Addressing Cybersecurity in Energy Islands

Per-Arne Jørgensen
Dep. of Risk, Safety and Security, Institute for Energy Technology, Norway. E-mail: per.arne.jorgensen@ife.no

John Eidar Simensen, Coralie Esnoul, Xueli Gao, Silje Arendt Olsen and Bjørn Axel Gran
Department of Risk, Safety and Security, Institute for Energy Technology, Norway.

Addressing cybersecurity threats in energy island is about balancing technical infrastructure and assets risks with business needs and protecting data from unwanted or unintentional information disclosure. Every organization that implementing smart grid functionality address cybersecurity issues that are diverse and complex for the organization. Especially when relying on existing legacy systems and infrastructure when interoperate with new assets connected to the smart grid. This potentially introduces new operational risks for the operator. This paper summarizes identified cybersecurity risks relevant for energy island as identified during the development phase of the E-LAND toolbox. Some of these risks include the local energy systems operator's exposure of existing legacy operational systems infrastructure, security and privacy concerns in multi-cloud environments, asset hardening and integration requirements, establishing a common baseline for network security and best practices, and data ownership and management to name some. The risks are discussed in more detail and exemplified through general use case examples before suggested mitigations for the risks are provided.

Keywords: E-LAND, energy island, cybersecurity, risks, privacy, data protection, system integrity.

1. Introduction

Digitalization is permeating domains and society, and 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. It is a challenge to provide innovative and economically viable solutions for extending the lifetime of current energy infrastructure. 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 allows for scheduling and planning of future energy use by enabling grid actor communication. The digital transformation has made cybersecurity a central challenge for the energy grid. When multiple digital systems are connected in new ways (e.g. internet of things and 5G) as 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, cybersecurity becomes complex. For the energy utilities and Local Energy Systems (LES) owners, the connected grid presents possibilities that both creates more revenue and value, but at the same time introduce 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 E-LAND project aims to provide a synergistic solution between technological, societal and business challenges that the energy sector faces. The main concept 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 realizing the project, which contains and contributes to a wide range of risks such as project risks, technical risks, information security risks and cybersecurity risks to name a few. The different types of risks require mitigations, actions and decisions made to prevent or reduce one type of risks might not be suitable for another. In this paper we focus on the process of identifying cyber risks related to the products developed in it.

The remainder of the paper is structured as follows: section 2 provides a high-level introduction to how we address risk in the project and address how cyber security risks are addressed generally, chapter 3 goes into detail on the risk identification process and provides examples from the use cases.

2. Background

In this chapter we present the foundation for the E-LAND project and go into more detail on the projects approach and main deliveries.

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

2.1 E-LAND project overview

The energy grid has in recent years seen a renaissance in most countries. Old grids have seen an influx of cheap sensors and increased data available to both maintain the grid and boost service reliability, and more modern grids have seen a transition from analogue to digital components throughout the grid enabling data of higher granularity, two-way communication and the use of advanced control and decision making algorithms, a potential that the E-LAND project is addressing specifically. E-LAND is a Horizon 2020 EU project to create novel solutions for decarbonized energy islands, comprising stakeholders across industries and countries around the globe. The E-LAND project consist of 14 partners: University of Girona, Schneider Electric, Borg Harbor, GECO Global, Smart Innovation Norway, Intracom SA Telecom Solutions, the Reiner Lemoine Institute, Valahia University of Targoviste, Centre for Resources in Energy Efficiency and Climate Change, the University of St. Gallen, Instrumentación y Componentes INYCOM, BSES Yamuna Power Limited, Tata Power Company and Institute for Energy Technology (IFE).

2.2 E-LAND risk management

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. IFEs 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 ISO 27002 and NIST 7628 guidelines. For a description of the risk assessment in the E-LAND project, as well as experiences on the risk and security practices, see ESREL 2020 paper by Gao et al (2020) and ESREL 2020 paper by Olsen et al (2020). The project explores possibilities and develops a toolbox through a practical use case approach which is detailed in the following.

2.3 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 cybersecurity issues is very important for all project participants. The high-level concept of the E-LAND toolbox in Figure 1 shows the main functional layers of the tools and the connection to the site-specific instances exemplified by pilot cases in the project.

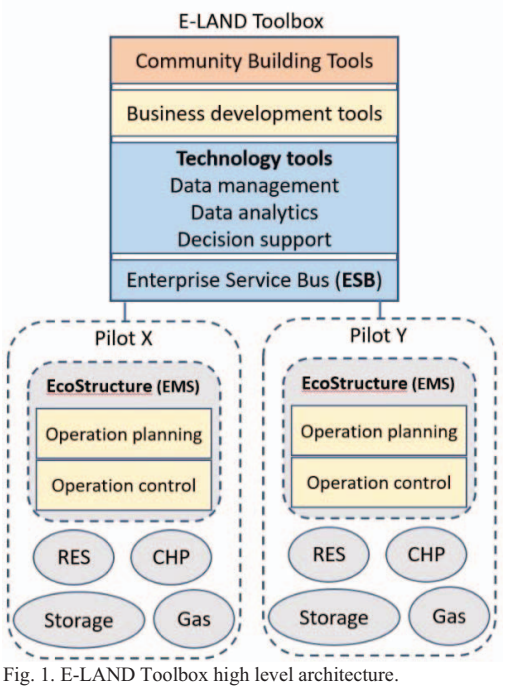

Fig. 1. E-LAND Toolbox high level architecture.

2.4 E-Land use cases

The E-LAND project contains three pilot sites: The Port of Borg in Norway, UVTgv University Campus in Romania, and the Walqa Technology Park in Spain. This paper focus on the pilot site in Norway, The Port of Borg specifically, an industrial area in the city of Fredrikstad with various industrial actors consuming large amounts of energy. The pilot site provides means to practically apply E-Land toolbox solutions and gain insights to valuable knowledge iteratively during development. At the site a mix of existing energy infrastructure such as a battery park and electric loading cranes will be mixed with solar heating (collectors), geothermal heating, solar cells for electricity and the reuse of electrical car batteries for storage. The use case provides a good mix of technologies and possibilities for exploration as a large part of the technological infrastructure will be deployed throughout the duration of the project.

3. E-Land cyber security risk assessment

Cyber security risk assessment in E-Land follows best practice approach of defining assets,

identifying main threats and identifying and mapping vulnerabilities in order to deal with these systematically. Cyber risk management is a subset of risk management and is seen in conjunction with the main risks of the project.

3.1 Overall risk assessment approach in the project

In order 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 cybersecurity 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. One way to achieve enough understanding is to apply the STRIDE threat model by Microsoft in conjunction with the domain specific Threat Landscape for Smart Grid (ENISA, 2013). ENISA 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. We applied Application Threat Modelling (OWASP 2020) as the approach for analyzing 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.

3.2 Model-based risk and threat assessment

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?

the STRIDE model in an E-LAND context with relevant examples identified by the use case analysis is described in Figure 2. Applying the STRIDE model on the use cases and addressing these questions gives a rapid understanding of the usage and possible high-level security risks with the different components building up the toolbox functionality and the architecture.

3.3 Stepwise risk assessment through applying the method on the use case

The development and integration of new functionalities in engineering systems requires a proper analysis and definition methodology in order 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. 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, the IEC 62559-2 standard series and the CEN/CENELEC/ETSI Smart Grid Coordination Group Grid Architecture Model (SGAM) Framework In the following we provide some examples from Secondary Use Cases (SUC) describing high-level functionality and intention in the E-LAND toolbox, and we exemplify for SUC2 and SUC6 (below) how applying the STRIDE method helped in identifying high level risks

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 tampered intentionally by hackers. Incorrect historical data is provided to the Energy Forecaster.
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 system calls
Information Disclosure	Confidentiality	Leakage of sensitive information	Personal (GDPR) information available on the internet. Poorly securing and handling of username and password in the system.
Denial of service	Availability	Non-availability of service	Web application not responding to user requests.
Elevation of privilege	Authorization	Able to perform unauthorized action	Normal user access can delete an admin account

Fig. 2. Threat and risk example overview.

SUC1: Forecast RES production

The RES production forecaster gives detailed data about the operations of the Energy Forecaster (EF). The EF is a module responsible for providing local RES production forecasts for 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: Communicate with field devices

This describes the process of the EMS for sending/retrieving data from the field devices of the LES, either directly or through the Building Management System (BMS). EMS is a system responsible for controlling the various assets of the LES as well as for the orchestration of its optimal operation. Energy Management application (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 Distributed Energy Resources (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 Energy Management System (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 EM) should have a well-defined API in order 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?* 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 have errors 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/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.

3.4 Summary – use case high level risks

Summarizing the identified risks we found that risks include the LES operator's exposure of legacy operational (OT) infrastructure, security and privacy concerns in multi-cloud environments, asset hardening and integration requirements, establishing a common baseline for network security and best practices, and data ownership and management to name some key risks. The schematic overview providing high level risks examples, sorted by type, is already provided in Figure 2.

For the E-LAND toolbox the integration of the following sub-systems and assets are relevant:

- 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 analyzing 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. Below the risks are discussed in more detail and exemplified through general use case examples before suggested mitigations for the risks are provided.

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 3.

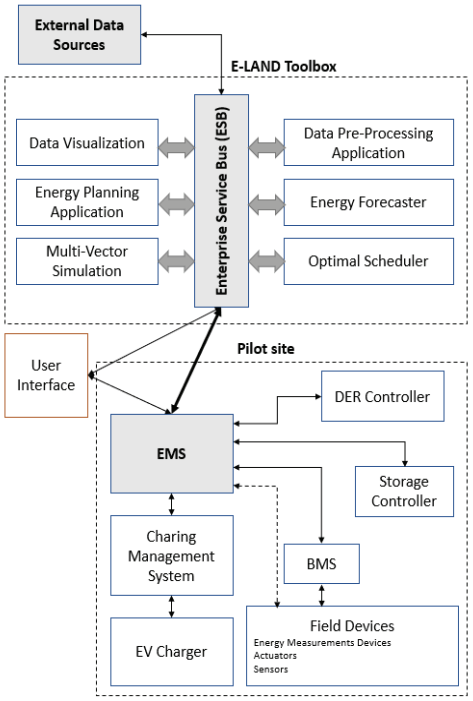

Fig. 3. Components of the E-LAND toolbox and the Pilot sites.

4. Discussion – cyber risk mitigation on the technical solution

In this chapter risks mitigations through the technical solution are discussed.

4.1 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 1, 2 and 3 provides mitigation examples on how these risks could be mitigated:

Table 1. 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.

Table 2. 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 3. 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.

Table4. 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.

4.2 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 4.

In our experience we find that custom application event logging is often missing, disabled or poorly configured, as identified in Table 5. 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 5. 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 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 (NIST 800-145, 2011). There is a complexity with interoperability between different cloud providers when addressing 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 datacenters 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 (Cloud Security Alliance, 2019). 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 (Simula, 2019). 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 6. Mitigation strategy: EMS Interfaces

Mitigation ID	MIT 11 EMS interfaces
Component	DER
Risk	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.
Mitigation	Protection from unauthorized access, authentication and secure transaction for all interfaces as well as accounting shall be supported.

4.4 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. When introducing DER equipment and integrating the toolbox different services in a multi-cloud environment this tends to be more complicated for the owners, especially understanding how their asset and information are being exposed and what kind of risks are introduced when integrating to the toolbox. The convergence of IT and OT infrastructure is still a challenge that needs to be addressed for better interoperability between these environments. The E-LAND toolbox will 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 7. 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.

5. Conclusions and Further Work

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. 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.

Next project activity for Borg harbor is to perform a detailed security mapping of assets and threats in order to identify site specific security requirements for the site. 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.

Acknowledgement

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

References

E-LAND: https://elandh2020.eu/ (last visited 10.01.2020)

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

ENSIA (2013), Smart Grid Threat Landscape and good practice (SGAM)

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

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

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

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

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

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

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

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

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

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

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