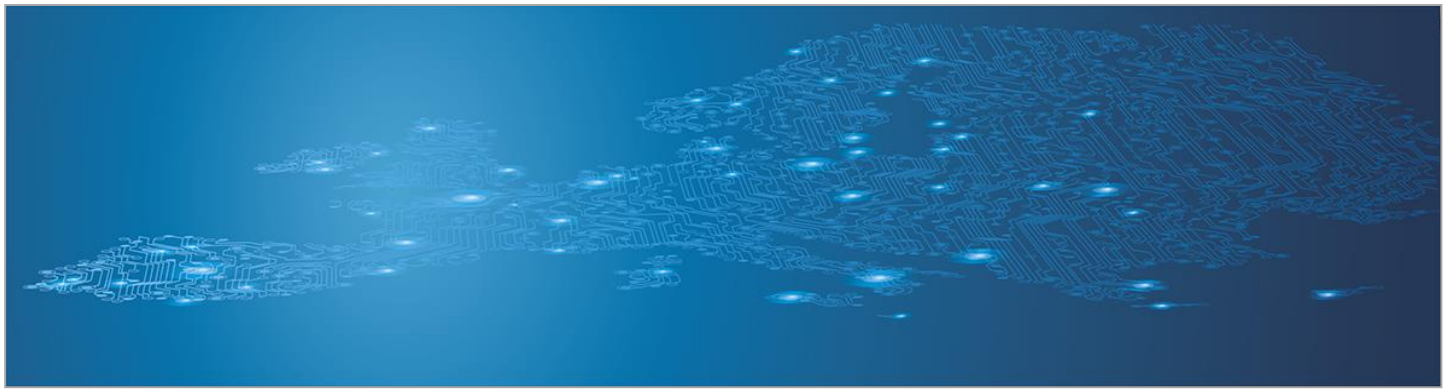

Certification of Cyber Security skills of ICS/SCADA professionals

Good practices and recommendations for developing harmonised certification schemes

December 2014

European Union Agency for Network and Information Security www.enisa.europa.eu

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

- Adrian Pauna (ENISA)

Contributors

- Samuel Linares (CCI)
- Ignacio Paredes (CCI)
- José Valiente (CCI)
- María Pilar Torres Bruna (everis Aeroespacial y Defensa)
- Sara García-Mina Martínez (everis Aeroespacial y Defensa)
- Auke Huistra (Suver)

Contact

For contacting the authors please use resilience@enisa.europa.eu

For media enquires about this paper, please use press@enisa.europa.eu.

Acknowledgements

The consortium would like to acknowledge the contributions of the following experts that agreed to be interviewed during the development of this report:

- Patrick Miller (Archer Energy Solutions)
- Ayman Al-Issa (Booz Allen Hamilton)
- Marc Blackmer (Cisco)
- Robert M. Lee (Dragos Security)
- Fred Streefland (ENCS)
- Matt Bohne (GE Oil & Gas)
- Joel Langill (Infrastructure Defense Security Services)
- Trevor Niblock (IOActive)
- Cristian Camilo Isaza (Isagen)
- Juan David Victoria Morales (Isagen)
- Jim Gilsinn (Kenexis Security)
- Sergiu Lascu (Transgaz)
- Adrian Tudor (Transgaz)
- Catalin Udeanu (Transgaz)
- Matt Bancroft (Wipro)

We would also like to acknowledge the following professionals that have been involved in the reviewing process:

- Bernhard M. Hämmerli (ACRIS)
- Adrian Munteanu (Alexandru Ioan Cuza University)
- Xavier Vila (Altran)
- Joe Weiss (Applied Control Solutions)
- Javier Pages (Arkossa)
- Luis Otero (Arkossa)
- Ingo Jensen (Bayernwerk)
- Geir Mork (Blue Coat Systems)
- Ayman Al-Issa (Booz Allen Hamilton)
- Jens Wiesner (BSI)
- Marc Blackmer (Cisco)
- Hideaki Kobayashi (CSSC)
- James Gannon (Cyber Invasion Ltd.)
- Robert Lee (Dragos Security LLC)
- Alessandro Lazari (EC - JRC)
- Johanna Orjuela (Ecopetrol)
- Annabelle Lee (EPRI)
- Fred Cohen (Fearless security)
- Erick Knapp (Honeywell)
- Tim Harwood (HS and T)
- Marta Inmaculada Oliván Ordás (Indra)
- Joel Langill (Infrastructure Defense Security Services)
- Eireann Leverett (IOActive)
- Dr. Aleksandra Sowa (ISACA)
- Peter Burnett (Meridian Process)

- Jan Tore Sørensen (mnemonic as)
- Simen Sandberg (mnemonic as)
- James Acord (Piemdont Natural Gas)
- Gleb Gritsai (Positive Technologies)
- Sergey Gordeychik (Positive Technologies)
- Dieter Sarrazyn (PwC)
- Doug Wiley (Rockwell Automation)
- Michael Assante (SANS)
- Tony O'Keefe (SANS)
- Derek Harp (SANS)
- Ernie Hayden (Securicon)
- John Dickinson (Sellafield Ltd.)
- Beatriz Martinez Candano (SIGEA)
- Marc Vael (Smals)
- Arkaitz Gamino (Tecnalia)
- Eric Luiijf (TNO)
- Daniel Ehrenreich (Waterfall)
- Jake Brodsky (WSSC)
- Graham Speake (Yokogawa)

ISBN: 978-92-9204-110-6, DOI: 10.2824/53667, Catalogue Number: TP-07-14-040-EN-N

Executive summary

The industrial world is constantly evolving, including new technologies adapting to market requirements. One of the most transcendental adaptations the industrial world is currently experiencing is the convergence between Operations Technology (OT), the operations needed to carry out the industrial processes, and Information Technology (IT), the use of computers to manage data needed by the organisation's enterprise processes. This convergence has many advantages (optimisation of operations, better use of resources, cost savings, etc.), but it also raises additional issues, such as the need for cyber security of industrial control systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems.

This convergence, which affects hundreds of thousands of systems worldwide, implies that professionals with knowledge of cyber security for ICS/SCADA will be needed. However, currently, there are very few professionals with the proven skills available to do this work.

This document explores how current initiatives on certification of professional skills are related to the topic of ICS/SCADA cyber security. It also identifies the challenges and proposes a series of recommendations towards the development of certification schemes for ICS/SCADA cyber security professionals.

Challenges identified in relation to operational issues of certifications included the following:

- The need to handle the confluence of contents, objectives and needs of two very different topics such as cyber security and industrial automation within a number of different industrial sectors (energy, oil & gas, automated manufacturing, water treatment, chemical, pharmaceutical, etc.)
- The complexity of including topics and content relevant to different roles and profiles. In the field of cyber security for ICS/SCADA systems there are implications ranging from the lower operative levels to the top management.
- The challenge to include an important practical component, in future certification contents, able to take into account the nature of the operations performed over industrial control systems. This can be a complicated issue since the operations where ICS are involved, usually need to be executed continuously making it difficult to put them in practice on production systems.

Challenges related to the societal aspects include the following:

- Avoiding commercial interests that could impair the credibility of certifications.
- Obtaining stakeholders' support to underscore the relevance, credibility and strength of future certifications.
- Ensuring that the future certifications will improve compared with existing ones in regards the level of knowledge related to cyber security for ICS/SCADA.
- Exploring the professional roles and specific knowledge needed by cyber security professionals for ICS/SCADA.

Pursuant to interviews with experts worldwide and the analysis of the results of an online survey, this report proposes a series of recommendations for the development of cyber security certifications for ICS/SCADA professionals.

This report concludes that the development of an overarching certification scheme is of paramount importance to allow European professionals to achieve the degree of measured knowledge needed to deal with the cyber security issues in ICS/SCADA systems. This would create a suitable workforce for

European industrial organisations to face the cyber security challenges related to these systems. Certification should be multi-level to allow reaching a wide range of professionals from different fields of practice ; it should include not only operational but managerial topics and it should contain practical aspects, to guarantee that the knowledge of certified professionals is not only theoretical and can be directly applied to industrial operations.

Other proposed recommendations, relevant for both the public and private sectors, with special focus on the European Union institutions, are to:

- Create a steering committee formed by independent experts in charge of evaluation of criteria for reviewing and assessment of current and future certifications.
- Take into account existing certifications to get support of the global community and obtain a critical mass of certificates.
- Develop simulation environments for practical training and testing of skills without effecting production environments.
- Create a framework which defines the main features and contents of future European ICS/SCADA cyber security certification schemes.

Table of Contents

1 Introduction

Events such as Stuxnet[1], Havex[2] or the publication of APT1 report[3] by Mandiant[4] have raised concerns among the general public towards cyber security. Additionally they have matched the growing concern of governments about cyber threats and attacks originating from rogue agents. This has made Critical Infrastructure Protection, the preparedness and response to serious incidents involving critical infrastructures of a nation, a priority for governments worldwide.

The European Union, through the European Programme for Critical Infrastructure Protection[5] (EPCIP) has set the principles and instruments that EU member states need to implement in order to protect their critical infrastructures.

Many of these critical infrastructures belong to industrial sectors that have a deeply rooted concept of security. Industrial security has been mainly focused on physical security as well as in health and environmental safety. Nowadays cyber security has become a new important component of industrial security. This is a novelty for many industrial organizations that is causing different sets of problems for them to achieve the required degree of cyber protection.

Traditionally, the cyber security literature has not taken into account the specific features and needs of Industrial Control Systems (ICS) and Supervisory Control And Data Acquisition (SCADA) systems. These systems are widely used in industries from different sectors (energy, oil & gas, automated manufacturing, water treatment, chemical, pharmaceutical, etc.) to control, monitor and execute operations related to physical processes. ICS/SCADA systems are prone to malfunction when methodologies and tools widely used in IT environments, are run on control networks. The potential impact of this is significant since incorrect operation of these devices can negatively impact the physical environment in which these systems operate.

In a similar manner, industrial automation standards and good practices have not followed developments in cyber security. This has resulted in a vacuum that has increased the risk that many industrial organisations face due to cyber threats.

In terms of political response to these challenges, in March 2013, Jose Manuel Barroso, the then President of the European Commission, presented to the European Council a forecast about digital jobs where he stated that Europe faces up to 900,000 unfilled ICT jobs[6]. In September 2014, the Senate of the United States passed a cyber security skills shortage bill[7] granting the Department of Homeland Security[8] (DHS) the authority to hire qualified experts paying salaries and incentives able to compete with the private sector.

This chronic shortage of digital skills affects all ICT sectors, but it is especially noted in the cyber security for industrial control systems area. One way to tackle this problem would be to make available

[1] Stuxnet was a malware that in 2010 attacked industrial programable logic controllers, specifically those involved in the uranium enrichment process.
[2] Havex is a remote Access Trojan that targets industrial control systems from different vendors. https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-176-02A
[3] Report focused on a cyber espionage campaign apparently sponsored by the Chinese government. http://intelreport.mandiant.com/
[4] http://www.mandiant.com/
[5] http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33260_en.htm
[6] http://europa.eu/rapid/press-release_SPEECH-13-182_en.htm
[7]http://www.govinfosecurity.com/senate-passes-cybersecurity-skills-shortage-bill-a-7340?utm_content=buffer5faec&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer
[8] http://www.dhs.gov/

certification schemes for cyber security of ICS/SCADA professionals. This would allow professionals with a background on cyber security or industrial automation or any other related area, to gain knowledge and develop their skills on cyber security for ICS/SCADA. Proper certification schemes on this topic would generate a pool of skilled professionals, available in the market. This would provide to the European industry a suitable workforce able to deal with the cyber threats effecting industrial control systems.

1.1 Objectives and scope

The objectives of this report are to:

- Analyse current certification schemes and their validity for ICS/SCADA systems for European Members.
- Assess, through an on-line survey and interviews, the need among Member States and the relevant private sector for a voluntary or mandatory scheme for the Certification of Cyber Security Skills of ICS/SCADA experts.
- Identify the main challenges to be covered by Member States and private sector actors involved in developing Certification of Cyber Security Skills of ICS/SCADA expert's schemes.
- Make the necessary recommendations, that cover all the challenges presented, that will allow Member States to develop new and harmonized certification schemes for Cyber Security Skills of ICS/SCADA experts.

This report provides a good practice guide and a set of recommendations to develop ICS/SCADA cyber security certification schemes applicable in the European Union.

1.2 Policy context

According to Article 2(3) of the ENISA regulation[9], the Agency shall assist the European Commission and EU Member States, and in consequence cooperate with the business community, in order to help them meet the requirements of network and information security, thereby ensuring the smooth functioning of the Internal Market. As described in the ENISA regulation, one of the objectives of the Agency is to assist the Union institutions, bodies, offices and agencies in developing policies in network and information security, so, including building expertise related to availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via those networks and systems. For instance, the new ENISA regulation mentions the necessity to analyse current and emerging risks (and their components), stating: "*the Agency, in cooperation with Member States and, as appropriate, with statistical bodies and others, collects relevant information*". In particular, under Article 3, Tasks, d), iii), the new ENISA regulation states that ENISA should enable effective responses to information security risks and threats.

[9] REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL : http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:JOL_2013_165_R_0041_01&qid=1397226946093&from=EN

In its 2014 Work Programme (WP2014)[10], ENISA included the activity related to Certification of Cyber Security Skills of ICS/SCADA experts. Details about this action are laid out in Work Package (WPK) 2.2.

1.3 Target audience

The target audience for this report includes professionals and organisations who desire to get involved in the development of certification schemes of cyber security skills for ICS/SCADA professionals; owners of current certification schemes that could be adapted to include ICS/SCADA cyber security topics; and both public and private bodies and authorities concerned about creating a workforce able to provide the market capabilities to deal with cyber threats over industrial and automation control systems.

1.4 Methodology

To develop this report, the following methodology was followed:

1) **Analysis of current initiatives**: The first phase that led to the current report was the identification and analysis of related initiatives.
2) **The experts' and stakeholders' point of view through an online questionnaire:** the second phase was to obtain experts and stakeholders' opinion. The following figure summarises the flow used for information gathering:

3) **A list of experts from various countries and environments:** emphasis was placed on wide representation from the EU Member States, of which 108 experts from ICS/SCADA organisations were enlisted. From the group of experts, 84 completed the online questionnaire.
4) **Interviews:** the following figure summarises the methodology used to gather experts' point of view:

A panel of 27 experts on ICS/SCADA Cyber Security were interviewed. The interview questions can be found in Annex B

5) The fourth step was to **analyse the results** of the on line survey and of the interviews and identify the professional roles needed in ICS/SCADA Cyber security and the knowledge areas for each role.
6) Finally, a set of **challenges** were identified and described, and a set of **recommendations** have been proposed to solve the identified challenges for the development of cyber security certification schemes for ICS/SCADA professionals in Europe.

[10] ENISA – Work Programme 2014 : https://www.enisa.europa.eu/publications/programmes-reports/work-programme-2014

1.5 Report Structure

The report is structured as follows:

- Chapter 1, “Introduction”
- Chapter 2, “Existing certification schemes”, provides a description of three certification schemes specific to ICS/SCADA systems, of the other four relevant certification schemes for this study and finally, three safety certifications. The end of the chapter also includes an analysis of the results.
- Chapter 3, “Professional roles and knowledge areas needed in ICS/SCADA Cyber Security”, lists the necessary management roles and technical roles in ICS/SCADA systems. It also presents an overview of the necessary areas detailing their content.
- Chapter 4, “Results of analysis”, debriefs the results encountered after analysing the input from the desktop research, the survey and interviews.
- Chapter 5, “Challenges” provides the list of challenges identified during the study and description of them.
- Chapter 6, “Recommendations for a European certification scheme on ICS/SCADA Cyber Security Professionals”, presents the seven recommendations, equally important, to solve the identified challenges for the development of cyber security certification schemes for ICS/SCADA professionals in Europe.
- Chapter 7, “Conclusions”, presents the conclusions of the study.
- Chapter 8, “Glossary”, includes the necessary terminology to understand the study.

2 Existing Certification Schemes

In this section the main points related to the development of certification schemes in the European Union have been summarised.

The objective was to identify helpful aspects for the development of future certification schemes regarding ICS/SCADA cyber security skills.

The following certification schemes have been identified, through desktop research:

- ICS/SCADA Cyber security certification schemes:
  - ISA99/IEC 62443 Cyber Security Certificate Program.[11]
  - Certified ICS/SCADA Security Architect (CSSA)[12]
  - SANS Global Industrial Cyber Security Professional certification (GICSP)[13]
- Other relevant certification schemes:
  - European Computer Driving License (ECDL) / International Computer Driving License (ICDL)[14] / NIS Driving License.
  - National Cyber Security Workforce Framework.[15]
  - Certified Automation Professional (CAP)[16].
  - Industrial Security Professional.[17]
  - Department of Defense Directive 8570 for Information Assurance (DODD 8570)[18].

A detailed description of each of the eight relevant initiatives selected is provided in Annex A: Detailed Analysis of initiatives. Figure 1 maps these different schemes regarding their application to physical security, ICS, and cyber security.

[11] https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/
[12] http://www.iacertification.org/cssa_certified_scada_security_architect.html
[13] http://www.giac.org/certification/global-industrial-cyber-security-professional-gicsp
[14] http://www.ecdl.com/
[15] http://csrc.nist.gov/nice/framework/
[16] https://www.isa.org/isa-certification/certified-automation-professional/
[17] http://www.ncms-isp.org/ISP_Certification/index.asp
[18] http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

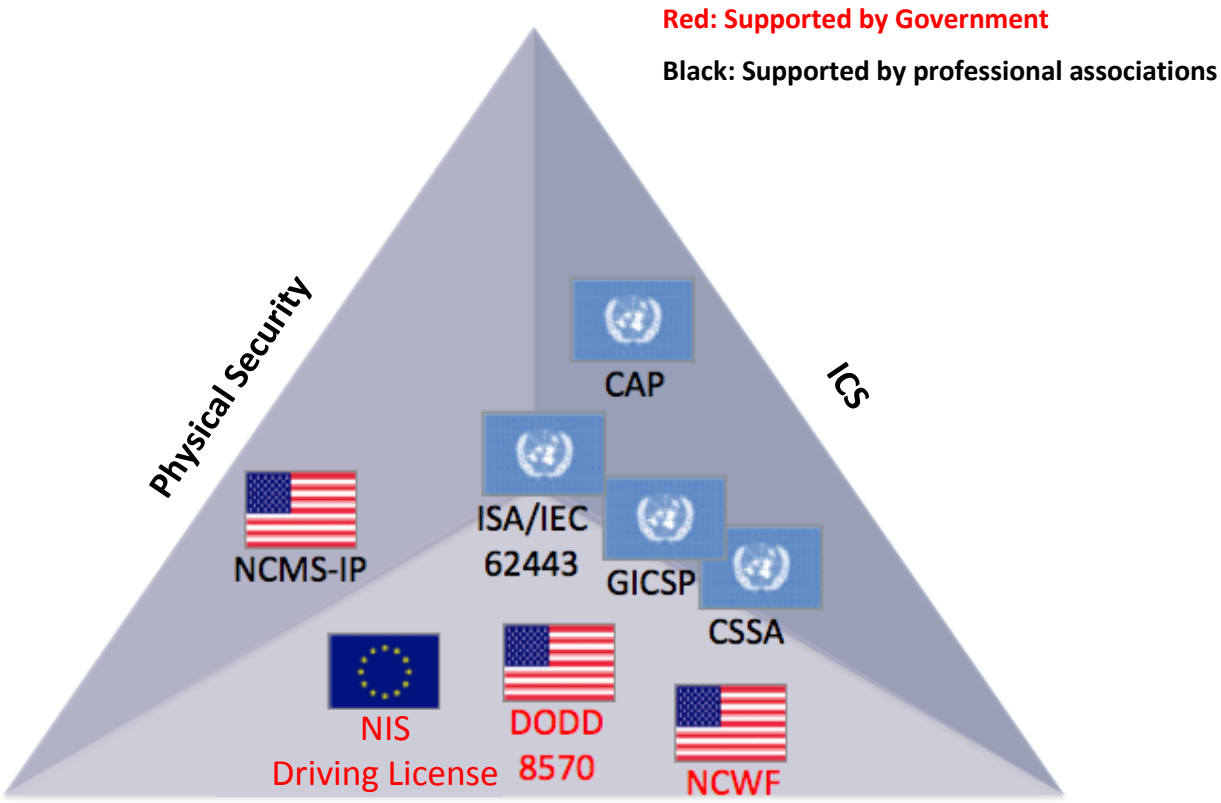

Figure 1 – Relevant schemes

The analysed initiatives can be sorted according to the following features:

- Orientation: The main topics addressed by the analysed initiatives are:
  - Physical security: Industrial sectors have been always deeply committed with physical security, so this is a topic always present in ICS/SCADA related certifications.
  - Industrial Control Systems: Their features, operation and management are major topics in ICS/SCADA initiatives related to certification and/or training.
  - Cyber security: This is a new dimension of security that is starting to play a prominent role in today's industrial systems.
- Support: Who is backing the various initiatives:
  - Governments and public bodies
  - Private sector and professional associations
- Scope: Geographical scope of the certification:
  - Global/International
  - Europe
  - United States

2.1 Certification schemes specific to ICS/SCADA cyber security

2.1.1 ISA 99 / IEC 62443 Cyber Security Certificate Program

ISA 99 / IEC 62443 is focused on cyber security in industrial environments. It is supported by a well-known professional association, the International Society of Automation (ISA), which adds to its

strength and credibility. One of its main features is that standards and documents released by ISA are developed by professionals.

This certification program is a work in progress on cyber security fundamentals targeted towards ICS professionals who wish to enter the field of cyber security. Dealing with topics coming from two very different fields such as cyber security and ICS/SCADA is challenging. Related contents may allow the entrance of professionals coming from both disciplines. This implies having basic knowledge of both domains.

ISA 99 scope is limited to the ISA 99 standards; as such it lacks comprehensive coverage of the ICS/SCADA security landscape.

2.1.2 GIAC[19] Global Industrial Cyber Security Professional (GICSP)

GICSP is part of the GIAC family and it is supported by SANS. It is a global certification that brings together IT, engineering and cyber security to achieve security for industrial control systems from design through to retirement. GICSP is targeted at professionals, worldwide and across industries, who engineer or support control systems and share responsibility for the security of these environments. These professionals can come from different backgrounds, such as Engineering, Cyber Security or IT.

This certification has been developed by GIAC in cooperation with an industry consortium consisting of ICS/SCADA security professionals from industry leaders. One of the key features of the GICSP is that it possesses a steering committee that has guided its development process.

GICSP has been developed under the international standard ANSI/ISO/IEC 17024[20], designed to harmonize the personnel certification process worldwide and create a more cost-effective global standard for workers. ANSI/ISO/IEC 17024, officially entitled "General Requirements for Bodies Operating Certification Systems of Persons," plays a prominent role in facilitating global standardization of the certification community, enhancing consistency, and protecting consumers.

2.1.3 Certified SCADA Security Architect (CSSA)

CSSA is a professional certification from the Information Assurance Certification Review Board, a non-profit organisation formed by information security professionals. CSSA is targeted towards network administrators and their managers, as well as IT professionals and their managers.

CSSA contains the following domains:

- SCADA security policy development
- SCADA security standards and best practices
- Access Control
- SCADA protocol security issues
- Securing field communications
- User authentication and authorization
- Detecting cyber-attacks on SCADA systems
- Vulnerability assessment

The goal of CSSA is to guarantee that certified professionals possess adequate knowledge to properly secure SCADA systems. It is designed to be relevant for power transmission, oil and gas and water

[19] Global Information Assurance Certification is a certification body completely owned/supported by SANS.
[20] http://www.iso.org/iso/news.htm?refid=Ref1625

treatment industries. The most appreciated features of this certification are related to the quality of the training courses, its instructors, and especially to the practical work during the training.

2.2 Other relevant certification schemes

2.2.1 European Computer Driving License (ECDL) / International Computer Driving License (ICDL) / NIS Driving License

The European Computer Driving License (ECDL) and International Computer Driving License (ICDL) are international standards in digital skills certifications. They are part of an initiative and a set of certifications programmes targeted towards the public in general (i.e., individuals, employers, teachers, students).

Despite the ECDL/ICDL not being related to cyber security or ICS/SCADA, they are pan-European efforts that contain valuable features. These can be used as reference in the development of future European certifications on cyber security for ICS/SCADA professionals.

ECDL is made up of a range of modules, providing a practical programme of up-to-date skills and knowledge areas that are validated by a test for each module.

In an area with multidisciplinary knowledge requirements (such as IT, OT, cyber security, etc.) as ICS/SCADA security, a modular approach like the one followed by this programme, seems to be interesting and valuable.

The most appreciated feature of this certification programme is the broad support of key public bodies and governments (such as the European Commission, Member States, UNESCO, etc.). This is a key for the success (but not the only one) and should be a taken into account for any certification that aspires to be widely adopted and required in the industry.

The EU Cyber Security Strategy “An Open, Safe and Secure Cyberspace”[21] proposes the development of a roadmap for a "Network and Information Security driving licence" (NIS Driving License) as a voluntary certification programme to promote enhanced skills and the competence of professionals.

There is a current effort[22], led by ENISA, that has taken its first steps towards producing a roadmap through a consultation process to involve the relevant stakeholders identify gaps between available training, certifications and NIS education needs and propose scenarios to narrow the gaps and provide best practices to organisations from all Member States.

The NIS Driving License develops different scenarios where are described their main features, target audience, involved stakeholders, and are proposed incentives, objectives and means to achieve them.

The current described scenarios are:

- Health care
- Data Protection officers
- Small and Medium Enterprises
- Continuing education for teachers
- Digital forensics

[21] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf
[22] https://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/roadmap-for-nis-education-programmes-in-europe

2.2.2 National Cyber Security Workforce Framework

The National Cyber Security Workforce Framework, as published by the United States National Institute of Standards and Technology (NIST), is seen in the U.S., as a national resource that categorizes, organizes and describes cyber security work. It has been developed by the National Initiative for Cyber Security Education[23] (NICE) in order to provide educators, students, employers, employees, training providers and policy makers with a systematic way to approach cyber security work, and describe what is required of the cyber security workforce. This framework is a thorough approach to describe cyber security workforce related initiatives. It is backed by the United States Government and it is being followed by different federal agencies as such it is becoming a de-facto standard. It is not a certification scheme, but a comprehensive definition of cyber security workforce related contents that should be taken into account in any certification scheme development in order to guarantee a proper definition and scope of contents.

2.2.3 Certified Automation Professional (CAP)

The Certified Automation Professional (CAP) serves as a third party endorsement and documentation of the skills and knowledge for professionals of the automation industry worldwide. CAP is targeted at people working in automation at the professional level, technical supervisors, technical sales personnel as well as automation educators. It does not include cyber security topics. CAP is backed by the International Society of Automation, which makes it to be the most reputable certifications in the industrial automation world. The CAP Certification is widely used by companies to evaluate hiring candidates and making contracting decisions. CAP provides very comprehensive and detailed contents about automation, including security and safety topics; nevertheless cyber security is just slightly addressed in domain IV related to software development, and just from a very general point of view without detailing the specifics of cyber security in Industrial Control Systems.

2.2.4 Industrial Security Professional Certification (NCMS-ISP)

The Industrial Security Professional (ISP) Certification is provided by The Society of Industrial Security Professionals (NCMS). The intent of the ISP designation is to award professional certification and recognition to qualified candidates who demonstrate the knowledge, skills, and abilities their profession demands. It is targeted at qualified candidates who work within the U.S. National Industrial Security Program.

ISP has a strong focus on physical security. Information Security is part of the certification, but ICS/SCADA Security is not.

2.3 Safety Certifications

Traditionally, in the industrial world, most of the effort and resources invested in security were related to safety. Today, due to convergence between operations technology and information technology, cyber security is achieving an importance equal to that of safety among industrial companies and also forced failure of systems via cyber-attacks may have a safety impact. The industrial security market has a number of initiatives related to the training and certification of safety professionals.

The main features of safety certifications are:

- Complexity:
    - Different disciplines such as safety, health, environment protection are involved.

[23] http://csrc.nist.gov/nice/

  - Different environments: emergency management, engineering, ergonomics, fire protection, risk management, occupational safety, etc.

- Multiple levels of certification: allowing safety professionals to achieve professional recognition regardless their education and giving priority to experience.

In this section two of the most relevant initiatives on this field are being outlined. Their features and history could be used as reference in the development of cyber security certifications for ICS/SCADA professionals.

2.3.1 The Board of Certified Safety Professionals

The Board of Certified Safety Professionals[24] (BCSP) began in 1969 as a peer certification board whose objectives are to:

- Set standards for professional, technician, technologist, and supervisory level safety practices.
- Evaluate the academic and professional experience qualifications of certification applicants.
- Administer examinations.
- Issue certificates to candidates who meet BCSP's certification qualifications and successfully pass the examination(s).
- Monitor continued professional development through mandatory recertification requirements.

BCSP maintains multiple certifications and professional programs which amounts to more than 30000 certified individuals:

- CSP: Certified Safety Professional
- OHST: Occupational Health & Safety Technologist
- CHST: Construction Health & Safety Technician
- STS: Safety Trained Supervisor
- CET: Certified Environmental Safety and Health Trainer
- ASP: Associate Safety Professional
- GSP: Graduate Safety Practitioner
- BCSP certified professionals are from countries across the globe however most of them come from the U.S.

2.3.2 The European Network of Safety and Health Professional Organisations

The European Network of Safety and Health Professional Organisations[25] (ENSHPO) brings together health and safety professional organisations from across Europe.

The main objectives of ENSHPO are:

- To ensure participation from all of the professional organisations across Europe and represent the views, opinions and concerns of this group.
- To operate as a dialogue partner with relevant national and international authorities.
- To co-operate with other organisations, institutions, and federations within Europe and beyond.

[24] http://www.bcsp.org/
[25] http://www.enshpo.eu/home

- To primarily act as a forum where practitioners can exchange information, experiences and good practices on a wide variety of pertinent topics.
- To develop a European-wide recognition of Occupational Safety and Health (OSH) practitioner qualifications and training.

The member organisations of ENSHPO have agreed to create two standardised Europe-wide certifications. They allow eligible health and safety practitioners to use the designation EurOSHM (European Occupational Safety and Health Manager) and EurOSHT (European Occupational Safety and Health Technician).

National professional organisations of European countries can present their own certification schemes for standard verification. These schemes are reviewed by the ENSHPO Certification Committee (ECC) for deciding what additional qualifications are necessary to obtain the EurOSHM or EurOSHT title.

2.3.3 Specific training on cyber security for ICS/SCADA

Currently, there is not a wide offer of training specialized in cyber security for ICS/SCADA in the market. Table 1 presents a list of courses available on this topic.

Course	Description	Vendor
Training on Industrial Cybersecurity and Critical Infrastructure Protection (Ciberseguridad Industrial y Protección de Infrastructuras Críticas[26])	Training on industrial cyber security and critical infrastructure protection	CCI- ES
Cyber security course[27]	Industrial control system and smart grid cyber security course	ECNS
Cyber security for Industrial Control Systems[28]	The course contains modules covering many aspects of cyber security for industrial control systems.	ICS-CERT
GICSP Training[29]	Preparation for GICSP certification	Firebrand
Industrial Control (SCADA) systems Cyber Security Awareness[30]	Contents aimed at process operators and production staff that need to know the special features of cyber security in industrial environments.	InfoSecure

[26] https://www.cci-es.org/en/web/cci/detalle-evento/-/journal_content/56/10694/107592
[27] https://education.encs.eu/
[28] https://ics-cert-training.inl.gov/Pages/Catalog/CourseCatalog.aspx
[29] http://www.firebrandtraining.co.uk/courses/giac/gicsp-certification
[30] http://www.infosecuregroup.com/awareness-training/industrial-control-scada-systems-cyber-security-awareness.html

Course	Description	Vendor
Introductie Security van Industriele Controle Systemen [31]	Introduction to security for industrial control systems	TSTC
Operational Security for Control Systems[32]	This training cover standard OPSEC practices, with a focus on the control system environment.	ICS-CERT
SCADA Security[33]	Differences between industrial and business IT, including the difficulties of implementing common security practices on SCADA systems.	Deloitte
Understanding, Assessing and Securing Industrial Control Systems[34]	Course focused entirely on securing or the industrial control system (ICS) architecture.	SCADAHacker

Table 1 – Courses available on cyber security for ICS/SCADA

[31] http://www.tstc.nl/training/242/introductie-security-van-industriele-controle-systemen-scada/
[32] https://ics-cert-training.inl.gov/Pages/Catalog/CourseCatalog.aspx
[33] https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/deloitte-academy/Course%20Overview%20Cyber%20Security%202014%20-%20ENG%20-%20FINAL%20v1.pdf
[34] https://www.scadahacker.com/training.html

3 Professional roles needed and knowledge areas in ICS/SCADA Cyber Security

This chapter outlines, based on existing studies, some of the relevant elements regarding professional roles and knowledge areas that combined will improve the overall security of an organization that uses ICS/SCADA.

3.1 Professional roles needed in ICS/SCADA Cyber Security

To secure ICS/SCADA environments, organisations need to build a capable workforce. Within the Thematic Group 'Industrial Automation & Control Systems (IACS) and Smart Grids[35] of the European Reference Network for Critical Infrastructure Protection[36] (ERNCIP) programme in which a broad range of public and private organisation from across Europe have participated, a high level description of training and certification needs for ICS Cyber Security professionals has been created. It is presented in Table 2:

	Target Audience	Roles	Learning goals	Means / Methods	Test
Skills, Knowledge and Abilities	**Level 4:** People with responsibility for the security in the IACS domain.	CEO, CFOs CIO, CISOs, Auditor, Risk manager, IACS Security Lead.	• How to build a security program. • Risk management and compliance in the IACS domain.	Video Short pitches Risk management modules.	No
	Level 3: People that have a specific security role within the IACS domain – junior, intermediate and senior level.	**Securely provision** (Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development) **Operate & Maintain** (Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security).	TBD	Hands-on training (with Red/Blue team exercises) Hands-on training to develop detailed technical knowledge (small specialist groups) Tailored E-training modules	No
	Level 2: People that have specific roles in developing, implementing, deploying and maintaining IACS.	**Securely provision** (Specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development) **Operate & Maintain** (Specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security).	Role based knowledge of security and how to incorporate this in the daily work.	Tailored E-learning modules Security modules in the education of these people	Yes

[35] https://erncip-project.jrc.ec.europa.eu/networks/tgs/iacs
[36] https://erncip-project.jrc.ec.europa.eu/

	Target Audience	Roles	Learning goals	Means / Methods	Test
Awareness	**Level 1:** All People that have interaction with IACS.	Engineers, vendors, integrators, etc.	Basic understanding of the general Networking and Security Fundamentals on the plant floor as well of all the base practices.	Video Generic E-learning modules.	Yes
	Level 0: All people that enter an operational environment, where IACS is being deployed.	Facility management (cleaning etc.), visitors, etc.	Basic understanding of the risk and threats as well as of the most elementary base practices.	Video Posters Simple tests Etc.	No

Table 2 – Training and certification needs for ICS Cyber Security professionals (ERNCIP)[37]

Within this group the workforce has been divided roughly into two subgroups:

1. **The general workforce** that interacts with and maintains these systems. This group can target general awareness campaigns explaining risks; it also provides simple do's and don'ts.
   - Examples are operators in plants, vendors and integrators of systems, developers of ICS systems.

2. **ICS/SCADA Cyber Security professionals** that have specific accountability or responsibility for ICS/SCADA Cyber Security. This is the group that needs to be trained (and if needed) certified. This group can be divided in groups as well:
   - **Management roles:**
     - ICS/SCADA Security Manager (e.g., responsible person for central team of specialists/Centre of Excellence).
     - Manager in the business with accountability for ICS/SCADA Cyber Security (often line manager, such as engineering manager, plant manager, OT manager, IT Manager, maintenance manager, Integrator of IT and OT environments).
     - Management of process control systems and associated maintenance responsible control system engineers.
   - **Technical roles:**
     - ICS/SCADA focal points in the business
     - ICS/SCADA Security Operations Centre personnel
     - ICS/SCADA (Forensic) Analysts
     - ICS/SCADA Incident Response professionals
     - ICS/SCADA Cyber Security Architects
     - ICS/SCADA Cyber Security Analyst
     - ICS/SCADA Cyber Security R&D personnel
     - Cyber Security professionals in ICS Development organisations
     - ICS/SCADA Cyber Security testers

[37] Created by the ERNCIP Thematic Group Industrial Automated Control Systems and Smart Grids, work stream Workforce Development Framework

3.2 Knowledge areas for ICS/SCADA Cyber Security Professionals

The most important knowledge areas for professionals have been identified taking into account the existing ICS/SCADA Cyber Security Certification schemes and other relevant studies. The following uses as reference the work done under the ERNCIP Thematic Group on IACS and Smart Grids. One of its subgroups has focused on defining the competences, qualifications and experience, needed by ICS Cyber Security Professionals. The result is a high level overview of the knowledge areas that need to be developed (Figure 2):

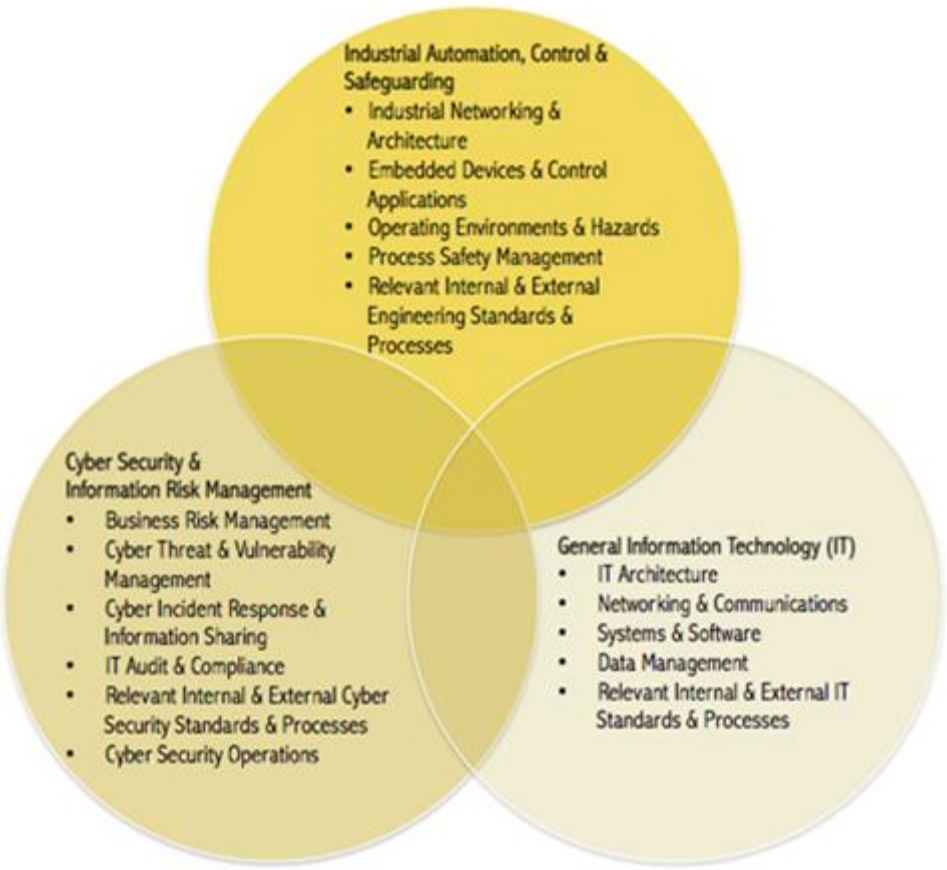

Figure 2 – Knowledge areas[38]

This ERNCIP work has been adopted by the industry consortium developing the list of certification objectives and outcome statements that has been used by GIAC to develop the GICSP certification. This list of knowledge areas is open source material available for all organisations that wish to develop an ICS Cyber Security certification scheme.

[38] Created by the ERNCIP Thematic Group Industrial Automated Control Systems and Smart Grids, work stream Workforce Development Framework

The knowledge areas are presented in Table 3:

Knowledge areas	Content
Industrial Control Systems	• **Basic process control systems** (e.g., RTU, PLC, DCS, SCADA, metering/telemetry, Ethernet I/O, buses, Purdue Model (ISA 95[39])) • **Critical infrastructure subsectors** (e.g., chemical, waste water, drinking water and water quantity management, electricity, oil and gas, manufacturing, transport) • **Safety and protection systems** (e.g., SIS, EMS, leak detection, FGS, BMS, vibration monitoring)
ICS Architecture	• **Communication medium** (e.g., VSAT, RF, cell, microwave) • **Defence in depth** (e.g., layered defines, IDS sensor placement, security system architecture, virtualisation) • **External network communications** (e.g., access points into ICS/SCADA systems, VPNs, vendor/third party access points, mobile devices) • **Field device architecture** (e.g., relays, PLC, switch, process unit) • **Industrial protocols** (e.g., Modbus, Modbus TCP, DNP3, Ethernet/IP, OPC) • **Network protocols** (e.g., DNS, DHCP, TCP/IP, UDP) • **Network segmentation** (e.g., partitioning, segregation, zones and conduits, reference architectures, network devices and services, data diodes, DMZs) • **Wireless security** (e.g., Wi-Fi, wireless sensors, wireless gateways, controllers)
ICS Modules and Elements Hardening	• **Anti-malware implementation, updating, monitoring, and sanitisation** • **Application security** (e.g., OWASP[40], database security) • **Embedded devices** (e.g., PLCs, controllers, RTU, analysers, meters, aggregators, security issues, default configurations, embedded applications (e.g., Windows XP embedded) • **End point protection including user workstations and mobile devices** (e.g., anti-virus, white listing) • **Network security/hardening** (e.g., switch port security) • **Operating System security** (Unix/Linux, Windows, Windows XP embedded, least privilege security, virtualisation) • **Removable media** (e.g., USB device security, optical)media, external drives) • **Persistent memory (hard disks)**

[39] http://www.isa-95.com/subpages/technology/isa-95/isa-95-01.php
[40] https://www.owasp.org/index.php/Main_Page

Knowledge areas	Content
ICS Security Governance and Risk Management	• **Global security standards, practices, and regulations** (e.g., IEC/ISA 62443, NIST 800-82[41], ISO 27000 standards) • **Risk management** (e.g., PHA/HAZOP usage, risk acceptance, risk/mitigation plan) • **Security lifecycle management** (e.g., acquisition and selling of an asset, procurement, commissioning [e.g., secure deployments], maintenance, decommissioning) • **Security policies and procedures development** (e.g., exceptions, exemptions, requirements)
Cyber security Essentials for ICS	• **Attacks and incidents** (e.g., man in the middle, spoofing, social engineering, denial of service, denial of view, data manipulating, session hijacking, foreign software, unauthorized access) • **Availability** (e.g., health and safety, environmental, productivity) • **Cryptographic** (e.g., encryption, digital signatures, certificate management, PKI, public versus private key, hashing, key management, resource constraints) • **Security awareness programs** (e.g., employees / management) • **Security tenets** (e.g., CIA, AIC, non-repudiation, least privilege, separation of duties) • **Threats** (e.g., nation states, cyber criminals, general criminals, inside and outside malicious attackers, hacktivists, inside non-malicious such as errors and omissions)
ICS Security Assessments	• **Device testing** (e.g., communication robustness, fuzzing) • **Penetration testing and exploitation** • **Security assessments** (e.g., risk, criticality, vulnerability, attack surface analysis, supply chain) • **Security tools** (e.g., packet sniffer, port scanner, vulnerability scanner) • **Device testing**
ICS Security Monitoring	• **Archiving** • **Event monitoring and logging** • **Network monitoring and logging** • **Security monitoring and logging**

[41] Guide to ICS security. http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

Knowledge areas	Content
Access Management	• **Access control models** (e.g., MAC, DAC, role-based • **Directory services** (e.g., active directory, LDAP) • **User access management** (e.g., user accounts, service accounts, temporary accounts, default accounts, guest accounts, account expiration, access control list, access reconciliation)
Configuration/Change Management	• **Change management, baselines, equipment connections, and configuration auditing** • **Distribution and installation of patches** • **Software reloads and firmware management, software version management**
Physical Security	• **Physical security**
Disaster Recovery and Business Continuity	• **Site redundancy** (e.g., hotsite, off-site backup) • **System backup** (e.g., security, data sanitisation, disposal, redeploying, testing backups, operational procedures) • **System restoration** (e.g., full, partial, procedures, spares)
Incident Management	• **Incident recognition and triage** (e.g., log analysis/event correlation, anomalous behaviour, intrusion detection, egress monitoring, IPS) • **Incident remediation/recovery** • **Incident response** (e.g., recording/reporting, forensic log analysis, containment, incident response team, root cause analysis, eradication/quarantine)

Table 3 – Knowledge areas and their content

This list embeds all the knowledge areas that were named in the interviews and the survey for this research (see previous chapter). These knowledge areas are the foundation for all the technical ICS/SCADA cyber security roles.

All roles with accountability or responsibility of ICS/SCADA cyber security would need the basic competence across these knowledge areas. Where more specialist roles are defined, for example ICS/SCADA forensic analyst, ICS/SCADA Incident Response professional, more detailed knowledge, skills and abilities on that specific topic will be needed.

4 Results of the analysis

The details of the analysis of the identified related initiatives, together with the results of the online survey and interviews can be consulted in Annex B ***Online survey & Interviews with ICS/SCADA experts***. In this section are presented the most relevant results that allow the further identification of challenges and recommendations for the development of certifications for ICS/SCADA cybersecurity professionals.

Intention towards certification

ICS/SCADA cyber security is important to safeguard the Critical Infrastructures in Europe. It is important to have professionals trained and certified to implement and maintain the right level of ICS/SCADA cyber security controls.

As presented in Figure 3, three quarters of the respondents to the survey are considering getting certified, to prove their cyber security ICS/SCADA knowledge, but just one third have already obtained or are in process of obtaining a cyber security ICS/SCADA related certificate.

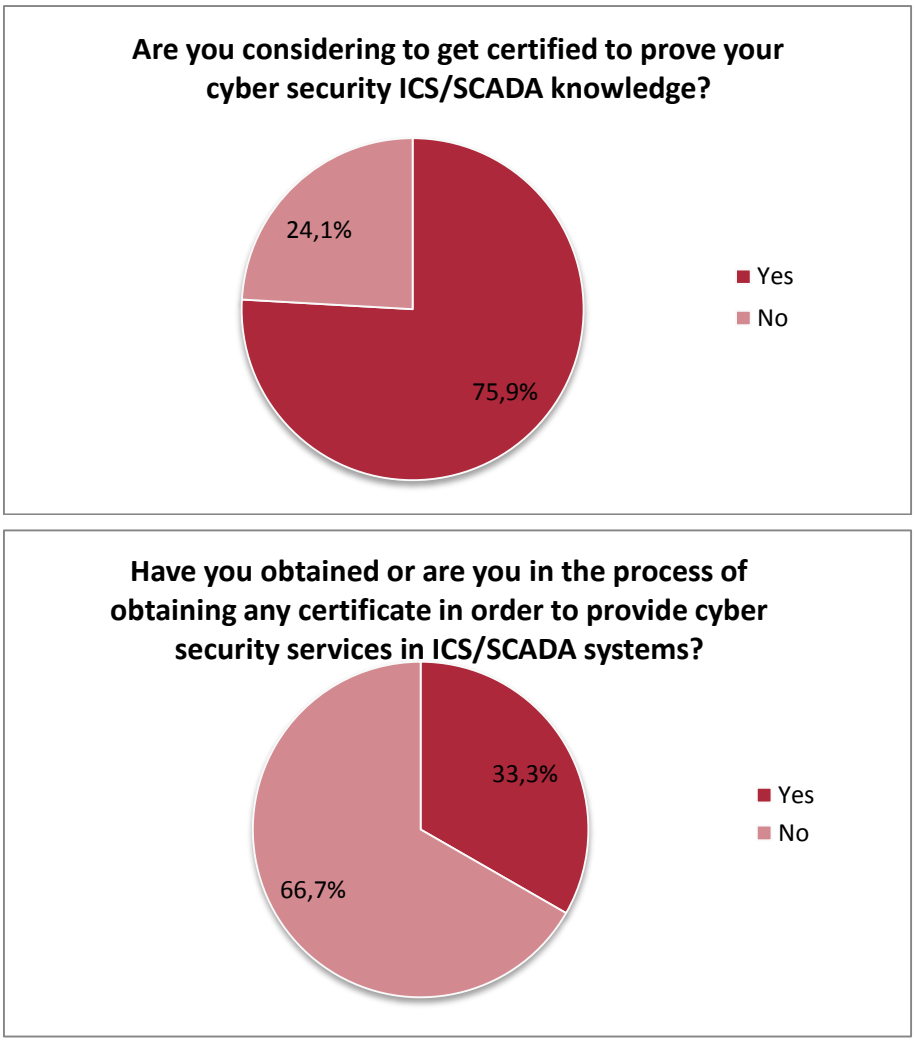

Figure 3 – Survey Results. Intention regarding certification

Approach to building cyber security certification schemes

When asked about the approach to building an ICS/SCADA cyber security certification scheme, most of the professionals consider that new certifications should combine baseline knowledge with specialised certifications focused on different knowledge areas (Figure 4).

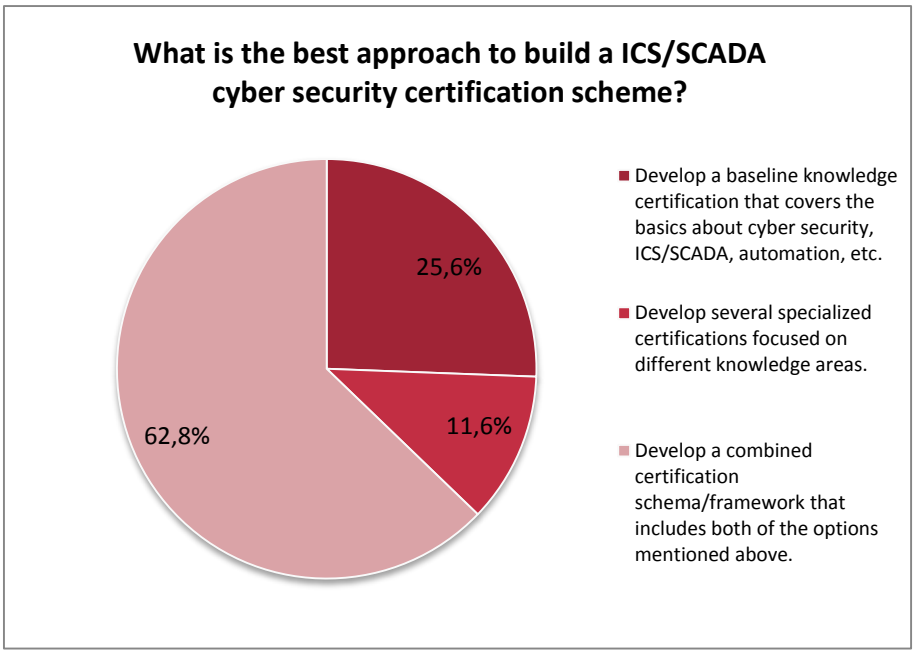

Figure 4 – Survey Results. Approach to build certification schemes

The research has shown that for certain positions it would add value to certify these professionals. There are already a few certifications available in the market, but they are still on a foundational level and there is not yet a complete certification scheme that covers both, the certification of skills and abilities in cyber security for ICS/SCADA professionals. As the community of organisations using ICS/SCADA systems shows a demand for further development of these kinds of certifications, it seems that it is the moment to define a framework to allow the development of ICS/SCADA cyber security certifications that meets or exceeds the needs of all the stakeholders and considers different perspectives in a coherent manner.

Nature of cyber security certification schemes for ICS/SCADA

The research conducted shows that there are open discussions about the nature that cyber security for ICS/SCADA certifications schemes should have. For instance, 51% think that they should be sector specific while 49% think that they should be generic (Figure 5). Also, 85,2% of professionals do not know any position where an ICS/SCADA certification is mandatory.

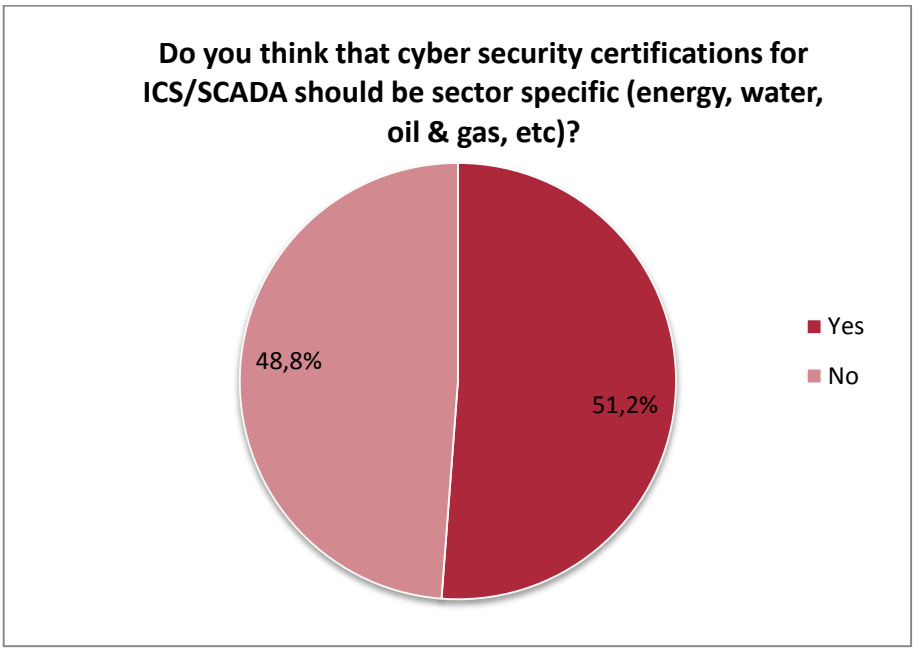

Figure 5 – Survey Results. Generic vs. Specific certifications

Most of the professionals believe that having a panel of recognised experts involved in the creation of the certifications would be very valuable, as presented in Figure 6.

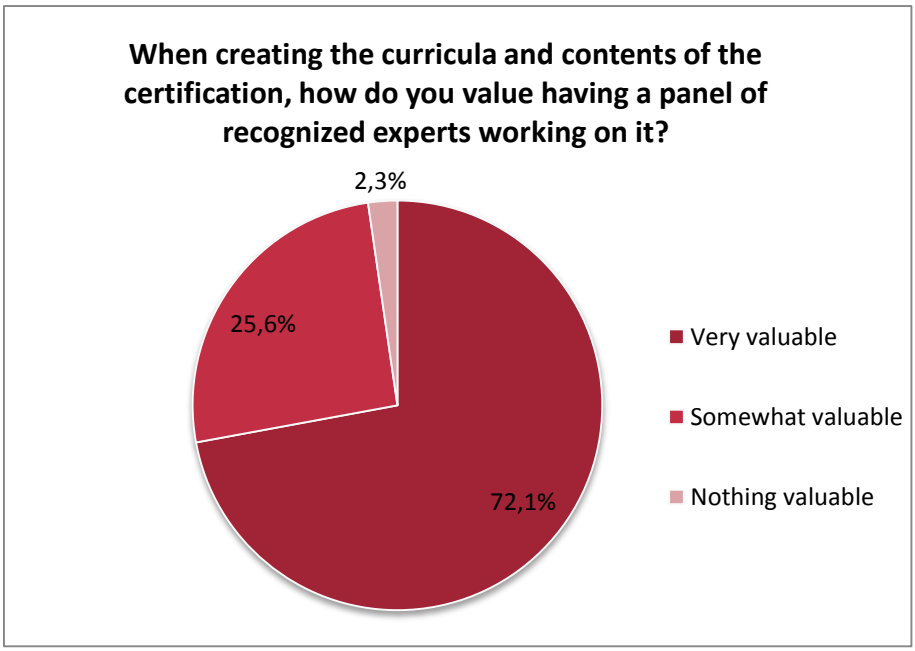

Figure 6 – Survey Results. Involvement of experts

An impartial review/assessment of existing and future certifications could help reach a consensus on these topics.

This should be made through a committee able to validate the quality, impact and applicability of the certification and to ensure that these ICS/SCADA Cyber Security Certification schemes will be supported by the European Commission, EU member states governments, industry bodies, critical infrastructures and all their stakeholders, such as asset owners, suppliers, vendors, integrators,

government and regulators. Such a committee should be credible for the community of experts and professionals in order to earn recognition and support.

Knowledge about existing certifications of ICS/SCADA cyber security professionals

More than 55% of professionals are aware of existing certification schemes, as presented in Figure 7. Besides this, as stated in Section 2, there exist good certification schemes that could prove useful foundation for the development of new certifications.

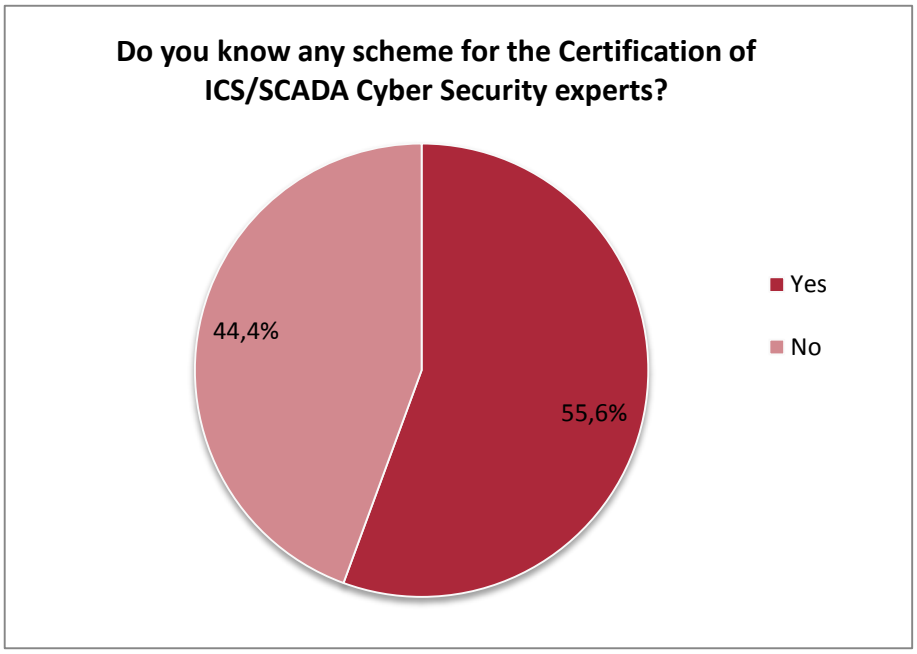

Figure 7 – Survey Results. Knowledge of certification of ICS/SCADA cyber security professionals

There is a small number of ICS/SCADA Cyber Security Certifications available in the market that focus on the foundational knowledge of professionals. The experts interviewed suggested there is a need to build comprehensive European certification schemes on the ICS/SCADA cyber security topic based on existing certifications.

Certification credibility factors

Figure 8 presents the results to the question “What makes a certification credible?”. From the total number, 76,7% of professionals think that practical training makes a certification credible and more valuable.

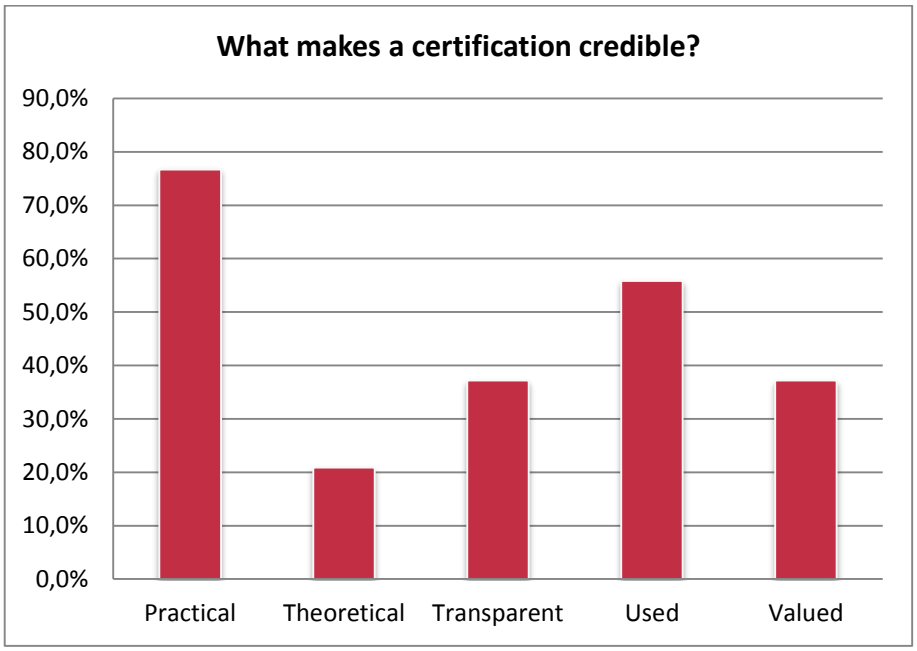

Figure 8 – Survey Results. What makes a certification credible?

Until now, the most relevant certifications available in the ICS/SCADA cyber security community focused on testing the foundational knowledge of professionals, but do not include the testing of practical skills. Given the nature of the operations executed by industrial control systems, it is of importance to include the development and test of practical knowledge skills in future certification schemes.

Practical experience as an integral part of certifications

From the total number presented on Figure 9, 72,1% of professionals think that to demonstrate knowledge and applied principles, the certification should include the demonstration of practical experience.

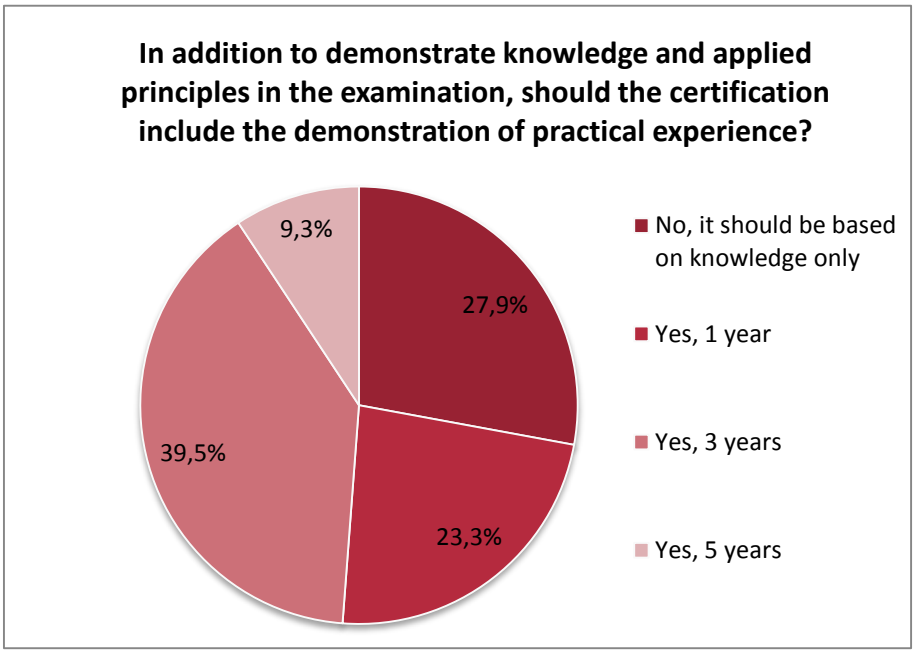

Figure 9 – Survey Results. Demonstration of knowledge and practical experience

When asked about the introduction of practical aspects some of the interviewees introduced the idea of using a simulator, as training in real environments can be impractical. From this point of view, the idea of promoting simulation environments seems good and will probably be supported by the promotion of European Commission of serious gaming technologies.

The nature of operations conducted on industrial control systems requires that the professionals in charge possess practical experience. This is something difficult to achieve and demonstrate through theoretical certifications, so, to include practical work is very important for future ICS/SCADA cyber security certifications for professionals.

Inclusion of management topics in certification schemes

The majority of the interviewed experts recognize the necessity of including management levels in certification schemes, the only opinions against this were related to different sets of priorities, but were still considering it a necessity.

A target group in the ICS/SCADA Cyber Security domain are the people in management positions, senior professionals who oversee activities in this area and need to ensure that in their environments include the right controls in place to mitigate the risk to their organisation to an acceptable level. They also need to be able to explain this to top management in their organisations.

Main features of ICS/SCADA cyber security certification schemes

For European certification schemes to work, it is important to develop content in ways in which such schemes would work. Part of this should be to decide under which premises new certifications will be developed:

- Do we want to create an entity (or select an entity) that develops specific certifications? Or,
- Do we create a certification framework in which organisations that use ICS/SCADA initiatives can be assessed, validated, approved and supported by European agencies or public bodies? This approach could be similar to the way the DODD 8570 framework is operated in the US.

In either case, to keep an adequate level of credibility, validating certifications should be exempt of commercial interests.

5 Challenges

The studies made during the development of this work as well as the interviews carried out and the online survey results have identified some challenges and issues. This section lists the main challenges that should be addressed when developing certification schemes for testing the skills of cyber security ICS/SCADA professionals.

The challenges identified are supported in the answers made by experts in the online questionnaire and during the interviews, and also in perceptions obtained in workshops and conversations with experts combined with the experience of the main authors of this work.

5.1 Obtain stakeholder support

The support of professional associations and organisations is one of the key issues for the success of any certification. The public highly values the involvement of well-known professionals and strong organisations in the development and support of professional certifications. However, 44,3% of professionals involved have not heard about ICS/SCADA certifications.

Raising the relevance, credibility and strength of future certifications related to the cyber security skills of ICS/SCADA professionals will require to engage well-known and respected professionals from the fields of cyber security and industrial operations technology.

Also, obtaining a consensus about contents and target audience will be an important issue since currently there are ongoing major discussions involving important topics such as whether certification must be sector oriented or not.

5.2 Avoid commercial interests

Stakeholders involved in the analysis process expressed their concern that some existing certifications have strong commercial interests, since selling certifications is part of the business model of many certification bodies. This in itself is not a problem, since this budget is also needed to keep the content of the certification up-to-date and provide professional certification environments. It does imply, however, the necessity of an objective validation of the quality of the certification by an impartial body. This would allow checks of the quality of the certifications according to an objective checklist and criteria.

5.3 Manage the confluence ICS/Cyber Security

The contents of certifications on cyber security skills of ICS/SCADA professionals are related to two very different worlds: cyber security and operations technology in industrial environments. The results of the questionnaire and interviews reflect that, besides IT and cyber security contents, all the professionals surveyed would include specific OT knowledge. This would be a challenge since it implies the development and integration of contents coming from very different subjects.

5.4 Cross sector contents

ICS and SCADA systems are used in a number of different industrial sectors. Despite the fact that the underlying technology is common among sectors, and these face similar technical problems, operational processes are different, so addressing the different requirements and necessities of every sector may be difficult.

5.5 Cover the different positions involved in cyber security for ICS/SCADA

The development of contents for future certification schemes should take into account different professional profiles from the functional point of view (e.g., operators, engineers, IT technicians, cyber security personnel, physical security personnel, …) but also from a broader point of view (e.g., managers, section chiefs, field workers, …). This would add complexity to the contents of future certifications since they will have to deal with many different points of view.

5.6 Obtain a critical mass of certificates

As the number of certified professionals increases, a certification scheme becomes more representative in the community. Also the involvement of well-known professionals in the creation of certifications is important because they would serve as role models for their peers.

The more focused a certification scheme is the number of wide range professionals interested in the scheme decreases. Broader differentiation into sub-tier certification levels may be a successful approach. With ICS/SCADA Cyber Security being a growing area of expertise worldwide, this is needed, since it adds value to professionals and the industry.

5.7 Avoid the appearance of too many similar certifications

Industrial cyber security is a topic that will gain prominence in the market place in the coming years, so it is foreseeable that this will be accompanied by a growing a broader interest by IT, OT and operational professionals and therefore a number of organisations will find it appropriate and suitable to support the development of certifications.

A wide number of certifications will scatter possible professionals among all of them. This will complicate the development of relevant certifications that will serve as a reference for the ICS/SCADA cyber security market. This is something that is currently happening with IT or cyber security related certifications, where different organisations, vendors and public bodies propose their own certifications making difficult for any of these to differentiate from the others.

5.8 Adapt existing certifications to include ICS/SCADA cyber security topics

Most of the existing cyber security certifications do not include topics related to ICS/SCADA; additionally industrial certifications do not include cyber security in their curriculum. The adaptation of these certifications to include topics specific to ICS/SCADA cyber security, will boost the general knowledge among the community of professionals and therefore will increase the cyber security of industrial facilities. However, the developers of existing certifications will not be willing to adapt their contents unless there exists a proper pressure from the market.

However, aligning and trying to improve and add content to existing certifications can be a lengthy process. Also working together with other initiatives around the world will take a considerable effort and considerable amounts of communication and meetings to reach alignment.

5.9 Inclusion of practical aspects

Due to the nature of operations made over industrial control systems, future certification schemes should include practical knowledge in the form of hands-on laboratories, simulations or other practical testing methods.

However, it is possible that practical assignments do not reflect thoroughly the daily practice. It is difficult to test all practical skills and abilities for all possible roles, especially in a simulation

environment. This might be the reason to develop a whole set of certifications (with different topics and objectives) focusing on practical skills and abilities for different target groups (e.g., Incident Handling in ICS environments, Ethical hacking in ICS environments, Forensics in ICS environments, etc.).

The development of valid simulators can be a costly effort. This will only be feasible if the simulation environment can also be used for other purposes like component testing, exercises and training.

6 Recommendations for an European certification scheme on ICS/SCADA cyber security

This section presents a series of recommendations aimed to address the identified challenges for the development of cyber security certification schemes for ICS/SCADA professionals In Europe. The recommendations are extracted from the data provided by experts through interviews and the online survey.

The recommendations are related to each other and are considered equally important. Recommendation 1 presents the framework under which the subsequent recommendations should be included and interpreted. The remaining recommendations should be coherent between them and with the common reference of Recommendation 1.

The detailed descriptions of the recommendations contain the following sections:

- **Description**: where the core content of the recommendation is presented. It can be considered as the "what" and the "how" parts of the recommendation. What should be its architecture, how to design and manage it.
- **Challenges addressed:** set of challenges that are addressed by the current recommendation.
- **Good practices**: suggestions to successfully implement the recommendation.

In Recommendation 1 the following sections can be found:

- **Objectives:** what the recommendation aims to address.
- **Steps**: next actions to be executed to achieve the recommendation.
- **Stakeholders affected:** It provides information concerning the stakeholders for whom each the tasks of the recommendations is specially addressed. 'Leading' entities are intended to take initiative and decisions, 'cooperating' ones would have to develop specific tasks including actions or documentation delivery, 'consulting' stakeholders would only be considered for informational aspects.

Recommendation 1: Create an overarching ICS/SCADA cyber security certification scheme for ICS/SCADA cyber security professionals.

Description:

The European Union should promote, fund and support the development of an ICS/SCADA Cyber Security Certification Scheme for the European ICS/SCADA Cyber Security community. This will make it possible to validate and assess current and future certifications in this domain. These certification schemes will also stimulate the market to develop relevant new certifications.

Challenges addressed: 1, 2, 3, 4, 5, 6, 7, 8, 9

Objective:

The good practices and recommendations described in this document have to serve as a reference for the development of such a comprehensive ICS/SCADA cyber security scheme as well for the development of new certifications. It should meet the demand of the ICS/SCADA Cyber Security community. The following points should be considered when building such comprehensive ICS/SCADA Cyber Security Certification scheme:

- Data gathered through the survey and from the interviewed experts suggest that new ICS/SCADA cyber security certifications should be multi-level as this will allow the certification to reach a broader range of professionals (from entry-level to expert) as well as different fields of application. In this way, a multi-level scheme could reflect the difference skill-set that are needed for professionals (e.g., management vs. specialist or generalist vs specialist). Being

able to place certifications on multiple levels allows the inclusion of a wider range of people, including entry level and experienced professionals. An example of these levels could be:

- Foundational level: Where all the basics of ICS/SCADA security are introduced to the students, requiring them to pass a (theoretical) exam that tests the (applied) knowledge of the candidates. This is the entry level. Only professionals that already have some relevant experience should be able to pass this exam. Professionals on the Knowledge level are able to interpret and evaluate information and advice from experts in an area of expertise. They can operate with help of more senior professionals.
- Advanced level: The certifications on this level should contain assignments to test the practical skills of the candidates. This would be interesting for people with either 5-8 years of relevant experience and with the Knowledge level certification passed. The candidates will have to pass a theory and practical exam, with practical assignments in a simulator environment. Professionals on this skill level are able to consistently carry out ICS/SCADA Cyber Security activities.
- Master's level: This level is for experienced professionals on ICS/SCADA Cyber Security in specific roles. They will need more than ten years of relevant experience and will need to have passed the skill level. At this level sector specifications might be considered as well. A theory and practical exam should be passed with corresponding practical exercises performed in the simulation environment. People on a mastery level are thought leaders who are able to diagnose and resolve significant, unusual problems and to successfully adapt all ICS/SCADA cyber security aspects.
- Management level: focused on the skills of managers in this domain. The main objective will be to explain the impact of low security and how a good cyber security strategy supports the general strategy of a corporation.

This separation in levels can also enable the introduction of topics specific to certain industrial sectors, and will reflect the experience, skills and abilities of ICS/SCADA Cyber Security professionals and will offer the possibility to distinguish between professionals.

Steps:

- At the EU level, create, fund and support an initiative to set-up a project to develop this certification scheme, the assessment criteria as well as the set-up of the independent committee (see next recommendation) that will operate the certification scheme.
- Invite the most relevant stakeholders, both public and private, to take part in this effort. Include appropriate knowledgeable representatives from outside the EU.
- After building the certification scheme and the assessment criteria, assess existing foundational ICS/SCADA Cyber Security certifications to see if they meet the criteria and actively stimulate the market to fill in the gaps in the scheme. Do not limit the scheme to European certification initiatives, but also include international certifications in the framework.

Stakeholders affected:

- Security Test Lab Experts: consulting
- Manufacturers and integrators: consulting
- ICS Security tools and services providers: consulting
- Operators: cooperating
- Academia and R&D: leading
- Public bodies: leading
- Standardisation bodies: consulting

Recommendation 2: Create an independent committee that assesses (and endorses) current and future certifications.

Description:

It is recommended to create an independent committee that develops evaluation criteria, reviews and assesses current and future certifications and endorses them when they meet the established criteria. This will give the applicable weight and will maximize the adoption of the certifications by private and public organisations as well as motivate professionals to obtain these certifications. It should be note that, achieving a critical mass of certificates will be a key issue to the success of future certifications.

To achieve this, it will be necessary to identify renowned stakeholders from the industrial cyber security arena including asset owners, suppliers, vendors, technical educators, integrators, government and regulators. People from these stakeholder communities can apply for participation in this independent committee and will be vetted.

Part of the work of this independent committee, in close cooperation with ENISA, could aim at stimulating the market to develop relevant certifications for ICS/SCADA cyber security professionals and to provide guidance on how to develop new uniform certification scheme at EU level.

Having a sound validation process in place will also prevent the proliferation of multiple certifications related to cyber security of ICS/SCADA as this could disperse the efforts made and scatter potential certified professionals among them.

Challenges addressed: 1, 2, 6, 7

Good Practices:

- Create an independent committee with vetted experts (from industry but also with certification development and accreditation as expertise) that will assess and (potentially) endorse ICS/SCADA Cyber Security certifications for professional skills.
- Develop assessment criteria for the assessment of ICS/SCADA cyber security certifications.
- Establish a straight-forward process of cooperation for the committee, with regular meetings and defined short, medium and long-term objectives.
- To involve relevant stakeholders in order improve the credibility of the committee.

Stakeholders affected:

- Security Test Lab Experts: consulting
- Manufacturers and integrators: consulting
- ICS Security tools and services providers: consulting
- Operators: consulting
- Academia and R&D: cooperating
- Public bodies: leading
- Standardisation bodies: cooperating

Recommendation 3: Take into account existing global certifications.

Description:

Use existing ICS/SCADA Cyber Security Certifications as a basis to build European ICS/SCADA Cyber Security certification schemes. This implies working closely together with the providers of existing certifications to ensure that they also cover European specific regulations and legislation.

By adapting existing relevant ICS/SCADA cyber security initiatives to the development of European certification schemes, the effort is likely to gain the support of the global community and multinational organisations. This will also facilitate the creation of a critical mass of certified professionals who will

find it easy to achieve the new certifications if parts of them are based in previous knowledge and experience.

The project groups, leading the effort to build certification schemes, should take an active approach in validating these certifications and work on improving them hand-in-hand with the provider organisations. Also, it will be important to work together with similar initiatives outside Europe to ensure global alignment.

Of course these existing schemes will need to be assessed as soon as the overarching ICS/SCADA cyber security certification scheme is released.

Challenges addressed: 6, 8

Good practices:

- Use comprehensive schemes such as the National Cyber Security Workforce Framework as a basis to define the contents of future certifications.
- Take into account the most relevant initiatives and certifications identified and analysed in Annex A: Detailed Analysis of initiatives to be included in future European certification schemes.
- Evaluate the content of these certifications on their alignment with European legislation and regulations.
- Work together with the providers of these certifications to add relevant European legislation and regulation to the certification objectives and outcome statements of these certifications.

Stakeholders affected:

- Security Test Lab Experts: consulting
- Manufacturers and integrators: consulting
- ICS Security tools and services providers: consulting
- Operators: consulting
- Academia and R&D: consulting
- Public bodies: leading
- Standardisation bodies: consulting

Recommendation 4: Include practical assignments in new certifications.

Description:
The recommendation promotes the inclusion to future certification schemes of several hands-on sessions to test the practical skills of the students. This will be needed to go a step further than testing candidates on the theoretical knowledge level, since knowing how to act against risk and vulnerabilities in ICS/SCADA environments cannot be learned by just studying books.

Future certifications shall include mandatory practical work, where besides taking a theory exam, students would have to complete and pass some practical assignments in a simulation environment.

The objective is to create comprehensive schemes in which certifications are being developed containing practical assignments. The students will need to apply all their theoretical knowledge for ensuring that certified professionals have the right level of skills and abilities to meet real risk situations. This test will assure that they have at least some experience with practical successes where they were able to manage the situation and act to solve the problems.

Challenges addressed: 9

Good practices:

- Take into account real field work requirements to develop an inventory of target groups that need certifications with practical elements included such as calibration of devices, scanning of ICS/SCADA networks or proper isolation of devices.
- To make an inventory of real situations that should be included in the training to finish the certification scheme.
- To involve industrial infrastructures in the inventory definition.
- To propose viable ways to provide practical training taking into account the cyber security and safety aspects of real environments.

Stakeholders affected:

- Security Test Lab Experts: cooperating
- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: cooperating
- Operators: cooperating
- Academia and R&D: consulting
- Public bodies: leading
- Standardisation bodies: consulting

Recommendation 5: Create a simulation environment to test practical skills and abilities.

Description:

For new ICS/SCADA cyber security certifications to contain practical assignments, it is necessary to develop simulation environments to test the students. The same environments could also be used for training purposes.

These environments should be realistic simulations that can be used for the practical part of the certifications where students can develop and demonstrate their practical skills and abilities in, e.g., simulated cyber-attacks.

The environments might be either physical places with physically simulated industrial environments or virtual industrial environments.

Challenges addressed: 9

Good practices:

- The creation of an inventory of such simulation environments available in the European and global market.
- Define the use cases for these simulation environments.
- Align with the European Computer Emergency Response Teams (CERT) and critical sectors to keep the threat catalogue of the simulation environment up-to-date.
- Work towards the creation of test beds, simulation environments and laboratories that allow students to develop and test their practical skills.
- To promote new technologies needed to develop the simulators.
- To promote business models to make viable simulators as a business.
- To promote collaboration between the industrial infrastructures and the potential developers of the simulator.

Stakeholders affected:

- Security Test Lab Experts: consulting
- Manufacturers and integrators: cooperating
- ICS Security tools and services providers: leading
- Operators: consulting

- Academia and R&D: consulting
- Public bodies: leading
- Standardisation bodies: consulting

Recommendation 6: Include Management Certification in the Certification schemes

Description:

As in existing certification schemes such as 'regular' IT Security, a specific management related content would add value. The focus would be more on topics like business impact, regulations, ICS/SCADA Risk Management and Incident Management.

This will ensure that managers of ICS/SCADA Cyber Security organisations or departments are qualified to give clear guidance to the top management of their organisations and to make the right decisions in crisis situations.

Challenges addressed: 5

Good practices:

- Include managerial topics in the contents developed for future certifications.
- Take into account methodologies focused on understanding how ICS/SCADA cyber security supports the strategy and results of the organisation.

Stakeholders affected:

- Security Test Lab Experts: consulting
- Manufacturers and integrators: consulting
- ICS Security tools and services providers: consulting
- Operators: consulting
- Academia and R&D: consulting
- Public bodies: leading
- Standardisation bodies: consulting

Recommendation 7: Define main features and contents of European ICS/SCADA Cyber Security Certification Schemes

Description:

There are multiple ways of implementing an ICS/SCADA Cyber Security Certification Scheme. It is important to make a choice in the approach to take.

For every certification that will be part of the certification scheme it is important to clearly state:

- Define base level of expertise before entering the framework.
- Recommendations about how skills are maintained (Continuing Professional Development (CPD) or forced refreshers)
- What the certification objectives and the outcome statements are.
- How the weighting of these items is in the exam.
- The way the exam is taken (questions / use cases / proctored or not).
- Policies for retaking exams, extensions, recertifying process, etc.

A key issue will be to keep an adequate balance between the cyber security and ICS/SCADA related contents. This will make the certification suitable for professionals coming from both the IT and OT domains.

To make it practical the creation of an ICS/SCADA Cyber Security Certification Framework that provides organisations the opportunity to develop certifications that will be validated and approved by an appointed organisation on the European level, e.g., ENISA is proposed.

Certifications should be developed under strict guidance before being approved and integrated in the European certification framework. Next to the approval of the assigned entity, the certifications should also have ANSI/ISO/IEC 17024 accreditation. This international standard (ANSI/ISO/IEC 17024) was designed to harmonize the personnel certification process worldwide and create a more cost-effective global standard for workers. ANSI/ISO/IEC 17024, officially entitled "General Requirements for Bodies Operating Certification Systems of Persons," plays a prominent role in facilitating global standardization of the certification community, enhancing consistency, and protecting consumers.

Challenges addressed: 2, 3

Good practices:

- First step towards the creation of new certification schemes will be the development of an ICS/SCADA Cyber Security Framework with all the following elements:
  - Framework.
  - Certification process.
  - Appoint entity guiding the process.
- Include balanced contents of cyber security and operations technology on ICS/SCADA systems.
- Setting this up should go hand-in-hand with creation of the workgroup that has to stimulate development of new certifications.

Stakeholders affected:

- Security Test Lab Experts: consulting
- Manufacturers and integrators: consulting
- ICS Security tools and services providers: consulting
- Operators: consulting
- Academia and R&D: cooperating
- Public bodies: leading
- Standardisation bodies: cooperating

Table 4 is a mapping of how the proposed recommendations address the identified challenges.

	Rec 1	Rec 2	Rec 3	Rec 4	Rec 5	Rec 6	Rec 7
Ch 1		✓					
Ch 2		✓					✓
Ch 3							✓
Ch 4	✓						
Ch 5	✓					✓	
Ch 6		✓	✓				
Ch 7		✓					
Ch 8			✓				
Ch 9				✓	✓		

Table 4 – Mapping between challenges and recommendations

7 Conclusions

The general opinion of stakeholders and experts involved in the development of this report is that specialized certifications on cyber security for ICS/SCADA professionals would be advantageous to businesses in various industrial sectors and subsectors across Europe. However it is also noticeable that most of the experts have not heard about many existing certification schemes. This is a trending issue which is starting to gain importance.

The field of cyber security for ICS/SCADA is complex due to its main features:

- The involvement of different disciplines such as cyber security, operations technology and information technology, which implies dealing with different objectives and bodies of knowledge. This also implies dealing with different cultures and attitudes towards security in both the IT and OT domains.
- The broad range of sectors that use industrial control systems (automation, energy, chemical, pharmaceutics, energy, etc.). Despite all of them use similar physical systems, there are important differences in their processes and operational procedures as well as health, safety and environmental consequences due to a failure of a system or component.
- Current certifications focused on related to ICS/SCADA cyber security have a theoretical approach; nevertheless, practical aspects should be included in future certification schemes.

For any initiative to succeed in this complex field, guidance and expertise are needed. It is highly advisable to create a steering committee in charge of assessing future certifications and providing guidance in its development.

ICS/SCADA cyber security is a growing trend that during the upcoming years will have an important presence in the market with many commercial and industrial opportunities. This has the following implications:

- Development and exploitation of certification schemes can be a profitable business, but by no means the main objective of the certifications should be forgotten: improving the skills of professionals on ICS/SCADA cyber security. Everything else is secondary.
- One of the key factors for the success of any certification is the number of certified professionals. The bigger the amount, the more relevance the certification will obtain. Despite the foreseeable growth of the subject of ICS/SCADA cyber security is a very specialised discipline with a relatively low number of professionals involved. This could make it difficult to obtain a critical mass of certificates.

8 Glossary

AIC: Availability, Integrity, and Confidentiality

ASP: Associate Safety Professional

BCSP: Board of Certified Safety Professionals

BMS: Burner Management System

CAP: Certified Automation Professional

CERT: Computer Emergency Response Team

CET: Certified Environmental Safety and Health Trainer

CHST: Construction Health & Safety Technician

CIA: Confidentiality, Integrity, Availability

CPD: Continuing Professional Development

CSP: Certified Safety Professional

CSSA: Certified ICS/SCADA Security Architect

DAC: Discretionary Access Control

DCS: Distributed Control System

DHS: Department of Homeland Security

DMZ: Demilitarized Zone

DNP: Distributed Network Protocol

ECDL: European Computer Driving License

EMS: Emergency Medical System

ENISA: European Union Agency for Network and Information Security

ENSHPO: European Network of Safety and Health Professional Organisations

EOSHM: European Occupational Safety and Health Manager

EOSHT: European Occupational Safety and Health Technician

EPCIP: European Programme for Critical Infrastructure Protection

FGS: Fire and Gas System

GIAC: Global Information Assurance Certification

GICSP: Global Industrial Cyber security Professional

GSP: Graduate Safety Practitioner

HAZOP: Hazard and Operability Study

ICDL: International Computer Driving License

ICS: Industrial Control Systems

ICT: Information and Communication Technologies

IDS: Intrusion Detection System

IP: Internet Protocol

IPS: Intrusion Prevention System

ISA: International Society of Automation

ISP: Industrial Security Professional

IT: Information Technology

LDAP: Lightweight Directory Access Protocol

MAC: Mandatory Access Control

NCMS: The Society of Industrial Security Professionals

NIS: Network and Information Security

OHST: Occupational Health & Safety Technologist

OPC: OLE for Process Control

OSH: Occupational Safety and Health

OT: Operations Technology

OWASP: Open Web Application Security Project

PHA: Process Hazard Analysis

PKI: Public Key Infrastructure

PLC: Programmable Logic Controller

RF: Radio Frequency

RTU: Remote Terminal Unit

SCADA: Supervisory Control and Data Acquisition

SIS: Safety Instrumented System

STS: Safety Trained Supervisor

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

VPN: Virtual Private Network

VSAT: Very Small Aperture Terminal

TP-07-14-040-EN-N

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

ISBN: 978-92-9204-110-6
DOI: 10.2824/53667

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