AMSTERDAM, OCTOBER 15, 2012

ENISA'S WORK ON ICS AND SMART GRID SECURITY

Dr. Evangelos OUZOUNIS
Head of CIIP & Resilience Unit
ENISA

Why is it important?

- Industrial networks is the CI for the SCADA and the future smart grid
- Key components for the wealth of the society
- Great impact in case of attack
- Increased connectivity to Internet
- New types of attacks (i.e Aurora project, Stuxnet)
- Smart grids will dramatically change the electric grid as we know it today
- Most regulatory/legal texts do not (or not thoroughly) focus on ICS security
- ENISA identified the problem and launched several ICS and smart grid security activities

Studies

- Protecting Industrial Control Systems, Recommendations for Europe and Member States, (Dec 2011).
  - Gaps identified
  - 7 recommendations
- Smart Grid Security, Recommendations for Europe and Member States, (Jul 2012).
  - 90 key findings
  - 10 recommendations
- Minimum Security Requirements for Smart Grids, (to be finished by the end of this year).
  - identify the minimum set of security measures for a more secure smart grid
  - address the different sophistication levels for smart grid implementations

Key Findings (1/2)

- Lack of a standard reference architecture
- Cyber security and privacy addressed independently
- Security addressed more as an overlay than as part of the design phase
- Cyber security – only a second-line issue in ICS-SCADA and smart grid pilots and is tested in massive deployments
- Need for a specific risk assessment methodology
- Lack of a unified and uniform European wide security certification process

Key Findings (2/2)

- Necessary to train and raise awareness among operators, manufacturers and consumers
- Security efforts should not only focus on smart meters but also on substation automation, micro grids, SCADA, telecommunication networks, etc.
- Security initiatives: duplicity of topics, lack of visibility, same experts in all initiatives, …
- Need for a coordinating entity on ICS-SCADA and smart grid cyber security and privacy initiatives
- Need for regulation on incident management
- A European entity for the coordination of large scale cyber security incidents

Recommendations

- Pan-European and National ICS and SG Security Strategies
  - Improve the regulatory and policy framework
  - Synergize with national and international cyber security initiatives

- Foster dissemination, knowledge sharing, awareness raising and training
- Develop a minimum set of reference standards, measures and guidelines
- Promote security certification schemes for products and organisational security in the field
- Foster the creation of test beds and security assessments
- Define and test response and recovery measures and capabilities at corporate and national level
- Foster research in ICS and SG cyber security

Current Work
Minimum Security Measures

- Allying the varying levels of security of operators with a minimum national framework
- Providing an indication of a minimum level of security in the Member States by avoiding the creation of the "weakest link"
- Ensuring a minimum level of harmonisation
- Setting the basis for a minimum auditable framework
- Facilitating the establishment of common preparedness, recovery and response measures
- Contributing to achieve an adequate level of transparency in the internal market

An example

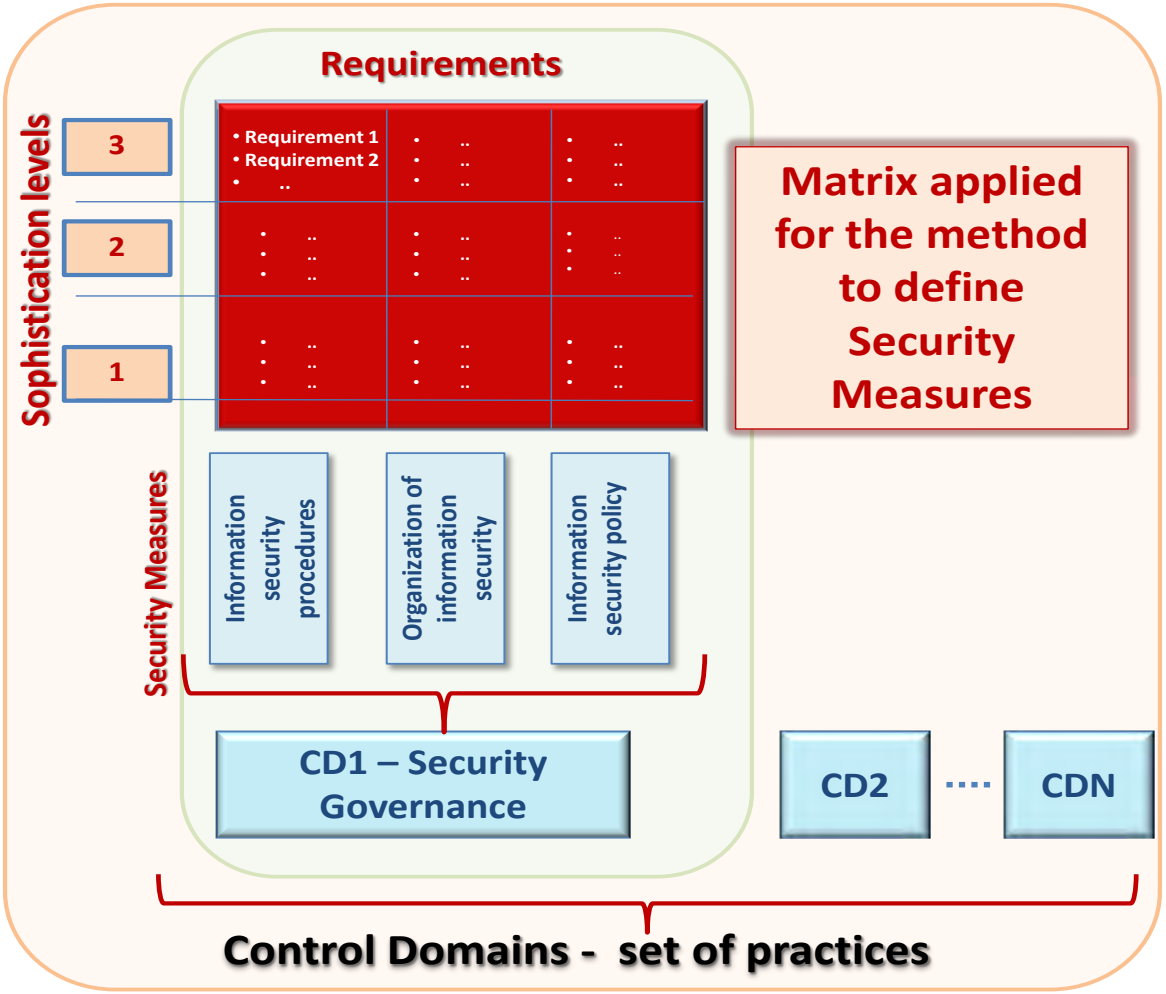
SM 1.1 Information security policy
The provider should establish and maintain an appropriate information security policy.

Level	Requirement	Evidence
1	❖ Key security activities on the smart grid information system are performed by the organisation.	✓ Documented security procedures that address the key security activities.
2	❖ An information security policy that addresses a secure and reliable energy supply and legal and regulatory requirements is available and approved by management. ❖ Employees are aware of the existence and behave accordingly.	✓ Approved information security policy covering most aspects of security containing at least: o Scope of the information security policy; o Applicable laws and regulations; o Security objectives; o Management commitment with the security policy. ✓ Proof of the information security policy communication among staff. ✓ The information security policy is easy accessible for staff.
3	❖ The information security policy is regularly reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.	✓ Last planned review has been done according with the review process. ✓ Records of the management review. ✓ Meeting minutes of review sessions.

Our Approach

- Risk instead of compliance based approach
- Three level approach
  - Risk assessment (by operators)
  - Appropriate measures (baseline)
  - Three levels per each measure (implementation sophistication)
- 10 domains
- 38 measures

Conceptual model



Domains (draft)

- Security governance and risk management
- Third parties management
- Secure lifecycle process for smart grid
- Human resource security
- Incident response and Information sharing
- Audit and accountability
- Continuity of operations
- Physical and environmental security
- Access management
- Network security

Relevant Initiatives

- CEN/CENELEC/ETSI (M490)
  - Common architecture, Security and Privacy issues
- EC Expert Group
  - On the security and resilience of communication networks and information systems for Smart Grids
- EG2
  - Recommendations for data handling, data, security and data protection
- EuroSCSIE
  - European SCADA and Control Systems Information Exchange
- ERNCIP
  - European Reference Network for Critical Infrastructure Protection
- EU-US WG
  - EU-US Working Group on Cyber Security and Cyber Crime

Open Issues

- Smart Grids
  - Governance Model/Regulatory Framework
  - Minimum Security Measures for Providers
  - Incident Reporting for ICS-SCADA/Smart Grids
  - Certification of Smart Grids Components and the role of NCAs
- ICS-SCADA
  - Testing and Patching guidelines for ICS-SCADA
  - Certification of ICS-SCADA cyber security experts
  - ICS-CERT

What's Next ?

- Minimum Security Measures workshop, November 29, Brussels
  - validate with the stakeholders the findings of the study
  - consult with the constituency the key areas of interest
- Participants: national authorities, EU officials, hardware and software manufacturers, energy service providers and standardization bodies from EU
- http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2012/Validation%20Workshop

Thank you!

Contact point: Dr. Konstantinos Moulinos

http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services