Risk And Security Practices: Experiences From The E-LAND Project

Coralie Esnoul

Institute for Energy Technology, Os Alle 5, 1777 Halden, Norway. E-mail: coralie.esnoul@ife.no

Silje Arendt Olsen, Bjørn Axel Gran, Xueli Gao, Per-Arne Jørgensen, John Eidar Simensen
Institute for Energy Technology, Os Alle 5, 1777 Halden, Norway.

The increasing availability of renewable energy sources and the high expectations from end-users regarding energy dependability has forced a re-thinking of how the full potential of energy supplies can be released. E-LAND is a European project which concept is to develop a service bus application enabling energy islands to optimize the management of energy production and consumption, which focuses on communities of end-users' needs instead of addressing the system operators' requirements. In this new organization of the energy market, the risk ownership on devices and energy costs are shared by the energy islands, the grid owner and the energy supplier. To support the energy islands in their new role, the E-LAND final product must not add risk in the management of energy. Thereby, a risk assessment is performed to ensure that the concept, the solution, and the application to be delivered in E-LAND are safe, secure, and reliable. This paper describes the project risk management for the E-LAND project and gives examples of future potential users, best practices on how to access, communicate and manage project risks with multi-disciplinary and international partners. As the E-LAND solution needs to collect data from the users, this article also addresses the risk regarding privacy/security, how this particular risk is understood and communicated through mitigations to ensure that the final product is in agreement with the standards.

Keywords: E-LAND, Risk Management, Project Risk, Privacy, Product Reliability, Cybersecurity.

1. Introduction

The goal of the European-funded Horizon 2020 project E-LAND is to provide a synergistic solution between technological, societal, and business challenges that the energy sector faces (E-LAND). E-LAND assumes that the needs in energy supplies are changing according to the new usages of electricity (e.g. electrification of transportation, buildings, and even industrial uses). The electricity production has traditionally been governed by fossil fuels, with a combination of large centralized power plants, in addition to smaller distributed combined heat and power plants. Today, environmental concerns, the availability of technology, commercial and economic factors under both national and joint-European initiatives, have promoted the use of renewable energy resources. However this energy production is strained by: (i) the high fluctuation of the production needs depending on the change of season or the cycle of the day and (ii) the motivation for decarbonated energy sources and renewable energy sources, that enables (iii) the increase of decentralized production sites, known as energy islands.

Energy islands are communities of prosumers, producing and consuming a part or the total of their energy needs which may experience dependency on external energy supply (E-LAND). These modern shares between local and traditional energy suppliers force a rethink of the customary rules on how the energy grid is managed. New solutions are required to facilitate the balance on the grid as the current network is designed to for one-way electricity and data. Building new infrastructure is not viable from a cost point of view. Besides, delivering electricity to accommodate the rising needs in both cities (central) and to the isolated population (decentral) presents a challenge in where energy production takes place that drives costs up further. One possibility is to make use of new technologies to adapt the production to the demand and thus reach a better, more reliable energy management. Traditional energy grids are mainly centralized with a unidirectional energy flow from production to consumption, where demand governed production and cost. A Smart Grid (INCITE) provides two-ways communication and services, enabling consumers and providers to share a real time understanding of current and upcoming energy need which leads to improved flexibility for energy production. In addition to bidirectional communication, upgrades to Smart Grids can allow for bidirectional energy flow as well. E-LAND aims to develop and integrate a tool suite that changes the role of the energy islands from passive customers into active stakeholders in the energy market by providing Smart Grid services to the grid.

2. E-LAND

2.1 *Scope and main goals*

The availability of local renewable resources presents a potential advantage that E-LAND will explore to establish and validate new approaches for local energy systems. To achieve this objective, E-LAND is developing multi-vector energy optimization algorithms that consider the current and the future estimations of energy storage needs and end-user flexibility. The main objective is to implement a modular toolbox which uses data on energy consumption, market price and weather forecast to provide an optimal scheduling to product, store, buy and sell energy. A goal in the project is that the solution should motivate community engagement towards technology and business. The toolbox is intended as a decision-making tool to optimize energy usage but will not be an automatic control solution that governs e.g. battery parks and storage solutions, nor any infrastructures. Figure 1 illustrates where the E-LAND toolbox is included in an energy management process.
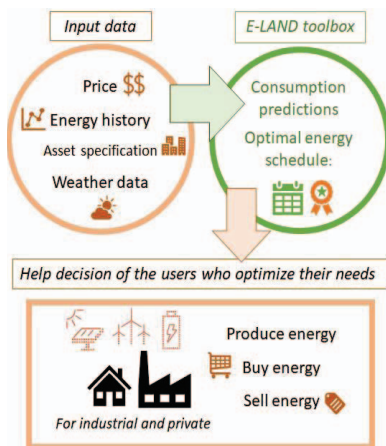

Fig 1: Inclusion of the E-LAND toolbox in the decision process.

2.2 *Partners and applications fields*

The project gathers 13 European partners, with diverse fields of expertise, from academia to industry, including: University of Girona, Schneider Electric, Borg Havn, GECO Global, Smart Innovation Norway, Intracom SA Telecom Solutions, the Reiner Lemoine Institute, Valahia University of Targoviste, Centre for Resources in Energy Efficiency and Climate Change (CREESC), the University of St. Gallen, Instrumentación y Componentes (INYCOM), BSES Yamuna Power Limited and the Institute For Energy technology (IFE). The variation of needs, interests and technology among the partners presents the project with a unique possibility to create a product with a broad field of impact that is sufficiently general to be applied for stakeholders beyond the participants of the project.

To realize this, the data of different communities and partners are identified to model the scope of the toolbox. The needs of different stakeholders are mapped depending on their abilities and resources, and the factors that may impact their engagement (e.g. technology, strategy) are listed. In the study, four pilot sites have been identified among the partners. Pilot sites' energy usage, i.e. energy production and consumption will be analyzed to make sure the final toolbox fulfills the needs of the end-users. This process also allows the development of general business models that can be replicated in across regions. The pilot sites represent a large variety of countries, locations climates, populations, cultures, sizes, activities (from the industrial harbor in Norway to the living buildings of a university in Romania), and span various infrastructures and technologies to produce and store energy (e.g. solar panels, battery, etc.). Table 1 gives an overview of each pilot sites' expectations regarding their activities (E-LAND). The pilot sites will be the first to test the E-LAND solution in June 2020.

Table 1. Energy needs depending on the pilot sites, first users of the E-LAND toolbox.

		Spain University of Girona	Romania University of Targoviste	Norway Borg Havn Harbor	India Mumbai Metropole
Needs of optimal management	Building	X	X		X
	Industrial uses			X	
	Vehicles	X		X	X
Need of optimal scheduling for storage	Battery H		X	X	X
	Thermal network storage	X			X
	Excess generation in thermal network		X	X	
Optimization of energy	Capacity/Costs/Maintenance	X	X	X	X

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference

4344

2.3 *Risk ownership in the energy islands*

As the energy islands become energy suppliers by using the E-LAND solution, they will be facing the same responsibilities as those of the traditional energy grid suppliers and will be responsible for equipment and infrastructures similarly. This means that risk, safety, and security must be handled to such a degree that the E-LAND solution can be accepted by the energy islands. This is achieved through proactive risk management of the project and the product of E-LAND. The next part describes the risk analysis process undertaken to ensure that the E-LAND concept and toolbox are sufficiently reliable to not impose further risks on the users.

3. E-LAND risk management

Internal and external factors can impact the quality of scheduling in the project as well as the final product delivery. Potential change in both types of factors presents a risk which needs to be followed up, foreseen, updated and acted upon throughout the full lifecycle of the project and the developed product. IFE has been assigned the role of risk manager in the project and are responsible for; performing risk assessment for both project and technical requirements, assigning risk ownership, updating and communicating risk status, following up existing risks and identifying potential new incoming risks through all phases of the project. The risk manager must ensure that all activities are being monitored and handled during the project. IFE's risk management team consists of personnel with risk, safety, and ICT security competence, responsible for performing the day-to-day overall risk management of the project. In the following the approach to reduce risk in the project and the final E-LAND solution is described from the risk manager side.

3.1 *Management of risk towards project goals*

With a project gathering multiple international partners there are factors that should be regarded such as: several languages, multiple cultures, academic and industry environments, needs and goals, variance in responsibility and requirements to name some. Project risk management must be aware of these factors and their development throughout the project. The project defines risk management as the process of identifying, analyzing, and then responding to any risk that arises over the life cycle of a project. The risk management will contribute towards achieving a reliable and sustainable product, supporting organized scheduling, optimal resources management and good communication among the partners. The project risk management is central for the project to remain on track and meet its objectives (delivery, milestones, engagement of partners, etc.).

3.1.1 *General process*

The E-LAND consortium established a Risk Management and Contingency Plan as a continuous process to be executed throughout the whole life cycle of the project (E-LAND). The plan defined a risk reporting hierarchy but did not go into details about the execution of the risk management. The first step was therefore to choose a methodology that would fit the multiple partners and the project organization. The project board did not set up specific requirements or guidelines to favor one method towards another for handling the risk management, apart from the reporting hierarchy. The E-LAND project is divided into eight Work Packages (WP), which constitute the lowest level of the project organization. Within each WP there are with several sub-tasks and deliveries. Each WP is assigned to a WP leader who is in charge to collect the potential risks from the WP. All new risks are evaluated and mitigate before a monthly Technical Management Team (TMT) meeting (top level of organization). Potential risks are discussed, and decisions are made whether to included them in the register or if considered business as usual and will be solvable within the WP. The process can be divided in the following steps:

- *Step 1 – Preparation:* Templates was prepared to gather and present information in a consistent and structured way. One template was the risk register, a spreadsheet for tracking identified risks, status, updates, new potential risks and comments. The other was a power point deck for presenting the content from the risk register in a convenient way.
- *Step 2 – Gathering status updates:* Monthly 1-on-1 meetings was scheduled with each WP leader. In the meeting we reviewed and updated the risk register together and discussed potential new risks. After the status from all the WPs was collected, the power point was updated.
- *Step 3 – Presenting and communicating the risks:* In the monthly TMT status meetings, the risk status was presented and the reported issues that potentially could be risk was discussed, followed by a decision to accept the risk into the register.
- *Step 4 – Traceability and maintenance:* The risk register, and presentation were updated afterwards with decision made in

the TMT meeting. A copy of the presentation was archived to have traceability which made the possibility to update the same presentation for each meeting.

3.1.2 *E-LAND project risk register*

The risk register records the description of the all project risks, the likelihood and the impact on which WP as described respectively in Tables 2, and 3. The type of risk are linked to organizational risk, business risk and human risk. All risks are assigned to an individual to ensure ownership and accountability.

Table 2. Project risk impact matrix.

Impact	Technical performances	Project management and execution
Very high	Severe degradation. Cannot meet KPI or key technical or supportability threshold. It will jeopardize project success	Cannot meet key project milestones.
High	Significant degradation or major shortfall in supportability. It may jeopardize project success	Project critical path affected.
Medium	Moderate reduction with limited impact on the project objectives	Minor schedule slips. Able to meet key milestones with no scheduled float.
Low	Minor reduction can be tolerated with little or no impact on the project	Able to meet key milestones
Very low	Minimal or no consequence	Minimal or no impact

Having an individual as risk owner is an important step toward ensuring that a response plan is developed and acted upon in a timely manner. The risk owner has the responsibility to address and mitigate the relevant risks. The project risks are added to the risk register provided in the startup of the project. These are then monitored throughout the duration of the project. The risks which were judged as negligible were also included in order to keep track on their development. Regardless of this way of working,

both risk reporting and risk following-up are experienced as challenging. One reason is the added complexity of having many involved partners. To simplify the process, the following steps have been followed to improve the risk collection and the understanding of the partners.

Table 3. Project risk likelihood matrix.

Likelihood		Probability of occurrence
Near certainty	Very High	~90%
Highly likely	High	~70%
Likely	Medium	~50%
Low likelihood	Low	~30%
Unlikely	Very low	~10%

3.1.3 *Project risk understanding: risks collection and communication*

A project risk register is updated throughout the entire life cycle of the project to ensure quality of the final delivery. In this work we found that some partners experienced difficulties to understand what the project risk register is, why this project register is separated from the technical risks register and what they should report into. To make every partner aware of the possible risks and remind them their responsibilities, 1-to-1 phone calls were arranged with each responsible person a week before the TMT meeting. This approach allowed more specific explanations and focus only on the concerns of each WP. These calls were first scheduled to 0.5 hours in order for the risk manager to explain the method to the partners. Then the time was reduced successively as the project risks were resolved or identified. In the first meeting with each WP the entire risk register was discussed. In the next meetings, the project risk register was communicated selectively according to the risk relevance for the WPs. The risk register file containing the latest updated version of all risk was shared with everyone. Later, only the changes to the risk register were presented to simplify and shorten the meetings even further.

3.2 Management of privacy, safety and security in the product

3.2.1 *Process*

The principle of the E-LAND toolbox is to analyze a combination of data to determine an

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference

4346

optimal scheduling on when to produce, store, buy and sell energy. The computations are based on the following data:

- Market history with current and past prices
- Weather forecast and weather history data
- Energy consumption history
- Energy storage and production capacity

To answer to the end-user's requirements, a list of nine high-level use cases, technical functions and business requirement have been defined for the toolbox (E-LAND D3.2, 2019) and are further developed in a technical specification which is confidential. The risk assessment process for cyber and information security was based on ISO 27002 (ISO-27002, 2013) and NIST 7628 guidelines (NIST-7628, 2010). To prepare the risk assessment, a part of the technical documentation and functionalities of the toolbox has been shared with the team. However, the final architecture was not established during this activity and we expect further iterations during development.
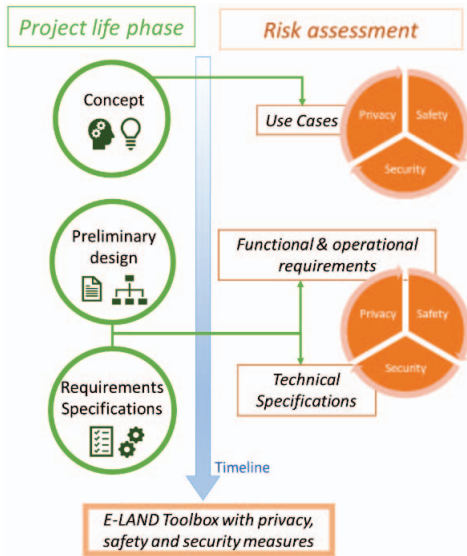

Fig 2: Risk management steps: risk assessment depending on the use cases and the specification, to establish the safety, the security and the privacy mitigations.

The risk assessment was first conducted at a high-level given that the toolbox knowledge at this time of the project was limited. The risk identification was performed before the integration and the development of the toolbox, following the protocol described in Xueli et.al. (Xueli et. al., 2020) based on the most relevant user case scenario, which included all aspect of the solution. Figure 2 describes the different steps on a timeline.

For the use case definition, the functional and operational requirement identification, and the technical specification, risk analysis was performed to identify risks pertaining to safety, security, and privacy. The solution in E-LAND will include, either through storage or through connecting information sources and stakeholders, and there are clear risks connected. For example, in order for information management to be in accordance with new regulations from European commission regarding the privacy on data collection by enterprises, the risk regarding the data collection must follow the same regulation. In the following we present examples of risks and their belonging mitigations from this activity.

3.2.2 *Proposed mitigations related to safety, security and privacy risks*

A list of 14 mitigations has been proposed in a high-level detail action, according to the template in Table 4.

Table 4. Mitigations template relative to the security and privacy risk identified for the E-LAND toolbox.

Proposed mitigation ID	Mitigation unique number
Title	Short title of the mitigation
Description	High-level description to detail the scope of the mitigation
Risk	Description of the risk
Rationale	Description of why the mitigation is asked
Risk Owner	Responsible of the Risk
Component	Component of the architecture or concerned asset
Risk Category	Origin of the risk
Verification Measurement	Input of potential solution measurement (proposal)
Source/Related Requirements	link to the functional requirements and the business case directly affected by the risk.

The mitigations are relevant for privacy, security, and cybersecurity. They are used in most use

cases and business scenarios and applicable for all data storage device. This format was chosen in order to simplify the communication to all the partners

3.2.3 *Privacy risk and further steps*

To enable the best energy management, the E-LAND solution is collecting different types of data such as names, addresses, emails, energy consumption, etc. Although privacy was an area of focus, there was first unclear how to tackle this part of the project. The assessment of privacy early in the solution design was limited as there was not enough details at this point to make accurate assessments. The responsibilities and ownership to the solution was not clear. The project was setup differently than the typical organization-user relationship, having several independent partners with their own tasks and deliveries. Determining who would act as Controller and Processors was a challenge. Concerns were expressed when installing and using the toolbox on the pilot sites without any privacy notice.

To address this, we defined a process to gather the data and perform the assessment in the project. We based the process on the General Data Protection Regulation (GDPR) guidelines and templates provided by official supervising authorities (EU GDPR). The following section describes the proposed process to gather information needed for the assessment.

Preparation activities: Technical solution documents were used for creating an initial assumption about the extent of personal data in the toolbox. Based on this a questionnaire was sent to WP leaders to supplement the documentation. An additional goal for the questionnaire was to create awareness and introduce concepts early in the process. In the future, meetings presenting more detailed definitions of personal data will be held with WP leaders. The goal is to make sure everyone has a common understanding of what is considered as personal data and thereby minimizing the risk of missing something.

Data collection and assessment: After the initial meetings, individual meetings will be scheduled with key persons to gather the required details. The result will be documented in a spreadsheet. The output of this phase should be to document how the application collect and process personal data and draft appropriate privacy notices.

Risk assessment: Risk assessment on personal data was a part of the earlier assessment on the system design documents. However, since we did not have a full overview at the time there should be a reassessment once we have completed the data collection. The type of data collected will determine the extent of the risk assessment. If the collection and processing of personal data can put the natural person's privacy rights at risk, the controller is required to carry out a Data Protection Impact Assessment (DPIA). DPIA is a structured way to assess the risks involved in the data processing. While risk assessments conducted in an organization commonly considers the impact on itself, and in some cases health and environment, the DPIA assess the impact on the data subject. The DPIA must be documented. Various templates exist and one may choose freely, for instance the template provided by the European Commission (EU, GDPR).

4. Discussions

4.1 *Evaluating the project risk management process*

One of the main challenges was to decide on which risk management approach would be the most beneficial for the partners as a lot of freedom was given by the board at the project initialization.

According to direct feedbacks from our partners, the 1-to-1 calls were well received and were considered as an easy way to communicate due to the availability of the person in charge of the risk management and the short duration of the required meetings. From a risk manager point of view, direct phone calls enable us to verify that the understanding of the risk status was correct and that the risk was communicated and understood by all WP leaders. One of our initial concerns was that the term "risk" was not interpreted the same way by everyone. The 1-on-1 calls gave the opportunity to clarify the risk management (depending on the needs, background, or part of the project where the partner is involved). For example, the partners frequently asked to explain a specific vocabulary or the reason of some risk inclusions to the risk register that only affected a narrow part of the project and which even might not impact their own WP. Discussions were further refined through providing precise information for risk description, likelihood, or impact of each project risk for each relevant WP in order to improve understanding in time-restricted meetings.

As a risk manager, being able to ask questions and get additional information from the WP leaders when recording new potential risks, helped in understanding the potential cross linked between each part of the project. Such understanding might reduce the probability of missing risks. Further, the risk manager can be better to identify cross-WP and project wide risks. By encouraging commitment and assist the risk understanding, the WP leaders has considered some project risks that were not highlighted at the

Proceedings of the 30th European Safety and Reliability Conference and
the 15th Probabilistic Safety Assessment and Management Conference

4348

beginning of the project, while the project risk register is sometimes not considered as important. The 1-on-1 calls provided flexibility for the parties involved compared to larger meetings and ensured that everyone had the opportunity to talk and directly express their opinion and concerns on risk for both current and future work. Additionally, the 1-to-1 phone call provided a human-connection element as opposed to update requests by email. This we found contributed towards building trust and commitment among the participants and lessened the threshold for contact between the people in charge of the project risk management across the WPs.

As the E-LAND project constitutes a multinational group, we would argue that this way of working reduced the possibility of missing risks as it counteracts participants differences. Being engaged and finding it easy to voice questions and concerns we believe is a key element of good risk management. On the contrary, a drawback of this method is the time used by the risk manager to update the project risk register. As more risks are identified the time needed will increase severely with the individual meeting approach. The risk manager being mostly one person also introduce a single point of failure motivating a solution where a risk-informed board, with a full project overview, is in charge of the risk register.

4.2 *Evaluating the technical risks assessment and mitigations*

Even though our general understanding is that mitigations have been well received and understood by the partners, the definitions of and the distinguishing between, security, safety and privacy might have been even more clear to the project partners had they been discussed to more detail earlier in the project. Regardless, in our experience this was done sufficiently early (prior the development phase and in accordance with the scheduled deliverables) to include requirements as to ensure a safe and secure final product. As the project is currently still in the development phase, the following main actions are planned to follow up risks:

- Continue the regular contact meetings with partners and focus on individual risk mitigations for the solution
- Support individual partners in choosing the right methodologies and approaches to realize the suggested mitigations.

The two suggested actions are motivated from the risk of lacking clear decision makers and risk owners at the projects' edges, i.e. close to where (most) mitigations must be realized. For example, we found that assigning risks on cyber and

physical security was difficult without a defined hierarchy and risk ownership in the project. Compared to a single company or organization where risk ownership is clear from the hierarchy, sorting out risk ownership and responsibilities in a multi-partner project is more challenging. When it comes to risks that can only be mitigated through a joint effort from several stakeholders, this is especially the case. From a project point of view, strong leadership where risk ownership is taken early and distributed clearly during the project, is needed to ensure that risks are managed to a comparable level to that of risk-mature organizations.

4.3 *Challenges pertaining to definitions and understanding - privacy risks for sharing consumption data*

Privacy is often mentioned as a challenge when smart grids, smart metering, IoT and other data capturing methods are involved. Therefore, there was a general awareness of privacy from the start of the E-LAND project. Privacy and GDPR compliance were included in the tender, the risk process planning and the use case risk assessment. During the project we experienced that the different partners had different experience and expectations to privacy, GDPR and information management in general. The understanding of individual responsibility to fulfill privacy requirements was variable among the project participants. Our experience from other projects indicates that this is not in the least unique for E-LAND. In this regard for the risk manager to solely request information is not sufficient, instead one must proactively inform and empower participants by explaining what type of information is needed, providing templates and being available to answer questions. We experienced that for some data, decisions are required, or follow-up evaluations are needed. Therein, that the risk manager has the authority and resources to ensure these are undertaken is critical in the project.

5. Conclusions

5.1 *Lessons learned*

Experience from the E-LAND project has shown that the difference between project risk and technical (product) risks seem to be unclear for many. Even among those with a safety and/or security background there are discussions on this topic. In business it might happen that requirements are predominately motivated by functionality and not necessarily from an overall focus on all aspects, in which case privacy and cyber security risks might be unclear, underestimated or even neglected. One takeaway

in this regard is to provide definitions and descriptions early to ensure that there is a uniform understanding of safety, security, and privacy concepts. E.g. for privacy we suggest introducing GDPR role definitions in the beginning of a project to establish an early understanding of Subject owner, Controller, Data processor and Supervisor roles. Further, an information asset inventory should be established to identify required data for the product, and map this to the roles (above), system owners and stakeholders.

Having individual risk management meetings with single WP's leader seems to have a positive effect. As mentioned, to provide the risk manager with the ability to address specific risks, issues and questions for each WP, lowered the threshold for asking questions, and additionally this provided for better socializing than what is usually achieved in large meetings. In our experience this is well worth the extra costs of individual meetings, especially given the variation in concept understanding among the project participants.

Balancing product and process risk management across stakeholders with different practices pertaining to risk is nothing short of challenging. Agreeing early on methodology and responsibilities for following up the different risk types can save considerable work, and more importantly result in a safer, more secure, and better product. Although this has been said before, allowing efforts early to agree on the way of working, even if that means that some stakeholders have to do things a little bit differently, we believe is well worth it from the overall project point of view.

5.2 *Conclusion*

This paper has presented risk management in the ongoing E-LAND project with a particular focus on information assets and challenges pertaining to privacy. The role of the project's risk manager has been explained and the work activities undertaken by the risk manager has been described in more detail. The E-LAND project is currently in its development phase and the next steps concerning data and privacy management, as well as how to follow up the different work packages were presented. An important challenge identified in the project relates to a difference in understanding and experience among the project participants concerning product and process safety management. Lastly, lessons learned and takeaways from the project has been presented.

Acknowledgement

References

E-LAND website: https://elandh2020.eu/ (last visited 13.02.2020)

E-LAND 3.2, Functional and operational requirements, E-LAND public deliverable, 2019.

EU GDPR, General Data Protection Regulation, website: https://gdpr-info.eu/ (last visited 13.02.2020)

INCITE, EU Smart Grid Project, website: http://www.incite-itn.eu/blog/introducing-microgrids-local-energy-communities/ (last visited 13.02.2020)

ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls

NISTIR 7628 Revision 1 2010, Guidelines for Smart Grid Cybersecurity", Available: https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf (last visited 13.02.2020)

X. Gao, C. Esnoul, P.A. Jørgensen, S. A. Olsen and B. A. Gran (2020). Risk Assessment in the E-LAND Project, Paper accepted for ESREL 2020.