ENISA’S WORK ON SMART GRID SECURITY

Dr. Konstantinos MOULINOS

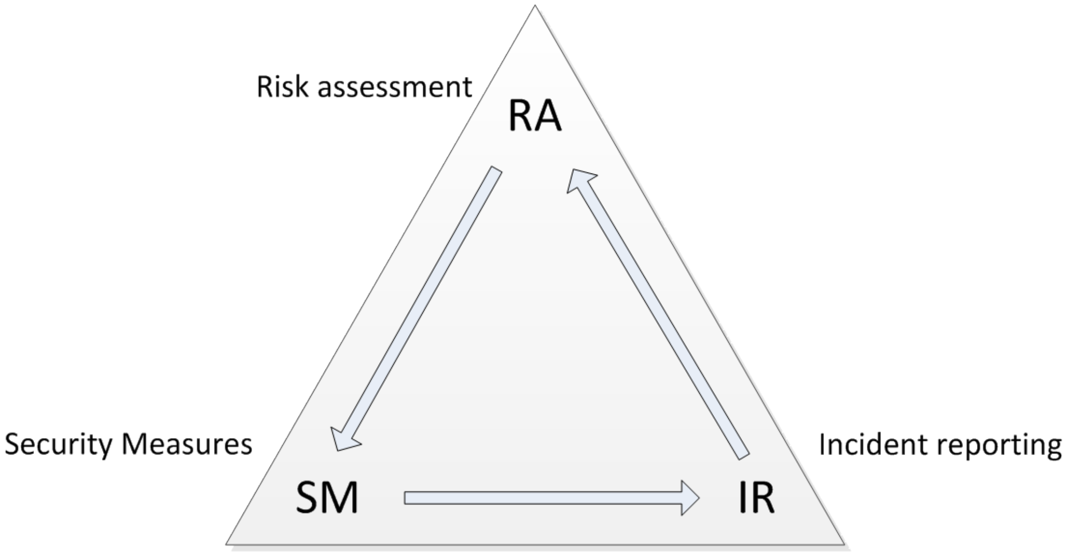
Agenda

- Activities
  - Security measures for smart grids
  - EG2 deliverable on smart grids’ security measures
- Key findings-Challenges
- NLOs role

Activities

- Smart Grid Security, Recommendations for Europe and Member States, (Jul 2012).
  - 90 key findings
  - 10 recommendations
- Workshop on security certification of smart grid components (June 2012).
- Minimum Security Measures for Smart Grids, (Dec 2012).
  - identify the minimum set of security measures for a more secure smart grid
  - address the different sophistication levels for smart grid implementations
- EG2 deliverable on smart grids' minimum security measures (Dec 2013).
- Threat landscape for smart grids (Dec 2013).

Governance


Risk assessment
RA
Security Measures
SM
Incident reporting
IR

Setting a baseline cyber security measures: identifying the need

- 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

enisa
European Network and Information Security Agency

Appropriate security measures for smart grids

Guidelines to assess the sophistication of security measures implementation

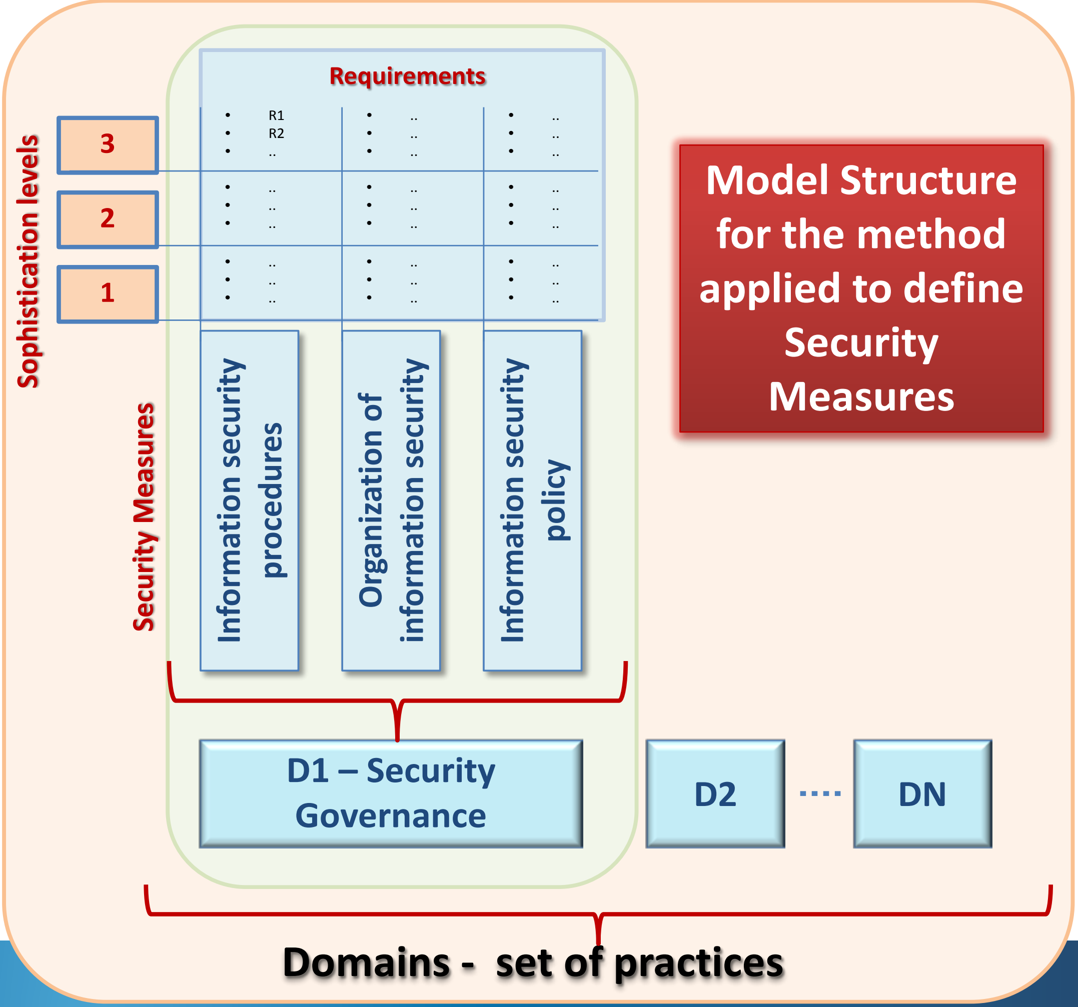
[2012-12-06]

[1] Copyright TenneT

Setting a baseline cyber security measures: the challenge

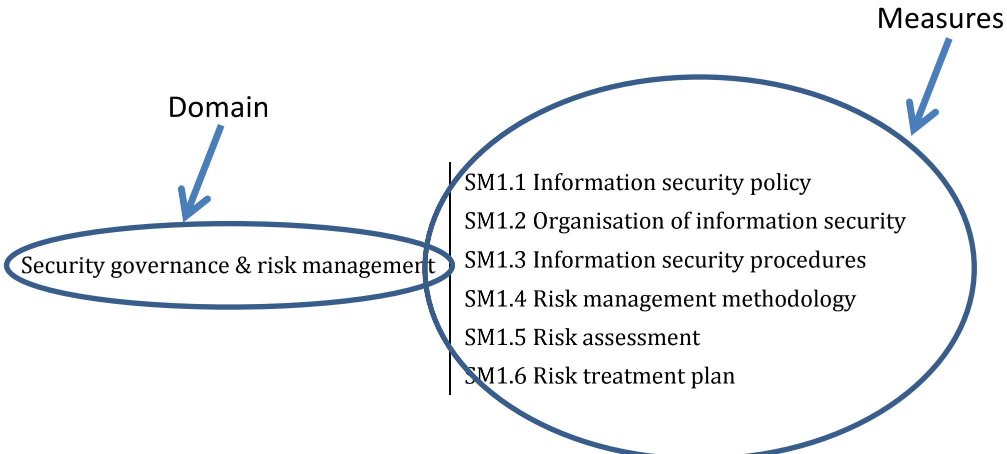
- Not an easy task
- Different stakeholders
  - Bulk generation and ‘bulk’ renewables (e.g. wind mill farmers), Transmission/Distribution system operators, prosumers, vendors, third party providers, legislators, …
- Various sizes of organizations
  - Budgets, business needs, human resources, organizational processes…
- Not a clear view of the market
  - A few real establishments, unclear use case scenarios, vague legal mandate and responsibilities, no factual data on cyber security incidents,…

ENISA's approach

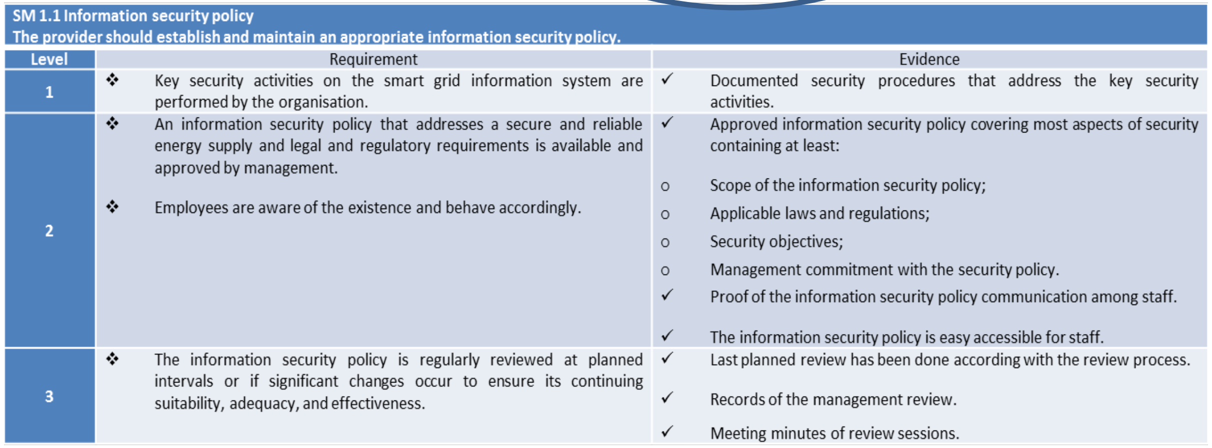

Requirements
R1
R2
Sophistication levels
3
2
1
Security Measures
Information security procedures
Organization of information security
Information security policy
D1 – Security Governance
D2
....
DN
Domains - set of practices

Model Structure for the method applied to define Security Measures

An example



Measures
Domain
Security governance & risk management
SM1.1 Information security policy
SM1.2 Organisation of information security
SM1.3 Information security procedures
SM1.4 Risk management methodology
SM1.5 Risk assessment
SM1.6 Risk treatment plan



SM 1.1 Information security policy

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

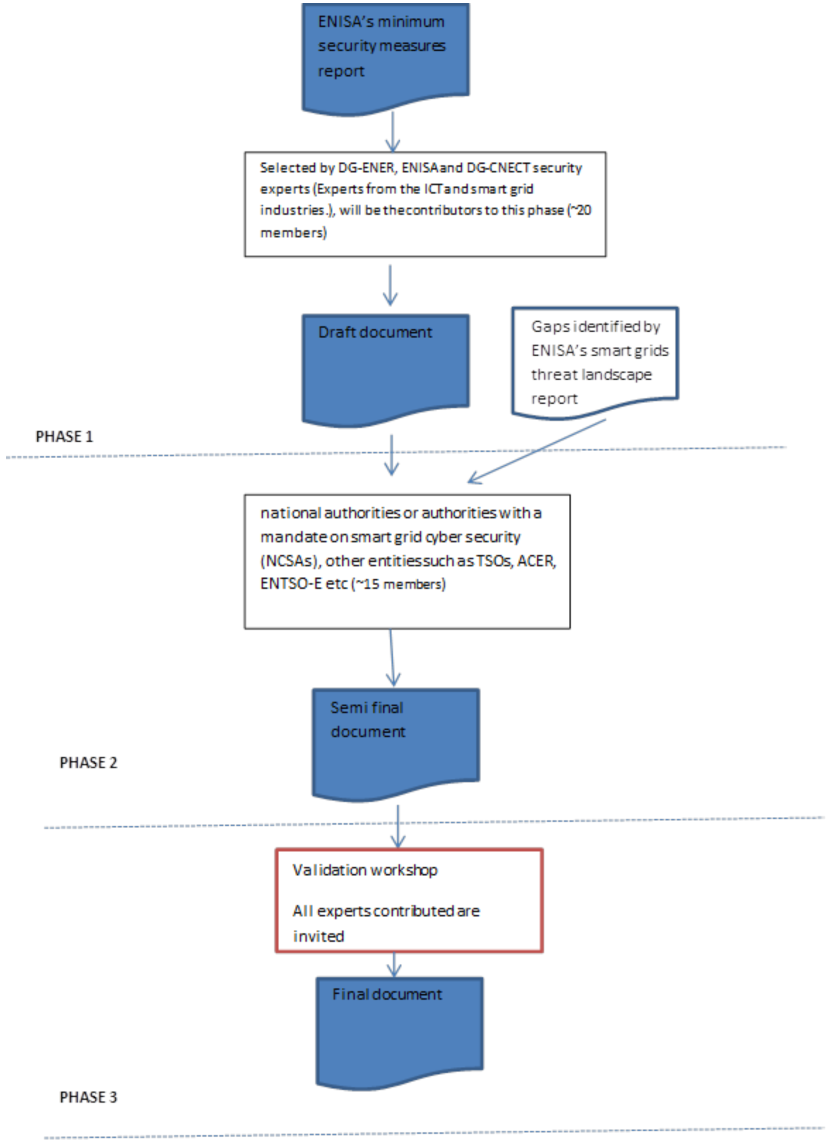
Level	Requirement	Evidence
1	❖ Key security activities on the smart grid information system are performed by the organisation.	✓ Documented security procedures that address the key security activities.
2	❖ An information security policy that addresses a secure and reliable energy supply and legal and 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.

EG2 deliverable: security measures for smart grids

- Objective:
  - organize consultations and collect feedback on these measures from national cyber security authorities, energy and ICT industries, and possibly also selected non-EU partners
  - draft, based upon this process, a document with recommendations to Member States on appropriate cyber security requirements
- Use as a basis ENISA's study on appropriate security measures for smart grids

  https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids
- ENISA, with the support of EC, will chair the process
- EG2 deliverable
- Based on such document, CNECT and ENER will prepare a draft for a Commission Recommendation during 2014

Working Method



ENISA's minimum security measures report

Selected by DG-ENER, ENISA and DG-CNECT security experts (Experts from the ICT and smart grid industries.), will be the contributors to this phase (~20 members)

Draft document

Gaps identified by ENISA's smart grids threat landscape report

PHASE 1

national authorities or authorities with a mandate on smart grid cyber security (NCSAs), other entities such as TSOs, ACER, ENTSO-E etc (~15 members)

Semi final document

PHASE 2

Validation workshop

All experts contributed are invited

Final document

PHASE 3

- Both already existing and new contacts have been facilitated in order to shape the EG
- Each expert has been contacted on an individual basis (email exchanges and private conf calls)
- In order to facilitate its tasks, a private work space at ENISA's portal has been allocated to the expert group
- Interface with EG2 and M/490 SGIS

Domains

- Security governance and risk management
- Management of third parties
- Secure lifecycle process for smart grid components/systems and operating procedures
- Personnel security, awareness and training
- Incident response and Information exchange
- Audit and accountability
- Continuity of operations
- Physical security
- Information systems security
- Network security
- Resilient and robust design of critical core functionalities and infrastructures

What is new to the current document?

- Security measures
  - 42 measures in 11 domains
- A set of Smart Grid assets
- A set of Threats
- How Threats apply to assets
- How security measures protect Threat exposure

Proposed security measures for smart grids

SMART GRID TASK FORCE
EG2 DELIVERABLE

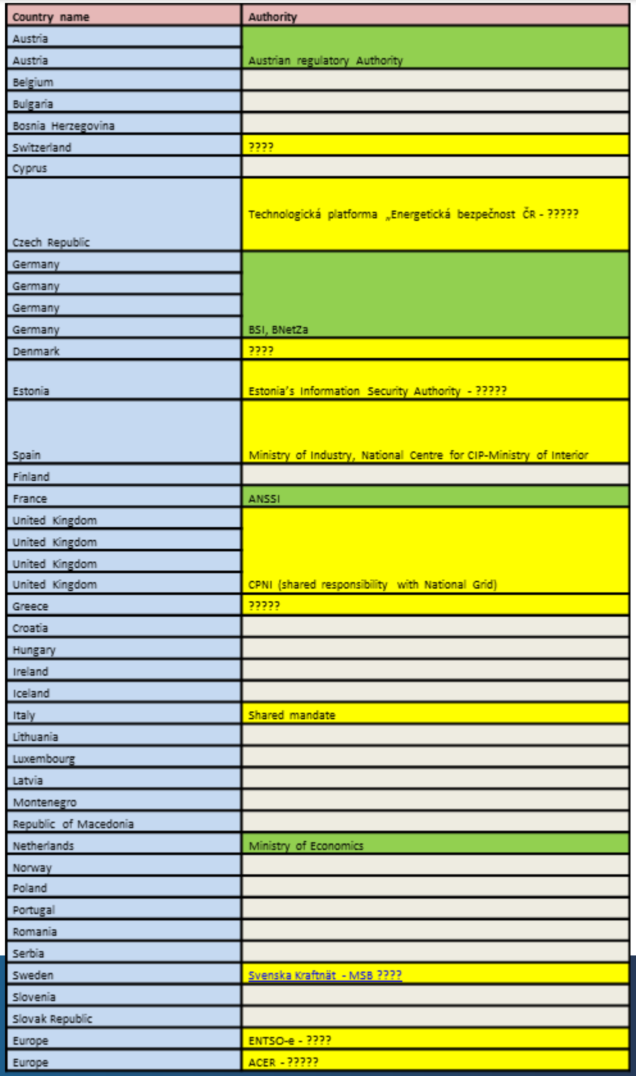
Proposal for a list of security measures for smart grids

Column Break

FINAL

Governance - Mandate

- Shared mandate
- TSOs: not consider it as their problem
- Different types of authorities
- Energy regulators: usually not involved
- Poor participation of Public authorities in EG2



Country name	Authority
Austria	Austrian regulatory Authority
Austria	
Belgium	
Bulgaria	
Bosnia Herzegovina	
Switzerland	????
Cyprus	
Czech Republic	Technologická platforma „Energetická bezpečnost ČR - ?????
Germany	BSI, BNetZa
Germany	
Germany	
Germany	
Denmark	????
Estonia	Estonia's Information Security Authority - ?????
Spain	Ministry of Industry, National Centre for CIP-Ministry of Interior
Finland	
France	ANSSI
United Kingdom	CPNI (shared responsibility with National Grid)
United Kingdom	
United Kingdom	
United Kingdom	
Greece	?????
Croatia	
Hungary	
Ireland	
Iceland	
Italy	Shared mandate
Lithuania	
Luxembourg	
Latvia	
Montenegro	
Republic of Macedonia	
Netherlands	Ministry of Economics
Norway	
Poland	
Portugal	
Romania	
Serbia	
Sweden	Svenska Kraftnät - MSB ????
Slovenia	
Slovak Republic	
Europe	ENTSO-e - ????
Europe	ACER - ?????

The role of NLOs

- This year ENISA will take stock on the SG cyber security mandate in MS
  - Responsible authority
  - Relevant regulatory framework in place
  - National Information sharing platforms
  - ……
- NLOs assist in stock taking
  - Identify who has the mandate in each MS
    - Public authorities, Energy regulators, TSOs etc
  - Provide ENISA with contact details

Thank you!