E-LAND

PRIVACY, SECURITY, AND SAFETY

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 824388

E-LAND

Integrated multi-vector management system for **E**nergy is**LAND**s

Deliverable nº:	**D4.7**
Deliverable name:	**Privacy, security, and safety**
Version:	**1.0**
Release date:	**20/11/2020**
Dissemination level:	**Public**
Status:	**Submitted**
Authors:	**IFE - Coralie Esnoul**
	IFE - Silje A. Olsen
	IFE - Bjørn Axel Gran
	IFE - Xueli Gao
	IFE - P.-A. Jørgensen
	IFE - Julia Wind
	IFE - Preben J. S. Vie
Contributors during risk assessments:	
	ICOM, UdG, RLI, BIKS, INYCOM, UVTgv, SE

This project has received funding from the European Union's Horizon 2020 Research and Innovation programme under Grant Agreement No 824388.

Document history:

Version	Date of issue	Content and changes	Edited by
0.1	01/11/2020	First draft version	Team at IFE
0.2	16/11/2020	Updated based on peer review	Team at IFE
0.3	20/11/2020	Updated section 2.2 and 5.4 based on peer review	Team at IFE
1.0	20/11/2020	Minor edits for publication	Joseph Negreira

Peer reviewed by:

Partner	Reviewer
BIKS	Per Olav Dypvik
SIN	Sanket Puranik

Deliverable beneficiaries:

WP / Task
WP3 / T3.2 - T3.3
WP4 / T4.1 – T4.6
WP5 / T5.2 -T5.4
WP6 / T6.2-T6.3
WP7 / T7.2-7.3
WP8 / T8.1

Table of contents

Abbreviations and Acronyms

Acronym	Description
5G	Fifth-generation wireless
ALARP	As Low As Reasonably Practicable
API	Application Programming Interface
CO_2	Carbon dioxide
DER	Distributed Energy Resources
DPA	Data Protection Authority
DPIA	Data Protection Impact Assessment
EF	Energy Forecast
EMA	Energy Management Application
EMS	Energy Management System
ENISA	European Network and Information Security Agency
ESB	Energy Service Bus
ESREL	European Safety and Reliability Conference
GDPR	General Data Protection Regulation
HMG	Her Majesty's Government
ICO	Information Commissioner Office
ICT	Information Control Technology
IFE	Institute for Energy Technology
IS	Information Security
IT	Information Technology
ISO	International Organization for Standardization
KPI	Key Performance Indicator
LES	Local Energy Systems
NIST	National Institute of Standards and Technology
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation
OT	Operation Technology
OWAPS	Open Web Application Security Project,
PMC	Project Management Committee
PSAM	Probabilistic Safety Assessment and Management Conference
PUC	Primary Use Case

Acronym	Description
PV	Photovoltaic
RES	Renewable Energy Resources
SA	Supervisory Authority
SUC	Secondary Use Case
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges
TMT	Technical Management Team
UC	Use Case
UVTgv	Valahia University of Targoviste
WP	Work Package
WPL	Work Package Leader

Executive summary

The goal for E-LAND, is to support the decarbonisation of energy islands and isolated communities by developing an E-LAND Toolbox for Multi-Energy Islands, implement the toolbox and demonstrate the viability and impact of the tools and methods created in 3 locations in Europe. In doing this, the E-LAND final product must not add risk in the management of energy. Thereby, a risk assessment should ensure that the concept, the solution, and the application delivered in E-LAND are safe, secure, and reliable. This report contains Deliverable D4.7 – Privacy, security, and safety. As part of describing the risk management, also the ownership of risks are elaborated upon.

As a large variety of risk analysis methods are available, spotting the appropriate methodology is not obvious considering the number of business use cases and technical requirements. Here we present the risk assessment approach applied in the E-LAND project. Risks and vulnerabilities are identified at a sufficiently detailed level to provide mitigation input to the architecture design, starting from the use case level. Addressing cyber security threats in an energy island is about balancing technical infrastructure and assets risks with business needs and protecting data from unwanted or unintentional information disclosure. This report summarizes cyber security risks relevant for energy island and addresses the challenges in applying risk analysis methods and describes how these challenges were met.

Furthermore, this report describes the project risk management for the E-LAND project and gives examples for future potential users on 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 report 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. The tools used in E-LAND for communication provides, as fare as the team has evaluated, an innovation. In order to reduce risks and optimize the potential of the solution, knowledge about relevant information pertaining to each stakeholder should be easily available This information has been shaped as flyers to be easily accessible, short, precise, and in illustrative way.

Finally, batteries play a crucial role in localized energy storage and are thus a crucial asset when it comes to reducing the overall environmental footprint and eventually CO_2 neutral energy islands. In an appendix some guidelines and recommendations for the use of batteries are provided.

1 Introduction

1.1 The E-LAND project

The continued decarbonisation of the energy sector using renewable energy sources provides both interesting opportunities for Local Energy Systems (LES) and challenges for existing electricity networks. Mainland regions such as isolated villages, small cities, urban districts, or rural areas often have issues with weak or non-existing grid connections. These areas are known as energy islands.

The goal of the European-funded H2020 project E-LAND is to provide a synergistic solution between technological, societal, and business challenges that the energy sector faces. The main outcome will be the E-LAND Toolbox – a modular set of methodologies and ICT tools to optimize and control multi-energy islands and isolated communities. The modular toolbox can be customized to meet local requirements and is expandable to incorporate new tools as new challenges arise.

1.2 Purpose

The main delivery of the E-LAND project is a toolbox containing a set of modular methodologies and ICT tools to control and optimize energy islands and isolated communities. Sufficiently safe and secure solutions are prerequisites for the realization the project, which contains and contributes to a wide range of risks such as project risks, technical risks, information security risks and cyber security risks to name a few.

The purpose of this document is to define the methods and approaches that has been applied to identify risks, point to some of the risks and their mitigations and pinpointing the plans and needs for following up on these risks during piloting and in future business cases. This report takes as input the risk management approach (see delivery D1.3, [1]) laid out at the beginning of the project, the Use Cases Definition (see delivery D3.1, [2]) and the Functional and Operational requirements (see delivery D3.2, [3]). The risk analysis conducted provided a set of mitigations as input to the Technical Specification (see delivery D3.3, [4]), which are followed up in the other work tasks under WP4. The risks and identified mitigations should be monitored in the pilots and are therefore important input to WP5 and WP6. Finally, some of the risks will also affect future operation involving the E-LAND toolbox. Therefore, this report provides useful

input to WP7. When future users of the E-LAND see that the project has addressed privacy, safety and security in a proper manner, it will thus provide trust to the E-LAND toolbox.

The document addresses two types of stakeholders: roles associated with the development of the system (i.e. SW designers and developers), and roles associated with operation of the system (i.e. end-users). The method, results and experiences from this work are published through 3 conference papers at the PSAM-ESREL conference, [5] [6] [7].

Finally, for any energy island there are objectives to produce green energy locally, use energy efficiently, reduce peak loads by applying energy storage systems, assisting in balancing renewable energy sources and thereby significantly reduce CO_2 emissions. In doing this, batteries play a crucial role in localized energy storage and are thus a crucial asset when it comes to reducing the overall environmental footprint and eventually CO_2 neutral energy islands. To ignore aspects of batteries would therefore trigger a risk to the efficacy and usability of the E-LAND toolbox. Details on this can be found in Appendix A: The role of battery safety in energy islands.

1.3 The challenges relative to privacy, security and safety risk in E-LAND

Digitalization is permeating domains and society. Within the energy sector, we witness how novel technologies and solutions are employed to become cheaper, reliable, smarter, and greener. The high cost of modernizing and renewing electrical infrastructure is a main driver for exploring the use of inexpensive technology and novel solutions to achieve more functionality and realize higher potential from existing infrastructure. Innovative and economically viable solutions for extending the lifetime of current energy infrastructure are a challenge to provide. Smart grid is one approach for extending this lifetime. A smart grid is basically an energy grid with two-way communication, and typically connected technologies and advanced sensors are introduced which transforms the energy grid from analogue to digital. This connection allows for scheduling and planning of future energy use by enabling grid actor communication. The digital transformation has made cyber security a central challenge for the energy grid. When multiple digital systems are connected in new ways (e.g. internet of things and 5G) as this is the case for the distributed renewable energy resources (RES), storage assets located at the edges of the electricity grid, and distributed computers for decision making, cyber security becomes complex. For the energy utilities and Local Energy Systems (LES) owners, the connected grid presents possibilities that creates more revenue and value, but at the same time introduces

potential safety and security related issues. For example, for the operating- and ICT system landscape, new digital risks could disturb the stability and operation of the grid.

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.

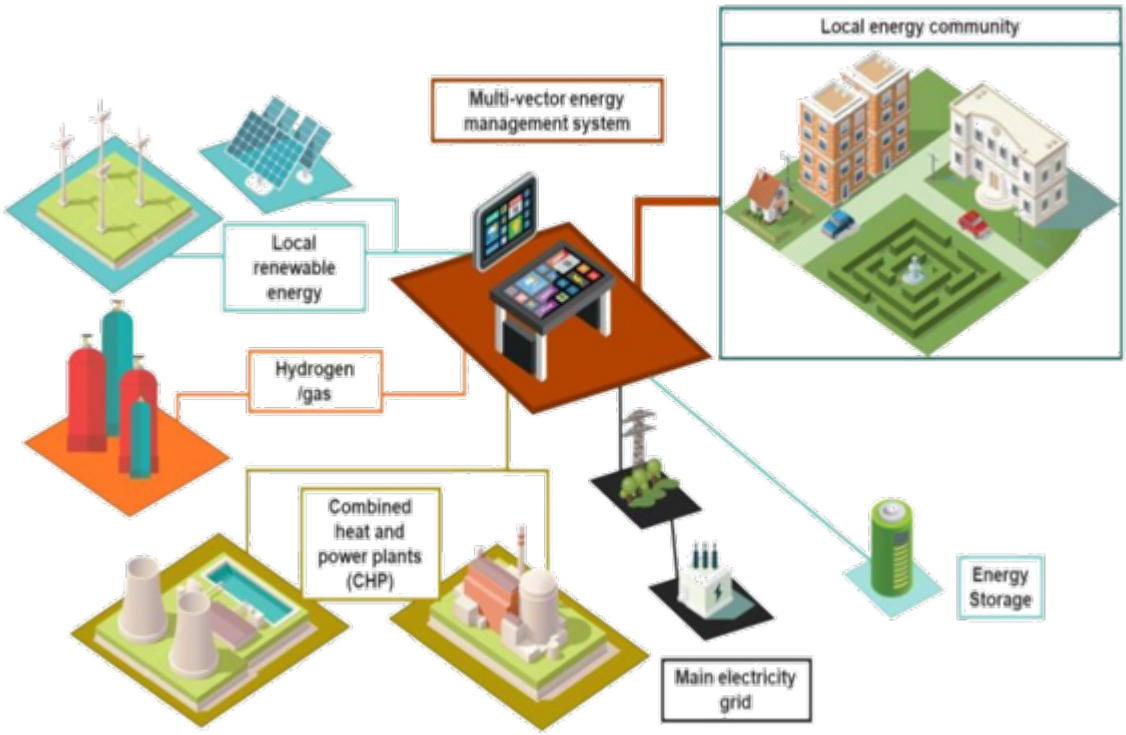


Figure 1: Inclusion of the E-LAND toolbox in the decision process (published in [6])

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 is important to identify potential risks in order to define adequate information security and system security requirements. These risks and mitigations are followed up in a dedicated project risk register.

1.4 Organisation of this report

The remainder of the report is structured as follows:

- section 2 provides a high-level introduction to how we address risk in the E-LAND project and address how cyber security risks are addressed generally;
- section 3 goes into detail on the risk identification process and provides examples from the use cases;
- section 4 describes the results of the risk assessment with the provided mitigations;
- section 5 proposes a process with a follow-up plan to assure a safe and reliable use of the toolbox. This section also proposes a draft of guidance for the pilot site to choose the solution to manage their energy;
- section 6 concludes on the main findings of the risk assessment and highlights the future work.

Detailed information of the process can be found in appendixes:

- Appendix A described the role of batteries;
- Appendix B provides an overview of the risk assessment through a set of flyers;
- Appendix C detailed the privacy notice template related to the data privacy.
- Appendix D gives the template for the mitigations addressed for E-LAND Toolbox.

2 Background on Risk assessment and management

2.1 The risk management process

IFE has the role as risk-manager in the project with the responsibility of following up existing risks, as well as identifying new risks during all project phases. IFE's risk management team consists of personnel with risk, safety and ICT security competences, who is responsible for performing the day-to-day overall risk management of the project. This includes monitoring all project activities as they are performed and to ensure risks are attributed to a risk-owner and handled. The risk management process is based on the guidelines ISO 27005 [8], ISO 27002 [9] and NIST 7628 [10]. The ISO 27005 is sued as a basis and is described further in section 2.4, while the ISO 27002 and NIST 7628 are used as supplements. This is further explained in section 2.7.

2.2 The importance of the technical risk management

The "Swizz cheese model" (Figure 2) is often used to illustrate how hazardous situations occur. The cheese sizes represent safeguard, systems, processes etc. The holes represent vulnerabilities or failures. A single vulnerability or failure can have no consequence on its own, but several such "holes" lining up could lead to a hazardous situation.

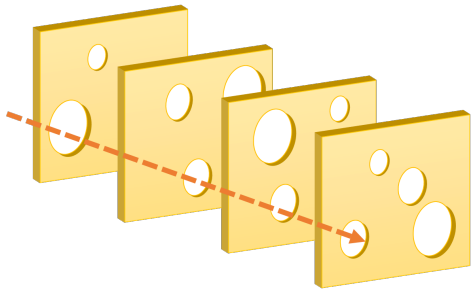


Figure 2: Swizz cheese accident model

The introduction of digital systems, where software allows for unlimited complexity, have made identifying and eliminating holes challenging. Though systems are developed with the intention to be secure, accidents still happen. Even in industries were safety is regarded as a top priority, and accidents could cause severe economic losses or major injury or death, there are many examples of situations that led to accidents:

- A navigation error caused NASA's Mars Climate Orbiter to miss its intended position [11]. Mismatch between units, causing the probe to miss its intended position in orbit and disintegrate in the Martian atmosphere;
- Analysis of the Boeing 737 Max crashes in 2018 and 2019 point to several things that contributed to the accidents [12]. A faulty design and assumptions created a vulnerability in the airplane support systems, and omissions and errors made through the design and certification process. Analysis of the 2018 accident also revealed shortcomings in the carrier's procedures or failure to follow them.

2.3 Managing different types of risk

The risk management process, described in delivery D1.3 [2], addresses the common rules to be respected when preparing for and managing crisis situations (as set out in the new risk preparedness regulations). The results are (i) a strategy for risk evaluation towards agreed acceptance criteria, (ii) an early identification of potential risks, (iii) development of mitigation and requirements for the non-acceptable risks, and (iv) needs for risk monitoring.

The process includes following up on risks towards project goals and risks related to the functionality of the toolbox, here referred to as *technical risks*. Though the risks are connected, the process for managing them are separated as they involve different activities, different actors, and the analysis results serve different purposes as seen in Figure 3.

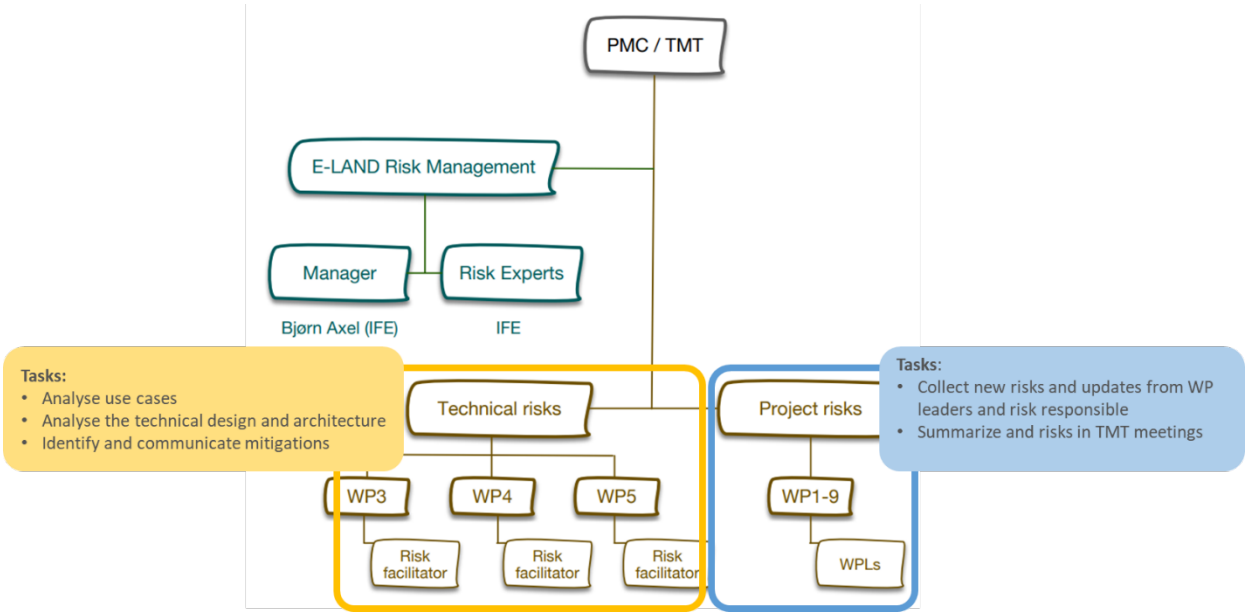


Figure 3: The risk management process covers the whole project. The risks are followed up differently based on type (figure taken from the E-LAND risk management process D1.3 [2])

Project risks affect goals such as keeping timelines and meeting KPIs for stakeholder engagement. However, achieving such goals does not automatically result in a reliable design of the toolbox. The toolbox is designed based on the requirements identified from the use cases. Though the requirements are fulfilled in the design and implementation; they may not cover scenarios caused by unwanted and unexpected incidents. It is these gaps that the technical risk assessment aims to uncover. Knowledge of the gaps makes it possible to implement mitigations.

As also shown in Figure 3 we organize risks in two main groups with individual subgroups [2]. Risks tied to the project management and execution may affect schedule and the project deliveries. These risks are handled as a part of WP1 (Project management).

The other group are risks tied to technology and are risks that can degrade the solution when implemented in the pilot cases. These are further divided in risks tied to privacy, safety and security. The technical risks are a part of the deliveries in WP4 (Multi vector energy management), but the assessments are performed in collaboration with WP3 (Use case development) to provide input on the toolbox design at an early stage. Identified mitigations are also provided as input to WP5 (System integration and Realisation).

As a part of the risk management process described in delivery D1.3 [2], a risk reporting hierarchy is defined. Initially, at partner level (partners involved in each WP), the partners may identify situations or events in a particular area of the project that can lead to the occurrence of a determined risk. This could typical be a technical risk related to a specific use case or a set of use cases. At this point the issue has become a part of the E-LAND technical risk register.

The identified risks should then be communicated to the work package leader (WPL) in order to share suggestions and to spread the perspective of the exercise. Being the person responsible for the WP, the WPL will summarize and analyse the risk, and determine if the risk should be submitted to the consideration of the TMT or the PMC. This is done when the WPL consider that the risk can have a negative impact on the E-LAND project. Criteria for evaluating this are project internal and documented in D1.3 [2]. At consortium level, the TMT / PMC take the decision to include or not each submitted risk into the dedicated E-LAND project risk register. Starting from that moment, the included risk is considered a potential risk of the project and will be managed following the rules stated in the risk management process. The TMT or the PMC will qualify the identified risks and assign a risk “owner”.

The ownership of a risk is dynamic and changes depending on the phases of the E-LAND project:

- during the specification phase the risk typical is owned by the party that is responsible for the development of the specification;
- when the specification is handed over to implementation, the implementer becomes the owner of the risk;
- when the tool, algorithm, service etc is then deployed at a pilot site, the risk becomes a shared ownership. The pilot site will have ownership to the risk because they have to take the consequences of a risk actual occurring. However, the provider of the tool, algorithm, service also has a ownership to the risk, since they may be put responsible for compensating for the consequences. Finally, also the E-LAND project will have ownership to the risk, because the reputation of the E-LAND project may be impacted, and the business possibilities may be reduced.

2.4 Risk assessment methodology

This chapter introduced a general methodology description the risk assessment. The risk assessment process for cyber and information security is based on ISO 27005 [8]. According to ISO 27005, with the identified basic criteria, the scope and boundaries, and the organization for the information security risk management process being established, the risk should be identified, quantified or qualitatively described, and prioritized against risk evaluation criteria and objectives relevant to the organization.

Implementation guidance from ISO 27005:

A risk is a combination of the consequences that would follow from the occurrence of an unwanted event and the likelihood of the occurrence of the event. Risk assessment quantifies or qualitatively describes the risk and enables managers to prioritize risks according to their perceived seriousness or other established criteria.

The risk assessment consists of the following activities:

- Risk identification;
- Risk analysis;
- Risk evaluation;
- Risk treatment.

Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist (or can exist), identifies the existing controls and their effect on the risk identified, determines the potential consequence and, finally, prioritizes the derived risks and ranks them against the risk evaluation criteria set in the project. These were set as part of the risk management and contingency plan (see deliverable D1.3, [1]) and are repeated in section 2.5.

For all identified risk, a risk treatment plan should be defined to control the risks. If the risk is not acceptable towards the defined acceptance criteria, the mitigation actions should be allocated. Information about risk should be communicated and/or shared between the decision-maker and other stakeholders. The risk management process is illustrated in Figure 4.

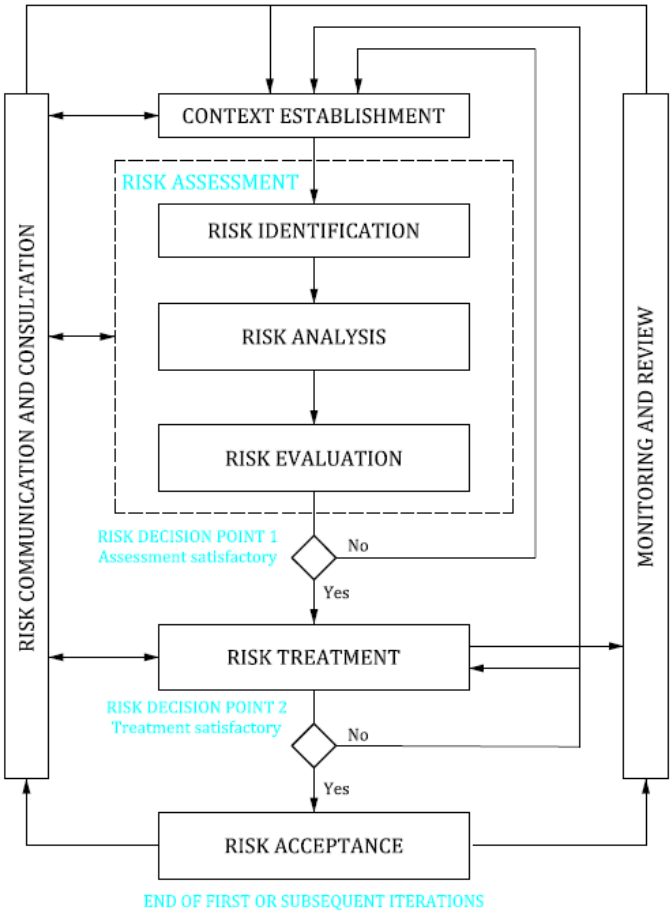


Figure 4: Illustration of an information security risk management process. (Figure 2 in ISO 27005, [8])

In this report, how the risk assessment is performed in E-LAND is further described in section 3.3 through a step-by-step process. The risk assessment was performed in an iteration process. First, a preliminary level assessment was performed on the use case level to identify potentially high-level risks. This was done by a team consisting of a risk facilitator, risk experts, ICT and cyber

security experts at IFE, based upon the inputs provided from the developers. After the E-LAND toolbox architecture was available, a detailed risk assessment was performed with combined information from both use case definition and the functions/data flows defined in architecture. This was done by the same team, but now including sessions with the teams responsible for specifying and implementing the architecture.

For the risks which were not acceptable by the project (see decision prosses described under management of risks in section 2.3, and risk acceptance criteria in section 2.5), mitigation actions were allocated. Furthermore, the mitigation actions were communicated by risk manager to project for implementation. The risk manager is continuously monitoring and following up the implementation status for risk evaluation. If the remaining risks are still not acceptable, a new round of risk assessment process will be performed until the all the risks are controlled within the accepted level.

2.5 Risk Criteria used for E-LAND technical risk management

The basic criteria used for E-LAND technical risk management are defined at the beginning of the risk management process and is presented below.

Risk evaluation criteria: threat event occurrence as it was ranked in the risk assessment planning phase in the project is provided in Table 1.

Table 1: 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	

Impact criteria: the Risk Impact Level used in the assessment was determined in the risk assessment planning phase is shown in Table 2.

Table 2: 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 operations, assets, individuals, organizations, etc.
Very low	Minimal or no consequence on operations, assets, individuals, organizations, etc.

Risk acceptance criteria/Risk Matrix: the Risk acceptance criteria was determined in the risk assessment planning phase is shown in .

Table 3. The colouring describes three outcomes:

- Acceptable (green) meaning that no mitigation strategy is needed;
- ALARP - As Low As Reasonably Practicable (yellow) meaning that the risk shall be evaluated, but that the mitigating strategy should be evaluated with respect to if it is reasonable practicable – e.g. due to cost, technology, etc;
- Unacceptable (red) meaning that a mitigation strategy is required.

The risk mitigation strategy could be to accept (Recognizing residual risks and devising responses to control and monitor them.), avoid (Seeking to eliminate uncertainty), Mitigate (Reducing the probability and/or severity of the risk below a threshold of acceptability) or Transfer (Passing ownership and/or liability to a third party).

Table 3: Risk Matrix

Impact	Very high					
	High					
	Medium					
	Low					
	Very low					
		Very low	Low	Medium	High	Very high
		Likelihood				

Legend: Unacceptable ALARP Acceptable

2.6 Privacy background and definitions

Privacy assessments have been performed on the architecture design to identify the use of private data in the toolbox and possible consequences. The General Data Protection Regulation (GDPR) legislation have been used as a basis for the assessment as it covers so many aspects of privacy related issues. The following sections describes key elements and terminology in GDPR.

GDPR is a European Union directive created to protect an individual's right to privacy [13]. The key element in GDPR is that it is the individual that owns their data they have a right to be informed about why they need to provide the data, what it will be used for and which rights they have after they have provided it. This information is usually provided in a privacy notice.

When it is legal to collect personal data?

To be allowed to collect personal data you must have a lawful basis. One cannot collect it because it is "nice to have" or "might need it later". The conditions for collecting personal data are described in Art.6 in the GDPR legislation and can be summarized as follows:

- **Freely given consent** – It should be clear what the consent is for. Processing is limited to the consent. Controller must be able to document the consent. Consent can be withdrawn;
- **Contract** – Data provided in exchange for a product or service. One can think of it as an individual letting companies and organizations borrow their personal data in exchange for services, products etc;
- **Legal obligation** – For instance records required for financial requirements;
- **Vital interest** – Life and death scenarios. For instance, provide urgent health services;
- **Public interest** – Required to perform official functions required by law;
- **Legitimate interests** – GDPR is a recent legislation and so far, there have been few cases in court where judges have addressed what "legitimate interest" means (lack of precedence). Though the title may sound like it covers many scenarios, it is actually very strict. If one is unsure if the data collection can be based on this lawful basis it is probably wise to consult legal experts.

The organization collecting the data is required to assess and document all these elements to show they are complying with the GDPR directive.

Privacy notice requirements

The privacy notice is a part of the Subjects right to be informed. It must:

- be easy to understand;
- be transparent on how the data is used by the Controller;
- be easy to access;
- be presented at the time of collection.

The right to be informed also applies when information is collected from sources other than the individual.

What is personal data according to GDPR?

The definition of personal data is "Any information relating to an identified or identifiable natural person" - Article 4(1). A natural person is an individual human being. In the legislation it is referred to as the data subject, and this is also the term used in this document. For information to be considered personal, it must either be related to the person or make it possible to identify or single out an individual by combining information from several sources. The distinct pieces of information (name, birthday, email, gender etc.) is referred to as data elements. Special considerations are required for sensitive personal data. Example of such data are information about health, sexual orientation and political opinions. A full description of this category can be found in Article 9(1). Anonymized data is not considered personal information, but pseudo-anonymized data are. Note that it is not always possible to anonymize data.

Roles

Certain terms are used for the roles when handling personal data. Each role has their own rights and responsibilities according to GDPR. A brief explanation of the roles as relevant to understand this document are provided in Table 4.

Table 4: Overview of roles in the GDPR legislation

	**Subject**: The individual that owns the data that is being gathered.
	**Controller**: The organization/agency/natural person/authority that collects the information about the subject. Determines the means and purpose of the processing. Can be a shared role. Both controllers and processors have accountability, but controllers have a slightly more responsibility are they are the decisions makers.

	**Data processer**: A service provider that acts on the instructions from the controller. Does not make decisions about how data will be used.
	Supervisory authority (SA)/ Data Protection Authority (DPA): Handles complaints

2.7 Security risk assessment

To balance technical and assets risk with business risk there is a need to better understand the impact of choices and solutions with regards to information risks. Addressing cyber security threats in energy islands is about balancing these technical infrastructure and assets risks with business needs and protecting data from unintentional information disclosure and data leakage.

STRIDE

One way to achieve enough understanding is to apply the STRIDE threat model by Microsoft [14] in conjunction with the domain specific Threat Landscape for Smart Grid provided by the European Network and Information Security Agency (ENISA) [15]. The STRIDE model was invented back in 1999 and adopted by Microsoft in 2002 and is a mature threat-modelling method for identifying computer security threats. STRIDE stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privileges. Applying STRIDE on the detailed system design and the use cases helped us narrowing down from a high-level approach to more detailed level when identifying potential risks and mitigations. It also helps with the identifying new technical requirements early in the development phase.

The ENISA Threat Landscape for Smart Grid was chosen because it provided a developed threat-taxonomy as well as a detailed threat overview for smart grids and was a framework with which we already had good experience.

The STRIDE model dictates that the following questions should be asked for the consideration of a threat model:

1. What are we building?
2. What can go wrong?
3. What are we going to do about that?

OWASP

We applied the Open Web Application Security Project (OWAPS) Application Threat Modelling [16] as the approach for analysing the security of an application. It is a structured approach that enables the identification, classification, ranking, comparison, and prioritization of security risks associated with an application.

NIST and ISO

The Guidelines for Smart Grid Cyber Security by the US National Institute of Standards and Technology (NIST) [17] 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 [18].

NIST-IR 7628 and ISO 27002 standards [9] have been the basis for a report on smart grid security by ENISA [19] which provides a set of specific security measures for smart grid service providers, aimed at establishing a minimum level of cyber security. 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 the Guidelines for Smart Grid Cyber Security by NIST [17], the approaches OCTAVE [20] and HMG IS1 [21] and the tool MAGERIT [22] [23]. Most examples are based on the principles identified in ISO 27005 [8], 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 cyber security 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 because of degraded or loss of services, resulting in injury or loss of life [23].

3 Risk Assessment in E-LAND

3.1 E-LAND toolbox

The E-LAND project aims to realize energy island potential through developing a tool that provides necessary functionality to make well-planned decisions about energy, including estimating future production and consumption.

The majority of the functionalities are realized through digital means, either in hardware, software or both, and the matter of addressing cyber security issues is very important for all project participants. The high-level concept of the E-LAND toolbox in Figure 5 shows the main functional layers of the tools and the connection to the site-specific instances exemplified by pilot cases in the project.

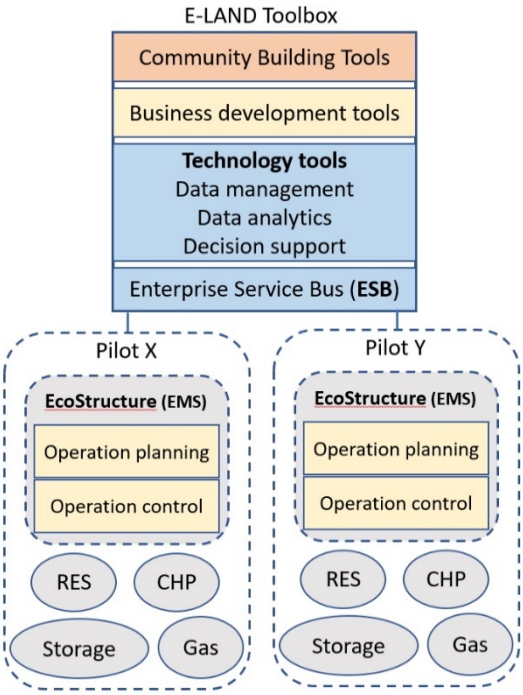


Figure 5: E-LAND Toolbox high level architecture

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 E-LAND toolbox [3] and are further developed in a technical specifications document which is confidential. To prepare the risk assessment, a part of the technical documentation and functionalities of the toolbox was available. However, the final architecture was not established during this activity.

The risk assessment was first conducted at a high-level, given that the toolbox knowledge at this time of the project was limited and before the integration and the development of the toolbox. The risk identification followed the protocol described in section 3.3 using the most relevant use case scenarios, which included all aspect of the solution.

The solution in E-LAND will include, either through data 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.

Another example if for the E-LAND toolbox integration of the following sub-systems and assets:

- EMS: integrating the traditional DER owner energy monitoring and control solution;
- DER Controllers: On-site devices offering monitoring & control of the production assets of DER Owners;
- BMS: offering a monitoring network at a building level (evaluate energy usage/needs, occupancy, production, weather, etc.) as well as assisting real-time, data-driven decisions for the optimization of the consumption, by analysing offering various modes of operation (demand response, store energy) for various vectors;
- Field Devices: for sensing or actuation of various loads, integrated through the BMS or directly;
- External Data Sources: for weather forecasting and energy prices
- Advanced tools (functions): for EF and for optimal scheduling (Optimal Scheduler) and planning
- Enterprise Service Bus (ESB): a system enabling the integration of the above sub-systems

These assets introduce potentially technical risks when developing a toolbox for optimizing a LES. A more detailed overview of internals of the E-LAND toolbox, the components of the external sites and their interconnections can be found in Figure 6.

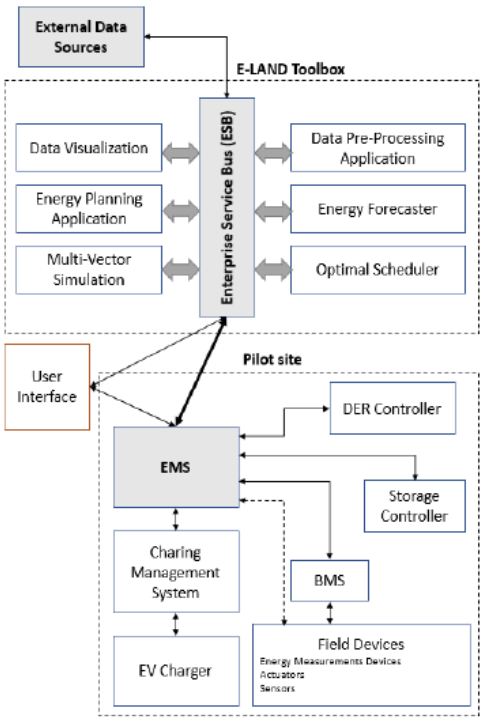


Figure 6: Components of the E-LAND toolbox and the Pilot sites

3.2 E-LAND use case

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 was used in E-LAND project. The different use cases established, such as high-level UC, business UC and device/system UCs, addressing different development objectives can be found in D3.1 [2].

This section takes a technical point of view, focusing on devices and system use cases which was further expressed through a set of Primary Use Cases (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 on a lower level. A SUC is more granular, less abstract, and describe core functionalities that are used by multiple PUCs.

In the following focus is on a specific PUC with one relevant SUC as described in the following. There are several SUCs defined in project. Here is SUC 01 is described an example. The use case numbering used corresponds to the numbering used in D3.1.

PUC 04: Optimal scheduling of thermal and electrical storage

PUC 04 models the optimal scheduling and 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 CO_2 emissions and costs and optimize the use of Battery Energy Storage System. 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 CO_2 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.

Step 1 - break down of use case

With the defined PUC and SUC, we can 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, where 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 the input for the risk assessment and will help to identify specific information assets. Since the risk analysis establish the linkage between different level use cases, the risk analysis retains the traceability and allocate consequence to prior identified risks at the lower level of use cases.

Step 2 – identify assets

The identification of relevant assets is preferably done based on low-level use cases. An architecture description established in project is a good tool to identify the information assets. When categorising information assets, the ENISA/EG2 report "Proposal for a list of security measures for smart grids" can be used as reference [19]. 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 [23]. 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 EF software module.

The identified asset can be categorised as an Information Asset.

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

Step 4 – Threats identification

There can be several threats linked to the identified potential risks. In this step, the expert judgement is used have a comprehensive analysis. The most critical threats should be registered in the risk table. In addition, ENISA/EG2 report “Proposal for a list of security measures for smart grids” [19] 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 5 below.

Table 5: 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.
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.

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. Reference can made to the NIST Guide for Conducting Risk Assessments [17]. In E-LAND we applied the likelihood rankings shown in Table 1 defined in D1.3 [17].

To analysis the likelihood of different threats, the threat agents with different capabilities, resources and motivation should be assessed with considering the supporting assets, e.g. the different pilot sites in ELAND project provide different influence on the likelihood identification:

- 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.

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 Levels used in the assessment are shown in Table 2.

With risk analysis on the ELAND toolbox at early stage, 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 implemented, the risk item ranking is expected to be improved (i.e. decrease).

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, see .

Table *3* that identifies criticality levels, depending on the impact and likelihood of an information asset being compromised.

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 section 3.4 and 3.5.

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 section 5.

3.4 Model-based threat assessment

The STRIDE model in an E-LAND context with relevant examples identified by the use case analysis is described in Table 6. STRIDE dictates that the following questions should be asked for the consideration of a threat model: 1. What are we building? 2. What can go wrong? And 3. What are we going to do about that?

Table 6: STRIDE - Threat and risk example overview

Threat	Property Violated	Definition	Risk examples from E-LAND
Spoofing	Authentication	Impersonating something or someone else	Pretending to be someone else. A person, system, or a process.
Tampering	Integrity	Modifying data or code	Software configuration changes tapered intentionally by a hacker. Incorrect historical data is provided to the Energy Forecaster.

Threat	Property Violated	Definition	Risk examples from E-LAND
Repudiation	Non-repudiation	Claiming not to do a particular action (audited)	"I have not sent an email to Silje". No audit logging on user and systems calls.
Information Disclosure	Confidentiality	Leakage of sensitive information	Personal (GDPR) information available on the internet. Poorly securing and handling of username and password (identity) in the system.
Denial of service	Availability	Non-availability of service	Web application not responding to user requests.
Elevation of privileges	Authorization	Able to perform unauthorized actions	Normal user access can delete an admin account.

Applying the STRIDE model on the use cases and addressing these questions gives a rapid understanding of the usage and possible high-level cyber security risks with the different components building up the toolbox functionality and the architecture.

Stepwise assessment through applying the STRIDE method on the use case

The development and integration of new functionalities in engineering systems requires a proper analysis and definition methodology to enable the successful identification and understanding of technical requirements. Specifically, for delivering novel Smart Grid functionalities in terms of combined software- and hardware-based advances, the use case approach were functionalities and solutions are applied in a real-life solution has been successful. The stepwise risk assessment followed by the analyse of:

1. individual and cross risk of use cases-based design from UML and described in Use Case Methodology standard [28] to identifying assets/component and critical functions.
3. (2) Identifying cyber threats and cyber security risks using the STRIDE threat model and ENISA Smart Grid Threat Landscape and Good Practice Guide.
4. Suggested mitigations both generic for the project and specific for the use cases.

Due to the high interest of use case methodology, several standardization activities are currently being carried out aiming at providing the fundamental definitions, templates and guidelines which will support such an approach in energy, e.g. the ISO/IEC 19505-2:2012 [29], the IEC 62559-2 standard series [28] and the CEN/CENELEC/ETSI Smart Grid Coordination Group Grid Architecture Model (SGAM) Framework [30]. In the following we provide some examples from Secondary Use Cases (SUC) describing high-level functionality and the intention in E-LAND

toolbox, and we exemplify for SUC2 and SUC6 (below) how applying the STRIDE method helped in identifying those high-level risks.

SUC1: Forecast RES production

The RES production forecaster gives detailed data about the operations of the EF. The EF is a module responsible for providing local RES production forecasts for Photovoltaic (PV) panels, wind turbines and/or solar thermal. With a valid dataset this will provide an optimal schedule and operation of a LES with different time horizons based on prediction for intraday forecasting (e.g. hours ahead), day-ahead forecasting (e.g. day ahead) or long-term (e.g. week or month ahead). The production forecaster correlates historical production data and meteorological data and relates this with weather forecasts to predict future production.

SUC2: Forecast Consumption

The EF module is also responsible for providing the load consumption forecasts (electrical loads, thermal loads, gas loads) concerning intraday forecasting (e.g. hours ahead), day-ahead forecasting (e.g. day ahead) or long-term (e.g. week or month ahead). For this operation, load consumption and weather historical data are required (optionally occupancy related data) and weather forecasts to predict generation from wind turbines and PV panels as well as local consumption. Applying the STRIDE method on these two secondary use cases singled out one main question, namely; **What are we building**? The simple answer was a software module to predict and forecast energy consumption based on historical weather data and demand for energy now or in the future. The next question was; **What can go wrong**? Group brainstorming identified e.g. that there is a risk that no historical weather data is provided to the EF. This could be triggered by threats like unintentional loss, outage through loss of electricity or internet/network connections, intentional damage such as denial of services attacks or loss of field devices. Further we found that the impact of no data can lead to incorrect power generation and consumption that can result in wrong decisions. Lastly, we asked: **What are we going to do about that**? Here we identified that a possible error in validation of the input could break the integrity and that this should lead to a fallback response message with an action that data is not valid. This raises to new requirements such as verifying both external data services and the communication to the Energy Management System (EMS) with:

1. integrity checks for input data before storing to database;
2. integrity of data when calculating forecasts from the database; and
3. check the integrity and validation of the external data for calculations.

SUC6: Field-device communication

This describes the process of the EMS for sending/retrieving data from the field devices of the LES, either directly or through the BMS. EMS is a system responsible for controlling the various assets of the LES as well as for the orchestration of its optimal operation. EMA is a software component that is designed to relay signals to and from the Enterprise Service Bus. The EMS provides a user interface for the day-to-day operation of the LES. Such operations will be operated by the DER Box, which will be responsible for proxying/relaying signals to and from the Enterprise Service Bus and the LES's assets. The scope of this use case is to describe the way in which field data is exchanged from the various pilot sites by the EMS, in order to facilitate the advanced operations of forecasting and optimization as is described in e.g. SUC1, SUC2 and other use cases.

We applied STRIDE the same way for this use case and asked: **What are we building**? An interface enabling communication with field devices for sending and retrieving data. The EMS should have a well-defined Application Programming Interface (API) to provide information regarding the operation of the LES, as well as receive the results of the forecasting and optimization processes. This approach aimed at achieving wider interoperability of the solution, which imposed adaptations to existing field devices provided by an EMS. **What can go wrong?** Group brainstorming identified that there are several possible scenarios that could impact the communication with field devices. Here is a subset of risk triggers identified during the assessment; In correct Sensor readings: (1) errors due to communication or physical sensor failure, (2) sensor firmware has error and data not retrieved. Sensor readings could also be manipulated either by accident (reallocation of sensors) like unprotected storage of data that could lead to accessible data from the network or the storage device placed in a non-secure location and with non-secure protocols. **What are we going to do about that**? A common practice at many sites today, is to collect energy data through the BMS. This is practical since it can use existing infrastructure, it also uses an interface that the building operator is already familiar with. However, it is not ideal in an advanced LES, as the data aggregators for a typical BMS system are not designed to transfer the type and amount of energy data needed. Another practice is to transmit energy data directly to the EMS. This does yield better field data quality, but often incurs a higher cost since there will be two separate data collection infrastructures. Mitigating actions could be to add redundancy on sensors, make sure firmware are up to date, and address physical placement and protection of sensors against external access and compromising factors. For the scenarios where assets lacked data, measurements or values,

rules can determine if available (e.g. previous) data can be used based on the importance of the asset or the quality of the data. A list of 14 mitigations was proposed in a high-level detail action, according to the template given in Appendix D. Risk Mitigation Template. This format was chosen to simplify the communication to all the partners.

The mitigations identified are relevant for privacy, security, and cyber security. They are used in most use cases and business scenarios and applicable for all data storage device.

3.5 Privacy assessment

Technical solution documents were used for creating an initial overview about the extent of personal data in the toolbox. Based on this, a questionnaire was sent to WP leaders to supplement the documentation. After getting an initial overview, further meetings were arranged with relevant WP leaders. The process is recall in Figure 7.

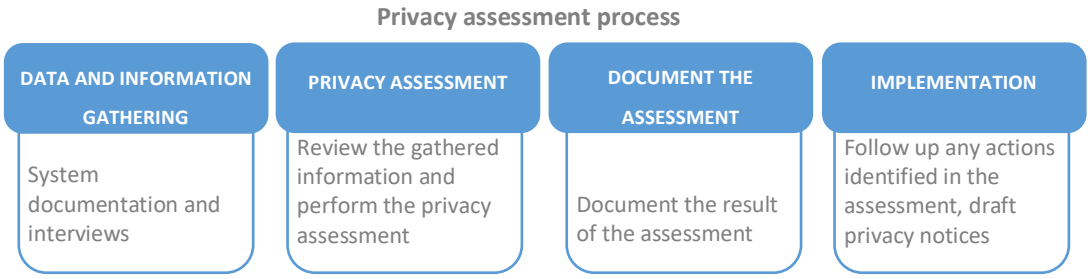


Figure 7: High level process to manage privacy issues

After identifying where personal data was used, assessment was performed and documented according to the requirements. The activities in the assessment is summarized below.

Define data categories and subjects: The type of information collected and from whom. Architectural diagrams of the toolbox were analysed to identify whether or not the different components would use or store any personal information and what that information was.

Data transfers: Reference to other systems if the data is transferred. This required identification of data flows between the main components in the toolbox.

Processing purpose, lawful basis and data source: Description of why the data is needed and what it will be used for. Determine which lawful condition according to Art.6 in the GDPR legislation (see section 2.6) that applies for the collected data. Provide information on whether data is provided by the subject or it is gathered from other sources.

Retention schedule: Clarify when the data will be deleted. Can be either a condition or a date range or both.

The subject's rights: Clarify which rights the subject have; Access, data portability, rectification, objection, erasure. This is mainly determined by lawful basis and what is possible. For instance, data that is provided when the subject is anonymous cannot be deleted. Deleting data provided to fulfil a service the subject has asked for would not be possible before the service has been provided.

Security measures and location of personal data: Clarify how the data is secured and where it is stored. This requires assessment of the cyber security measures in the toolbox. The risk assessment performed on the toolbox, described in this report, was used as input to this task.

Link to consent: If the lawful basis of processing is based on consent, then a reference to the location of this must be provided.

Specification of the controller, processors and contact persons: Identification of roles. Who to contact in the organisation and the Data Protection Officer if required? In situations where a person is interacting with company, for instance registering in a web shop, the roles are easy to identify. The organisation of the project is however very different considering is a funded project operated by multiple partner organisations. There were not many documented examples of similar situations that could be used as a reference. An analysis of how the definitions of the Controller and Processor roles in GDPR applied to the project was performed. A Data Protector Officers was also consulted on this topic.

A privacy notice was drafted using the details gathered. GDPR Art. 13 states which information must be provided to a person when their data is collected. As the required information is specified, there are several templates available. The EU Privacy Policy template was used in this process [13].

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 nature of the data used in the toolbox will determine if such an assessment is required or not. The analysis did not uncover any type of personal data that required a DPIA.

The Controller needs to document that they have implemented the requirements for handling personal data. The documentation can be in the form of text documents and/or spreadsheets. We used a template provided by ICO for this purpose [24] as it had tables that structured the information based on the articles in GDPR. This made it convenient to collect and summarize results and information from the assessment.

4 Results and mitigations

4.1 Technical risk register

A risk register is a living document through the project used to document the identified risks, mitigations, risk assessment process, etc. The E-LAND technical risk register has been issued to the project and documented in WP3 [2], and an outline is provided in Table 7. The complete E-LAND technical risk register is however not displayed in this report as it contains data that should not be displayed in public. It could e.g. be data which someone could misuse to explore potential vulnerabilities in the E-LAND toolbox. Displaying them would therefore be a risk to the business development of the E-LAND toolbox.

Titles for each column together with one example are explained in the following:

- **New ID**: ID number of the risks identified based on use case risk assessment;
- **Previous ID**: ID number of the risks identified from the preliminary assessment;
- **Register date**: the date when risk is identified;
- **Risk owner**: Parties who own the risk and are responsible for following the mitigation;
- **Asset and Asset description**: identified asset group related to the risk.

Example: Historical weather data which is provided from external sources (and EMS as back up) and flows through several systems before it reaches the Energy Forecaster software module.

- **Data, module, component supporting the asset**: more specific component or asset.

Example: The components supporting the asset are: External data source and EMS.

- **Risk Description**: description of the risk scenarios.

Example 1. Incorrect historical data is provided to the Energy Forecaster.

Example 2. Historical weather data is not provided to the Energy Forecaster.

Note: for the example above there are 11 risk scenarios with ID from 1-a to 1-k identified.

(explanation continue after the tables)

Table 7: Outline of the risk register issued for the project (here modified for repeated text to ease readability. Also note that the lines shown do not represent the current state as the technical risk register is a living document) – displayed in three parts

New ID	Previous Risk ID	Registered date	Risk owner	Asset	Asset description	Data, module, component supporting the asset	Risk Description	Risk trigger
1-a	PUC04.1	xx/xx/xxx	ICOM/ Schneider Electric	Information Asset	Historical weather data is provided from external sources (and EMS as back up) and flows through several systems before it reaches the Energy Forecaster software module.	External data source/EMS	Historical weather data is not provided to the Energy Forecaster.	There is no data provided by the external source/EMA.
1-b		10.02.2019	As for 1-a	Information-Historical weather data	As for 1-a	As for 1-a	As for 1-a	As for 1-a.
1-c		10.02.2019	As for 1-a	As for 1-b	Historical weather data is provided from external sources (and EMS as back up) and flows through several systems before it reaches the Energy Forecaster software module.	As for 1-	Historical weather data is not provided to the Energy Forecaster.	There is no data provided by the external source/EMA.
1-d		10.02.2019	As for 1-a	As for 1-b	As for 1-c	As for 1-a	As for 1-c	The provided data is not on the required format.
1-e		10.02.2019	As for 1-a	As for 1-b	As for 1-c	As for 1-a	As for 1-c.	As for 1-d
1-f		10.02.2019	As for 1-a	As for 1-b	As for 1-c	As for 1-a	As for 1-c	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"

New ID	Threats group	Threats (Failure modes)	Impact Description	Impact	Impact reasoning	Likelihood/ Frequency	Likelihood reasoning
1-a	Unintentional loss.	System and service malfunction, loss of service, degraded systems and services, etc.	Lack of data can lead to incorrect power generation and consumption forecast that can lead to wrong decisions that can have economic impact. As the period of lacking data increases the impact increase.	Very high	The forecast module is an essential part of the toolbox and important for project success. Relevant to all PUCs.	Unlikely	Should describe the reasoning for the likelihood level - in this case "The system is designed after XX and YY principles and in accordance with standard ZZ. In addition, not having access to the data does not automatically constitute an incorrect decision leading to a serious economic loss."
1-b	Outage	Loss of electricity, internet outage, etc.	As for 1-a	Very high		Low likelihood	
1-c	Intentional damage	Intentional attacks, Damages from penetration testing, etc.	As for 1-	Very high	As for 1-a	Low likelihood	The likelihood of this is deemed as larger as the included component in the information supply line can suffer intentional damage from a range of sources and attacks.
1-d	Unintentional loss	External data source/EMS receives incorrectly formatted information and sends this information to the Energy Forecaster.	As for 1-a	Very high		Unlikely	
1-e	Intentional damage	External data source/EMS is changed due to an attack and the data sent to the forecaster is wrong/erroneous.	As for 1-a	Very high	As no information is provided for forecasting, malicious attacks changing the information has the same impact as unintentional loss of information.	Low likelihood	As for 1-.c
1-f	Unintentional loss	System and service malfunction, loss of service, degraded systems and services, etc.	As for 1-a	Very high		Unlikely	

New ID	Risk Action	Risk status / situation	Risk strategy	New requirement (if required)	Category	Risk comment
1-a	Validation of data to verify integrity. Fallback action if the data is not valid. Detection of lack of integrity is important to mitigate this.	Surveying	Avoid	Mitigation 1: Integrity of input data to the database Mitigation 2: Integrity of data from database to calculations Mitigation 4: Integrity of external data to calculations	Security/ integrity	
1-b	Set system reliability/availability requirement, refer NF-ESB-01	Resolved	Avoid	N/A	Security/ integrity	
1-c	Validation of data to verify integrity. Fallback action if the data is not valid. Detection of lack of integrity is important to mitigate this.	Surveying	Avoid	Mitigation 1 Mitigation 2 Mitigation 4	Security/ integrity	Fallback action if the data is not available. Redundancy and fallback data sources.
1-d	Validation of data to verify integrity. Fallback action if the data is not valid. Detection of lack of integrity is important to mitigate this.	Surveying	Avoid	Mitigation 1 Mitigation 2 Mitigation 4	Security/ integrity	
1-e	Cyber security measurement for ISPs, Refer NF-ET-16, Encryption, refer NF-ET-13	Resolved	Avoid	N/A	Security/ integrity	
1-f	Validation of data to verify integrity before using it in the calculations. Fallback action if the data is not valid. Detection of lack of integrity is important to mitigate this.	Surveying	Avoid	Mitigation 1 Mitigation 2 Mitigation 4	Security/ integrity	

- **Risk trigger**: A risk trigger is a condition or other event that will cause a risk to take place.

Example 1. For incorrect historical data is provided to the Energy Forecaster:

  - *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.*

Example 2. For historical weather data is not provided to the Energy Forecaster 2 risk triggers:

  - *There is no data provided by the external source/EMA;*
  - *Not enough storage space on database.*

- **Threats group**: the group which the threats belongs to, according to ENISA [15], [19].
- **Threats (Failure modes)**: the potential harm that can come to an asset.

Example for the risk 1-a: System and service malfunction, loss of service, degraded systems and services, etc. which is belongs to threat group: "Unintentional loss".

- **Impact description:** estimate of the potential losses associated with an identified risk.
- **Impact reasoning:** the reason of allocated risk impact.
- **Likelihood/Frequency:** the probability that a threat event might occur.
- **Likelihood reasoning:** the reasoning of estimated likelihood.

Example for risk 1-a in Table 8:

Table 8: Example from the risk register

Impact description	Impact	Impact reasoning	Likelihood/ Frequency	Likelihood Reasoning
Lack of data lead to incorrect power generation and consumption forecast that can lead to wrong decisions that can have economic impact. As the period of lacking data increases, the impact increase.	Very high	The forecast model is an essential part of the toolbox and important for project success. Relevant to all PUC´s.	Unlikely	Should describe the reasoning for the likelihood level – in this case "The system is designed after XX and YY principles in accordance with standards ZZ. In addition, not having access to the data does not automatically constitute an incorrect decision leading to a serious economic loss".

- **WP**: relevant WP for the risk scenarios.
- **Risk Action**: action at high level proposed to mitigate the risk scenarios.

Example for risk scenario 1-a is: validation of data to verify integrity. Fallback action if the data is not valid. Detection of lack of integrity is important to mitigate this.

- **Risk status / situation:** surveying/ Pending/ Happened/ Resolved.
- **Risk strategy: a**ccept/ Avoid/ Mitigate/ Transfer.
- **New requirement** (if required): the mitigation actions identified from the risk register and not covered in project [3], which need to be followed up through the project.

Example for risk scenario 1-a:

  - *Mitigation 1: Integrity of input data to the database.*
  - *Mitigation 2: Integrity of data from database to calculations.*
  - *Mitigation 4: Integrity of external data to calculations.*

- **Risk category:** security/integrity/privacy.
- **Risk comment**: comments which need to be noted.

4.2 Mitigating actions

Mitigation actions are allocated for the unacceptable risks. Some of the mitigation actions can be found in the Functional and operational requirements document (D3.2) [3]. For the actions which were not covered in D3.2, they were included as proposed mitigations for deliverable D3.3 [4], and should be followed up through the toolbox implementation.

The mitigation actions are followed up for WP4 and WP5 in E-LAND by the risk manager. This is described in detail in section 5.1.

4.3 Cyber risk mitigation on the technical solution

4.3.1 Exposure of existing legacy operational infrastructure

The DER Box provides communication between on-site equipment (pilot site) and the E-LAND Toolbox - ESB via a secure communication. The DER Box is a machine-to-machine gateway which permits on-site equipment management from the EMA cloud platform, with main functions: (1)

Collect data from the on-site equipment and send it to the E-LAND toolbox, (2) transmit service orders from the E-LAND toolbox to the on-site DER, (3) facilitate on-site equipment maintenance and (4) host local distributed intelligence. Only the DER Box communicates directly with the external environment. It is the only link between the ESB/E-LAND toolbox and the onsite equipment/DERs, meaning that only one IP address needs to be configured in order to have Internet access. The DER box needs to be connected to the internet with a wired network, using the onsite VLAN. In order to expose data and retrieve dispatch commands, the DER box makes an outgoing call using HTTPS protocol. The communication between the various DERs and the DER box will be using Modbus TCP protocol. The information shared between the DER Box and the DER are shared through a Modbus table hosted in the DER-device. The DER box is identified as critical asset to enable data and functionality for the integration of the toolbox. For each risk identified in the risk analysis, mitigation(s) has been proposed, formulated as a high-level detail action, applicable to most of the use cases/technical functions and components of the E-LAND solution. In this scenario the SUC6 is relevant for describing how the communication with field devices is carried out from the pilot-site perspective. Table 9, Table 10 and Table 11 provide mitigation examples on how these risks could be mitigated. Also note, that the mitigations shown here do not say to which extend and how they are actually implemented in the E-LAND toolbox.

Table 9: Mitigation strategy: Physical protection of storage device, encoded files or storage area

Mitigation ID	MIT 12 Physical protection of storage device, encoded files or storage area
Component	Applies to all components
Risk	Compromised DER; Sequence of Commands Causes Power Outage.
Mitigation	Physical protection of storage device to avoid damage.

Table 10: Mitigation strategy: Security

Mitigation ID	MIT 8 Security
Component	DER, connections to DER
Risk	Malware/harms - Introduced in DER system during deployment
Mitigation	Policy/limitation on what an external e.g. DER can do of operation and interaction with Data API.

Table 11: Mitigation strategy: Establish network security best practices

Mitigation ID	MIT 6 Establish network security best practices
Component	Applies to all components
Risk	Through the incorrect connection to the Internet, a threat agent gains control of the DER system and alters the operation of the DER functions to make them ignore utility commands and to turn off the "acknowledge command" interaction with the utility.
Mitigation	• Authenticate users for all user interface interactions; • Change default access credentials after installation; • Enforce limits in hardware so that no setting changes can damage equipment; • Train personnel on secure networking requirements so that DER owners will understand the impact of bypassing security settings; • Require approval of next level of management for critical security settings.

4.3.2 Asset hardening and new integration requirements

During the risk assessment we found that hardening of each component and proper configuration management of the assets are important when operating an LES. New integration requirements were also identified, such as having a trusted and reliable time synchronization source and logging of both user and system (application) activities, as shown in Table 12.

Table 12: Mitigation strategy: Reliable clock and time synchronization

Mitigation ID	MIT 8 Incorrect Clock
Component	EMS, interfacing components with EMS, ESB, EF, OS, DPA
Risk	The clock needs to be synchronized between components. For example, incorrect clock can cause the substation DER system to calculate wrong forecasts and mismatches between planned and provided energy
Mitigation	Need of a common trusted source for setting the time.

In our experience we find that custom application event logging is often missing, disabled or poorly configured, as identified inTable 13. Custom logging provides much greater insight than standard infrastructure logging alone. Application logging should be consistent within the application, consistent across the environment and use industry standards where relevant, so the logged event data can be consumed, correlated, analyzed, and managed (OWASP, Application Logging).

Table 13: Mitigation strategy: Extensive audit logging

Mitigation ID	MIT 14 Event logs from components
Component	Applies to all components
Risk	Protection of information. No logging options to backtrack events triggered by the user and system
Mitigation	Each component should have logging functionality like an audit log for event triggered by the user and system (see ISO 27001 "12.4.2 Protection of log information")

4.3.3 Concerns in a multi-cloud environment

NIST defines cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [25]. There is a complexity with interoperability between different cloud providers when addressing cyber security issues and maintaining compatibilities and monitoring of resources, e.g. enough storage and maintaining encryption key services. The ESB should enable a secure and seamless data integration and orchestration for advanced tools e.g. forecasting, optimization to external sources of data (e.g. weather forecasts) regardless of where the service is provided. Introducing scenarios where different parts of the toolbox services are provided by different vendors in a multi-cloud environment could introduce operational risks that impact the functionality and trust in the E-LAND toolbox. Central components, like the ESB, are more exposed in regards of providing a communication layer between applications and therefore more vulnerable to denial of service attacks and cloud outage issues. An example is when cloud providers experiences service denial issues causing datacentres to overload on incoming traffic, preventing legitimate users from accessing services (e.g. APIs) on the same networking channels. The result of this resource exhaustion can impact the services developed in the project.

Data privacy concerns in the project accounts the number of stakeholders, systems and interconnections, and the risk of exposing data through the many API's is considered high as poorly designed APIs could lead to misuse or data breach [26]. For the project data protection and data privacy has become a shared, but distributed responsibility much in thread with the definition stating that privacy concerns the ability of an individual or group to privately and selectively share information only amongst themselves [27]. For the project, data privacy concerns relating to GDPR between different third-party cloud providers is a concern and there

is a need for control and review of e.g. encryption services and third-party provider's internal controls.

Table 14 shows the proposed mitigation. Here is also the content of other fields in the mitigation template to visualise the traceability back to the use cases.

Table 14: Example of a mitigation

Proposed mitigation ID	Mitigation 6
Title	Network security.
Description	Authenticate users for all user interface interactions. Change default access credentials after installation. Enforce limits in hardware so that no setting changes can damage equipment; Train personnel on secure networking requirements so that DER owners will understand the impact of bypassing security settings. Require approval of next level of management for critical security settings.
Risk	In case of wireless connections, DER's rogue wireless connection exposes the DER system to threats.
Rationale	Through the incorrect connection to the Internet, a threat agent gains control of the DER system and alters the operation of the DER functions to make them ignore utility commands and to turn off the "acknowledge command" interaction with the utility.
Risk Owner	DER owner? – To be identified
Component	DER, communications and connections to the DER.
Risk Category	Security/integrity.
Verification Measurement	Validation, error message for non-valid data.
Source Risk Analysis	Risk ID. 19; 20; 21; 31-b.
Source/Related Requirements	PUC2, PUC4, SUC4, e.g. BN-FM-01, BN-FM-02, BN-AG-01, BN-AG-02, BN-AG-04, BN-MO-01, BN-MO-02, BN-MO-04, FUN-ET-01, FUN-ET-02, FUN-ET-03 NF-ET -2.

4.3.4 Asset hardening and integration requirements

A common situation for the end users and pilot site owner is the fact that many existing energy systems lack ICT-based interconnections to achieve a cost-efficient integrated local energy system. A good knowledge about existing IT (Information Technology) and OT (Operation Technology) assets- and infrastructure is an important matter for a successful integration. When introducing DER equipment and integrating the toolbox different services in e.g. a multi-cloud

environment this tends to be more complicated for the owners to deal with, especially understanding how their asset and information are being exposed and what kind of risks are introduced when integrating the toolbox. The convergence of IT and OT infrastructure is still a challenge that needs to be addressed for better interoperability between these environments. It easy to underestimate the complexity also in existing legacy infrastructures. Organization have different maturity level and readiness level on how to adopt new technologies and it often comes down to how well the business aligning with a holistic view on process, technology, and organization to manage their digital transformation. Table 15 provides an example of a mitigation: *Security measure on password and username storage*.

Table 15: Example of a mitigation: Security measure on password and username storage

Proposed mitigation ID	Mitigation 10
Title	Security measure on password and username storage
Description	Security measure on password and username storage
Risk	DER system registration information stolen.
Rationale	GDPR
Risk Owner	To be identified
Component	User databases
Risk Category	Privacy/ integrity
Verification Measurement	Validation, error message for intrusion
Source Risk Analysis	Risk ID. 31-i.
Source/Related Requirements	All PUCs. e.g. FUN-ET-01, FUN-ET-02, FUN-ET-03, NF-ET-1.

The E-LAND toolbox extensively rely on components with API interfaces across multiple clouds and infrastructure services that rises the complexity of keeping track of vulnerabilities and impact of absent. Therefore, properly application (API) hardening against attacks and resilient to compromises in a multi-cloud environment is stated to be more complex to protect and operate. Table 16 provides an example of a mitigation strategy: protect information.

Table 16: Mitigation strategy: Protect information

Mitigation ID	MIT 13 - Historical data is made available to unwanted parties
Component	Applies to all components
Risk	Unprotected storage of data, data is accessible from the network or the storage device placed in a non-secure location. Non-secure protocols. GDPR.
Mitigation	Cyber protection of storage device, encoded files or storage area

4.4 Results from the privacy assessment

The analysis identified personal data in the user interface application and are tied to user management. The user details are required to ensure user authentication and account protection. Table 17 lists the identified data. In Figure 8 the components contain this data are highlighted. The summary of the analysis is listed in Table 17 and in Table 18.

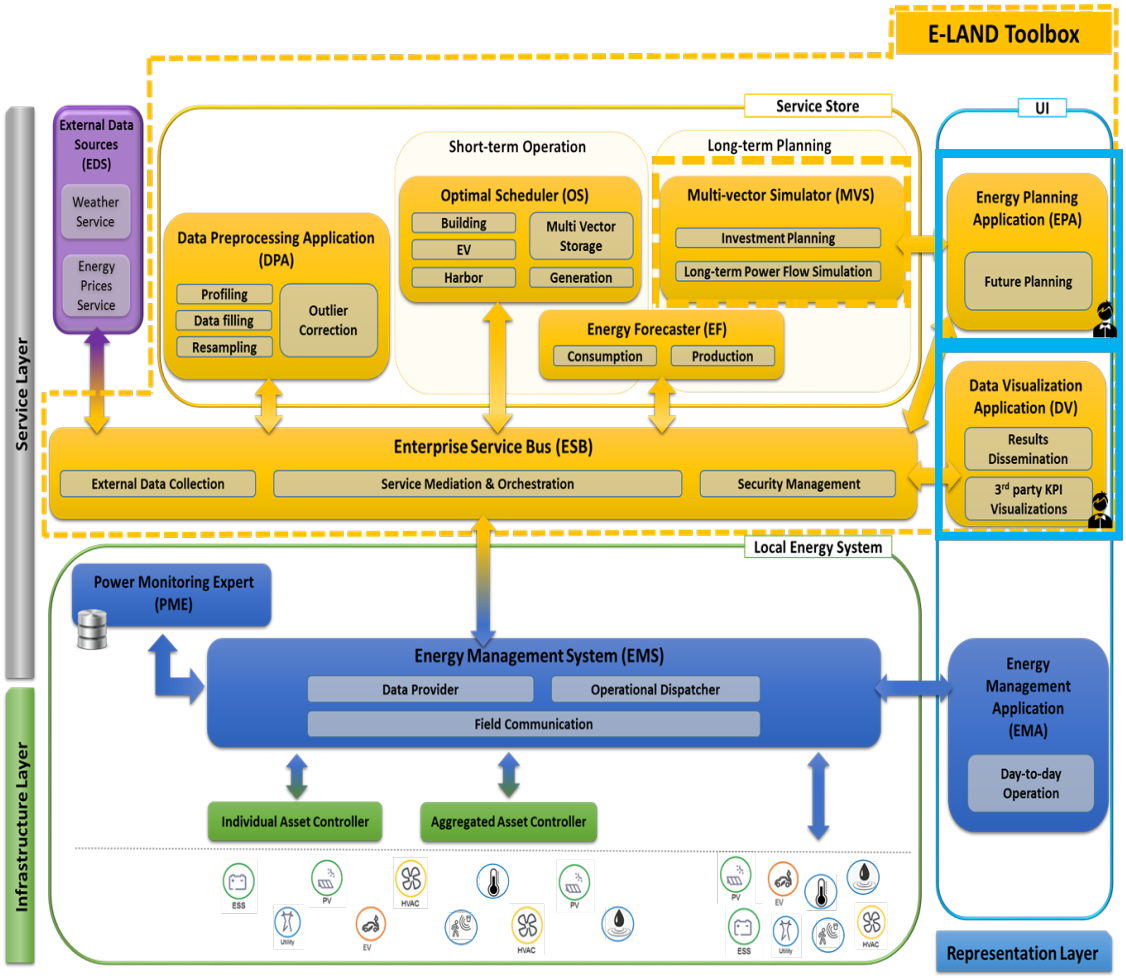


Figure 8: Components containing personal data

Table 17: Overview of personal data in the toolbox

Categories of individuals	Categories of personal data	Categories of recipients
Software users of the toolbox	Username	Pilot site toolbox administrators
Software users of the toolbox	E-mail	Pilot site toolbox administrators
Software users of the toolbox	Role and user type	Pilot site toolbox administrators

Table 18: Risks tied to privacy identified during risk assessment of use cases and technical design

	Privacy Risk 1	Privacy Risk 2
Risk Description	Historical power consumption data is made available to unwanted parties.	DER system registration information stolen.
Risk trigger	Unprotected storage of data, Data is accessible from the network or the storage device placed in a non-secure location. Non-secure protocols.	A threat agent accesses the DERMS systems and steals the customer DER registration information, using it for industrial espionage or other purposes, causing confidentiality impacts to these utility customers. For example, if stolen, this information could allow other DER owners to manipulate the retail (or wholesale) energy markets, for instance by bidding in prices or energy products that make it less likely the DER system (whose data was stolen) would be willing/able to bid, or if they did bid, making it less cost-effective for them.
Threats	Information leakage.	Unnecessary access is permitted to system functions in the DERMS system; System makes private data accessible to unauthorized individuals while at rest; System relies on credentials that are easy to obtain for access to customer DER registration information.
Impact Description	Data can be manipulated or deleted, both intentional and by accident. Data could provide details about usage patterns at the pilot site that should not be available. For scenarios where the consumer is a person the historic data is protected by law and is considered as personal data.	Breach of utility confidential information; Financial losses due to the security breach.
Risk Action	Physical protection of storage device, encoded files or storage area. Audit log.	Encrypt data at rest, specifically DER registration data; Require approved cryptographic algorithms for encrypting DER registration data; Require intrusion detection and prevention as part of the DERMS network and system management capabilities; Protect credentials that permit access to customer DER registration data; Create audit log that records accesses to the registration data files.

The analysis of personal data did not reveal any new risks but provided input to risks in the technical risk register (In the technical risk analysis, a risk of leaking personal data was identified. At the time there was not an overview of what type of data the system would contain, where it would be stored or how it would be used. In other words, there was a high uncertainty. The privacy assessment of the toolbox was therefore a key activity to resolve this risk.

The personal data identified was tied to user management. Cyber security measures for this data is resolved by implementing "*Mitigation 9: Security measure on password and username storage* and *Mitigation 12 Physical protection of storage device, encoded files or storage area"*. Table 19 shows the results from the privacy analysis.

Table 19: Results from the privacy analysis

Required information	**Analyses results**
Define data categories and subjects	Username, email and role/user type collected from the users of the toolbox on account creation.
Data transfers	Data is not transferred
Processing purpose, lawful basis and data source	Processing purpose: User management. Authentication, authorisation for using the applications in the E-LAND toolbox Lawful basis: Article 6(1)(b) – contract Data source: Data provided by the subject
Retention schedule	As long as the user wants access to the application or end of E-LAND piloting
The subject's rights	Access, correct and delete their data
Security measures and location of personal data	Access control to server room, IT cyber security with firewall. Password hashing, TLS certificates. See D3.3 for security specifications [4]. Data located on onsite servers at the Organizations site.
Link to consent (if required)	Not required as the data is gathered based on Article 6(1)(b) – contract
Specification of the controller, processors and contact persons	Determining the roles of Controller and Processors. Subject: Employee that uses the toolbox applications. Owner of username, email and role Controller: The pilot sites The pilots collect data from their employees. Data is hosted locally on organization site. They have control of how they chose to use the application, who has access, local security measures etc. They can update and delete users. Hence, they are the Controllers. Data Processor: None An analysis was performed to assess if anyone acted as a processor. ICOM is responsible for developing the application that handles the personal data. However, they do not have any control or access after the development and won't have access to the actual personal data. They do not handle deletion, adding users, communicate directly with subjects etc. In the E-LAND project, they can be considered as vendor. They are therefore not a Processor. This assumes the application is hosted on-site (not cloud). As a vendor, ICOM should through the E-LAND project implement appropriate cyber security measures so the Pilot sites (Controllers) can comply with GDPR. E-LAND have identified these cyber security measures through the risk assessment described in this report. DPA/Supervisory Authority: Country specific Handles complaints. An outside party.

5 Evaluation and follow-up plan

As introduced in previous chapters, the mitigation actions should be communicated to the project for implementation. In E-LAND the team of the risk manager is continuously monitoring and following up on the implementation and status of the risks. This chapter elaborates on the communication process and follow-up plan of the risk assessment during E-LAND toolbox design, implementation, and application for the pilots. In addition, the challenges we experienced and expected are introduced.

5.1 Communication about status on risks/mitigations

Failure to address technical risks could impact both the performance of the E-LAND toolbox in operation as well as the E-LAND KPIs. Therefore, the project risks register contains risks that relate to the overall cyber security of the toolbox. Currently there are two such risks:

- *DoA06.1 Security, safety or privacy vulnerabilities detected WP1, WP3 and WP4*; and
- *DoA.13.1 Lack of security measure on password and username storage*.

DoA06.1 was identified as a project risk already at the time of application. This project risk led to the technical risk analysis being included as a task in the project. It does not link to a specific technical risk. The DoA13.1 was identified later as an outcome of the technical risk assessment. The project risk thereby indicates the summarized status of project and technical risks as shown in the lower part of Figure 9.

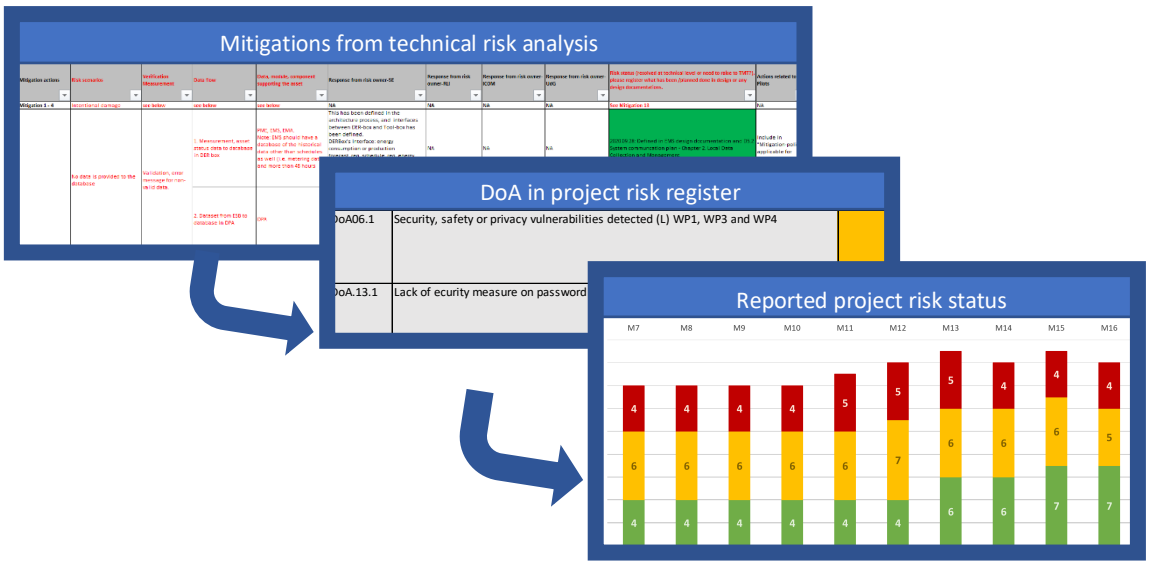


Figure 9: Technical risks and Project risks (DoA) are aggregated and reported in TMT meetings

An example of how the risks was reported during the first project review is provided Figure 10. This provides an overview of all risks which is easy to understand and tributes to the risk tracking in the project. It allows the E-LAND management and participants to monitor the progress of the risks without requiring the people to dive into the details of each risk. E.g. for the each of the technical risks, the mitigation and details about triggers and causes would be irrelevant when providing a general overview of project risk status. This form of risk communication is, as fare the risk management team has evaluated the references presented in the background in section 2, not been presented before. As such this is an innovation provided by E-LAND.

Figure 10: How the individual risks have developed over a time period

5.2 Evaluating the technical risks assessment and mitigations

The risk assessment and mitigation actions are communicated by risk manager to the project for implementation. Similar communication approach as above is used. First, the 1-to-1 calls were used for communicating between the risk manager and different design partners. From a risk manager point of view, direct phone calls enable us to verify that the understanding of the technical risk status was correct and that the risk was communicated and understood by all design partner. 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. 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. In addition, since there are some joint responsible tasks for some of mitigation

actions, the 1-on-1 calls conducted helped risk manager to have a better understanding of the clearly defined responsibility and the joint responsibility. For the responsibility which clearly defined for each partner, the risk manager can follow directly from the specific partner. For the actions with joint responsibility, common meetings were facilitated by the risk manager with different designer. In all of the meetings, the pilot's coordinator was involved for a understanding of actions which might influence the toolbox implementation on pilots and any following up actions which need to take during pilots installation and operation phase.

A full list of the mitigation list used as communication tool in the project is not shown here as it may contain sensitive information in the same way as the technical risk register. A part of the mitigations table is presented in Table 20 in order to show the template. The content of each column is explained below the table.

Table 20: Template of the mitigations.

	A	B	C	D	E	G	H	I	J	K	L
1	Mitigation actions	Risk scenarios	Verification Measurement	Data flow	Data, module, component supporting the asset	Response from risk owner-SE	Response from risk owner-RLI	Response from risk owner-ICOM	Response from risk owner-UdG	Risk status (resolved at technical level or need to raise to TMT?), please register what has been /planned done in design or any design documentations.	Actions related to Pilots
2	Mitigation 1 - 4	intentional damage	see below	see below	see below	NA	NA	NA	NA	See Mitigation 13	NA
3		No data is provided to the database	Validation, error message for non-valid data.	1. Measurement, asset status data to database in DER box	PME, EMS, EMA Note: EMS should have a database of the historical data other than schedules as well (i.e. metering data) and more than 48 hours	This has been defined in the architecture process, and interfaces between DER-box and Tool-box has been defined. DERBox's interface: energy consumption or production forecast_req, schedule_req, energy real-time and historic data to external systems, status of local assets (e.g. SoC of batteries) to external systems. Using Modbus TCP/IP protocols for	NA	NA	NA	2020.09.28: Defined in EMS design documentation and D5.2 System communication plan - Chapter 2. Local Data Collection and Management	Include in "Mitigation-policy applicable for Pilots"
4				2. Dataset from ESB to database in DPA	DPA	NA	NA	Proposed: Run the data through the DPA component before storing them in the DB. ESB will not store data - it is an integration module- but it can facilitate the process of data cleansing before	DPA will ensure the integrity of data to be used by other tools	Will be included in design documentation of DPA. UdG to explain which documentation is it. 2020.09.28: D5.2 System Communication Plan describes in chapter.4 End-to-end test - that DPA will verify data accuracy, detect label missing data, outliers and wrong measurements.	Include in "Mitigation-policy applicable for Pilots"

- **Mitigation action**: the mitigation actions identified from the risk register which need to be followed up;
- **Risk scenarios**: the risk scenarios identified from risk register related to the mitigation actions listed in this table. There can be several risk scenarios relate to one mitigation actions;
- **Verification measurement**: verification or validation measurement for each risk scenario;
- **Data flow**: related data flow for corresponding the risk scenarios;
- **Data, module, component supporting the asset**: related asset for corresponding the risk scenarios;
- **Response from risk owners**: how the mitigation implemented in the system;
- **Risk status**: what is the implementation status, how to trace the implementation, i.e. in design documents, operational procedures, etc;
- **Actions related to pilots**: any mitigations need to be implemented/followed by pilots.

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 as they had 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. The following main actions are continuously performed to follow up risks:

1. Continue the regular contact meetings with partners and focus on individual risk mitigations for the solution;
2. 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. This is especially the case when it comes to risks that can only be mitigated through a joint effort from several stakeholders. 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.

5.3 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:

1. 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;
2. 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 [29].

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. A cost – effectiveness 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. 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).

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 fulfil 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.

5.4 Pilot to do's

5.4.1 Risk observing from the point of view of the Pilot sites

A task in the risk management activity is to follow closely the development of this minimum set of requirements and guidelines for security in the project and ensure that each pilot site is monitored closely and supported during the implementation. For existing equipment where the viability of the common baseline might be less optimal, a good understanding of how risks could impact existing infrastructure is needed. The pilot sites address different risks in the project. The combined risks and mitigations across pilot sites should be relevant for single sites when the toolbox is developed. In addition, the pilots needs to get all technical parts up and running and may miss parts that are not regarded crucial at WP level. Thus, the pilots will be included as separate entities that are asked for their perception of key risks, separate from the WP's. A collection of the five most important risks as seen from each of the three pilots may give a different picture than the one given by the WPs.

Next activity planned I WP4 task 4.7 (for which this report is a delivery) is to perform a detailed security mapping of assets and threats in order to identify site specific security requirements for the pilot. This bottom-up approach is intended to compliment the top-down risk analysis

performed thus far in the project. The gained site-specific security knowledge will be generalized into the overall solution. Initial preparations on this have been started by IFE and SIN.

5.4.2 Communication through flyers to introduce the risk process

The risk assessment in the E-LAND project is combining security and safety risk assessment method. Each different steps of the risk assessment are mostly unknown or understood differently, dependently on users' objectives to use the toolbox. Increasing the understanding of the toolbox for future users can reduce potential risks to arise, by putting across the solution. In this purpose a series of flyers have been created to ease the communication and guide the pilot sites through the process.

The purpose of the Flyers

In order to reduce risks and optimize the potential of the solution, knowledge about relevant information pertaining to each stakeholder should be easily available. The relevant information was shaped as flyers to be easily accessible, short, precise, and illustrative way to present an overview of the process and the topics that have been undertaken. Flyers are applicable both internal and external to the project.

Flyers format

For these reasons, this format traditionally consists of one-page quick introductions to a topic. One-page topical flyers should present a combination of illustrative figures, catering to the understanding of a variability of readers. The combination of figures and text provides a redundant way of presenting information, and perhaps more importantly avoid erroneous interpretations. Additionally, flyers require reduced efforts for any reader to go through and this increases the probability that the reader will invest their time on.

Overview of created flyers

The different flyers presented in Table 21 cover three different important areas concerning risks. The full flyers are provided in Appendix B, section 8.2.

Table 21: Description of the four flyers related to risk, safety and security in E-LAND

Title	Main message	What should the reader understand?
An overview of our energy toolbox	The future pilots learn about the different steps to evaluate the risk on their own device. This flyer can be read as a table of content of all the topics cover in the Risk study.	The main topics cover by the risk assessment. Where to start, ask, or read to be able to evaluate/mitigate the risk taken by implementing the toolbox.
Risk Management in E-LAND	An overview of the risk management. This flyer gives the concept and the purpose of the risk management. The	Risk management is important to ensure that the concept, the solution, and the application to be delivered in E-LAND

Title	Main message	What should the reader understand?
	users are guided through the challenges of the risk management and will learn more on the main goals to study risk and how it was considered, in a high perspective.	are safe, secure, and reliable for the users.
Addressing Privacy Issues.	This flyer proposes simple definitions of the important wording used in the domain of data privacy. The users have insights of what should be taken care of, why and how it has been done in the project. Further details are available through standards and guidelines that are publicly accessible.	Personal data are any information relating to an individual or that make identification of an individual possible by combining several sources. It is important to take care of and knowing how to deal with data collection.
Addressing Cyber Security in E-LAND	Description of the risk assessment regarding cyber risks, safety and security. This flyer contains a short description of the process followed to assess the risk that have result to the mitigations.	The cyber security risks have been assessed in a systematic way, going through Use Cases that cover a wide variety of usages. The method has ensured that cyber risks are addressed early in the project. Implementing the final product in my own system can be done at lower risks.

6 Conclusions and Future work

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.

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. Even though most of the identified risks are identified as high-level risks for the E-LAND toolbox, cyber threats and risk identified during the requirement phase provide new insights and perspectives for the partners and developers. Addressing and implementing requirements and mitigations mentioned in this paper are but a subset of the safety and security requirements needed for achieving sufficient confidence and trust in the E-LAND services. It is important that interfaces particularly are designed to protect against both accidental and malicious attempts to circumvent the security policy. Everything from authentication and access control to encryption and activity monitoring should be addressed accordingly through a holistic process, technology, and organization approach. The identified safety and security risks have pointed to a need for a common baseline solution across the project. The work has started on establishing a baseline based on best practice for network security and application data management in order to; reduce variability across sites, solutions and stakeholders, reduce workload for patching and updates, and reduce the viable attack vectors across sites and equipment to name some. In addition, a common

baseline enables useful cross-project information sharing on risks, mitigations, and experiences across sites.

A task in the risk management activity is to follow closely the development of this minimum set of requirements and guidelines for security in the project and ensure that each pilot site is monitored closely and supported during the implementation.. Next project activity for Port of Borg is to perform a detailed security mapping of assets and threats in order to identify site specific security requirements for the site.

The E-LAND project has demonstrated that risk communication is a main contributor to identifying risks and finding appropriate mitigations. In doing this a meaningful risk picture is of high importance. The tools used in E-LAND for communication provides, as fare as the team has evaluated, an innovation. In order to reduce risks and optimize the potential of the solution, knowledge about relevant information pertaining to each stakeholder should be easily available. The relevant information has been shaped as flyers to be easily accessible, short, precise, and illustrative way to present an overview of the process and the topics that have been undertaken. These flyers are applicable both internal and external to the E-LAND project.

Finally, batteries play a crucial role in localized energy storage and are thus a crucial asset when it comes to reducing the overall environmental footprint and eventually CO_2 neutral energy islands. In an appendix some guidelines and recommendations for the use of batteries are provided.

7 References

[1]. D1.3 - *Risk management and contingency plan*, E-LAND Confidential deliverable, 2019.

[2]. D3.1 - *Use Case Definition*, E-LAND Confidential deliverable, 2019.

[3]. D3.2 - *Functional and operational requirements*, E-LAND Public deliverable, 2019.

[4]. D3.3 - *Technical Specifications*, E-LAND Confidential deliverable, 2019.

[5]. C. Esnoul, S. A. Olsen, B. A. Gran X. Gao, and P.A. Jørgensen, J. E. Simensen, *"Risk And security Practices: Experiences from the E-LAND",* Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference (ESREL), Virtual & Venice, 2nd -6th November 2020.

[6]. X. Gao, C. Esnoul, P.A. Jørgensen, S. A. Olsen and B. A. Gran, "*Risk Assessment in the E-LAND Project",* Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference (ESREL), Virtual & Venice, 2nd -6th November 2020.

[7]. P.-A. Jørgensen, J. E. Simensen, C. Esnoul, X. Gao, S. A. Olsen and B. A. Gran "*Addressing cybersecurity in Energy Islands*", Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference (ESREL), Virtual & Venice, 2nd -6th November 2020.

[8]. ISO/IEC 27005 (2018), *Information technology —Security techniques — Information security risk management (second edition).*

[9]. ISO/IEC 27002 (2013), *Information technology - Security techniques - Code of practice for information security controls (first edition).*

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

[11]. Mars Climate Orbiter, available https://solarsystem.nasa.gov/missions/mars-climate-orbiter/in-depth/ Page Updated: July 25, 2019.

[12]. *Final Committee Report: Boeing 737 MAX - Design, Development & Certification Sept. 2020*, available: https://transportation.house.gov/imo/media/doc/2020.09.15%20FINAL%20737%20MAX%20Report%20for%20Public%20Release.pdf

[13]. GDPR.EU, *Privacy Policy Template*, available: https://gdpr.eu/wp-content/uploads/2019/01/Our-Company-Privacy-Policy.pdf

[14]. STRIDE, Microsoft, available: https://docs.microsoft.com/en-us/previous-versions/commerce-server/ee823878%28v%3dcs.20%29 (last visited 09.10.2020)

[15]. ENSIA (2013), Smart Grid Threat Landscape and good practice (SGAM)

[16]. OWASP (2020), *Application threat modelling and application logging*, available: https://www.owasp.org/index.php/Application_Threat_Modeling and https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html (visited 17.01.2020

[17]. NIST (2012), *Guide for Conducting Risk Assessments- information security*.

[18]. 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)

[19]. 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*".

[20]. OCTAVE: Risk Evaluation, available: http://www.cert.org/octave/ (last visited 31.10.2010)

[21]. CESG National Technical Authority for Information Assurance, HMG IA Standard No. 1 Technical Risk Assessment (October 2009).

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

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

[24]. ICO - UK's independent body set up to uphold information rights, Documentation, available: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/ (last visited 30.10.2020)

[25]. NIST 800-145 (2011), The NIST Definition of Cloud Computing, Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[26]. Cloud Security Alliance (CSA), (2019), *Top Threats to Cloud Computing: Egregious Eleven* (version 08/06/2019).

[27]. Simula (2019), *An Overview of Multi-Cloud Computing*, Available: https://www.simula.no/publications/overview-multi-cloud-computing.

[28]. IEC 62559-2 (2015) - *Use case methodology - Part 2: Definition of the templates for use cases, actor list and requirements list.*

[29]. 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.

[30]. ENISA (2012), CEN/CENELEC/ETSI *Smart Grid Coordination Group Grid Architecture Model (SGAM) Framework*. (November 2012) version 3.0.

8 Appendixes

8.1 Appendix A: The role of battery safety in energy islands

8.1.1 Introduction

The role of batteries in E-LAND is to store green energy locally, use energy efficiently and reduce peak loads with energy storage systems. There is large potential in reduction in energy consumption, assisting in balancing renewable energy sources and thereby significantly reduce CO_2 emissions. Batteries play a crucial role in localized energy storage and are thus a crucial asset when it comes to reducing the overall environmental footprint and eventually CO_2 neutral energy islands. Amongst electro-chemical storage technologies, the lithium-ion battery is the most common and most promising, and the number of projects and installations using lithium-ion batteries is continuously increasing.

Size of a battery storage system

The size of a battery storage system can vary a lot from site to site. Within ELAND, 270 kWh batteries are included at the pilot site in Romania. Battery storage systems are included in other pilot sites, but to date no detailed information has been provided.

8.1.2 Battery safety

Battery safety

It is a well-known fact that lithium-ion cells can have safety issues. A large number of battery safety incidents has been reported worldwide over the past years within e.g. battery energy storage systems (e.g. the LG-Chem fire April 2019 in Arizona [31]), transport (e.g. fires in the APU battery of Boeing Dreamliner), electric and hybrid-electric ships, electric vehicles and mobile devices (e.g. recall of the Samsung Galaxy Note 7 model). Consequences of safety incidents in battery storage systems, such as fires, can be catastrophic. A thorough understanding of a battery's properties and behaviour, such as battery life, state of health and the corresponding safe operational conditions are thus vital for the safety of larger energy storage systems, especially for applications in energy islands.

Battery ageing and degradation

Li-ion battery safety incidents are most often related to the ageing and degradation of the battery cells. While the fact that aging of lithium-ion cells leads to a reduced capacity and cell life is extensively covered in the literature by several research groups, e.g. Vetter[32], the safety effects of ageing are far less studied, with only a handful of empirical studies published [33] [34] [35]. Ageing and degradation of Li-ion batteries will in many cases contribute to reduced thermal stability which potentially affects the safety performance of the batteries.

Battery life

A Li-ion battery's calendar and cycle life is dependent on the specific Li-ion chemistry used in the battery, the battery materials structure and quality (electrodes and electrolyte) and the parameter space for a battery's operating conditions (operating and storage temperature, charge and discharge current rates, maximum and minimum state-of-charge for operation, state-of-charge during no-load operation (storage) and cooling and heating of battery system). Due to the large number of different Li-ion battery chemistries and battery manufacturers, the details of a specific battery's cycle and calendar life are in general not well-known. In some cases, the battery manufacturers provide selected datasets, and/or research papers present battery life data for specific battery cells and chemistries. However, these data are often collected at extreme temperatures and/or presented as anonymised battery cells and can thus only give indications of the expected cycle life for a given Li-ion battery chemistry.

Lifetime testing

Assessing a battery's cycle life is time consuming. Accelerated cycling (i.e. employing higher than operational charge and discharge currents) is often performed to assess the cycle-life of a battery. However, such tests often yield too optimistic or entirely wrong cycle life predictions because these high currents can frequently be associated with higher internal temperatures.

Temperature

Temperature is recognised as the most important factor for Li-ion battery capacity decay and ageing: both, higher (> 30 °C) and lower (< 10 °C) temperatures affect the energy and capacity and will reduce the expected battery life. Additionally, charging at low temperatures has been reported to contribute to irreversible loss in capacity through Li-plating and can consequently impose a significant safety hazard through internal short-circuits within the battery cell.

Operational conditions

Besides external temperatures, certain operational conditions of a battery can lead to undesirable high temperatures: high operational current rates lead to a reduction in voltage and

an increase in the dissipated heat in the battery. The higher the current, the more heat will be produced in the battery. If the generated heat is not able to escape the battery cell, it can contribute to local heating effects in the electrode materials which again will contribute to cell degradation. Chen *et al.* [36] modelled the temperature distribution within a prismatic battery cell based on thermal conductivity data and reported that at high discharge rates (2C) the temperature in the battery could increase by 40°C at the end of discharge. This illustrates the importance of thermal control in connection with high current rates and its links to cycle life.

Lifetime testing results

Results from testing of selected commercial Li-ion cells at IFE's battery testing laboratory performed as part of the SafeLiLife NFR project (228739, [38]) confirm that the largest influence on a battery's cycle life is the temperature during cycling. Both, high (45°C) and low (5°C) temperatures significantly reduce cycle life compared to cycling at room temperature, i.e. 25°C. A general negative effect on cycle life was also observed on increasing the current rates. *Figure 11* shows an example for the cycle life for a selected lithium ion cell at various temperatures and current rates over the full state of charge window.

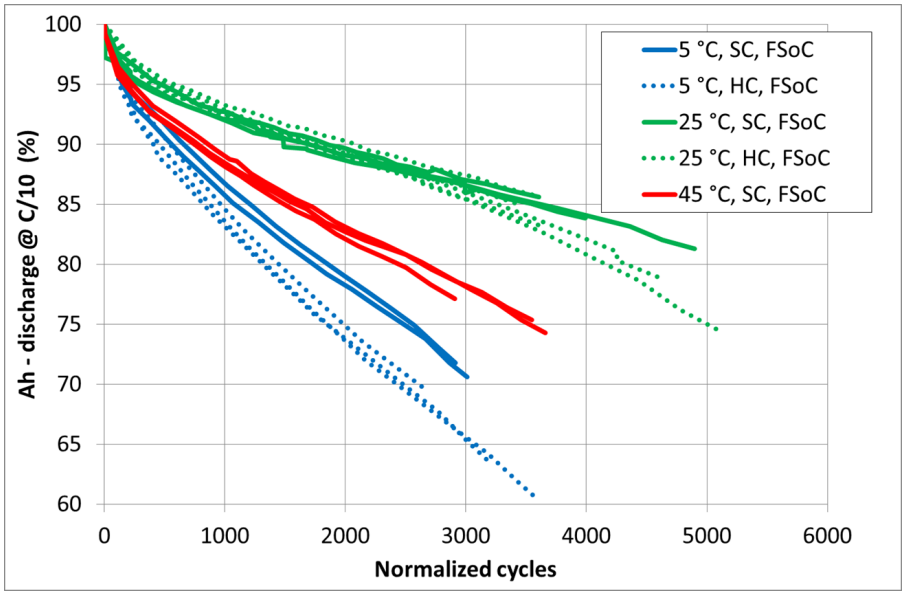


Figure 11: Cycle life for a selected lithium ion cell at several cycle temperatures and current rates in the full state-of-charge window (FSoC). The cycle life was measured as remaining capacity at C/10 discharge current vs normalized cycles.

8.1.3 Battery stability

Factors for battery instability

There are many factors that can make a lithium-ion cell unstable and eventually start a fire. These factors could be e.g. overcharge, overload, heat exposure, external short circuit, over-discharge (followed by a charge) and internal short circuit. If the cell/battery system is not able to handle the heat generation caused by these factors, this could evolve into decomposition of the cell material, physical reactions like ventilation, gassing, fire and in rare cases even explosions. Figure 12 illustrates different factors affecting the stability of a lithium-ion cell (yellow and blue circles) and the potential physical reactions (red figures).

Most of these factors can be controlled by an electronic system, the battery management systems (BMS) and consequently, the overall likelihood for a fire in a lithium-ion cell is very low. However, an internal short-circuit under development cannot be detected by the BMS or any other currently commercially available system. An internal short-circuit could for example be caused by production defects (e.g. particles) or occur as a result of cyclic degradation (e.g. mechanical stress or lithium dendrites) of the cell (blue circles shown in Figure 12).

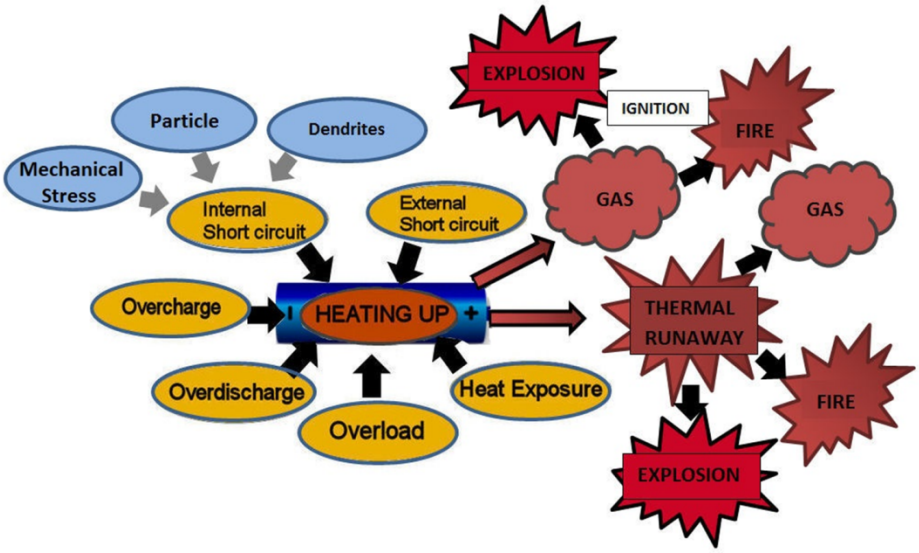


Figure 12: Overview of different factors that could affect the stability of a lithium-ion cell (yellow circles) and the reaction pattern leading to different physical reactions (red figures) (FFI)

Although the probability of a safety issue (fires and explosions) is in general very low (one in 1 million to one in 10 million), the consequences of such are catastrophic, and thus cannot be ignored.

Internal short-circuit & thermal runaway

One of the failure mechanisms related to degradation of safety properties of a lithium-ion cell is the development of internal short-circuits. An internal short-circuit is a mechanical connection between the anode and cathode material/current collector inside the lithium-ion cell. When a

cell shorts internally, the stored electrochemical energy is liberated as heat. If the cell is not able to remove the heat fast enough, a rapid temperature rise could appear at a localized spot in the cell. At temperatures above 190 °C (dependent on the cathode material) cathode materials will decompose and start liberating oxygen. At temperatures above 400 °C the autoignition temperature for most of the organic solvents (the electrolyte contains organic solvents) is reached and a fire could eventually start. Even if the short does not raise the temperature above 400°C, the amount of heat delivered at the short could make the battery material thermally unstable leading to exothermic decomposition of the material. This could eventually force the cell into thermal runaway (minimum 10 °C/min heat rate). Therefore, the thermal stability of cathode material is the traditionally way of ranging the effect of an internal short circuit in lithium-ion cells. According to Maleki *et al.* [37] an internal short could release up to 70 % of the battery's electrical energy in less than 60 seconds. This indicates that the short-circuit also depends on the cell's energy content (SOC, energy density and size).

Figure 13 shows that the cell that was cycled and aged at 5 °C went to "thermal runaway" at a much lower temperature than the other cycled cells for the same Li-ion type and chemistry.

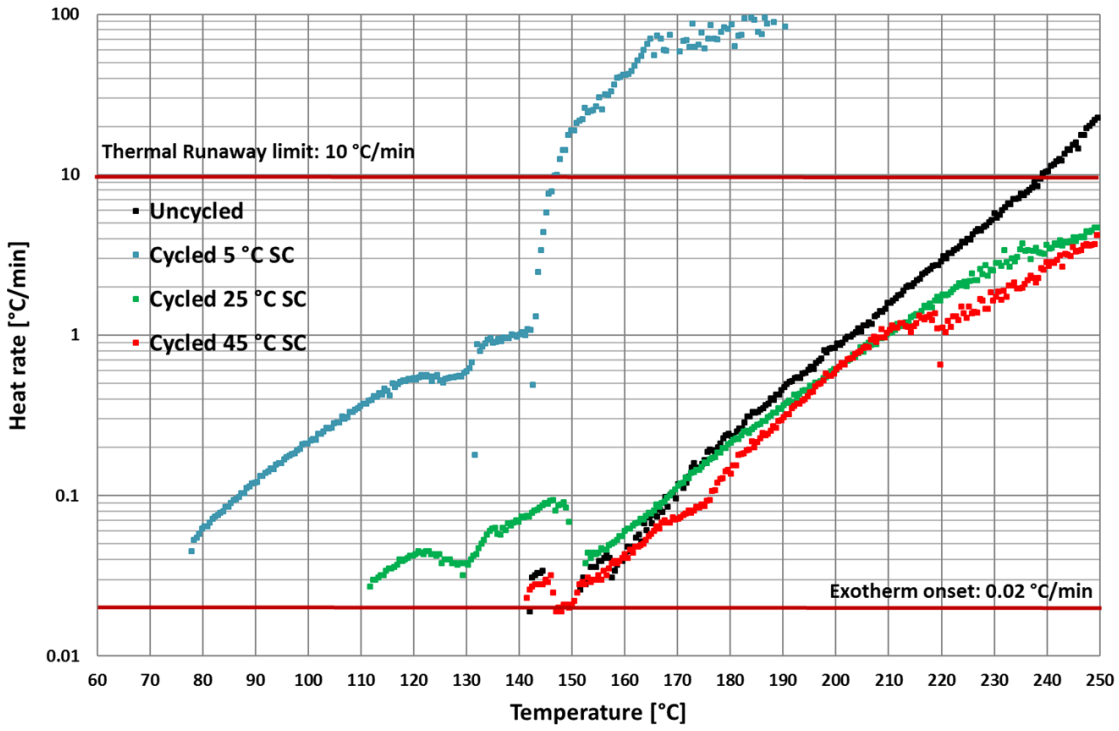


Figure 13: Results from safety tests of the cycled cells in Figure 11. Heat rates as a function of temperature for new and cyclic aged lithium ion cells observed in an accelerated rate calorimeter (ARC). The graph shows that the cell that was cycled and aged at 5 °C went to "thermal runaway" at a much lower temperature than the other cycled cells for the same Li-ion type and chemistry

The Li-ion cells can handle neither overcharge nor over-discharge. At temperatures above 60°C, the batteries can initiate a self-heating mechanism which eventually can result in both gassing of electrolyte and fire/explosion. When charging at low temperatures, metallic lithium can be formed at one of the electrodes. This can eventually cause an internal short-circuit of the battery, which again could cause a fire in the cell. Safety properties can be significantly different for new and aged cells: for aged cells it can be observed that the "thermal on-set temperature" is often reduced. This can lead to unreliable operation features and increased safety considerations and requirements. This is especially important for cells cycled at low temperatures.

The thermal stability for uncycled cell materials and cells is well-documented, but the effect of cyclic ageing on thermal stability is far less studied. If the thermal stability or physical reaction of the cell changes, it also could change its ability to pass a propagation test. The degradation effects of cyclic ageing of lithium-ion cells are complicated and not fully understood.

8.1.4 Conclusion and recommendations

Operational conditions

As described above, operational temperature is one of the most important factors when it comes to battery safety. The ideal temperature for battery operation is at room temperature, while storage at low temperature will prolong the battery life. Both, low and high temperature operation can be harmful to battery life and safety. Reliable temperature control of the battery at system, module and cell level is crucial to ensure safe and efficient operation. Battery management systems that track and control both, the system, module and individual cell temperatures, coupled to an appropriate cooling and heating system (e.g. water or air circulation) can significantly contribute to battery safety, reduce battery degradation and extend battery life.

Operation of batteries must be carried out well within the manufacturer's recommended operation conditions with respect to C-rate, state-of-charge and voltage window and temperature. Over-charge and over-discharge have to be avoided. The immediate effects of detrimental operating conditions are always enhanced under non-ideal temperature.

Different battery failure scenarios (e.g. thermal runaway) must be considered during design and testing of battery storage systems. This includes the assessment of associated hazards and their mitigation through design, monitoring and maintenance. In general, the installation of multiple small-scale systems that are well isolated from each other in terms of fire propagation is

recommended over the installation of one single large system. In case of incidents this will (1) reduce the severity of such an incident and (2) allow for an energy storage backup system to be in place. The latter is specifically relevant for energy islands that rely on the installed battery energy storage system.

2nd life use of batteries

With large volumes of used batteries soon becoming available due to the ever-increasing number of electric cars in use, the re-use (2nd life use) of batteries in energy storage systems is gaining increased attention. By changing the type of application and thus the usage patterns, the battery's life and thereby its value can be extended. In a project funded by ENOVA, AS Batteriretur is implementing a 2nd life battery storage system at one of ELAND's pilot sites, Borg Havn, using recycled high-performance batteries. Safety considerations for the operation of such 2nd life cells must be adjusted: Initial studies [38] indicate a significant increase in thermal instability for aged compared to new uncycled cells, strongly depending on the 1st life operating conditions. As shown in [39], coordinated use of numerous of second life batteries grouped together, for example in a container, can provide a more optimal operation of the batteries and prolong the lifetime of the batteries before they are recycled. However, the behaviour of 2nd life cells with respect to safety and the best operating conditions with respect to both, safety and lifetime are not well understood yet. Further and more detailed research on the state-of-health and state-of-safety of 2nd life batteries is required, and for the time being, very conservative operational conditions are recommended.

8.1.5 References

[31]. LG-chem: https://docket.images.azcc.gov/E000007939.pdf

[32]. Vetter, J., et al., Ageing mechanisms in lithium-ion batteries. Journal of Power Sources, 2005. 147(1-2): p. 269-281.

[33]. Fleischhammer, M., et al., Interaction of cyclic ageing at high-rate and low temperatures and safety in lithium-ion batteries. Journal of Power Sources, 2015. 274: p. 432-439.

[34]. Gilljam, M., et al., 7E. Effect of electrical energy and aging on cell safety, in Li-Battery Safety, J. Garche and K. Brandt, Editors. 2018, Elsevier.

[35]. Friesen, A., et al., Influence of temperature on the aging behavior of 18650-type lithium ion cells: A comprehensive approach combining electrochemical characterization and post-mortem analysis. Journal of Power Sources, 2017. 342: p. 88-97.

[36]. Chen, S.C., C.C. Wan, and Y.Y. Wang, Thermal analysis of lithium-ion batteries. Journal of Power Sources, 2005. 140(1): p. 111-124.

[37]. Maleki, H. and J.N. Howard, Internal short circuit in Li-ion cells. Journal of Power Sources, 2009. 191(2): p. 568-574.

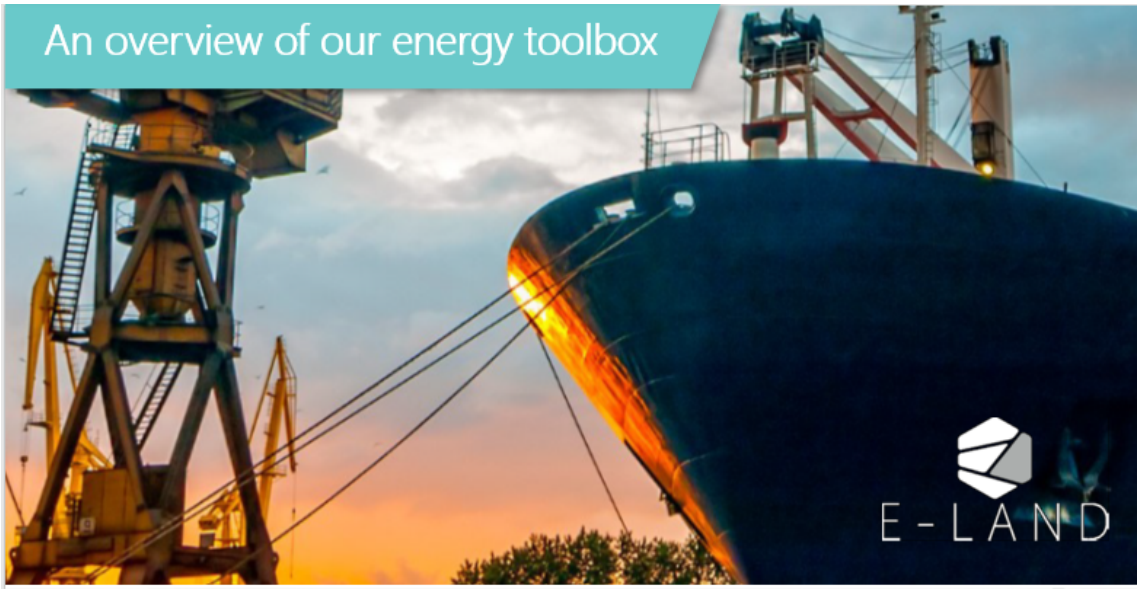
[38]. Lian T, Vie PJS, Gilljam M, Forseth S. (Invited) Changes in Thermal Stability of Cyclic Aged Commercial Lithium-Ion Cells. ECS Transactions. 2019. 89(1):73-81.

[39]. Faria R., Marques P., Garcia R., Moura P., Freire F., Delgado J., et al., Primary and secondary use of electric mobility batteries from a life cycle perspective. Journal of Power Sources. 2014. 262:8.

8.2 Appendix B: Flyers Description of the risk Privacy Security Safety

The three flyers found in the following have been created to simplify the ways that risk is communicated to the stakeholders, and especially to the future pilot sites and users. They address an overview of the risk management method as well as the key understanding with a dedicate focus on the different aspects of the risks related to data privacy, security and security.

8.2.1 An overview of our energy toolbox



E-LAND is developing a toolbox that provides an optimized schedule that enables the users to manage their energy needs in the most efficient way, at the lowest costs and with the least possible risks. This is what you need to know to connect the E-LAND toolbox to your existing infrastructure.

Risk management has been performed from the early stages of the project. The risk assessment has studied High Level uses cases defined by the project, to cover the maximum possibility and interaction within the toolbox and with the connected environment.

The risk assessment has identified risks pertaining to the solution and issued a risk register. This document is listing risks relevant to security, safety and data privacy, and evaluates the probability and the frequency for each risk.

.To help the future users doing through the risk study, the project has assigned three pilot sites, where the toolbox will be implemented and tested into different business environments, climate, European legislations, to cover most of concerns and the users' possibilities.

The experience from the pilot site will guide future users through potential risk faced during toolbox implementation.

Documentation regarding the risk assessment, the risk register and the implementation test will describe different process for each risk and step to ensure that the solution is secure, safe, and reliable for your site.

What type of information is available for the future users to assess the risk?
A technical description of the solution, comprehensive business cases and the risk management have been described in several reports publicly available. Additionally, several flyers are available describing the overall risk assessment process and activities to communicate how to better understand and how to best inform on Data privacy or warn Cyber risks.

More information on our websites: *https://elandh2020.eu* and *https://ife.no/prosjekt/e-land-horizon-2020-2/*

This project have received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

8.2.2 Risk Management

8.2.3 Privacy

Addressing Privacy Issues

E-LAND

Monitoring energy usage is essential to optimize and plan future usage. However, monitoring may capture information about individuals and impose on their right to privacy. Here are a few things to consider when planning and implementing the E-LAND toolbox.

Data collection: Even if a very few amount of data are collected or used in an area or by an equipment, the combination of this knowledge with energy usage patterns could tell you when someone arrives and which devices they are using. For instance, a specific office or electrical car charger stations.

Anonymization: Consider granularity needed for the purpose. Aggregations and groupings can make it harder to identify individuals. For instance grouping measurements in time intervals instead of timestamps, or group measurements from equipment or assets.

Cyber security: Outsiders could gain access to data and system settings through the network. Even if systems are not connected to the internet, weaknesses in an organization's network can be used as an entry point. Ensure proper security measures are taken to protect the organization's logical infrastructure.

Physical security: The system also need to be protected from physical threats. Ensure that outsiders can not access and manipulate components. Internals may also be a threat by unintentionally moving equipment, changing configurations, etc.

Compliance: Perform the proper assessments to ensure compliance with privacy laws, GDPR being one of the major policies in EU. Reassess the privacy. Changes are made both in systems and in organization. Consider if these changes require reassessments.

What is personal data?

Personal data are any information relating to an individual or that make identification of an individual possible by combining several sources.

More information on our websites: https://elandh2020.eu and https://ife.no/prosjekt/e-land-horizon-2020-2/

This project have received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

8.2.4 Security

The need to better understand the impact of choices and solutions with regards to digital risks has become more and more important. Addressing cybersecurity risks in energy islands is about balancing technical infrastructure and assets risks with business needs and protecting data from information disclosure and intentional harm.

Introducing new functionality, like the E-LAND toolbox to existing systems may introduce new vulnerabilities or weaknesses. Therefore risk assessment is performed to eliminate or reduce these risks. How have cyber risks been assessed in E-LAND?

First, an asset identification is performed: the information and assets are listed and analyzed for their confidentiality, integrity and accessibility.

Risk evaluation identifies the assets that are the most critical and provides priority for which cyber risks should be addressed first. In the E-Land project we started addressing cyber risks as early as in the conceptual stage by systematically evaluation high-level use cases.

The results of the analysis is a list of mitigations that propose solutions to reduce the risk and make the solution safer and reliable.

Communicating these aspects early is enabling all partners to have a focus on cyber risks throughout the E-LAND delivery product.

How to be sure that cyber risks are addressed in the E-LAND solution?
Addressing cybersecurity from the very beginning of a project is important to ensure that security be at the center of considerations. By addressing cyber risks from the design phase of the project, high-level requirements can be identified early and be used to involve all partners to ensure that cyber security is given a high priority throughout the project.

More information on our websites: https://elandh2020.eu and https://ife.no/prosjekt/e-land-horizon-2020-2/

This project have received funding from the European Union's **Horizon 2020 Research and Innovation programme** under Grant Agreement No **824388**.

8.3 Appendix C: Privacy notice template

This notice should be presented when the user enters the personal data. It should also be accessible if the user wishes to view it later. Pilot sites needs to fill in contact details (marked in yellow) in section 4) and 5). In section 6) the pilot site needs to fill in the party responsible for supervising privacy and GDPR (marked in yellow). This will be country specific. The pilot site functions as the Controller, meaning they are responsible for the collected data. The pilots collect data from their employees. Data is hosted locally on organization site. They have control of how they chose to use the application, who has access, local security measures etc. They can update and delete users. Hence, they are the Controllers. This privacy notice covers the use of toolbox in a piloting setting only.

Toolbox Privacy Notice

The software in this toolbox is developed as a part of the E-LAND project. Your Organization are participating in the project as a pilot site and you will be using the toolbox on behalf of your Organization. In this document you will find information about what data the application collects and how it's used, stored, your rights and contact details.

1) What data do we collect?

When you sign up as a user of the application, we collect the **name**, **username** and **e-mail** that you provide.

2) How do we use your data?

The data collected is needed for providing access to the application and its functionalities. At the time of sign-up, a user account is created for you. This account is used to for authentication when you access the application.

3) How do we store your data?

The user details are stored in a database at the Organization site. The database is protected by logical and physical security measures. It is stored as long as you wish to have access to the application. On account deletion the data is also deleted. For information about how to delete your account, see section

4) What are your data protection rights?

Access – You have the right to access your data. You can access this any time through your user account. **Rectification** – You have the right to request rectification of data. **Erasure** – You have

the right to erasure of your data by deleting your account or contacting us at [input company contact information]. Note that this will remove access to the application.

5) How to contact us

[Information about controller (Pilot site)] If you wish to exercise one of your data protection rights (access, rectification or deletion) you may contact us at: [Contact details for person on pilot site that handles this]

6) How to contact the appropriate authority

Should you wish to report a complaint or if you feel that we have not addressed your concern in a satisfactory manner, you may contact the [Information Commissioner's Office]. [Contact details]

8.4 Appendix D. Risk Mitigation Template

Table 22: Mitigation template relative to digital risks identified for 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.