27 March 2012

High Level Risk Assessment methodology for relevant assets

Expert Group on the security and resilience of communication networks and information systems for Smart Grids

Work Package 1.4

DRAFT 0.9

Team members

The Team consists of the following members:

- Sandro Bologna, Italy, Associazione Italiana Infrastrutture Critiche.
- Himanshu Khurana, U.S.A., Honeywell.
- Zoltan Precsenyi, Belgium, Symantec.
- Johan Rambi, Netherlands, Alliander.
- Hani Banayoti, Atos.
- Ralph Eckmaier, Austria

Mission, vision and goals

In consistency with the overall mission of the Expert Group, this Team's objective is to support market operators with guidance and recommendations for selecting and implementing an appropriate risk assessment methodology and giving guidance for selecting appropriate information security controls deployable within the Smart Grid infrastructures within the European Union.

Strategy

The Team will seek relevant materials already developed in the fields covered by the scope below, assess their applicability and relevance within the context of the Smart Grid, extract and combine valuable contents, point towards appropriate external references, identify possible gaps in existing documents and suggest further directions for research and development as appropriate.

Scope

The overall scope of the work of the Expert Group is the security and resilience of communication and information systems that determine the performance of the physical electricity infrastructure. More in particular, this Team focuses on proposing a high level methodology for Smart Grid risk assessment, and suggesting adequate security requirements in consequence.

Statement of Work

Electricity is an essential infrastructure necessary to enable and support all knowledge- and innovation-based economies. The 12.2 trillion euro economy[1] of the member states of the European Union depends on the reliable and continuous availability of electricity. From a European perspective, especially in the aftermath of the recent tragic natural disaster in Japan and major power outages within the US, increased national and transnational concerns about the security, resilience and robustness of critical infrastructures, in particular the Smart Grid, are evolving, especially because of an increasing and diversifying spectrum of possible threats. Secure and reliable operation of these power networks is fundamental to the European economy, societal security and quality of life for its citizens.

1.4.1 Develop a high-level security risk assessment methodology for relevant assets

***Objective**: Policy issues will include (but not limited to): objectives of risk analysis, enumeration of levels at which stakeholders should conduct risk analysis, process for prioritising risks, and phases and stages for risk mitigation.*

With clear threat profiles taxonomies (see 2.1.1. and 2.1.2.), a general risk assessment methodology for Smart Grids should be developed to aid in taking complete and effective measures against the risk encountered.

***Requirements**: The risk assessment methodology should cater for a continuous improvement rather than seeing security as an absolute. The typical stages of an in-depth security approach (prevent, detect, defend and recover) could be used as a model.*

Moreover, the traditional landscape (SCADA/DCS) of where we find control systems and meters is evolving also to other devices which calls for an end to end security perspective. This is also to be included in the threat landscape and also brings identity and access management to the forefront of a secure system design.

To complement the high level threat analysis and risk assessment other technologies are in scope, such as reputation and intrusion detection techniques, that can allow to pick up abnormal data flows and traffic patterns even in otherwise secured systems.

Possibly a case study can be conducted by applying the assessment methodology to an existing grid incorporating the Smart Grid plans in order to determine the adequacy of the high-level security risk assessment methodology for Smart Grids.

***Approach**: Usage of an existing risk assessment methodology and customization to the specifics of Smart Grids. The European Commission issued a Reference Security Management Plan for Energy Infrastructure[2] which provides a good high-level risk assessment methodology for electricity grid assets.[3]*

***Results**: A risk assessment methodology customized for Smart Grids to assist in selecting appropriate and effective measures against the risk encountered.*

***Deliverables**: A high-level information security risk assessment methodology.*

---

1 Eurostat, http://epp.eurostat.ec.europa.eu/tgm/refreshTableAction.do?tab=table&plugin=1&pcode=tec00001&language=en

2 EC (2010) A Reference Security Management Plan for Energy Infrastructure, Prepared by the Harnser Group for the European Commission, Under Contract TREN/C1/185/2009, http://ec.europa.eu/energy/infrastructure/studies/doc/2010_rsmp.pdf

3 Moreover, a thematic paper on risk assessment is to be issued soon on the topic of critical infrastructures.

The Team has considered and assessed several existing risk assessment methods in the field of Smart Metering and Smart Grid. The following are of particular relevance and have therefore been evaluated and may subsequently be referred to in more in depth:

- The Netherlands' privacy and security risk analysis of the advanced metering infrastructure[4];
- The UK Government's Technical Risk Assessment methodology[5].

However, it is worth noting that the former encompasses only the Smart Metering segment of the Smart Grid, whereas the latter is not Smart Grid specific, but generic. Therefore, at this date, the team has not been able to identify any concrete example of risk assessment methodology specific for the field of Smart Grid, adding to the relevance for this Expert Group to reflect on the matter. In doing so, this conclusion from the above-referenced U.S. NSTB study[6] is worth keeping in mind:

"There must be a coordinated and ongoing effort to secure the Smart Grid that includes the full development lifecycle. The development life cycle includes requirements, design, implementation, verification, validation, procurement, installation, operations, and maintenance. A failure in any phase of the lifecycle leads to defects, which lead to vulnerabilities that can be exploited by a skilled attacker."

The risk assessment approach proposed in this document is derived from the UK Government's Technical Risk Assessment Methodology which is widely applied in UK government organizations. The methodology has a number of characteristics which make it suitable for application in the domain of smart energy systems:

Tailored for assessing Information and Communication Techology (ICT) systems

Smart energy systems operate as an ICT layer on top of the physical energy grid. The proposed methodology specifically focuses on ICT systems, which shows in both the methodology's assessment steps and the explanatory text and examples.

Aligned with risk management standards such as ISO 27001 and ISO 31000

The HMG IS1 standard considers the risk assessment a 'snapshot' investigation of risks. A structural approach to securing ICT systems such as the Smart Grid demands that the risk assessment results fit into a security/risk management system. The HMG IS1 standard has been designed to fit into the frameworks provided by the ISO/IEC 27001:2005, ISO/IEC 27002:2005, ISO/IEC 27005 and ISO 31000 standards.

Supports design-time, iterative risk assessment

Smart energy systems development is still in an early stage. This allows taking a 'security-by-design' approach, using risk assessment results in the designing process. The HMG IS1 standard acknowledges that in the early design stage only a rudimentary conception of the system, its environment and relevant risks is possible. It therefore propagates an iterative approach, refining the risk assessment as the system design takes shape.

Provides a structured transparent approach

The HMG IS1 standard uses a highly structured approach, providing transparency about how risk ratings are derived. Transparency is a key requirement in the multi-stakeholder context of smart energy systems where consumers and politicians want to form their own opinion about the level of privacy and security level, and the rationale behind it.

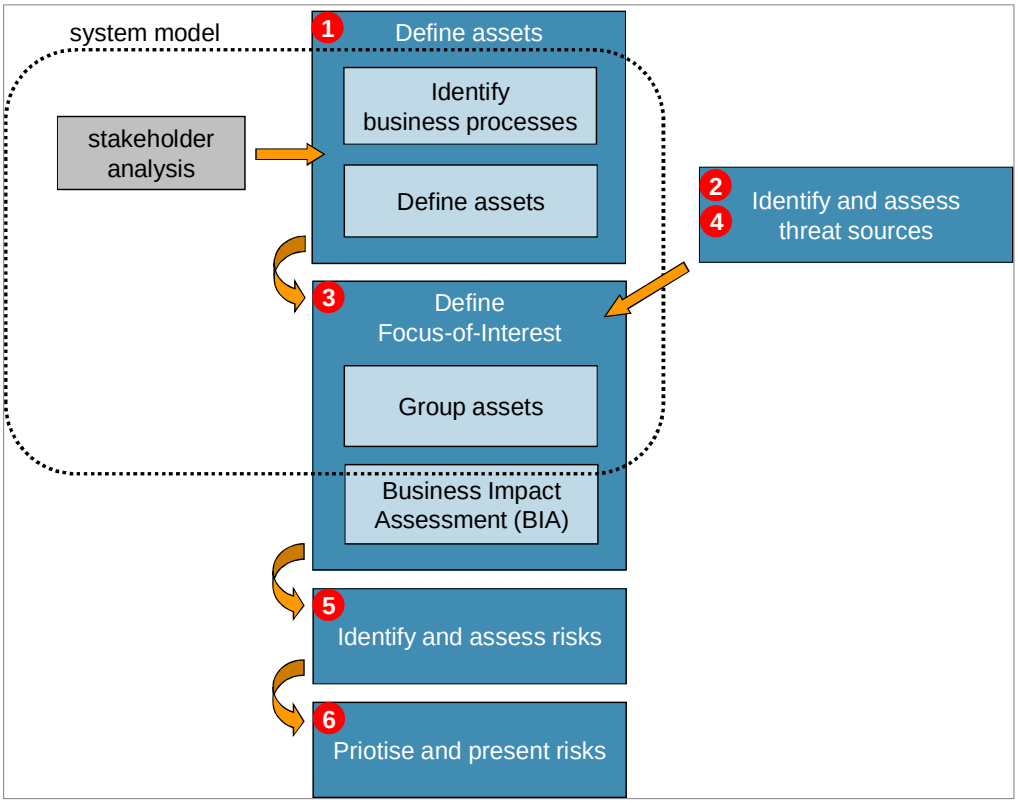
---

4 Netbeheer Nederland, *Privacy and Security of the Advanced Metering Infrastructure*, Appendix B, Risk Analysis, version 1.50 of October 2010, pending review and improvement in 2011, http://www.energiened.nl/_upload/bestellingen/publicaties/357_320007%20-%20PS%20M-RiskAnalysis.pdf

5 HMG IA Standard No. 1, http://www.cesg.gov.uk/publications/media/policy/is1_risk_assessment.pdf

6 See footnote 1

The proposed risk assessment method follows six defined steps. These steps allow the analyst to understand the system under consideration, define applicable threats and determine risks to the system with associated risk levels. The six steps are briefly described here, as well as some guidelines for how they may be applied in the context of smart energy systems.



Step 1: Identify Business Processes and define the assets

The objective of Step 1 is to describe the system (Smart Grid) and determine the assets that require protection against privacy and security threats. Assets are of value if they play a role in the 'business processes' of one or more stakeholders. Note that the nature of these business processes may vary greatly: whereas billing is a business process of both energy suppliers and consumers, it can be argued that 'protecting privacy' is a business process for the consumer as well. Business processes of the grid operator may follow from legal obligations and compliance requirements.

Like business processes, the nature of assets in the Smart Grid may vary as well. The following classes of assets may be identified:

- Information assets
  In ICT systems such as the Smart Grid, information is the key asset to protect. Especially for information assets, the impact of privacy and security breaches can typically easy be assessed.

- Functional assets
  This category includes systems functions such as 'energy consumption metering', 'scheduled device charging', 'remotely (de-)activating smart meter'. These functions are typically implemented over multiple system components and infrastructure.

- System assets
  System assets refer to specific system components or infrastructure. System assets may refer to a

system on an abstract level, or to system elements on specific OSI layers such as hardware configuration, an application or database etc.

An important decision concerns the asset's abstraction level. One should aim to define assets in such a way that they can be linked to threats and possible security countermeasures.

Step 2 and 4: Identify and Assess Threat Sources

Identifying threat sources is a matter of exercising professional judgment to decide who might deliberately attack the system and which external events could be a threat for the system (Smart Grid). Different threat sources may be used. Threat sources should be identified whether they can act as threat actors carrying out their own attacks or would have to coerce or subvert another threat actor to act on their behalf. Threat sources may include, but are not limited to:

- Disaffected or dishonest employees;
- Foreign Intelligence Services;
- Amateur or professional hackers;
- Virus and other malware writers;
- Terrorists;
- Commercial competitors (i.e. industrial espionage);
- Political pressure groups/activists;
- Organized criminal groups;
- Natural events;
- Major components failure;

Inadequate or untrusted technology supply-chain channels.

Step 3: Define the Focus of Interest (FoI)

The purpose of Step 3 is to define the specific groups of assets, features and facilities that will be the focus of a particular risk assessment. This is known as the focus of interest (FoI).

To some extent it is for the Analyst to decide what is included in a FoI. If assets are not grouped into a FoI each asset should be considered individually. This will mean more work for the Analyst than is required. If too many assets are grouped together then there are a number of dangers:

- That risks within a FoI will be missed in the analysis
- That more controls than are appropriate will be required, as the risk assessment will focus on the worst case (highest). Experience and judgment will help determine the optimum grouping.
- That pragmatic, appropriate and cost effective controls will not be applied at the right point in the system.

Step 5: Identify the Specific Risks and Estimate Risk Levels

Step 5 is one of the key parts of the risk assessment process. It results in the production of a list of risks and generates a risk level for each. This can be done by considering all possible FoI/threat group combination, using the most appropriate risk assessment technique.

Risk is considered to be a factor of threats, vulnerabilities and consequences. A risk exists if a cyber-attack can be executed against a particular system by exploiting some vulnerability leading to a negative consequence against the system. Estimating risk level for a particular risk, therefore, depends on 1) the likelihood of success of an attack and 2) the severity of consequence of that attack.

Identifying Risks: The analyst should follow the following steps to risks *all* risks within the FoI:

- Enumerate relevant threat sources for the FoI
- Consider potential attack paths within the FoI by exploring attack origin, action and target
- Study and enumerate vulnerabilities that may exist in the system and could be exploited in a given attach path
- Consider consequences of a successful attack in terms of state effect and performance effect
- Any issue that leads to a consequence other than "none" is deemed a risk

Estimating Risk Levels: the analyst should follow the following steps to estimate risk level for all identified risks (based on NIST 800-30):

- Determine likelihood that the vulnerability associated with that risk can be exploited for a successful attack (high, medium, low)High: threat-source is highly motivated and capable; security controls to prevent vulnerability exploitation are ineffective
- Medium: threat-source is motivated and capable; security controls are in place to impede attack success
- Low: threat source lacks motivation or capability, or effective security controls are in place

- Determine severity of the consequence that can be achieved by a successful attack (high, medium, low)
  - High: Consequences include loss of major tangible asset, significantly impact organization mission, or result in a significant safety issue
  - Medium: Consequences include costly loss of tangible asset, impact organization mission,or result in safety issue
  - Low: Consequences include some loss of tangible asset, noticeable impact on organization mission

Step 6: Prioritize and Present the Risks

The purpose of this step is solely to present a consolidated and prioritized list of risks in a relatively easily understood format. It is a natural breakpoint at which to review the assessment. Sort the risks into priority order with the highest risk level. The risk description and risk level should be recorded. The description should provide an understandable textual description of the risk in business language. Risks may be color coded to aid ease of understanding.

Conceptually, since risk levels are a combination of attack likelihood and consequences a two-dimensional table that maps likelihood with consequences for all risks can be an effective means of presenting the risks. Based on such a presentation a prioritization can be made to identify and put into place a range of security controls. Once security controls have been put into place the risk assessment table must be updated to make a note of updated risk levels associated with risks that are mitigated with the security control. In general, it is important to note that risk assessment is a continuous ongoing process whereby the risk assessment must be conducted on a periodic basis to account for changes in 1) threat sources, 2) changing FoI, 3) identification of vulnerabilities and 4) availability and use of effective security controls.

1.4.2 Security Requirements

***Objective**:*

***Requirements**:*

***Approach**: Use an existing control catalogue and customize it for Smart Grids.*

***Results**: A control catalogue specifying minimum requirements to secure the Smart Grid.*

***Deliverables**: A high-level control catalogue.*

It is proposed by the Expert Group to approach this task within the framework of ISO/IEC 27002:2005 in order to cover all relevant topics. ISO/IEC 27002:2005 contains 11 different categories to be considered:

1. Security policy
2. Organisation of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development, and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

While bearing that framework in mind, the recommendations of the Team feed more specifically into points 1, 2 and 6-11, and only to a lesser extent or indirectly into points 3-5. Indeed, the Team reflects on a high level methodology that allows to assess comprehensively and address effectively the new vulnerabilities and risks created by the introduction of new or upgraded devices (e.g. smart meters), processes (e.g. live data flows) and systems (e.g. SCADA operating the Smart Grid) into the electricity infrastructure. Recommendations are proposed for a policy that can guide EU Smart Grid operators in assessing risks, defining security objectives and taking appropriate measures accordingly to ensure the security and resilience of the Smart Grid. The focus is specifically on the ICT component of the Smart Grid, i.e. the involvement of electronic data flows and processing in operating electrical transmission and distribution grids.

Brief Biographies:

Sandro Bologna, graduated in physics from Rome University, has 30+ years experience at ENEA (The Italian National Agency for New Technologies, Energy and Sustainable Economic Development) and abroad, where he has held positions as Researcher, Head of Research Units, and Head of Research Projects at national and international levels. Recent main research activities deal with Critical Infrastructure Protection, with a special emphasis to vulnerability and interdependencies modeling, simulation and analysis. During his scientific career he has served in key roles representing ENEA participation in the multi-national research collaborations in Critical Infrastructure Protection, as well as Evaluator and Reviewer of EU Projects for different DGs. Has published more than 120 papers and has been referee of international scientific magazines and conferences, member of the Editorial Board of different Journals, member of the International Programme Committee of many International Conferences. At present he is President elect of the Italian Association of experts on Critical Infrastructures.

Dr. Himanshu Khurana is the Senior Manager for the Integrated Security Technologies section part of the Knowledge Systems Laboratory at Honeywell Automation and Control Systems. The Integrated Security Technologies section focuses on research, developed and technology transition in cybersecurity, computer vision, surveillance and biometrics. Dr. Khurana's research interests lie in the area of distributed system security, especially as applied to large-scale distributed systems and critical infrastructures. He has published over 45 articles covering a range of topics in distributed system security. He has co-developed the Secure Email List Services (SELS) toolkit for secure email used by several nation-wide CSIRTs. Before joining Honeywell, Dr. Khurana was Principal Research Scientist at the Information Trust Institute, University of Illinois, Urbana-Champaign and served as the Co-Principal Investigator and Principal Scientist for the Trustworthy Cyber Infrastructure for Power (TCIPG) center and the Program Lead for the Advanced Digital Sciences Center (ADSC) Power Grid IT Program. He has been involved with several Smart Grid initiatives including the North American Synchrophasor Initiative, NIST Cyber Security Working Group, DNP3 Technical Committee, and in developing relevant cyber security standards. He obtained his MS and PhD from the University of Maryland, College Park.

Mr. Johan Rambi is Privacy & Security Officer at Liander Infostroom, the business unit who is responsible for the deployment of the smart meters and maintenance of the Advanced Metering Infrastructure (AMI) at Alliander in the Netherlands. In this role Johan coordinates the Information Security and Privacy Management System (ISPMS) control cycle in the organization as Liander is certified compliant in privacy legislation. Further on, Johan Rambi is leader of the Dutch DSO workinggroup Privacy & Security from Netbeheer Netherlands, who developed the Dutch Privacy & Security requirements for AMI. In Europe Johan Rambi is active in several EC expert groups and standardization committees on Smart Meter Privacy & Security / Smart Grid Cyber Security. Before Johan joined Alliander, he worked as security architect and consultant at different organizations for the last 15 years.

Dipl.Ing. (FH) Ralph Eckmaier, MSc, CISSP-ISSMP, CISM, CISA is an independent consultant and accredited certification auditor for ISO/IEC 27001:2005. Mr. Eckmaier holds a MSc in Information Security Management from Donau-Universität Krems, Austria and additionally, an Dipl.Ing.(FH) in Electronics/Economics from FH Technikum Wien, Austria. Mr. Eckmaier is Head-of-Delegation for Austria within ISO/IEC JTC1/SC27. Furthermore, Mr. Eckmaier diligently participates and contributes to the topics of Risk Management, Cyber Security and overall concepts of Management System Standards in several ISO, ISO/IEC JTC1 and CEN/CENELEC/ETSI working groups. Before founding an independent consultancy, Mr. Eckmaier worked for more than 15 years in IT-Security as an integration engineer, Information Security consultant and also as an IT-Security Officer. Mr. Eckmaier has 4 years experience as an accredited certification auditor for ISO/IEC 27001:2005.