SMART GRID SECURITY METHOD: CONSOLIDATING REQUIREMENTS USING A SYSTEMATIC APPROACH

Marie CLAUSEN, Marion GOTTSCHALK, Sebastian HANNA, Christina KRONBERG, Christine ROSINGER, Maike ROSINGER, Judith SCHULTE, Johann SCHÜTZ, Mathias USLAR
OFFIS – Institute of Information Technology – Germany
Firstname.Familyname@offis.de

ABSTRACT

In this paper, we propose a method for a software engineering process to develop systems or architectures in the Smart Grid domain, also suitable for microgrids. It purposes – expanded with a visualization approach of Use Cases in terms of a Smart Grid Architecture Model – a better understanding by the different experts and a security consideration at a very early stage in the process. With this method, we want to establish a systematic approach in a standardized way.

INTRODUCTION

Due to the progress from a monopolistic power grid to a highly interconnected Smart Grid, new challenges emerge for ICT development of new components and systems in this domain. In this paper, we want to improve the development process of architecture and systems with a structured approach and address the three following challenges: The first one is to get a common understanding in the development process with experts of different domains. The second challenge deals with an interoperable and standardized design. And the third and currently highly topical subject is to get a secure design from the beginning of the development process *(security by design)*.
After this introduction, the following sections are structured as follows: First, we summarize the related work of this topic. Next, we explain the three steps of the systematic method in detail and give a short insight of the corresponding toolchain. After that, we demonstrate the method with an appropriate example for a small microgrid of the project µGrip[1]. Finally, we give a short conclusion and point out some further work.

RELATED WORK

The work presented within this contribution is based on several existing methods and standards which are applied in context. The most prominent standards will be presented in this contribution. One of the crucial aspects of security is the analysis of threats towards the systems in the critical infrastructure [1].
Systems can be secured in at least two ways. One way is to focus on the security at design time, taking into account requirements which are based on theory. The second way focuses on the aspect of legacy systems and their interfaces and make sure those systems remain safe and secure. In the US, the *National Institute of Standards and Technology (NIST)* has established a good set of mitigations for classes of interfaces generic in the Smart Grid. Various studies as well as projects have used this very set of mitigations. However, they do not provide a set for risk management and a way to map existing systems onto the conceptual model by NIST. In [2], we outline the need to come up with a meaningful structured way to create a system-of-systems architecture. Combining the state-of-the-art from NIST and the *European Network and Information Security Agency (ENISA)* in terms of security, in addition to the work from the M/490 mandate on the *Smart Grid Architecture Model (SGAM)* and use case elicitation [3], we establish a way to use architectural knowledge in the context of security analysis.

SYSTEMATIC METHOD

The adressed method consists of three steps and can be seen in Figure 1. The first step is the **elicitation of requirements**, the second one the **visualization** of the requirements and third step contains the **security analysis**. This method is supported by a toolchain of different tools which are listed on the right side below each icon, but which is not the main focus in this paper. To get a systematic method, different kinds of standards and standard-similar approaches are needed and listed as *Foundation* on the left side below every icon.

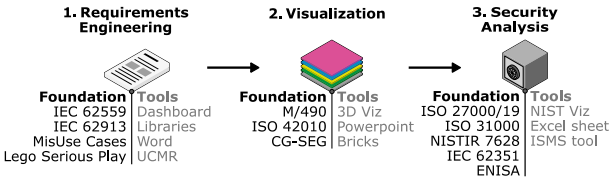

Figure 1: Systematic method (left) and toolchain (right) in three steps with standards & standard-similar documents

Step 1: Requirements Engineering

Step 1 of our method gives the developers a first mutual and consolidated view of the considered object. For this, the IEC 62559[2] or the IEC 62913[2] provide a guided structure with a template for gathering an appropriate Use Case (UC) with its functionalities and requirements. Within the templates the UC is described in detail, with

[1] The authors would like to thank the EC for funding the work presented in this very contribution under the ERA-NET Smart Grid+ funding schema with no. 77731 and H2020 with no. 774500.

[2] The IEC 62559 and IEC 62913 are available at http://www.iec.ch/.

UML diagrams, actor descriptions, exchanged information and requirements. This also includes security requirements but is not the main focus of these templates. Hence, an extension of the IEC 62559 UC Template to improve security issues is useful. For this, we use the concept of Misuse Cases with an additional Misuse Case Template. The document-based requirements engineering process can be supported using the more hands-on Lego® Serious Play® (LSP) methodology. LSP helps to build a shared understanding of the system and to elicit implicit and tacit knowledge that oftentimes gets lost in interdisciplinary contexts.

Requirements Elicitation

The European mandate M/490 developed a first version of a UC Methodology to describe requirements for the Smart Grid in a common, structured way. The IEC has decided to apply this methodology and published it in the standard series **IEC 62559 Use Case Methodology** in four parts. The standard explains the methodology, provides a UC Template and an XML structure, and mentions best practices to use it. The UC Template depicts the main part of the standard series and is divided in eight sections: (1) Description of the UC, (2) Diagrams of the UC, (3) Technical details, (4) Step by step analysis of UC, (5) Information exchanged, (6) Requirements, (7) Common terms and definitions, and (8) Custom information. This structure helps to consider requirements from different viewpoints – at the beginning from the management perspective and thereafter from technical view [4].

The **IEC 62913**, titled *Generic Smart Grid Requirements* contains a UC Template especially for the Smart Grid domain. Within the same-named working group TC8/WG6 of the IEC, a narrow number of generic UCs for Smart Grids based on the IEC 62559 Template are selected and published in the IEC 62913-1. This technical specification provides generic UCs with a comprehensive list of functional and non-functional requirements and applications for Smart Grids according to the IEC system approach. Thereby, the IEC 62913 aims at providing a consistent and directly applicable framework for every stakeholder of the power supply system and their Smart Grid project implementations.

Misuse Cases

In the IEC 62559 UC Template, the security aspect is hidden in the non-functional requirements. For an accurate analysis of security issues the **Misuse Case Template** provides a much more detailed way. The template based on the work of Sindre & Opdahl [5] and the IEC 62559. After creating the UCs, the possible misuses can be documented. The template has the opportunity to describe attacks of malicious actors, but also the Misuse Case by unintended behaviour. The connections and dependencies of the Mis- and Use Cases are indicated particularly in the diagrams.

Lego® Serious Play® (LSP)

The **LSP methodology** is a facilitation technique created by the LEGO Group. During the structured and guided process, a facilitator confronts participants with different tasks. Each participant then creates metaphorical Lego brick models as answers to those tasks and shares them by telling the story behind their model. The approach is based on research which suggests that hands-on, "minds-on" learning produces a deeper, more meaningful understanding of the world and its possibilities.

Step 2: Visualization

In Step 2, the **SGAM** is used to get a structured visualization of the described UC and a better understanding by the different experts. The SGAM bases on the IEC 42010 and is a result of the EU mandate M/490 and its successor *Coordination Group on Smart Energy Grids (CG-SEG)*. The SGAM, which is displayed in Figure 2, gives a 3-dimensional cube for the Smart Grid with its domains, zones and interoperability layers where the actors of the UC are placed accordingly with their communication interfaces.

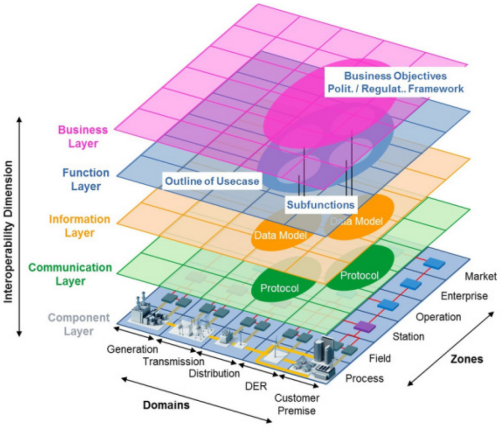

Figure 2: The Smart Grid Architecture Model (SGAM)

The information that is visualized within the SGAM can be derived from the UC description from Step 1; the used section for every layer can be seen in Table 1.

SGAM Layer	Information & Section of IEC 62559 Template
Business	Related business cases, Section 1.3
Function	Objectives, Section 1.3; Scenarios Section 4.1
Information & Communication	Information exchanged, Chapter 5; Requirements, Chapter 6
Component	Actors, Section 3.1; Step-by-Step analysis, Chapter 4

Table 1: Information from UC Template for SGAM layers

Step 3: Security Analysis

Step 3 describes the security assessment based on the gathered information of the former steps to identify appropriate security measures for the corresponding UC. For this, different security standards with management and technical viewpoints are used; these are listed in Figure 1 below the third step and will be described in the following paragraphs.

Information security management system (ISMS)

The **ISO 27000** and its different parts are the series of general security techniques for ISMS. It gives a framework and instructions for the certification of a company and its ISMS. Using an ISMS is state of the art and is

regulated in several domains by different laws, e.g. the German *IT-Sicherheitsgesetz* (IT security law) or the *Messstellenbetriebsgesetz* (measuring point operation law). There are also domain specific parts of this standard, e.g. the ISO/IEC 27019 for the energy domain.

Information security in the Smart Grid domain

The intermediate report **NISTIR 7628**[3] from the American **NIST**, 2014, deals with guidelines for Smart Grid Cyber Security and establishes an approach for a security analysis of communication interfaces. Besides a CIA (**C**onfidentiality, **I**ntegrity, **A**vailability) analysis for an interface, it provides several logical interface categories with a list of security requirements which have to be satisfied for certain levels of security and risk. To adapt this approach for our method, we made a mapping of the NISTIR 7628 actors to the SGAM [1].

The **ENISA** published their **technical guidelines** for *Appropriate security measures for smart grids* in 2012[4]. They are grouped in three sophistication levels and ten domains which give advice to the stakeholder about a framework of minimal cyber security measures. In their Chapter 6, they also include a table where the security measures of the NISTIR 7628 and the ISO/IEC 27019 are mapped and put into relation with each other.

In various parts, the **IEC 62351**[5], titled *Power systems management and associated information exchange – Data and communication security*, gives security recommendations for the energy domain. It describes different topics for security solutions, e.g. for different communication protocols, key management recommendations or architecture guidelines. In our method, this standard is not yet implemented in practice.

Risk management

In the third step the security analysis needs risk management as additional assessment. Hence, we apply the standard **ISO 31000** with the title *Risk management – Principles and guidelines* and the **ISO 27005** titled *Information security risk management*. The ISO 31000 is used for risk assessment in general and the ISO 27005 deals – as one part of the ISO 27000 series – with risk management for IT security. Furthermore, we apply some approaches from the Smart Grid Information Security group of the EU mandate M/490[6].

TOOLCHAIN

As previous described, each step of the proposed approach is supported by a mutually complementary and interoperable set of tools, which are depicted in Figure 1 on the right side of every step.

The **first step** of the process starts with the elicitation of requirements. Since the IEC 62559 describes a standardized UC Template for the Smart Grid domain that provides a structured process to collect requirements from different viewpoints as well as their relations to each other, it is useful to utilize that within the toolchain. In order to do this, the toolchain provides for the first step: a Word Template to document UCs in accordance to the IEC 62559 UC Methodology, a Use Case Management Repository (UCMR) to collect, manage and analyze the UCs, importable XML- and Excel-Libraries e.g. for actors and requirements and additionally, a Dashboard to summarize and analyze UCs and their Key Performance Indicators (KPIs).

At the **second step**, the previously described and collected UCs are visualized in a three-dimensional SGAM cube by a Power Point Add-on or the more sophisticated OFFIS 3D-Viz webviewer application. To support this process step, an interlinking between the UCMR and the OFFIS 3D-Viz allows the generation of semi-automated SGAM models. As a complement to the digital methodology, the SGAM model also can be constituted manually with Building Bricks and digitized with additional tools later. The advantage of the visualization by physical Building Bricks is the interactive and intuitive creation of SGAM models during meetings and workshops.

The resulting UCs and SGAM models form the basis for the subsequent security assessments of the **third step**; therefore, further tools are being developed. The NIST-Viz is an application, which links actors with security requirements and standards. Also, a collection of standards is summarized in an Excel Sheet. ISMS tools help to define manage and improve the information security for systems, e.g. by automated analyses with existing data from actors involved.

EXAMPLE

Exemplarily, we describe our method on the basis of a UC from the project µGrip which deals with the economic optimization of a microgrid. Thus, the title of the example UC is ***Optimization of revenue in microgrid***. Due to lack of space, in this section, only the main points of the introduced method are shown.

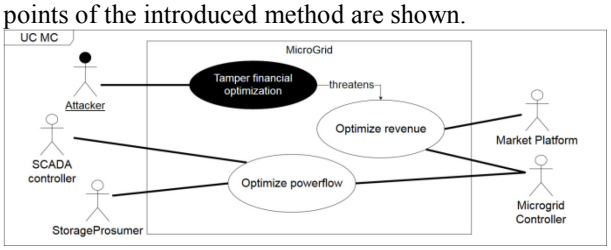

Figure 3: Use and Misuse Case Diagram of MG example

In **Step 1**, we gathered the information of this UC in the IEC 62559 Template. The objective of this UC is a financial optimization of the power flow in a microgrid. We identified the following four actors and described them in detail in the template with some illustrations like the UC diagram in Figure 3, where the actors are displayed as stickmen. The sequence diagram in Figure

[3] This publication is available free of charge from http://dx.doi.org/10.6028/NIST.IR.7628r1

[4] Free at https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids.

[5] A detailed insight of this standard can be found at http://iectc57.ucaiug.org/wg15public/Public_Documents/White_Paper on Security Standards in IEC TC57.pdf.

[6] EU Mandate M/490 SGIS-Intermediate-Report in 2014 https://www.dke.de/resource/blob/765980/6bed01cef75f11a3d0092c9eb9a20739/smart-grid-information-security-data.pdf.

4 represents the interaction of the actors which are displayed ahead of the illustration as objects. The first actor is a **microgrid controller (MC)**, which optimizes the power flow and the revenue of the microgrid. As second actor, there is the **market platform (MP)** which analyzes the market clearing prices for supporting the MC in optimizing the revenue of the microgrid. The third actor is a **SCADA controller (SC)**, which reacts to the signals of the MC and controls the energy production and consumption of the microgrid. For the fourth actor, we summarized the producing, consuming and storing actors (like wind or a gas turbines, households or cold warehouses and batteries e.g. in electric vehicles) in one actor, called **StorageProsumer (SP)**. At the upper left side you can see the actor **Attacker**, who wants to tamper the financial optimization. This black illustration represents a Misuse Case. This Misuse Case was documented in the Misuse Case Template which was described in the *Systematic Method* section in Step 1. An additional LSP-model was built, which supported us in constructing and gathering the UC.

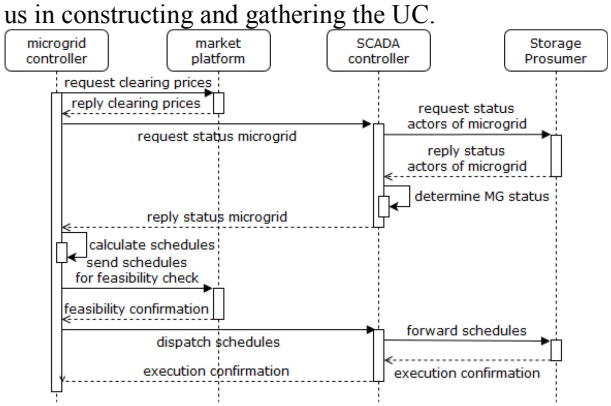

Figure 4: Sequence diagram of MG Example

In **Step 2,** we use the SGAM for a structured view of the UC to give the different experts the same sight in the different domains, zones and layers.

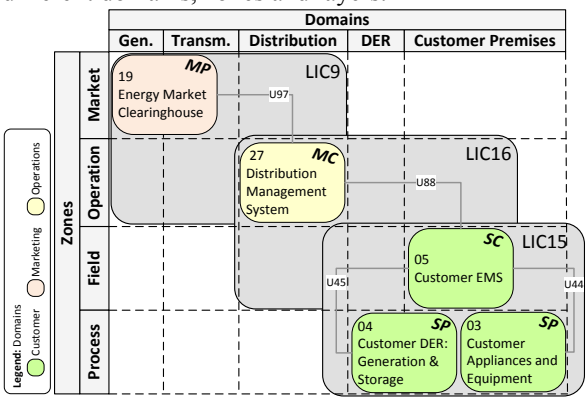

Figure 5: Illustration of Actors in the SGAM

We also use the SGAM illustration in **Step 3** for the security analysis. For this, we allocate the identified actors with the NISTIR 7628 actors and map them to the SGAM: The MC is represented by the *Distribution Management System* (No. 27); the MP by the *Energy Market Clearinghouse* (No. 19), the SC by the *Customer Energy Management System* (No. 05) and the SP by the *Customer DER* (No. 04) and the *Customer Appliances* (No. 03). With this, we can derive the interfaces between the actors and their appropriate **Logical Interface Category** (LIC), which is illustrated in the SGAM in Figure 5.

With that allocation, we use the **CIA assessment** of the NISTIR 7628 for the risk analysis for every interface of the UC which can be seen in Table 2. Next, the related **security requirements**, e.g. SG.AC-7: *Least Privilege* or SG.AC-21: *Passwords*, from the NISTIR 7628 and the ENISA can be derived for each communication interface of the UC by analyzing the LIC, the required impact level and the possible security enhancements from the respective domains. Finally, this approach leads to a holistic development process.

LIC	Description	C	I	A
9	Interface with B2B connections between systems usually involving financial or market transactions.	H	H	M
15	Interface between systems that use customer (residential, commercial, and industrial) site networks such as HANs and BANs.	L	M	M
16	Interface between external systems and the customer site.	H	M	L

Table 2: Identified Interface Categories of NISTIR 7628

CONCLUSION AND FURTHER WORK

In this paper, we introduced a Smart Grid Security Method as a systematic approach. We explained the method with an appropriate example of a microgrid. We also gave a short description of the supporting toolchain. The different steps, together with the toolchain, provide a holistic security method right from the beginning of the development process.

For further work, the integration of the not yet implemented standards and regulations, like the mentioned *IEC 62351* or the *General Data Protection Regulation*, will be in focus.

References

[1] M. Uslar, C. Rosinger, S. Schlegel: *Security by Design for the Smart Grid: Combining the SGAM and NISTIR 7628*. Computer Software and Applications Conference Workshops (COMPSACW), 2014.

[2] M. Uslar, D. Engel: *Towards Generic Domain Reference Designation: How to learn from Smart Grid Interoperability*. D-A-CH Energieinformatik, Karlsruhe, 2015.

[3] H. Englert, M. Uslar: *Europäisches Architekturmodell für Smart Grids-Methodik und Anwendung der Ergebnisse der Arbeitsgruppe Referenzarchitektur des EU Normungsmandats M/490*. Tagungsband VDE-Kongress 2012.

[4] M. Gottschalk, M. Uslar, C. Delfs: *The Use Case and Smart Grid Architecture Model Approach*. Springer Briefs, 2017.

[5] G. Sindre, A.L. Opdahl: *Template for Misuse Case Description.* Proceedings of the 7th Workshop Requirements Engineering Foundation for Software Quality, REFSQ, Switzerland, 2011.