Certification of Cyber Security Skills of ICS/SCADA Experts

Adrian PAUNA

NIS Expert

adrian.pauna@enisa.europa.eu

Positioning ENISA activities

Recommendations

Policy Implementation

Mobilising Communities

Hands on

EU context

- December 2006 the COM(2006) 786 “on a European Programme for Critical Infrastructure Protection” fixed the main aspects of a European Programme for Critical Infrastructures Protection EPCIP)
- COM(2006) 251, “A strategy for a Secure Information Society – Dialogue, partnership and empowerment”
- COM(2009) 149 on Critical Information Infrastructure Protection.
- COM(2011) 163, summarised the achievements of this plan and defined next steps to be taken. It also recognized that new threats have emerged, mentioning Stuxnet as an example. [none of the activities planned as next steps were specifically targeting Industrial Control Systems.]

EU initiatives

EuroSCSIE - It was formed in June 2005 providing confidentially to share mutually beneficial information regarding electronic security threats, vulnerabilities, incidents, and solutions in the SCADA and Control Systems environment.

EU-US Expert Subgroup - Information sharing, awareness raising, incident response and test bed coordination

European Reference Network for Critical Infrastructure Protection (ERNCIP) - ERNCIP aims at providing a framework within which experimental facilities and laboratories will share knowledge and expertise in order to harmonise test protocols throughout Europe, leading to better protection of critical infrastructures against all types of threats and hazards.

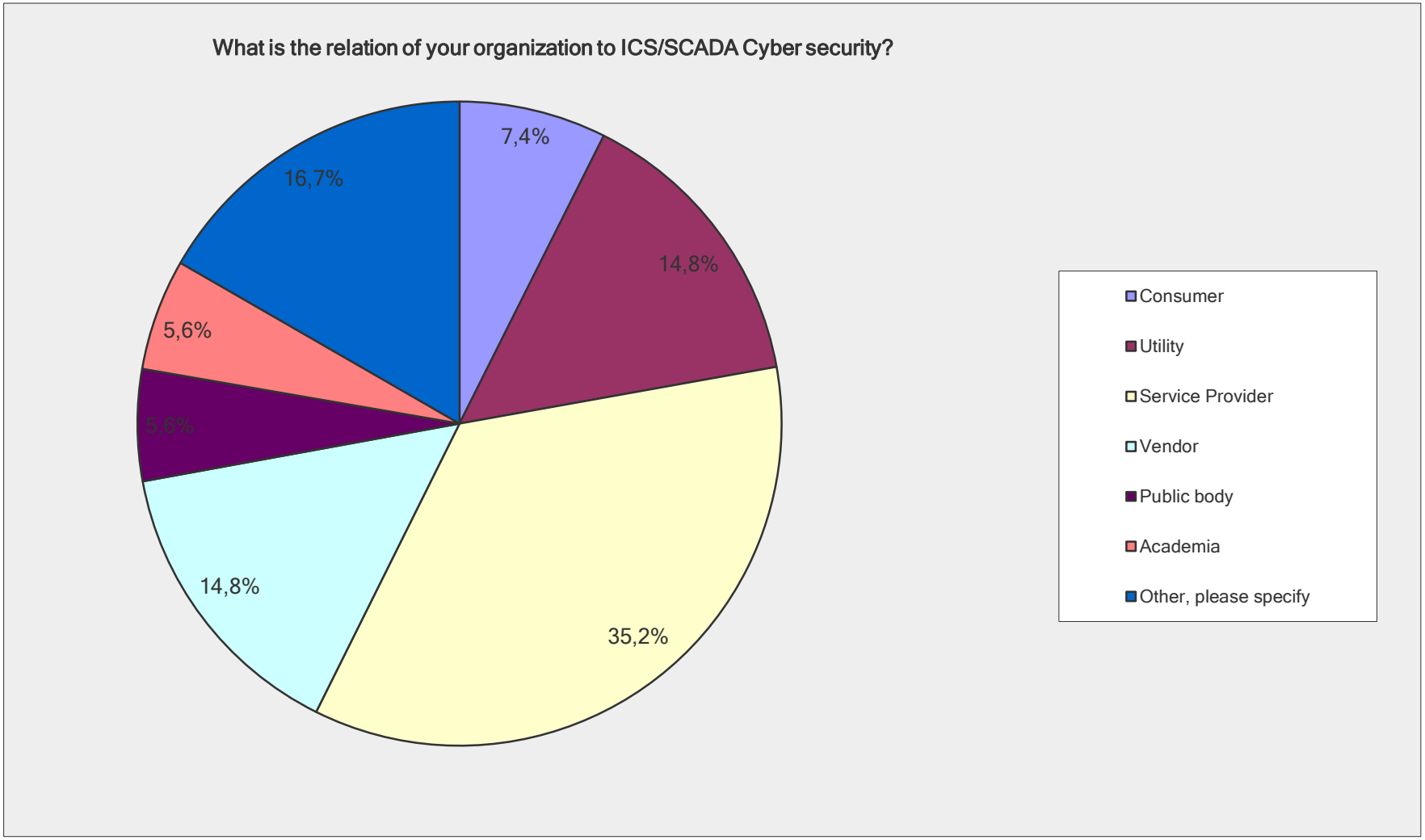
The Project - Objectives

- Assess the need in Europe for a scheme for Certification of Cyber Security Skills of ICS/SCADA experts
- Identify gaps between existing certification schemes
- Produce guidance for the development of new and the harmonization of current certification schemes
- Develop good practice on developing harmonized certification schemes at European level for Cyber Security Skills of ICS/SCADA experts

The Project – Tasks and methodology

- Stock taking of existing certification cyber security skills
  - Identification, analysis and comparison of good practices and frameworks to test ICS-SCADA experts skills
  - Desktop research
  - Online Survey
  - Review by stakeholders
- Challenges, Good practices and Recommendations
  - Analysis of survey data
  - Identification of challenges
  - Report on good practices and recommendations
  - Interviews with experts
  - Review by stakeholders

The Project – The survey



The Project – Interviewed experts

- Mr. Ayman Al-Issa (ADMA-OPCO)
- Mr. Jim Gilsinn (Kenexis Security)
- Mr. Joel Langill (Infrastructure Defense Security Services)
- Mr. Marc Blackmer (Cisco)
- Mr. Patrick Miller (The Anfield Group)
- Mr. Robert M. Lee (U.S. Air Force)
- Mr. Trevor Niblock (IOActive)
- Mr. Fred Streefland (ENCS)
- Mr. Juan David Victoria Morales (Isagen)
- Mr. Cristian Camilo Isaza (Isagen)
- Mr. Matt Bancroft (Wipro)
- Mr. Matt Bohne (GE Oil & Gas)
- Mr. Adrian Tudor (Transgaz)
- Mr. Sergiu Lascu (Transgaz)
- Mr. Catalin Udeanu (Transgaz)

Challenges

1. Obtain stakeholders support
2. Avoid commercial interests
3. Manage the confluence ICS/Cybersecurity
4. Cross sector contents
5. Cover the different positions involved in cybersecurity for ICS/SCADA
6. Obtain a critical mass of certificates
7. Avoid the apparition of a wide number of certifications
8. Adapt existing certifications to include ICS/SCADA cybersecurity topics
9. Inclusion of practical aspects

Challenge 1

- Obtain stakeholders support
  - The public values highly the involvement of professional associations and relevant organizations in the development and support of professional certifications.
  - The engagement of well-known professional individuals from the fields of cybersecurity and industrial operations will serve as a catalyst to the enrollment in the new certifications.
  - The support of public bodies will boost the prestige of future certificaitons.

Challenge 2

- Avoid Commercial Interests
  - The public perceives some certifications as a business model focusing on making money instead of improving knowledge.
  - New certifications should be independent and free of business interests.
  - This does not imply that certifications could not be used in the development of business, i.e. Courses, training facilities.

Challenge 3

- Manage the confluence ICS/Cybersecurity
  - We are dealing with two very different worlds: Cybersecurity and operations technology in industrial environments.
  - For new certifications to be comprehensive the confluence of this two worlds must be managed.
  - They should have basic contents from both sides, allowing the entrance of professionals coming from both worlds.

Challenge 4

- Cross Sector Contents
  - ICS and SCADA systems are used in a number of different industrial sectors.
  - The underlying technology is common among sectors, and these face similar technical problems
  - But operational processes are different, so addressing the different requirements and necessities of every sector can be difficult.

Challenge 5

- Cover different positions
  - The variety of professional profiles related to ICS/SCADA cybersecurity that should be included in the certification can add complexity to the development of suitable contents.
  - The development of contents for the future certification schemes should take into account different professional profiles from the functional point of view (operators, engineers, IT, cyber security, physical security, …) but also from the organic point of view (managers, chiefs, field workers, …).
  - This should include managerial positions since them will be able to enforce the necessity of such certified professionals through their organizations.

Challenge 6

- Obtain a critical mass of certificates
  - A big number of certificated professionals is a key factor to make the certification scheme representative enough.
  - It is difficult to achieve a balance between the certification having a focus on industrial cyber security which is a limiting factor due to the specific and specialized of this topic and the wish to reach out to a broader range of professionals.

Challenge 7

- Avoid the apparition of a wide number of certifications
  - Industrial Cybersecurity will have a big presence in market during the upcoming years.
  - Growing interest of professionals will make organizations to find suitable the development of related certifications.
  - A wide number of certifications will scatter possible professionals among all of them, complicating the apparition of relevant certifications that will serve as a reference for the ICS/SCADA cybersecurity market.

Challenge 8

- Adapt existing certifications to include ICS/SCADA cybersecurity topics
  - Current certifications of cybersecurity doesn't include SCADA topics.
  - Current industrial certifications doesn't include cybersecurity.
  - The adaptation of these certifications to include topics specific to ICS/SCADA cybersecurity, 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 probably not be willing to adapt their contents unless there exist a proper pressure from the market.

Challenge 9

- Inclusion of practical aspects
  - Due the nature of the 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.
  - It is difficult to test all practical skills and abilities for all possible roles.
  - The development of valid simulators can be a costly effort.

Recommendations

1. Create an overarching ICS/SCADA cyber security certification scheme for ICS/SCADA cyber security professionals.
2. Creation of an independent committee that assesses (and endorses) current and future certification.
3. Take into account existing global certification schemes
4. Include practical assignments in new certifications
5. Create a simulation environment to test practical skills and abilities
6. Include Management levels in certification schemes
7. Define main features and contents of European ICS/SCADA cyber security certification schemes

Recommendation 1

- Create an overarching ICS/SCADA cyber security certification scheme for ICS/SCADA cyber security professionals.
  - ICS/SCADA cyber security is important to safeguard the Critical Infrastructures in Europe. This implies having professionals trained and certified to implement and maintain the right level of ICS/SCDA cyber security controls.
  - Certifications on this topic will guarantee that professionals will possess a suitable degree of knowledge and experience on these topics.
  - New certifications will:
    - Be built upon existing ICS/SCADA and cybersecurity certifications.
    - Include practical aspects
    - Be multilevel
    - Include managerial topics

Recommendation 2

- Creation of a community for supporting and endorsing the new certification
  - Most of the professionals believe that having a panel of recognized experts involved in the creation of the certification is very valuable.
  - There are not consensus among the professional community on certain main features of future certifications.
  - An impartial review/assessment of existing and future certifications could help reaching a consensus on this topics.
  - The creation of an independent committee will allow the development of evaluation criteria, reviews and assesses on current and future certifications.
  - This will give the proper weight and will maximize the adoption of the certifications by private and public organizations as well as motivate professionals to obtain these certifications.

Recommendation 3

- Take into account existing global certification schemes
  - Existing certification schemes are well known by professionals.
  - They must be used as a basis to build European ICS/SCADA cybersecurity certification schemes
  - The adaptation of existing relevant ICS/SACADA cyber security initiatives will get support from the global community and facilitate the creation of a critical mass of certified professionals that will find easy to achieve the new certifications if parts of them are based in previous knowledge.
  - For achieving this will be necessary to work together with the providers of existing certifications.

Recommendation 4

- Include practical assignments in new certifications
  - Most of interviewed professionals think that practical training makes a certification credible.
  - Current specialized certifications focus on testing foundational knowledge not including the testing of practical skills.
  - Future certifications should include practical assignments to reflect real field work requirements.
  - This will allow going a step further than testing candidates on the theoretical knowledge level, since knowing how to act against risk and vulnerabilities in ICS/SCADA organizations can't not be learned just studying books.

Recommendation 5

- Create a simulation environment to test practical skills and abilities
  - The nature of operations made 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 it is very important for future certifications on this field to include practical work.
  - The development of simulation environments will be needed for testing and training purposes.
  - This implies the promotion of new technologies for developing the simulations, new business models based on the simulators and collaborations between industrial infrastructures and developers.

Recommendation 6

- Include management levels in certification schemes
  - People in management positions and senior professionals that oversee activities should be target groups of ICS/SCADA cybersecurity certifications.
  - A specific management certification or at least the inclusion of management contents will allow to focus on topics like business impact, regulations, ICS/SCADA Risk Management and Incident Management.

Recommendation 7

- Define main features and contents of European ICS/SCADA cyber security certification schemes
  - Create a Certification framework
  - Validated and approved by an appointed organization on the European level
  - Define
    - Objectives and outcomes of the certification
    - Bodies of knowledge and its weight in the certification
    - The way the exam is taken
    - Retaking and recertifying policies

Thank you for your attention

Follow ENISA: