Risk Assessment in the E-LAND Project

Xueli Gao
Department of Risk Safety and Security, Institute for Energy Technology, Norway. E-mail: xueli.gao@ife.no

Coralie Esnoul, Silje Arendt Olsen and Per-Arne Jørgensen, Bjørn Axel Gran
Department of Risk Safety and Security, Institute for Energy Technology, Norway.

The E-LAND concept uses the smart grid concept with a great potential to optimize the management of energy consumption. However, applying modernization of the management introduces new risks to relevant stakeholders, from energy producers to energy users. In order to protect all the stakeholders by providing effective controls to the risk in smart grid system, a risk analysis is conducted to evaluate the hazard, threats and vulnerabilities that are introduced into energy critical infrastructure. As a large variety of risk analysis methods are available, spotting the appropriate methodology in the E-LAND project is not obvious considering the number of Business Uses cases and Technical requirements. In this article, we present the risk assessment approach applied in the currently performed E-LAND project, which can be used to determine the risks associated with an architectural concept smart grid that includes both traditional systems and novel ICT concepts. Risks and vulnerabilities are identified at a sufficiently detailed level to provide mitigation input to the architecture design, starting from the use case level. The resulting mitigations and recommendations are based on a sound understanding of cybersecurity risks and have been given to design for implementing. This paper addresses the challenges in applying risk analysis methods as well as work process and describes how these challenges were met.

Keywords: E-LAND, risk assessment, safety, privacy and cyber security.

1. Introduction

The goal of the European-funded Horizon 2020 project E-LAND is to provide a solution for energy management by facing technological, societal and business challenges in the energy sector (E-LAND). The goal builds on the view that traditionally, energy sectors have been decoupled from both operational and planning viewpoints, whereas tight interactions have always taken place and are increasing between both actors. For instance, electricity, heating/cooling and gas networks interact in many cases through various distributed technologies such as combined heat and power, electric heat pumps, air conditioning devices, trigeneration of electricity, heat and cooling, and so on. Similarly, interactions between electricity, the fuel chain and the transport sector are increasingly envisaged or already take place by means of electric vehicles, biofuels, and hydrogen-based transport. With this outlook, a key prerequisite for evolving towards a cleaner and affordable energy system is to better understand these interactions and to develop integrated multi-vector energy systems, whereby electricity, heating, cooling, fuels, transport, and so on optimally interact with each other at various levels. Existing multi-vector energy systems lack ICT-based interconnections to achieve a cost-efficient integrated de-carbonised local energy system.

Another technology challenge is particularly related to the emerging trend of energy storage. Energy can be stored in many forms (such as batteries, thermal storage, etc.) and thereafter the stored energy can be used in any energy network. As there is no commonly agreed standard for energy system integration, the need for and development of optimisation tools to manage different energy storage types is lacking. Thus, there is a need for ICT tools that optimally manage various storage devices, supplying energy capacity and flexibility to different networks.

The concept of E-LAND integrates different energy vectors into a common system, which in turn provides an optimal energy balance for the local community. The concept, illustrated in Figure 1, transforms the way energy is produced, stored and consumed in an energy island context. The E-LAND project brings coherent innovation across three planes: technology, community and business. Currently, the E-LAND toolbox is in development phase.

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference
Edited by Piero Baraldi, Francesco Di Maio and Enrico Zio
Copyright © ESREL2020-PSAM15 Organizers.*Published by* Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

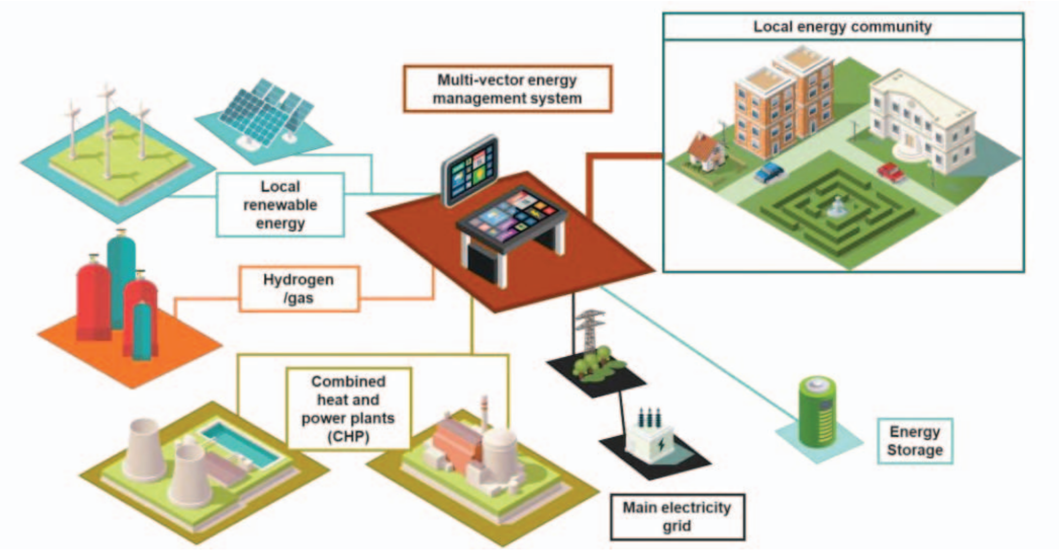

Fig. 1. Overall E-LAND's Multi-energy system overview for districts and remote area

2. Risk assessment methods

2.1 *Risk assessment and E-LAND*

New technology opens for several risks, such as, a leak of privacy data could potentially be a breach of laws and regulations. It will, therefore, undermine the trust in the services. Manipulation of data or denial of service attacks may have costs and undermine trust in services. Lack of well-defined and tested requirements for the management system could lead to unforeseen downtime and inefficient services. The lack of, or insufficient safety and risk assessment could lead to hazardous incidents from working with high energy supply, distribution or storage. It will be important to identify potential risks in order to define adequate information security and system security requirements. These risks and mitigations will be followed up in a risk register.

The primary objective of risk analysis in the E-LAND project is to get an overview of the amount of risks attached to the defined assets. The risks can appear from physical or cybersecurity failures and vulnerabilities within the given system setting. Furthermore, the risks are based on analysis of threats, attack vectors, likelihood and impact. Within this knowledge, stakeholders shall be able to define security requirements and select the right mitigation actions with focus on the most critical components. This paper provides a risk assessment method based on use case evaluation to show how different aspects related to security, safety and privacy can be assessed.

2.2 *Risk assessment guidelines for smart grid*

The Guidelines for Smart Grid Cyber Security by the National Institute of Standards and Technology (NIST, 2012) defines a high-level architecture categorizing the interfaces in a smart grid and presents an approach to identify security requirement for these interface categories by performing a risk assessment (NIST-IR 7628). NIST-IR 7628 and ISO 27002 standards have been the basis for a report on smart grid security by ENISA (2012) which provides a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cybersecurity. The importance of performing a comprehensive risk assessment before selecting appropriate measures is pointed out, but no specific methodology is recommended.

There are more high-level risk assessment methods that are applicable or relevant for smart grid risk assessment. Some examples include OCTAVE, HMG IS1 (2009), MAGERIT (L. Langer, et al. 2015), NIST (2012). Many of these are based on the principles identified in ISO 27005, which provides guidelines on how to implement an information security risk management framework within an organization. Whilst these risk assessment methods are useful, most of the methods are focusing on cybersecurity risk assessment and they do not provide specific guidelines suited for the attributes and practicalities of smart grid solutions. For example, as smart grids mostly can be regarded as cyber physical systems comprised by a range of different technologies, cyber-attacks on smart grids might have complex impacts on energy supply (service and equipment). Furthermore, attacks could result in safety-related incidents happening, both direct from the energy grid, or indirect as a result of degraded or loss of services, resulting in injury or loss of life. (L. Langer, et al. 2015)

3. Risk assessment on use case

This section introduces the use case methodology applied in the E-LAND project and how risk assessment has been performed based on use case application.

3.1 *Use case methodology and definition*

The development and integration of new functionalities in engineering systems requires unambiguous definitions and proper analysis methodology in order to enable the successful identification and understanding of their technical requirements. Specifically, for delivering novel smart grid functionalities in terms of future software and hardware-based advances, the Use Case (UC) approach has been used in E-LAND project. Different use cases have been established, e.g. High-level UC, business UC and device/system UCs, with respect to addressing different development objectives. This paper takes a technical point of view, focusing on device and system UC which is further expressed in a Primary Use Case (PUC). A PUC is a use case implemented in a specific system characterized by a defined boundary. In addition, it can be considered as a tool for reaching one or many goals that are described by High-Level UCs.

In E-LAND there are also Secondary Use Case (SUC), which are considered to be one a level lower. A SUC is more granular, less abstract, and describe core functionalities that are used by multiple PUCs.

3.2 *A use case description*

This paper focuses on one specific PUC with a relevant SUC as described in the following. There are several SUCs defined in project, but only SUC 01 is described here as an example. The use case numbering used below corresponds to the numbering used in project.

- PUC 04: Optimal scheduling of thermal and electrical storage

PUC 04 models the optimal scheduling and co-optimization of electrical and thermal Distributed Energy Resources (DER) in order to maximize the Renewable Energy Source (RES) share in the energy mix of the Local Energy System (LES), minimize energy wastes, improve reliability and power quality, reduce CO2 emissions and costs and optimize the use of Battery Energy Storage System. The technical actors involved in this PUC are the Energy Management System (EMS) acquiring the necessary filed data and controlling the field devices, the forecasting and optimization module as well as the Energy Service Bus (ESB) ensuring their secure and seamless integration and orchestration:

- EMS: A system responsible for controlling the various assets of the LES as well as for the orchestration of its optimal operation. Provides a user interface for the day-to-day operation of the LES.
- ESB: A system enabling the integration of the forecasting and optimisation tools, the EMS of the LES and the various external data providers.

SUC 01 is related to the above PUC 04.

- SUC 01: Forecast RES Production

A short description of SUC 01 is that the Energy Forecaster (EF) is responsible for providing local RES production forecasts that are needed for optimal operation of a LES. To create or exploit the forecasting models, historical weather and production data must either be available or be acquirable. As prerequisites, communication with ESB is established and ESB should have access to the necessary data.

3.3 *A step by step risk analysis on use cases*

This section introduced the main steps used in the E-LAND toolbox risk assessment concept phase.

3.3.1 *Step 1 - break down of use case*

With the defined PUC and SUC, we are able to break down the SUC to the sufficient detailed level, where it is possible to identify relevant assets and dependencies between the different assets. This is described through the following example from the E-LAND risk assessment. The SUC 01 can be breakdown to lower level use cases:

- Sub SUC 01: Historical weather data,
- Sub SUC 02: Weather forecast,
- Sub SUC 03: Historical RES generation,
- Sub SUC 04: Historical power consumption

The Sub SUCs defined here are used for the risk assessment purpose, which will help to identify specific information assets. Since the risk analysis is performed bottom up, it is important to establish the linkage between different level use cases to both retain the traceability and allocate consequence to prior identified risks at the lower level of use cases.

3.3.2 *Step 2 – identify assets*

The identification of relevant assets is preferably done in the low-level use cases. An architecture description established in project is a good tool to identify the information assets. When category information asset, ENIS/EG2 report "Proposal for a list of security measures for smart grids" can be used as reference (ENISA, 2013).

It should be noted that the supporting assets, that a primary asset relies on, must be identified and considered in the risk assessment as part of a dependency map, as these may have vulnerabilities that can be exploited in order to harm the primary asset. In case a particular information asset appears in different use cases, they should either be grouped and considered collectively, or the highest risk impact level for that asset across all use cases may be considered (L. Langer, et al., 2015). As an example, from the E-LAND risk assessment, the relevant assets identified for Sub SUC 01 are shown below:

- Historical weather data is provided from external sources (with EMS as back up) and flows through several systems, e.g. ESB, EMA, etc. before it reaches the Energy Forecaster software module.

The identified asset can be categorised as an Information Asset.

3.3.3 *Step 3 – identify risks*

Identify potential risk items based on identified assets in relevant use cases. Risk trigger is a condition or other event that will cause a risk to take place. Understanding risk triggers helps to develop a more efficient risk mitigation action. As examples from the E-LAND risk assessment are two potential risks identified on Sub SUC 01:

1. Incorrect historical data is provided to the Energy Forecaster with 3 risk triggers in below:
   - The provided data is not on the required format.
   - Wrong information is provided from the source (format is correct), e.g. "The data source used for historical weather does not apply to the pilot location"
   - Correct information is provided from the source/third party, but the information reaching the Energy Forecaster is incorrect.
2. Historical weather data is not provided to the Energy Forecaster with two risk triggers in below:
   - There is no data provided by the external source/EMA.
   - Not enough storage space on database

3.3.4 *Step 4 – threats identification*

There can be several threats linked to the identified potential risks. It is important to use expert judgement in this step to have comprehensive analysis. The most critical threats should be registered in the risk table. In addition, ENIS/EG2 report "Proposal for a list of security measures for smart grids" provided a good overview of the threat exposure of smart grid assets with established association between assumed threats and identified assets. One example from the risks presented in step 3 are listed in the table below.

Table 1. Treats group and treats identification

Threats group	**Threats (Failure modes)**
Unintentional loss	External data source/EMS receives incorrectly formatted information and sends this information to the Energy Forecaster.
	System and service malfunction, loss of service, degraded systems and services, etc.
	System and service malfunction, loss of service, degraded systems and services, etc.
Intentional damage	External data source/EMS is changed due to an attack and the data sent to the forecaster is wrong/erroneous.
	The information is altered in such a way that it is on the correct format but the information itself is incorrect/malicious.
	"Intentional attacks, Damages from penetration testing, etc. "
Legal	Untrusty and unreliable weather service providers. Dependency on external provider, which might not be 100% reliable.

3.3.5 *Step 5 - Estimate likelihood*

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (NIST 2012). Reference can made to the NIST Guide for Conducting Risk Assessments (NIST 2012). To analysis the likelihood of different threats, the threat agents with different capabilities, resources and motivation should be assessed with considering the supporting assets.

However, estimate both likelihood threat initiation and likelihood of threat resulting impacts requires a large amount of work especially when evaluating the likelihoods quantitatively. Considering that the project is in its early concept phase, without detailed design available, threat event occurrence as it was ranked in the risk assessment planning phase in the project is provided in Table 2. This makes the evaluation process efficient and accurate.

Table 2. Attack likelihood ranking

Likelihood	Short description	Detailed description
Very high	Near certainty	High – The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
High	Highly likely	
Medium	Likely	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	Low likelihood	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.
Very low	Unlikely	

It should be mentioned that three pilot sites in E-LAND project have been chosen:

- The Port of Borg is an industrial area on a small peninsula in Fredrikstad, Norway.
- UVTgv University Campus is located at the North side of Targoviste city in Romania.
- The Spanish pilot, Walqa, is a Technology Park where around 1000 people work in buildings rented out or owned by private companies and Technology Centres.

The three pilots represent great variability in the sense of geographic, demographic and available technology infrastructure perspectives. With those facts, the likelihood of threat event occurrence would be different caused by threat event initiation possibilities, with the same system design. To achieve same level of risk level, different mitigation actions might be proposed.

3.3.6 *Step 6 – risk impacts*

Risk impact is estimated and expressed in five Risk Impact Levels towards technical performances in different categories (safety, security/integrity, privacy). To determine the Risk Impact Level for a specific information asset, every category is evaluated against different scenarios. Risk Impact Level for only the worst-case category is selected when determining the Risk Impact Level for a specific information asset. The Risk Impact Level used in the assessment was determined in the risk assessment planning phase is shown in Table 3.

Table 3. Impact ranking

Impact	Technical performance
Very high	Severe degradation on operations, assets, individuals, organizations, etc.
High	Significant degradation or major shortfall on operations, assets, individuals, organizations, etc.
Medium	Moderate reduction with limited impact on operations, assets, individuals, organizations, etc.
Low	Minor reduction can be tolerated with little or no impact on on operations, assets, individuals, organizations, etc.
Very low	Minimal or no consequence on operations, assets, individuals, organizations, etc.

Due to that the risk analysis is limited on the E-LAND toolbox at current, the estimated impact for most of the risk items are ranked high and very high. As the project moves forward, and mitigations are suggested and developed, the risk item ranking is expected to be improved (i.e. decrease).

3.3.7 *Step 7 - Identify Risk Level*

The risk level for every information asset is identified by taking the Risk Impact Level and the likelihood. The Risk Level is identified using a risk matrix that identifies criticality levels, depending on the impact and likelihood of an information asset being compromised.

3.3.8 *Step 8 - Determine mitigation actions*

Based on the risk ranking that has be determined for every information asset, appropriate mitigation actions are selected. The actions need to be implemented with priority from high risk to low. Technical details of how the mitigation actions are defined are illustrated in another ESREL 2020 paper by Jørgensen et al.

3.3.9 *Step 9 - Communication and documentation of risk*

After mitigation actions are defined for each information asset, they must be documented and communicated to the use case and architecture design team for implementation. In the same way, the implementation status needs to be fed back to the risk register. Since risk assessment is a continuous process, these steps should be repeated periodically or when the nature of use cases changes. More details on this are discussed in another ESREL 2020 paper by Esnoul et al.

4. Main challenges

In a smart grid, ICT elements and physical elements are closely linked, and automated actions are triggered by sensors, actuators, and control elements. This means that i) in addition to the logical cyber and digital security vulnerabilities considered, physical and cyber-physical vulnerabilities and risks must also be assessed. This need will both increase the number of scenarios that have to be assessed and introduce the challenge of understanding the relative importance of cyber versus physical risk. ii) the physical impact of an attack must be assessed; e.g. it is not readily apparent what effect a DoS attack could lead to in a smart grid's ICT infrastructure, or its' effect on the physical operation of a grid (F. Skopik and P. Smith, 2015). In the E-LAND project we used a combined security and safety risk assessment method by categorizing risk impacts to safety, privacy and security in the same risk register table.

Evaluating both likelihood threat initiation and likelihood of threat resulting impacts require large amount of work especially when evaluating the likelihoods quantitatively. Considering that the E-LAND project is in early concept phase without detailed design available, a qualitative ranking of the threat event occurrence was performed. This made the evaluation process be more efficient and accurate.

Guidelines and standards on Smart Grid risk assessment provide good overview and recommended identification and description of assets overviews, threats, vulnerabilities, and security measures, etc. with established association between them. However, including all detailed recommended items in risk assessment is not realistic at the early phase of a toolbox development. Selecting the most relevant elements is challenging in the early phase and recommended from viable point of view. Cost – Effect evaluation should guide the selection of relevant elements.

Risk assessment on smart grid is challenging due to the complexity of the system and the dependency of the different type of consisting systems, incidents in each of the interconnected ICT sub-system have the potential to cause problems in another. A thorough understanding of such interdependencies is important when performing risk assessment.

Furthermore, due to the complex function dependency between different systems/elements in smart grid it is not easy to keep the traceability when ascertaining risk impact for each of the identified risk items, especially when the risks are identified at detailed level. In the project we experienced that the detailed sub-use case defined for risk assessment helped with asset identification, with linkage established between different level of use cases to keep the traceability of allocate the risk impact.

A high number of stakeholders with different roles, e.g. energy planner, LES operators, energy supplier, power distribution system operators, etc., provides its own set of risks as interdependencies grow, and supply chain management and operational processes become more complex. Systems of systems where variability of roles, functions and technologies are high, present a broad variety of both known and unknown vulnerabilities. New combinations of solutions and actors might even spur new, unintended novel vulnerabilities. In addition, it will also have an impact on the consumer privacy as more personal data is potentially shared with a larger set of stakeholders. A detailed discussion is included in another ESREL 2020 paper by Esnoul et al.

Many of the external systems and devices that have to be connected to the E-LAND toolbox are outside of the scope of the toolbox development. The interaction with external system introduces new challenges for security (that needs further inputs regarding solutions).

5. Conclusion and Future work

The smart grid system consists of a combination of systems with different technology generations. In some cases, the different technologies may not interact, e.g. because they use different protocols. The risk assessment for smart grids must be able to deal with a complex combination of systems and new technologies.

One of the next phases of the E-LAND project is to integrate the designed toolbox to the existing infrastructures. The plan is to follow up on the risks from the early design phase, and to identify topological vulnerabilities to ensure a secure architecture. New types of cyber threats coming from many different types of threat actors which may appear almost daily. Within the long-life time of the system, the risk assessment should be performed on a continuous process through all lifecycle phases of the project.

Acknowledgement

The E-LAND project has received funding from the European Union's Horizon 2020 Research and Innovation program under Grant Agreement No 824388. This document reflects only the author's views and the Commission is not responsible for any use that may be made of the information contained there.

The authors would like to acknowledge all efforts of the E-LAND project partners that have contributed to the results reported in this paper.

References

CESG National Technical Authority for Information Assurance, HMG IA Standard No. 1 Technical Risk Assessment, October 2009.

E-LAND website: https://elandh2020.eu/ (last visited 13.01.2019)

ENISA (2013), Proposed security measures for smart grids, Smart grid task force EG2 deliverable, Proposal for a list of security measures for 8 smart grids.

F. Skopik and P. Smith (2015), Smart Grid Security: Innovative Solutions for a Modernized Grid, Elsevier, ISBN: 978-0-12-802122-4. OCTAVE Information Security Risk Evaluation, http://www.cert.org/octave/ (last visited 13.01.2019)

ISO/IEC 27002 — Information technology — Security techniques — Code of practice for information security controls (first edition)

ISO/IEC 27005 (2011), Information technology — Security techniques — Information security risk management (second edition)

L. Langer, P. Smith and M. Hutle (2015). Smart grid cybersecurity risk assessment, International Symposium on Smart Electric Distribution Systems and Technologies (EDST).

MAGERIT v.3: Methodology of analysis and risk management information systems, http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=en (last visited 13.01.2019)

NIST (2012), Guide for Conducting Risk Assessments- information security.

NIST IR 7628 (2014), Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements.

P. A. Jørgensen, J. E. Simensen, C. Esnoul, X. Gao, S. A. Olsen and Bjørn Axel Gran (2020). Addressing Cybersecurity In Energy Island, Paper accepted for ESREL 2020.

C. Esnoul, S. A. Olsen, B. A. Gran X. Gao, and P.A. Jørgensen, J. E. Simensen (2020). Risk And security Practices: Experiences from the E-LAND Project, Paper accepted for ESREL 2020.

U.S. Department of Energy's Office of Electricity, White paper: Security for smart electricity grids. https://www.smartgrid.gov/files/White_Paper_Smart_Grid_Evolution_Independent_System_Operator_201001.pdf (last visited 13.01.2019)