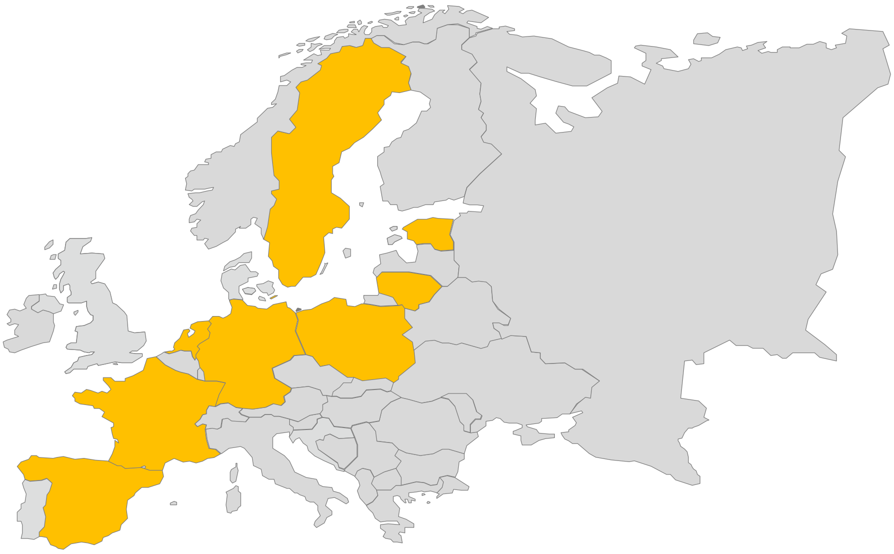


Figure 2: Geographic distribution of Member States covered by the study

All information on ICS-SCADA cyber security in the EU collected during the interviews were documented and additionally confirmed with interviewees. As for the information gathered during desk research, only reliable sources such as official publications of government entities or agencies were taken into consideration. The full list of research sources is included in Bibliography.

The captured data were analysed with the ICS-SCADA Cyber Security Maturity Model in order to supplement the qualitative research with quantitative analysis. The collected data was aggregated to identify existing profiles which represent different approach to ICS-SCADA cyber security in the EU. Additionally good practices and lessons learned captured across different Member State were collected and highlighted in the Report within chapters dedicated to particular aspects of ICS-SCADA maturity.

A draft of the study was sent for comment and preview to all the stakeholders involved and also to the members of the ENISA ICS stakeholder group and EURO SCSIE. A validation workshop was held in Luxembourg on the 30th of September 2015 and findings and recommendations were discussed and validated.

2.1 ICS-SCADA Cyber Security Maturity Assessment Model

To identify the level of cyber security maturity in Critical Sectors in the EU, the ICS-SCADA Cyber Security Maturity Model was created. The maturity model is dedicated to ICS-SCADA security in Critical Infrastructure and should be treated as an integral part of this analysis. The model was built from three major operating model dimensions further divided into nine operating model sub-dimensions. The three major dimensions include:

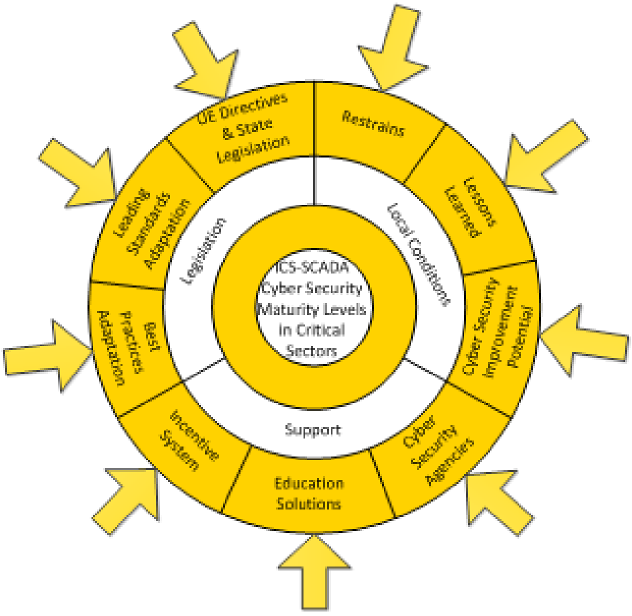

UE Directives & State Legislation
Restrains
Lessons Learned
Local Conditions
Cyber Security Improvement Potential
Cyber Security Agencies
Support
Education Solutions
Incentive System
Best Practices Adaptation
Leading Standards Adaptation
Legislation
ICS-SCADA Cyber Security Maturity Levels in Critical Sectors

Figure 3: Dimensions of ICS-SCADA Security Maturity Model

The **Legislation** - Operating Model Dimension describes how advanced is the legal model of particular Member States in terms of ICS-SCADA cyber security improvement. It covers responsibilities, regulations and policy activities in the area of ICS-SCADA cyber security at Member States level.

The **Support -** Operating Model Dimension captures how efficient Member States support critical service providers in improving ICS-SCADA cyber security by actively participating in cyber security assessments and development processes. It identifies actions aiming at increasing awareness, gathering and propagation of information on existing good practices.

The **Local Conditions** - Operating Model Dimension reports the opportunities and challenges in terms of ICS-SCADA cyber security improvement and identifies focus areas for the future.

Operating Model Dimensions are further dived into Operating Model Sub-Dimensions to specify thematic areas, structure the research and allow comparative analysis between different Member States.

Table 1: ICS-SCADA Cyber Security Maturity Model Dimensions

OPERATING MODEL DIMENSION	OPERATING MODEL SUB-DIMENSION	DESCRIPTION
Legislation	EU Directives & State Legislation	How do the EU and Member States create policy landscapes to support ICS-SCADA cyber security?
	Leading Standards Adaptation	Do Member States utilize industry standards to enhance ICS-SCADA security in Critical Information Infrastructure?
	Good Practices Adaptation	Do Member States develop a systematic approach to collect and exchange good practices among Critical Service providers?
Support	Incentive System	Do Member States support Critical Service providers and encourage them to improve ICS-SCADA cyber security?

OPERATING MODEL DIMENSION	OPERATING MODEL SUB-DIMENSION	DESCRIPTION
	Education Solution	Do Member States support Academics and promote ICS-SCADA cyber security knowledge?
	Cyber Security Agencies	Do Member States appoint dedicated bodies to support ICS-SCADA cyber security incidents?
Local Conditions	Cyber Security Improvement Potential	How efficiently do Member States plan and execute ICS-SCADA cyber security improvements?
	Lessons Learned	Do Member States monitor the results of their ICS-SCADA cyber security improvement activities and take the proper corrective actions?
	Restraints	How well do Member States cope with limitations affecting ICS-SCADA cyber security improvements?

Operating Model Sub-Dimensions are the thematic areas which determine the maturity level of ICS-SCADA cyber security in Member States. To capture the accurate level of maturity an underlying questionnaire was prepared to describe and valuate each Operating Model Sub-Dimension. The questionnaire included 82 questions divided into parts corresponding to the nine sub dimensions described above and (where feasible) with reference to the lifecycle of a process:

- Create - How is the process developed?
- Implement - How is the process deployed?
- Monitor - How is the process reported and monitored?
- Modify - How is the process adapted and changed?

Answers for each question were scored against a 5 level scale with clearly defined, question independent criteria. To ensure reliability of the results, when answers were gathered during the interview, assessment criteria were not shared with the interviewed stakeholders. The maturity levels used for the purpose of the study were:

- Basic – activities aren't conducted,
- Developing - activities are under development or conducted on ad-hoc manner,
- Established - activities are regularly conducted on the basic level,
- Advanced - activities are implemented with a deep understanding of ICS-SCADA specific requirements,
- Leading - activities are implemented in the level that exceeds current, basic needs (are design to address needs which arrival is foreseen).

To complement the analysis, information on additional non-standard activities around cyber security in ICS-SCADA area for individual Member States was taken into consideration. The mixed research methodology (qualitative and quantitative) provides advantages by relegating qualitative analysis to an exploratory tool. It gives a broader perspective over the cyber security maturity subject and enables to capture patterns and make statistical analysis which makes the study more comprehensive.

3. State of ICS security within the EU

ICS-SCADA Cyber Security Maturity Levels across EU Member States result from a number of variables which make up the presented Maturity Model. Based on the multidimensional analysis, the following four ICS-SCADA Cyber Security Maturity Profiles where observed:

Table 2: Cyber Security Maturity Profiles

TABLE HEADING	DESCRIPTION
Leading	With a strong legislation and supporting mechanisms dedicated to ICS SCADA cyber security improvement
Proactive Supporters	Focused on strong CI operators support and driving the ICS SCADA cyber security improvement
Reactive Supporters	Focus on lessons learned and reactive means of improving ICS SCADA cyber security
Early Developers	In the process of developing of legislation and supporting system to protect ICS SCADA in Critical Infrastructure

The profiles are based on the Desk Research as well as interviews with eight Member States who already initiated actions related to ICS-SCADA cyber security. Some of Member States which were initially asked to participate in the study openly declared that they were not ready to participate as they did not initiate any activities in the ICS-SCADA security and they would not bring any value to the study. According to the conducted desk research, it has been approximated that the percentage of such Member States is around 25% to 30%.

Each profile is characterized by a different focus on which the ICS-SCADA maturity is built. This is presented on the *"focus graph"* for each Profile. Also determinants are presented to better understand the characteristics of each ICS-SCADA cyber security maturity profile. Furthermore a SWOT analysis was performed to identify strengths and weaknesses as well as seize opportunities to improve the level of ICS-SCADA cyber security.

3.1 Profile 1: Leaders

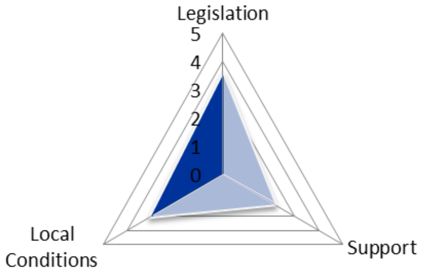


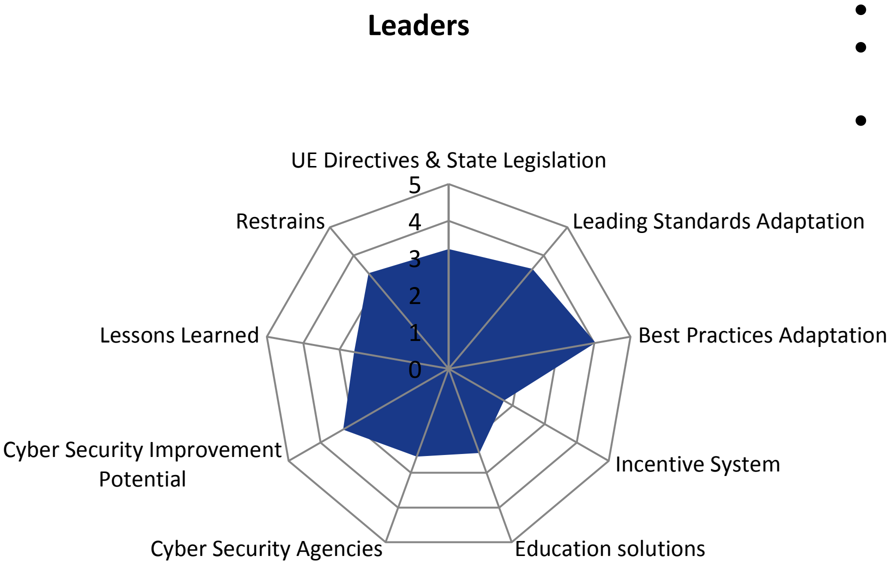
Figure 4 Focus Graph - Profile 1

Member States with the highest ICS-SCADA Cyber Security Maturity Level. They are characterized by a developed legal system and strategic vision which drives cyber security improvement initiatives in Critical Sectors.

"Leaders" have a very controlled and settled approach over ICS-SCADA cyber security and provide direct legislation to support it. The CI Operators are obliged to report incidents and incentive measures are in place to ensure compliance with minimal security requirements in the corresponding sector.

"Leaders" have significant ICS-SCADA cyber security awareness (government, CI operators) and a high level of public-private collaboration in this area. Dedicated groups responsible for CIP are skilled and trained in the area of ICS-SCADA cyber security. Academic and scientific centres are involved in the research and development process of ICS-SCADA cyber security countermeasures. Leading ICS cyber security standards are utilized in order to create own guidelines for CI Operators. Leaders are open to share knowledge and educate other Member States in this area.

Furthermore ICS-SCADA security is covered by Member States cyber security strategies, current security level is monitored (e.g. by audits). In order to ensure "security by design" ICS-SCADA suppliers are involved and certification processes for critical assets are being developed and planned to be implemented.



Determinants of the profile:

- Strong EU economies
- High level of automation and digitalization
- Mature cyber security policy

Below the SWOT analysis is presented for the ***Leaders Profile***. It identifies strengths and weaknesses of the profile as well as opportunities to improve the level of ICS-SCADA cyber security.

	STRENGTHS	WEAKNESSES
INTERNAL	● Long-time planning on the ICS-SCADA security improvement process ● Deep understanding of ICS-SCADA role in the CIP ● Established cooperation between CI operators and government ● Security-by-design approach - asset certification process in development	• Lack of incentive systems to promote ICS SCADA cyber security improvements • Still very few research programs to the ICS SCADA security improvement
	OPPORTUNITIES	**THREATS**
EXTERNAL	● ICS-SCADA cyber security good practices shared across EU (Member States with lower maturity may benefit from Leaders experiences)	• Few number of experts on the market with ICS-SCADA security background (ICS-SCADA security matters handled by personnel with purely IT background)

The study describes Leaders as mature Member States with various efforts identified in the area of ICS-SCADA cyber security including long term planning, alignment with CIIP efforts, trust between responsible government bodies and critical sectors as well as preventive activities including auditing and/or testing.

This role model can be followed among all Member States to leverage from previous experiences and is an opportunity to support attempts towards higher level of ICS-SCADA cyber security maturity across EU.

3.2 Profile 2: Proactive supporters

The "Proactive supporters" include Member States whose main focus is on equipping Critical Infrastructure operators with the necessary tools to continuously improve ICS-SCADA cyber security level. Strong government support and public-private partnership distinguish this profile. Academic and scientific centres are involved in the research and development process.

Proactive measures are being developed with a very close cooperation with internal (government, CI operators) and external (academics, private agencies) stakeholders. To obtain this, information sharing platforms are developed and working groups are settled.

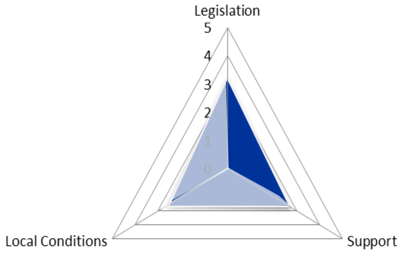
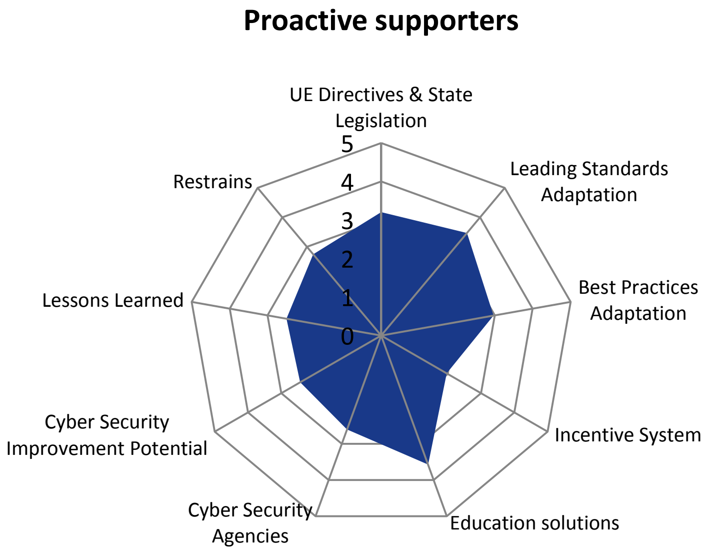


Figure 5 Focus Graph - Profile 2

The "Proactive supporters" put incentive systems in place in order to support CI operators and promote ICS-SCADA cyber security initiatives (e.g. use of EU funds for ICS-SCADA testing).

The Member States are strongly focused on building ICS-SCADA security awareness and understating among CI operators and the society, by enabling access to knowledge and specialized trainings. They create ICS cyber security guidelines in a cooperation with a wide ICS-SCADA community.



Determinants of the profile:

- Close private-public partnership
- Academic and scientific involvement
- Structural funding of ICS-SCADA security initiatives

Below the SWOT analysis is presented for the ***Proactive Supporters Profile***. It identifies strengths and weaknesses of the profile as well as seize opportunities to improve the level of ICS-SCADA cyber security.

	STRENGTHS	WEAKNESSES
INTERNAL	● Close private-public partnership ● Academic and scientific involvement ● A lot of educational measures developed ● Structural funding of ICS-SCADA security initiatives	• Only basic regulations implemented • ICS-SCADA security improvement process is less systemized
	OPPORTUNITIES	**THREATS**
EXTERNAL	● High trust between CI operators and the Member State allow for effective gathering of good practices developed by private sector	• Weaker regulation and planning may lead to conducting actions which in the future are likely to prove inaccurate or ineffective

The proactive supporters are characterized by close cooperation with various organizations (including private and public).These initiatives compensate the basic regulation and an ICS-SCADA cyber security improvement process that is less elaborate.

This "Proactive Supporters" create a good environment for knowledge and information sharing and may be a good source of ICS-SCADA cyber security good practices.

3.3 Profile 3: Reactive supporters

The “Reactive supporters” approach the ICS-SCADA cyber security by taking reactive actions and answering the rising need for cyber security on an ongoing basis. The main focus is on improvement of identified vulnerabilities or response after cyber security incidents (not particularly in this Member State).

Most of the ICS-SCADA related activities result from the awareness activities regarding relevant threats, not from the legislation itself. Organized working groups divided into individual critical sectors gather good practices and lessons learned for improvement of the ICS-SCADA cyber security level.

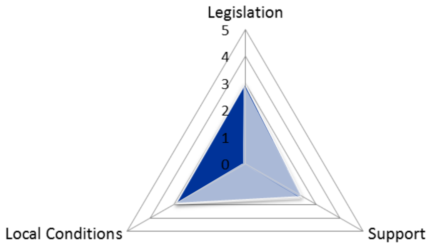
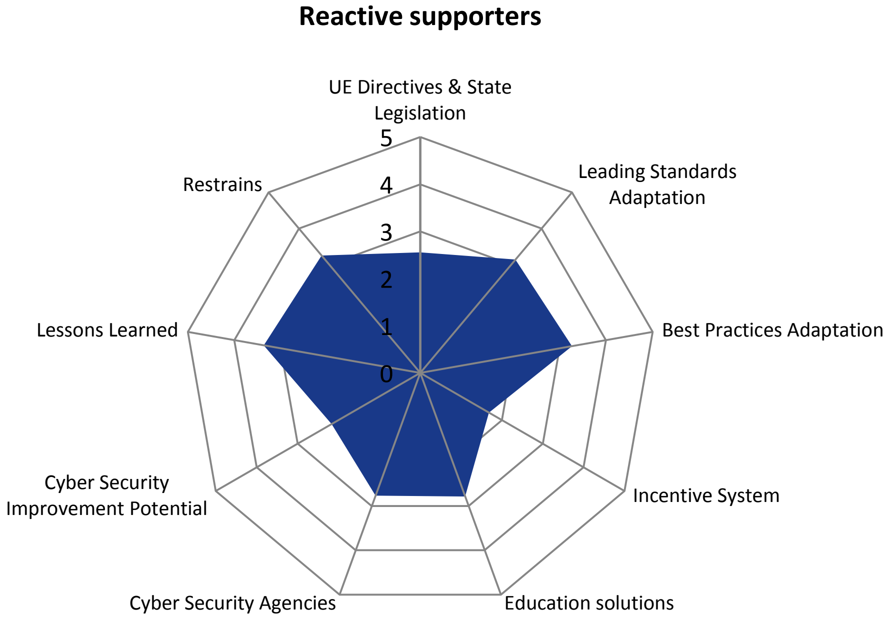


Figure 6 Focus Graph - Profile 3

The role of monitoring and improving ICS-SCADA cyber security is often informal and is combined with IT security activities.

The “Reactive supporters” understand the need for more specific legislation in the area of ICS-SCADA cyber security and put this high on their future agenda.



Determinants of the profile:

- High level of trust between CI operators and the Member State
- Extensive auditing and reporting process

Below a SWOT analysis is presented for the ***Reactive Supporters Profile***. It identifies strengths and weaknesses of the profile as well as opportunities to improve the level of ICS-SCADA cyber security.

	STRENGTHS	WEAKNESSES
INTERNAL	● Close private-public partnership ● Strong auditing and reporting regulation	● Focus on taking reactive actions rather that proactive initiatives ● Treating ICS-SCADA as traditional IT ● Ad-hoc initiatives (weak planning) ● No guidance or obligations towards ICS-SCADA security
	OPPORTUNITIES	**THREATS**
EXTERNAL	● Good understanding of existing threats in the ICS-SCADA environment can be propagate across other Member States	● Weaker regulations and planning may lead to conducting actions which in future will prove to be not accurate or ineffective

The strength of “Reactive Supporters” is in the auditing and reporting capabilities, which gives the opportunity to track and learn from past ICS-SCADA cyber security incidents.

This approach, however, does not provide sufficient means to leverage from this knowledge to ensure proactive process of improving the level of ICS-SCADA cyber security in Critical Sectors.

3.4 Profile 4: Early Developers

The "Early Developers" are characterized by a low maturity level of ICS-SCADA cyber security.

Cyber security legislation to distinguish Critical Infrastructure and developed ICS-SCADA related cyber security agenda, exists for less than 3 or even 2 years.

The list of critical assets has either been identified recently or has not been identified yet. Furthermore no guidelines on ICS-SCADA security have been developed yet.

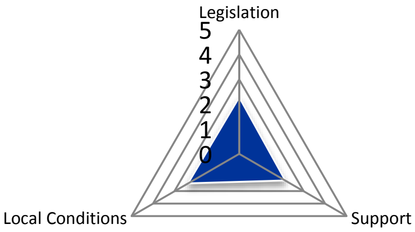
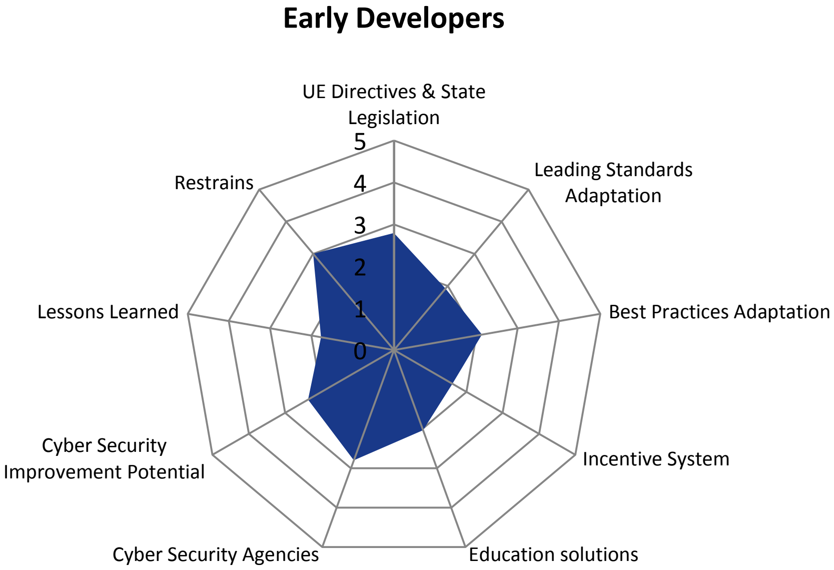


Figure 7 Focus Graph - Profile 4

The public-private partnership and academic involvement is in the very initial phase. There is little expertise in the area of cyber security in industrial control systems, thus little awareness of good practices and leading standards.



***Determinants of the profile*:**

- Cyber Security legislation implemented less than 2-3 years ago
- Limited awareness activities and expertise in the area of ICS-SCADA cyber security

Below a SWOT analysis is presented for the ***Early Developers Profile***. It identifies strengths and weaknesses of the profile as well as opportunities to improve the level of cyber security in ICS-SCADA.

	STRENGTHS	WEAKNESSES
INTERNAL	● Basic legislation background for Critical Infrastructure Protection is usually already in place ● Long-time planning (but are on much earlier stage than leaders)	● Little or no private-public partnerships ● ICS-SCADA treated as traditional IT ● No guidelines of how to protect critical assets ● Limited expertise (and experiences) in the area of ICS-SCADA cyber security
	OPPORTUNITIES	THREATS
EXTERNAL	● Opportunities to benefit from experiences of other, more mature Member States ● Use of available materials and programmes developed by other Member States in the area of ICS-SCADA cyber security	● Low trust between CI stakeholders may significantly slower the ICS-SCADA improvement process

For “Early Developers” there are usually only few initiatives which can be identified to be ICS-SCADA specific. Most of the early developing Member States begin with legislation which very often focuses on cyber security in general instead of distinguishing ICS-SCADA as a separate topic.

“Early Developers”, however, often leverage from already existing legislation and good practices which is an opportunity for more dynamic growth in ICS-SCADA cyber security maturity.

The difficulty which may be observed are resulting from low awareness, little ICS-SCADA cyber security expertise and little trust for public-private partnership.

4. ICS-SCADA cyber security activities in Member States

The following describes the activities and good practices among EU Member States in the area of ICS-SCADA cyber security.

The activities presented in this part of the study result from the ICS-SCADA Cyber Security Maturity Model, performed interviews with relevant Member States officials as well as desk research. They are divided into the following thematic areas:

- Organizational structures
- Regulations and Policies
- Assets covered
- Auditing and certification
- Incident handling
- Incentives
- Education
- Trainings and courses
- R&D
- Information sharing
- Public-Private Partnership
- Objectives and restraints

Next to each thematic area an example of good practices is shown with the indication of a respective Member State.

4.1 Organizational structures

The "Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection" not only points out the need to designate and protect Critical Infrastructure but also identifies actors responsible for different activities at high level.

At the EU level the European Commission acts as the executive body responsible for proposing legislation and implementing decisions. The Commission may also support Member States in identifying Critical Infrastructure on an ongoing basis.The Council Directive, however, acts only as a general framework for Critical Infrastructure Protection. The details on taking specific actions are under the responsibility of each Member State. This also includes the responsibility for specifying ICS-SCADA cyber security requirements for CI operators.

The Council Directive also suggests the designation of Security Liaison Officers for all identified ECIs in order to facilitate cooperation and communication with relevant national Critical Infrastructure protection authorities.[16]

Next to the main EU institutions, dedicated agencies and organizations are driving ICS-SCADA cyber security efforts. To enforce activities related to network and information security (also including ICS-SCADA) as well as help European Commission, Member States and business community, to address, respond and prevent network and information security problems, ENISA was established in 2004. Under ENISA, the ICS Stakeholder

[16] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection (OJ L 345, 23.12.2008, p. 75–82).

Group was created, in order to enhance the current efforts in improving ICS-SCADA cyber security across the EU. In 2015, ENISA took over also the coordination of EuroSCSIE (European SCADA and Control Systems Information Exchange). The aim of EuroSCSIE was initially to share information on electronic security threats, vulnerabilities, incidents and solutions as well as support Member States policy makers on the matter of Critical Infrastructure Protection[17].

At Member States' level various approaches regarding organizational structures is observed. Different roles within Member States can be divided into responsible, accountable, consulted and informed. Some Member States (e.g. Poland) directly implemented EU recommendation from the Council Directive 2008/114/EC.

Poland

Activities related to ICS-SCADA cyber security in Critical Infrastructure is the responsibility of RCB[18] (Rzadowe Centrum Bezpieczenstwa) who coordinates the creation of Critical Infrastructure Protection Plans. RCB is subordinate to the President of the Council of Ministers. Moreover Security Liaison Officers are designated in each Critical Infrastructure operator to inform RCB about major security incidents.

Others implemented their own, more extensive structures divided into each critical sector and including incident response capabilities:

France; Germany

In France and Germany a single security authority is responsible for Critical Infrastructure cyber security regulation, respectively German Federal Office for Information Security - BSI[19] and French Network and Information Security Agency - ANSSI[20].

They establish working groups dedicated to critical sectors (and sub-sectors were relevant). The output of these committees is further validated by the security authority and/or concerned ministries. A group dedicated to ICS-SCADA cyber security is in place to study and adapt good practices across critical sectors.

4.2 Regulations and Policies

The backbone for the ICS-SCADA cyber security has been established by "The Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection" which defined European Critical Infrastructure (ECI), CI protection, and the concept of the ECI owner (operator). The Directive also defines fundamental duties imposed on Member States with regard to ECI protection. Since then, European Member States have started to implement local regulations in the area of CIP, including those concerning cyber security of industrial assets (ICS-SCADA). For now three main kinds of regulation are implemented:

- Obligation of reporting on cyber incidents regarding Critical Infrastructure assets

[17] http://www.gcsec.org/
[18] http://rcb.gov.pl/eng/
[19] https://www.bsi.bund.de/DE/Home/home_node.html
[20] www.ssi.gouv.fr/

Such obligations have been implemented by all Member States covered by this study, which managed to formally identify its CI assets. Depending from the Member State, the incident may be reported directly to the entity responsible for the CI cyber security (e.g. in France, CI operators report security incidents to ANSSI) or through the national CERT (e.g. Lithuania). Besides that, some countries developed a dedicated, regulated communication channel between CI operators and responsible government entities. Such an example is Poland.

Poland

According to the “Polish Act on Crisis Management 21 from April 26, 2007”, every CI operator is obliged to have a clearly appointed person who acts as a primary contact with entities responsible for CI protection. This obligation has been additionally clarified by an “Act from March 18, 2010” which states, that the Management Board of a particular critical systems owner (supply of fuels and energy resources), in agreement with Director of RCB and the Ministry of State Treasury appoints a duly authorised representative responsible for the CI protection. The representative is an employee of the company, who monitors activities of the Management Board in relation to actions that may affect the continuous functioning of critical systems. This representative can act as a contact person mentioned in previous paragraph. Every quarter of the year, this representative drafts a report on the condition of CI protection in the company in question (so much more than just reporting on incidents), including the condition of cyber security. A copy of the report is sent to the Director of RCB.

- Obligation of fulfilling minimal security requirements
  Some countries have implemented industrial sector specific minimal security requirements with which CI operators have to be compliant (e.g. France). Even more countries are currently working on promulgating legal instruments on minimal security requirements.

Germany

In Germany, detailed regulations specific for each Critical Infrastructure sector are promulgated by working committees (one committee for each sector) composed of BSI personnel and representatives of CI operators. Each committee defines minimal requirements for securing ICS SCADA in each corresponding sector.

- Obligation to develop CIP plans
  Some EU Member States require by means of a regulation the development of CIP plans (including cyber security area). These regulations impose the obligation for CI owners to develop Critical Infrastructure Protection Plans addressing a description of threats, possible scenarios and implemented risk mitigation measures. The regulation refers to security in different areas: legal, physical, personnel and cyber. The advantage of such an approach is that protection of each CI site is treated as a whole system, which elements correspond to each other.

Spain

According to Spanish regulations, every Critical Infrastructure Operator has to develop a security plan or "Plan de Seguridad (PSO)" to lay out its Security Policy, Scope, Risk Assessment Methodology and guidelines for implementing the proper security measures in its infrastructure.

[21] http://rcb.gov.pl/eng/wp-content/uploads/2011/03/ACT-on-Crisis-Management-final-version-31-12-2010.pdf

Poland

CIP plans were introduced in Poland through "Regulation of the Council of Ministers on Critical Infrastructure Protection Plans, April 30, 2010". Every Critical Infrastructure Operator, who has been identified as such, has to develop a Critical Infrastructure Protection plan. The plan has to be updated every two years and it has to be agreed with national crisis management system stakeholders (protection of CI is part of the national crisis management system).

4.3 Assets covered

In 2015, ENISA released a guide entitled: Methodologies for the identification of Critical Information Infrastructure assets and services. Although the guide is focused on the identification of the data communication networks, described methodologies can be used for identification of other CI assets, including ICS-SCADA solutions supporting Critical Services[22].

In this study, we focus on the problem of identification of ICS-SCADA assets only. Generally, the main problem from the perspective of entities responsible for Member States cyber security in the context of CIP, is how to ensure that all ICS-SCADA assets which support services considered critical from the Member States perspective are identified and covered by CIP activities. Generally, Member States who have already identified their critical assets choose one of the two following approaches:

4.3.1 The State-driven approach

The state creates definitions regarding the conditions under which assets are considered to be critical. These definitions are being communicated to the CI operators who on this basis develop their list of critical assets.

4.3.2 The operator driven approach

The Member States are involved in the definition of Critical Infrastructure (physical locations) based on the criticality of the services. Following the creation of such a list, the critical assets (e.g. ICS systems) are identified by the Critical Infrastructure operator alone based on a risk analysis. In this approach, a list of Critical Infrastructure is created in cooperation with government and CI operators. The list usually includes the names and locations of physical sites responsible for Critical Services. Then, each CI operator on the basis of risk analysis techniques identifies threats scenarios which can influence continuity of each site operations. This covers all kind of threats, including cyber threats related to ICS-SCADA. On the basis of risk analysis, a CIP plan is created, which later is agreed upon with national entities responsible for crisis management.

Observation:

Not all Member States identified their Cricial Assets, including ICS-SCADA.

4.4 Information sharing

Building up partnerships between Critical Infrastructure operators (including those privately owned) and government institutions is crucial for successful building of CIP systems, as it allows for achieving mutual understanding of needs, priorities and restraints. Entities responsible for CI cyber security on the national level require a proper communication from CI operators to receive feedback on effectiveness of actions they conduct and for proper identification of assets which are critical to the performance of processes which are

[22] "Methodologies for the identification of Critical Information Infrastructure assets and services. Guidelines for charting electronic data communication networks." ENISA, 2014

important to society. CI operators on the other hand require a clear communication on government requirements and the purpose of operations that are expected from them.

Most Member States choose to build up partnerships on the basis of working groups dedicated to the development of some particular products, such us security guidelines or minimal security requirements dedicated to the various industrial sectors.

For example, ANSSI (France) established 18 working groups dedicated to critical sectors (and sub-sectors when deemed relevant). These committees are responsible for drafting proposals of regulations (specific requirements) for cyber security measures in the corresponding sectors. These proposals are then validated by several public administrations including ANSSI and the concerned ministries.

Apart from these working groups for regulation development, another wider working group exists which deals specifically with ICS SCADA security and aims at gathering information and adapting good practices. This group prepared inter alia a Protection Profile for industrial automation devices and systems such as PLC, SCADA Server, MES Server, Engineering Software, etc. This group has also produced the guides “Cybersecurity for industrial control systems: Classification method and key measures” and “Cybersecurity for industrial control systems: Detailed measures”, and the document “Training guide for ICS cybersecurity”.

Some countries, apart from product focus groups, build up ICS SCADA security community on the basis of periodic thematic meetings.

Netherlands

The Dutch Information Sharing and Analysis Centres (ISACs) are usually CI-sector specific security oriented public-private platforms. Organizations can exchange their cyber security problems experiences (incidents and best practices) in confidence and anonymously. Following an analysis, a warning can be issued to all participating organizations about a threat, vulnerability or incident, or about a good practice that can be applied to mitigate a risk. Most ISACs organize tactical level professionals from public or private CI operators. The technical and ISAC secretariat support is funded facilitated by the NCSC-NL. ISAC communication runs via closed mailing lists, tele-conferences, and physical meetings which are held on a regular basis.

As generally some sort of cooperation between CI operators and government entities responsible for ICS SCADA exist in the majority of Member States covered by study, some Member States referred to lack of trust between the two sites as a significant constraint in the process of ICS SCADA security improvement (or listed of building such a trust in a priority goals for the nearest future). From the discussions with various CI operators, it may be stated that such lack of trust originates from two sources:

- CI operators are afraid of sharing the information about any existing security problems with government, as they believe that at some point this information can be used against them (e.g. after implementation of law which imposes penalties). This anxiety is especially strong in publicly own companies, where management boards are to some extent dependent on political decisions,
- CI operators do not believe that government entities understand constraints and needs of their business processes. This may lead to the situation, when government representatives with some limited knowledge on the processes conducted by operators and their dependencies will try to enforce security controls, which from CI operator’s perspective are considered as non-cost-effective. To protect themselves from such situation, absurdly some CI operators choose to share only very limited information (only those which is required from them by law) to keep government in opinion that

"everything what is needed has already been done, there is nothing else to improve" (what is interesting, this kind of approach was observed not only on only on government / operators level but also even within large companies – e.g. company HQ / local branches).

As any Member State which already established a various working groups some time ago did not listed lack of trust as significant problem, this shows how important it is to build a community around CIP, including area of ICS-SCADA security. As building a trust takes time, the sooner any kind of cooperation is started, the greater chance that it will contribute to the development of effective CIP program. Most of high quality ICS-SCADA security guidebooks released in various Member States have been developed in cooperation between government entities and CI operators.

Observation:

Low trust between CII operators and public bodies and non-standardized approach for information sharing among Critical Sectors across Member States.

4.5 Auditing and certification

Implementation of auditing programmes always requires answering two questions:

1. **What should be audited?**
2. **What should be the reference point to the audit?**

This is why implementation of auditing and certification in the area of CIP is strictly related to the maturity of particular MS in the area of critical assets identification and legislation. Independently from the results of the maturity level assessment, most Member States consider future implementation of auditing and certification programmes.

Germany

Germany is one example of MS currently in the process of implement an auditing system. As regulations regarding the definition of critical assets and minimal security requirements are still being developed, no audit process has been implemented yet. After the corresponding executive orders are published, critical assets owners will have a 2 year period to implement the required controls. Audits will be conducted every two years by commercial companies, which manage to obtain BSI accreditation. For noncompliance with regulation penalties are foreseen up to 100 000€. The described model of obligatory audits conducted by accredited companies is the approach which is considered or already implemented by most Member States (in some cases however no penalties are foreseen).

A separate, but interesting and important case, is a certification program which is being currently developed in France.

France

Unlike other initiatives, France initiated a program dedicated to certification of ICS devices and service providers. The program is eventually going to bring benefits to both ICS vendors (who will be able to get independent confirmation that their products are being developed with a certain level of security) and users (who will be able to consciously choose devices which have been developed with security in mind). If the program is successful, it may be reasonable to consider its expansion to the whole EU.

4.6 Incident handling

The ability to respond to and mitigate the impact of ICS incidents is crucial to ensure security and continuity of Critical Services in Member States. However to provide meaningful support to critical service providers, appropriate resources need to be maintained.

Most of todays' incident handling capabilities in the EU, however, are limited to IT cyber security only. Limited resources are dedicated specifically to the industrial control environment. Sector specific agencies are often involved in the process of investigation/monitoring/ response to ICS SCADA cyber security incidents.

Spain

The Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (Secretary of State for Telecommunications and the Information Society) has concluded an agreement in which, amongst other matters, the terms for joint work between CNPIC and the Instituto Nacional de Ciberseguridad (National Institute of Cybersecurity – INCIBE) in the field of Response to Incidents for Spanish-based Information Technology Critical Infrastructures are laid out. This sets out how INCIBE functions as a tool for supporting CNPIC in the management of cybersecurity incidents.

Together, both institutions have set up a Security Incident Response Team, which specializes in the analysis and management of information technology security problems and incidents. This Response Team functions as a CERT, specialized in the management of Critical Infrastructure incidents on a national level. Whenever a Critical Infrastructure suffers a cybersecurity problem, the operator responsible for such matters can avail himself of the response team's services, making the incident known by means of the Single Contact Point set up to this end.

The ICS-SCADA incident handling topic has been recognized by ENISA in 2013, when recommendations for emergency response capabilities in the area of ICS-SCADA were published.[23] The report presents advantages and disadvantages of different types of organizations: ICS sector specific, national, regional and global. It also discusses the technical and organizational operational capabilities required for the provisioning of emergency response services. ENISA also points out the need for an on-going co-operation between CERTS's providing response services and other ICS stakeholders (ICS system providers and vendors, other CERT's, international initiatives in the area of ICS-SCADA protection).

4.7 Incentives

Application of incentive systems to promote ICS-SCADA cyber security and increase investments in this area is a subject of discussion as different approaches are presented by various Member States. Many Member States do not believe that financial incentives are the right direction to build awareness and ICS-SCADA cyber security backbone for Critical Infrastructure operators. The general belief is that Critical Infrastructure cyber security lays under the responsibility of the operator itself, therefore no incentive should be in place. On the other hand incentives were most frequently indicated by CII operators, as the expected means of Member States or EU support.

Three types of incentives in the area of ICS-SCADA cyber security were identified, as possible to implement in the future:

[23] "Good practice guide for CERTs in the area of Industrial Control Systems - Computer Emergency Response Capabilities considerations for ICS" - ENISA 2013-12-04

- Direct subsidy - refinancing of ICS-SCADA cyber security activities
- Tax exemption - tax relief towards Critical Infrastructure operators resulting from obtaining ICS-SCADA cyber security measures
- Discounts on insurance rates - lower insurance cost towards Critical Infrastructure operators resulting from obtaining ICS-SCADA cyber security measures

According to the study, only direct subsidies have been identified to be implemented in Estonia.

Estonia

As part of Critical Information Infrastructure protection, ICS security assessments are performed on a voluntary basis, sponsored by the Estonian Government. As part of the security testing, also comprehensive IT assessment is included. The security assessments included:

- **Information gathering from public sources: what kind of tools is each company using**
- **Networks perimeters: how is possible to protect different types of networks**
- **Workstation & servers**
- **Remote access: facing Internet**
- **Physical security: how much time security company takes to come**
- **Disaster recovery plans, architecture, security policies, etc.**

4.8 Awareness raising

Numerous Member States identified improvement on ICS-SCADA security awareness as one of the biggest priorities for upcoming years.[24] Several activities have been conducted to achieve this goal, but obtained results are difficult to measure. It is also clear that this area has a potential for further improvement. As high level of awareness is normal within personnel with an IT background, ICS engineers naturally focus themselves on the system functionalities and availability. However, as the number of ICS-SCADA cyber security incidents around the globe is rising and becomes a better-known topic, security researchers's efforts are increasing visibility and interest on the area. Such events naturally increase basic awareness in much broader a way than any other, government run or supported activities, however they lack of deeper expertise and real educational value. This is what makes a role of government entities and private associations so important. The following educational activities are currently being conducted by Member States to support Critical Infrastructure operators on ICS-SCADA security:

- Development of whitepapers and guidebooks dedicated to the ICS-SCADA security
  A lot of Member States government entities have published materials dedicated to the ICS-SCADA security. Some of those have been prepared in working groups with representatives of various ICS SCADA security stakeholders, e.g.: government entities, Critical Infrastructure operators, ICS-SCADA solution vendors and private security associations. In many cases such approach allowed for achieving of high quality of the prepared publications. The fact that some of those materials have been publicly released not only in national languages, but in English as well, makes them useful for the whole EU society. In Annex A is available the list of a few most worth mentioning publications publicly available.

Observation:

[24] Interviews with: RIA (Estonia) on 07 VII 2015, BSI (Germany) on 15 VI 2015, RCB (Poland) on 19 VI 2015,

Low awareness on ICS-SCADA cyber security topic and treating ICS-SCADA as regular IT.

4.9 Training

Currently, there is a very limited number of available courses on the ICS-SCADA cyber security. Below is an overview of the most notables examples. Related to this area, ENISA covered in 2015 also the topic of available certifications for skills in ICS SCADA[25].

INCIBE (Instituto Nacional de Ciberseguridad, Spain) has carried out the first MOOC Cyber Security Advanced Course in Control Systems and Industrial Automation. This course has been designed and developed in collaboration with leading Spanish industrial sector organizations and cybersecurity, as well as national and international expert highly, thus ensuring that the course includes both the required content, the experiences and advice of the most skilled professionals on the international scene. This course is taught through the MOOC approach (Massive Open Online Courses), namely, Online, massive and open to everyone so through the new training platform INCIBE.[26] The course required a student input of 50 hours over 6 weeks. The first occurrence of the course was closed in February 2015, event was attended by 3,200 participants, 11% of whom the completed the course successfully. The course was delivered in English and Spanish.

Another interesting Spanish initiative is development of two years cybersecurity research centric academic degree on MSc Research in Cybersecurity from Universidad de León. This Master's degree will be taught in two courses. The first course allows students to obtain knowledge in the most relevant cybersecurity research fields: systems (operating system and network) cybersecurity, software security, cyber-physical systems security (including industrial security), human aspects and legal implications of cybersecurity, mathematics for cybersecurity, and security auditing and forensics. All modules are mandatory, allowing students to gather knowledge enough to know where they would like to start their future research. The second course is split across two semesters; during the first one students choose elective subjects of their preference to expand their knowledge in their field of choice: systems, software, industrial, human & legal, mathematics, auditing and forensics, or even practical experience, a six month paid work experience in a cybersecurity related company; during the second part of the year, they work on their master thesis. This Master's degree will be taught completely in English and the content will be offered both in-classroom and online (using the AVIP platform of Spanish UNED). The Universidad de León is currently pending approval from Spanish ANECA (Agencia Nacional de Evaluación de la Calidad y Acreditación).

France pointed out how to increase in the number of ICS SCADA security competent personnel is one of the goals in its cyber security strategy[27]:

"The presence of information systems security experts in our industrial base must therefore be increased. Orienting young people towards such jobs will be encouraged in order to expand the pool of expertise available in the country."

To achieve this goal ANSSI promotes the idea of creating courses dedicated to ICS-SCADA security. For that purpose, ANSSI developed a guide for the entities who would like to conduct such trainings. If the guide will be successful, BSI (Germany) considers adapting this in the future for its own CIP programmes[28].

[25] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/scada-industrial-control-systems/certification-of-cyber-security-skills-of-ics-scada-professionals

[26] www.incibe.es and information provided by INCIBE in OT assessment maturity form, 2015

[27] "Information systems defence and security. France's strategy" Agence Nationale de la Sécurité des Systèmes d'Information, France, 2011

[28] Interview with BSI (Germany) on 15 VI 2015

Estonian, Latvian and Lithuanian Governments are cooperating with the USA and Idaho National Laboratory to train ICS SCADA experts on Information Security topics. The trainings are planned to be continued in the future[29].

Observation:

Currently, there is a very limited number of available courses on the ICS-SCADA cyber security.

4.10 Research & Development

Only few scientific programs have been identified during the study. In most Member States, there is no real cooperation between the scientific community and entities responsible for ICS SCADA security in Critical Infrastructure, although most of interviewed stakeholders mentioned that they are planning to initiate such cooperation in the future. In those few Member States where such cooperation exists, it seems that in the longer period of time such cooperation can bring a significant value to the protection of Critical Infrastructure in the whole EU. The most interesting identified research is a work of the SUPPRESS group of the University of León has designed a laboratory for research in cybersecurity of Critical Infrastructures, which replicates these control architectures in an environment that tries to replicate the real conditions. This platform is funded by the National Program of Scientific Infrastructures and Equipment, and it is currently in the equipment acquisition phase. The five main goals aimed with this design are:

1. To include industrial control equipment and software that is widely used in Critical Infrastructures.
2. To achieve enough flexibility to allow reconfiguration of the networks as well as the application of several combinations of security measures.
3. To allow replication of control and monitoring networks present in different sectors of Critical Infrastructures, particularly, industrial control systems, power management, building management and smart cities.
4. To allow testing at every level of the automation architecture, on heterogeneous equipment and on the most widely used network protocols in each application area.
5. To include a management system that facilitates testing, enabling data acquisition (from the control and monitoring system, network traffic, logs, alerts, statistics, etc.) and storage, as well as tools to manage networks[30].

Observation:

Few scientific programmes and no real cooperation between scientific community and entities responsible for ICS SCADA security in Critical Infrastructure.

4.11 Public-Private Partnership

Public-Private Partnership include cooperation between government entities and various organizations which specializes in delivering of cyber security services (e.g. vendors, consulting companies, private associations). This approach allows for very fast and efficient gathering information about world leading standards and trends.

Poland

The RCB is currently in the process of gathering information on leading standards by cooperation with entities and companies competent in various areas of safety/security. Such collaboration results in the

[29] Interview with RIA (Estonia) on 7 VII 2015

[30] Information provided by INCIBE in OT assessment maturity form, 2015

development of series of handbooks, each focused on different angle of security (e.g. technical safety – already released, cyber security – currently being developed).

4.12 Objectives and restraints

Representatives of entities responsible for the ICS-SCADA security in Member States covered by this study most often listed following goals in this area for the near future:

1. Raising of the awareness about ICS-SCADA security among all stakeholders
2. Building the willingness and mechanisms for effective sharing of information between stakeholders
3. Increasing the quality of ICS-SCADA products on the market from the point of view of security features

The first two goals were listed by countries with a lower level of maturity, which have just or are currently developing a fundament for the ICS-SCADA security improvement (regulations and mechanisms for good practices adaptations). Building of ICS-SCADA security community is believed by representatives of those Member States crucial for obtaining of CI operators understanding of need to increase security of industrial control systems and accepting it. The experience of Member States that have already reached a higher level of maturity prove that this is an appropriate approach.

The third and most popular goal has been quoted by countries which obtained higher scores in the maturity assessment. These Member States have already managed to achieve a high level of trust between ICS-SCADA security stakeholders and usually build up awareness with publications, seminaries, trainings, etc., often developed in cooperation with CI operators. Those Member States believe that they managed to implement organizational measures on a sufficient level – now the main challenge is to provide CI operators with security embedded technical solutions.

The list below includes restraints in the process of ICS-SCADA security improvement which were most often mentioned during the interviews with Member States representatives. All of them create a significant barrier in the improvement of ICS-SCADA security, but examples of achievements from various Member States described in the previous chapters proves, that they can be overcome with a proper approach. The names of corresponding chapters have been included in the brackets.

1. Lack of clearly identified Critical Infrastructure assets and their dependencies (see Assets covered).
2. The willingness to share information (see Information sharing and public/private partnership).
3. Lack of personnel with ICS SCADA security skills (see Education).

5. Recommendations

As a result of this study, six major recommendation were identified, which can significantly increase the level of ICS-SCADA cyber security maturity level across Europe.

All the recommendations are considered necessary to ensure a higher level of maturity in the area of ICS-SCADA cyber security and are in line with the EU vision towards Critical Information Infrastructure Protection. However to ensure unanimity and high effectiveness in realization of these recommendations, an open discussion needs to be initiated including all Member States, CII operators and academia. Moreover a joint effort during the realization phase needs to be ensured to enable a steady growth in the ICS-SCADA cyber security maturity level.

Recommendation 1: Align ICS-SCADA efforts with national cyber security strategies and CIIP efforts

The evolution of the current ICS-SCADA environment, which exposes Critical Infrastructure to more robust cyber threats, impose the need for coherent and planned actions towards higher security level. Current regulations and policies are aimed at a reporting obligation, minimal security requirements compliance or development of CIP plans.

At present ICS-SCADA cyber security is not aligned with National Cyber Security Strategies and CIIP efforts. National Cyber Security Strategies create a baseline for defining cyber space, cyber security objectives and areas of actions. As ICS-SCADA area is an integral part of the National and EU cyberspace and Critical Infrastructures, Governmental decision makers responsible for industrial security/Critical Infrastructure Protection should aligned all these activities with the NCSS as well as CIIP efforts.

Recommendation 2: Develop good practices specific to ICS-SCADA cyber security

Many Member States do not use industry good practices as a reference to set-up ICS-SCADA their cyber security baseline for Critical Sectors. Multiple guidelines, ICS-SCADA security standards and good practices are already developed in the ICS community as well as by individual Member States. It is recommended to leverage from this to develop a minimum security baseline and good practices for ICS-SCADA in Critical Sectors in EU.

This activity should involve relevant Member States agencies, ICS SCADA operators, vendors and standardization bodies. PPP initiatives using current ICS-SCADA forums aimed at ICS-SCADA cyber security guidelines development could be used. The goal should be is to ensure minimum baseline for ICS-SCADA security.

Recommendation 3: Standardize information sharing among critical sectors and Member States

Information sharing on ICS-SCADA cyber security incidents and good practices are not communicated in a standardized and frequent manner. Special emphasis should be given by ICS-SCADA operators and incident handlers in standardizing information sharing of good practices and known threats across critical sectors.

A common approach to report cyber security incidents and good practices should be fostered. For example, relevant Member States authorities and ICS SCADA operators could agree on a specific incident data scheme for ICS response and also incident report. Trust between CII operators and relevant Member States organizations should be built to ensure effective communication from, as well as towards, the operators.

Recommendation 4: Build ICS-SCADA cyber security awareness

A special emphasis should be given relevant Member States authorities on building awareness of ICS-SCADA cyber security aspects not only across CII operators, but also among decision and policy makers. Nowadays awareness is built mainly on serious security breaches and incidents. This however showcase the more reactive approach, which should be moved towards continuous awareness growth.

As a consequence the ICS-SCADA cyber security threats should be well understood and considered separate from IT security. This could be obtained through organizing ICS-SCADA cyber security related events involving sector specific platforms to share current challenges and good practices. Knowledge sharing and awareness building should result directly from the ICS-SCADA cyber security strategies.

Recommendation 5: Foster expertise with ICS-SCADA cyber security trainings and educational programmes.

Current ICS-SCADA cyber security threats multiply at a very rapid pace. Also more robust and technology advanced attacks (e.g. APT) are aimed at ICS systems. Moreover a lot of ICS-SCADA cyber security aspects are considered the same as in IT. This basic misunderstanding very often leads to security flaws in ICS-SCADA environment.

A deep understanding of the process as well as technology is needed in order to perceive the real risk and focus area for improving ICS-SCADA cyber security. This is why it is so important that relevant Member States authorities, operators and vendors of ICS-SCADA systems work together to raise future experts and leaders in the area of ICS-SCADA cyber security. This could be done by setting up and support new study programs for ICS-SCADA security as well as organize and promote related trainings among public bodies.

Recommendation 6: Promote and support ICS-SCADA cyber security research and test beds

Relevant Member States authorities, the European Commission and operators of Critical Infrastructure should encourage research and development programmes for ICS-SCADA cyber security and security test bed focused in ICS environments. The results of these activities will be beneficial for all operators of Critical Infrastructure and could represent a competitive advantage at European level.

The current ICS test bed initiatives in Member States are not mature enough in terms of technical versatility and fluency of work to assume immediate leadership of tasks testing in Europe. It is necessary to involve ICS-SCADA experts and system vendors in the process of addressing current and future cyber security related threats. Support in research programmes and creation of common test-beds can foster ICS-SCADA cyber security innovation and improve security-by-design concept.

Annex A – List of ICS publications

Below the list of a few most worth mentioning publications publicly available in English:

PUBLICATION	PUBLISHED BY	DESCRIPTION
"Cybersecurity for Industrial Control Systems. Classification Method and Key Measures"	ANSSI, France, December 2014	First of two ANSSI documents, without the force of law, used to define the methods for applying the measures set out within the framework of French law No. 2013-1168 of 18 December 2013, known as the Military programmatic law (LPM5).Describes a classification method for industrial control systems and the key measures to improve their cybersecurity.
"Cybersecurity for Industrial Control Systems. Detailed Measures"	ANSSI, France, December 2014	The second of the ANSSI guidebooks. Contains detailed technical and organisational measures to be implemented for ICSs according to the classes defined in the classification guide.[31]
"Guide to Increased Security in Industrial Information and Control Systems"	MSB, Sweden, 2014	The guide dedicated to increase awareness of the need for high security in industrial information and control systems. It include the overview of the role and architecture of ICS-SCADA and propose the list of 17 recommendations for Critical Infrastructure operators to achieve increased level of security.
"Critical Infrastructure Security – the ICT Dimension"	The Kosciuszko Institute, RCB, EY, Poland, 2015	The report contains a collection of articles on ICS-SCADA security in the context of CIP. Although some chapters concern Poland specific conditions, report is a good introduction to the ICS-SCADA issues and challenges for people who are begin to approach the topic.

There are some publications available in national languages only. Their quality was not assessed during this study, however the level of details of those publications suggest, that their eventual translation into English would bring significant profit to the EU society knowledge. These include:

PUBLICATION	PUBLISHED BY	DESCRIPTION
"ICS Security Kompendium"	BSI, Germany, 2014	Includes description of fundamentals on Security of Industrial Control System. Original version was dedicated to ICS-SCADA asset owners and operators. In 2014 a newer, extended version was released which additionally covered area

[31] "Cybersecurity for Industrial Control Systems. Detailed Measures" – ANSSI, 2014

PUBLICATION	PUBLISHED BY	DESCRIPTION
		of interest of ICS-SCADA manufacturers and integrators[32].
Series of Spanish guides of interest related to ICS SCADA cybersecurity	CNPIC/CCN, Spain, 2010	Guides include among others.[33] orientation on how to choose adequate security architecture for the process control systems and support on how to establish the response capabilities related to digital security threats in process control systems.
ICS-SCADA Protection profiles	ANSSI, France, 2015	Protection profiles were prepared for such assets as: PLC, SCADA server, MES server, Engineering software. ANSSI plans to translate profiles to English[34].
"ICS Security Kompendium"	BSI, Germany, 2014	Includes description of fundamentals on Security of Industrial Control System. Original version was dedicated to ICS-SCADA asset owners and operators. In 2014 a newer, extended version was released which additionally covered area of interest of ICS-SCADA manufacturers and integrators.

[32] Presentation prepared for ENISA workshop: "Developments in the CIIP security landscape: German approach", Jens Wiesner, BSI, 2015

[33] www.cnpic.es

[34] Presentation prepared for ENISA workshop: „Developments in the ICS security landscape: France Perspective", ANSSI, 2015

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-02-15-877-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-135-9
DOI: 10.2824/835661