ENISA – Recent evolution of the CIP and CIIP for SCADA & ICS security.

Adrian PAUNA

NIS Expert

adrian.pauna@enisa.europa.eu

Agenda

- EU context
- 2013's projects
  - Recommendations for Harmonized ICS Testing Capability in the EU
  - Window of Exposure … a real problem for SCADA systems?
  - Good practices for an EU ICS testing coordination capability (cont.)
  - ICS/SCADA certification
- 2014's projects:
  - CERTIFICATION OF CYBER SECURITY SKILLS OF ICS/SCADA EXPERTS
  - ICS SCADA Expert Group

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.]

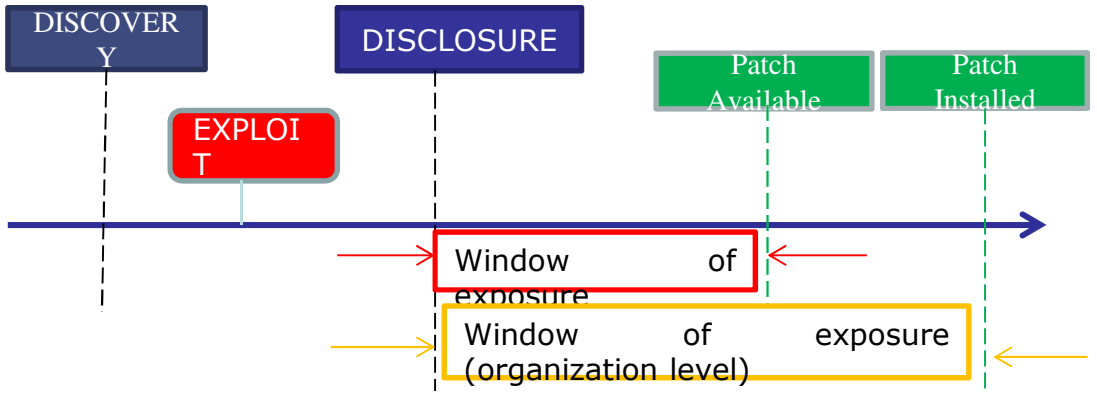
EU initiatives

- **EuroSCSIE** - It was formed in June 2005 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.

Can we learn from SCADA security Incidents? -2013-

- Recommendations for developing a **proactive environment** of an appropriate level of preparedness with respect to ex post incident analysis and learning capability
- ENISA identified several key activities that can contribute to this goal:
  - Facilitating the integration of cyber and physical response processes with a greater understanding of where digital evidence may be found and what would be the appropriate actions to preserve it.
  - Designing and configuring systems in a way that enables digital evidence retention.
  - Complementing the existing skills base with ex post analysis expertise and understanding overlaps between cyber and physical critical incident response teams.

Window of exposure… a real problem for SCADA systems? -2013

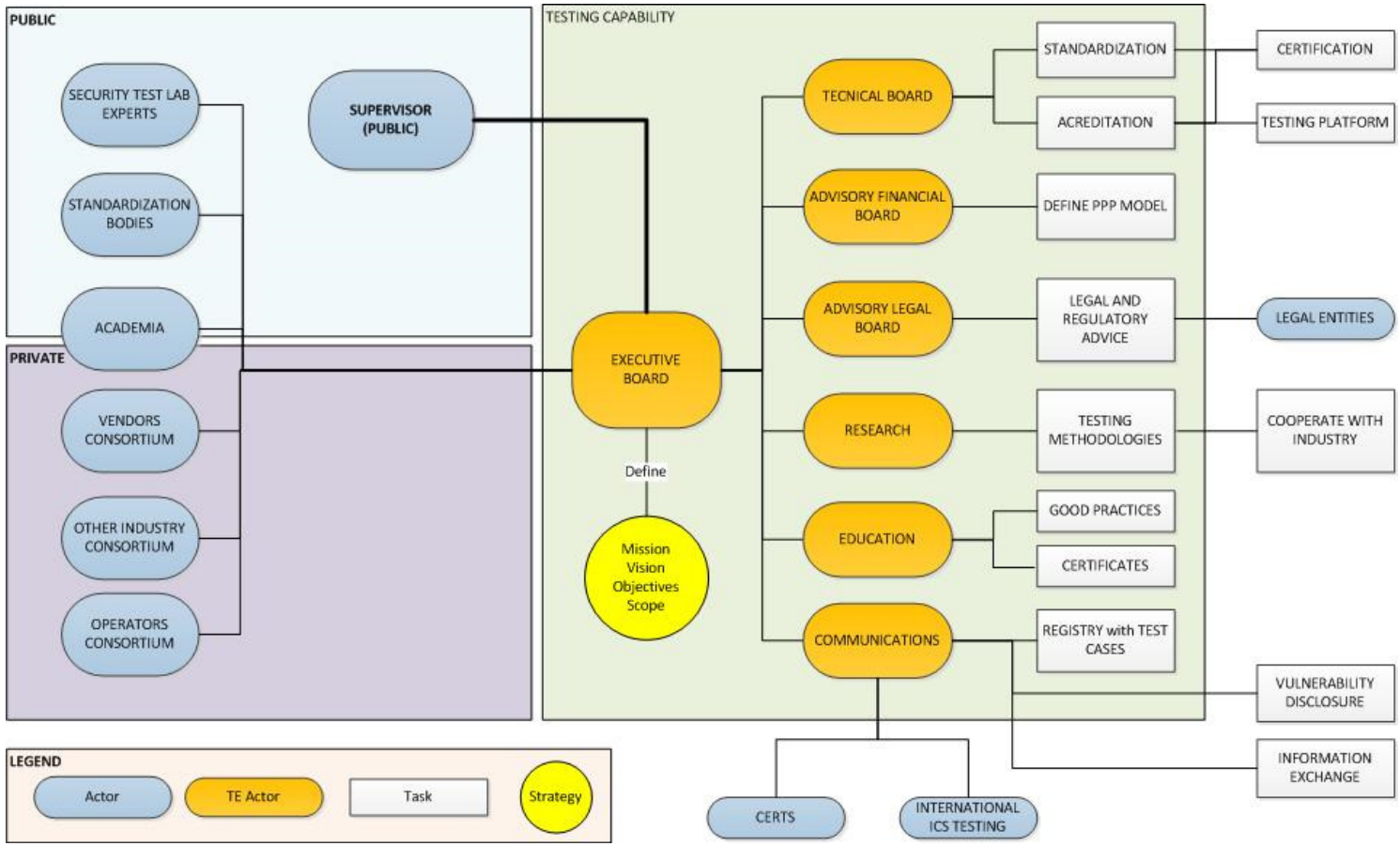


- **EU Member States** could proactively deploy patch management to enhance the security of SCADA systems
- Compensating Controls :
  - Increase in depth defence in depth through network segmentation to create trusted zones that communicate using access controls .
  - Hardening the SCADA systems by removing unnecessary features.
  - Usage of techniques such as Application White Listing and Deep Packet Inspection
- Patch management program and service contract:
  - Asset owners should also establish a patch management service contract to define on the responsibilities of both the vendor and the customer in the patch management process.
  - Asset owners should always conduct their own tests. This can be done virtually or by maintaining separate systems to test on.
  - Certified systems should be re-certified after a patch is applied.

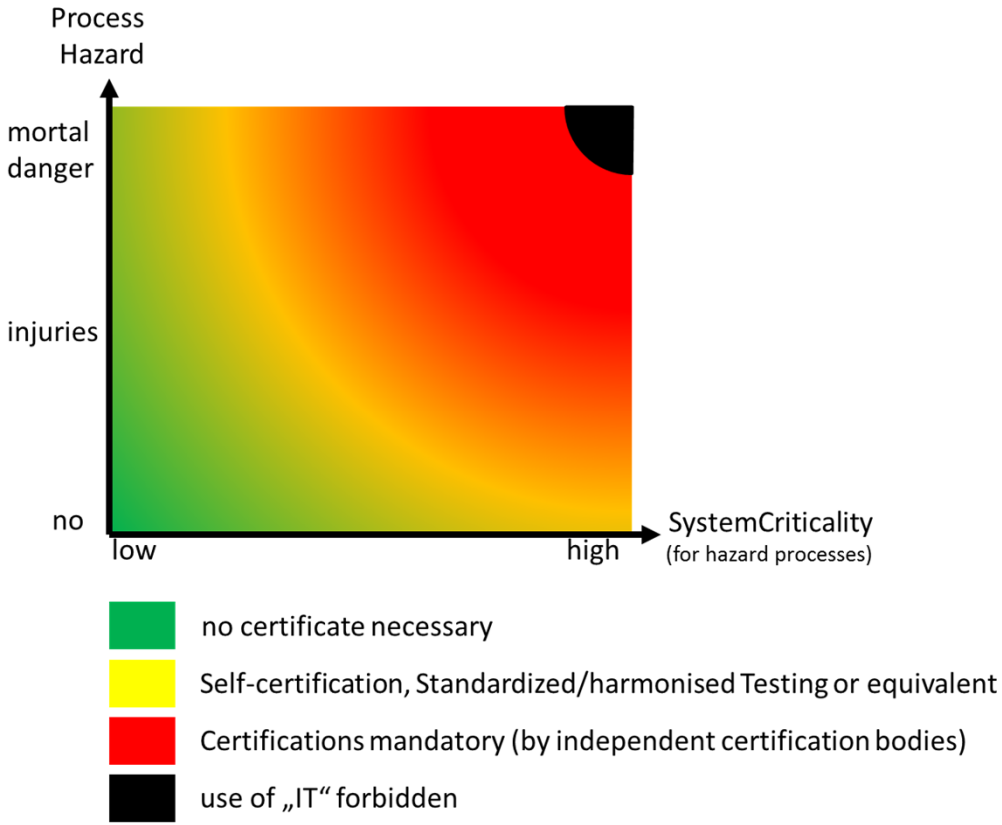
Good Practices for an EU ICS Testing Coordination Capability - 2013

- Explore how the European Union actions can be coordinated so to reach a level of harmonised, independent and trustworthy ICS testing capabilities, leveraging current initiatives
- The methodology included desktop research, an online survey and in-depth interviews with 27 experts from the European Union, the USA, Japan, India and Brazil.
- This research has led to 36 key findings and 7 recommendations, both for the public and private sectors, with special focus on the European Union institutions
- Relevant Recomms:
  - "Recommendation 1: The development of a Testing Coordination Capability under public European leadership "
  - "Recommendation 5: Carrying out a feasibility study for a Distributed Model of Operation "

Overview: 7 Recommendations



ICS/SCADA certification 2013



2013 Internal study - recommendations:

- **Mandatory ICS security certification** may depend primarily on the outcome of the Process Hazard Analysis (PHA)

- **Zone grouping** of Objects for ICS Security Certification
- A **certified system** needs to be designed, engineered, tested commissioned and validated based on specified security requirements within a certified organization

ICS security certification requirements could be prioritized based on the “Damage Extent” of consequences

CERTIFICATION OF CYBER SECURITY SKILLS OF ICS/SCADA EXPERTS
- 2014 -

- OBJECTIVES
  - A voluntary or mandatory scheme for the Certification of Cyber Security Skills of ICS/SCADA experts
  - Base-line skill level requirements for highly technical positions
  - Certification schemes that bring IT, engineering and cyber security professionals together so to achieve security for ICS from design through retirement
  - The need of a European recognized level of competence for ICS SCADA security
- Deliverable
  - Good practices on developing harmonized certification schemes at European level for Cyber Security Skills of ICS/SCADA experts

ICS SCADA Expert Group

- An Expert Group with role of organisation of consultations
- This work concentrates on both technological and organizational security aspects.
- Organize consultations and collect feedback on developing harmonized certification schemes at european level for cyber security skills of ics/scada experts
- Draft recommendations to Member States
- The work of the Expert Group will be supported by electronic means (ie secure portal, mailing list and teleconferences) as appropriate. At regular intervals there will be physical meetings.
- Security experts from national cyber security authorities, energy and ICT industries, and possibly also selected non-EU partners.

Thank you for your attention

Follow ENISA: