6-18-2022

Towards Cybersecurity by Design: A multi-level reference model for requirements-driven smart grid cybersecurity

Sybren de Kinderen
Eindhoven University of Technology, sybren.dekinderen@uni-due.de

Monika Kaczmarek-Heß
University of Duisburg Essen, monika.kaczmarek-hess@uni-due.de

Simon Hacks
University of Southern Denmark, shacks@mmmi.sdu.dk

TOWARDS CYBERSECURITY BY DESIGN: A MULTI-LEVEL REFERENCE MODEL FOR REQUIREMENTS-DRIVEN SMART GRID CYBERSECURITY

Research Paper

Sybren de Kinderen, Eindhoven University of Technology, Eindhoven, The Netherlands, s.d.kinderen@tue.nl

Monika Kaczmarek-Heß, University of Duisburg-Essen, Essen, Germany, monika.kaczmarek-hess@uni-due.de

Simon Hacks, University of Southern Denmark, Odense, Denmark, shacks@mmmi.sdu.dk

Abstract

This paper provides a first step towards a reference model for end-to-end cybersecurity by design in the electricity sector. The envisioned reference model relies, among others, on the integrated consideration of two currently fragmented, but complementary, reference models: NISTIR 7628 and powerLang. As an underlying language architecture of choice, we rely on multi-level modeling, specifically on the Flexible Meta Modeling and Execution Language (FMML^x), as multi-level modeling supports a natural integration across different abstraction levels inherent to reference models. This paper's contributions are a result of one full consideration of Wieringa's engineering cycle: for problem investigation, we describe the problems the reference model should address; for treatment design, we contribute the requirements the reference model should fulfill; for treatment implementation, we provide reference model's fragments implemented in an integrated modeling and programming environment. Finally, for treatment evaluation, we perform expert interviews to check, among others, the artefact's relevance and utility.

Keywords: Cybersecurity By Design, Smart Grid, Multi-Level Reference Model, Security Analysis.

1 Introduction

The electricity grid is increasingly reliant on IT, among others, to enable integration of both the behavior and actions of all users connected to it (Gunduz and Das, 2020; Mohassel et al., 2014), leading to the notion of a "smart grid" (Mohassel et al., 2014). This smart grid holds the promise of contributing to an economically efficient power system, as well as to security and continuity of power supply (Fang et al., 2012; Luthra et al., 2014). At the same time however, inherent to the increased reliance on IT is also an increase in IT security weaknesses, both unintentional and intentional, which potentially disrupt the balance of electricity supply and demand (Gunduz and Das, 2020).

Indeed, the existing security vulnerabilities highlight the need to foster smart grid security. In the past, organizations usually reacted to security threats, once they have occurred. However, the increasing frequency and sophistication of attacks requires a more proactive approach. To achieve this, organizations can apply a cybersecurity by design approach, which demands to account for cybersecurity concerns throughout an entire product lifecycle (Geismann, Gerking, and Bodden, 2018). To support cybersecurity by design, various instruments exist, e.g., standards and guidelines like the NISTIR 7628 (NIST Smart Grid Cybersecurity Panel, 2010), or the IEC 62351 (WG15, 2016), often complemented

by dedicated modeling approaches or instruments supporting the security-related analysis by means of (semi-)automated simulations using domain-specific languages (S. Hacks, Katsikeas, et al., 2020), or by fostering the discussion of the security architecture (Neureiter et al., 2016). Although all those approaches support a variety of security demands, they (1) are fragmented, in the sense that each initiative focus on selected aspects only, and do not cover all phases of cybersecurity by design process, (2) differ in the way they are disseminated (e.g., different language architectures are used), which may hinder their application in tandem, (3) are either too generic, to be applicable in a wide set of scenarios, and providing high-level guidance only, or too specific, and therefore, not easily reusable in other contexts. These issues hinder organizations to adopt a broader range of different approaches, as they all require certain capabilities in organizations.

Combining complementing approaches would ease the adoption and reduce the effort, as certain tasks are shared among the approaches. For example, consider two smart grid cybersecurity modeling languages: powerLang (S. Hacks, Katsikeas, et al., 2020), and reference model adaptations of the NISTIR 7628 (Kinderen and Kaczmarek-Heß, 2019, 2021). These languages, which will also form a basis for the main artifact presented in the paper, focus on different, but complementary aspects of smart grid cybersecurity. powerLang focuses on modeling and simulating attacks on smart grid assets, whereas NISTIR 7628 constitutes a reference architecture for defining ideal-type smart grid scenarios and associated security requirements. While both modeling languages are useful in their own right, it is difficult to use these languages together: besides different foci, they differ in their dissemination in terms of underlying language architecture, and offer differing capabilities of balancing the generic and the specific.

Especially the last point relates to the challenges that reference models sui generis face. Those can be categorized as follows (Kinderen and Kaczmarek-Heß, 2019, 2021): (1) challenges in accounting at the same time for both generic and specific aspects, (2) challenges in expressing variability and avoiding redundancies within a reference model, and (3) challenges connected with supporting application and adaptation of a reference model while ensuring its compliance. As the results of our previous work point out that multi-level modeling with integrated modeling and programming comes with a promise to address these challenges (Kinderen and Kaczmarek-Heß, 2019, 2021), thus, in this research we use multi-level modeling to integrate fragmented modeling approaches to address the needs of organizations to design and manage cybersecurity in a smart grid context with the aim to: (1) provide a comprehensive solution accounting for multiple perspectives on cybersecurity, (2) provide both general as well as specific guidelines to design secure systems, (3) ensure both the customization possibilities, as well as compliance.

This paper constitutes the first phase in the context of a larger research project aiming at proposing a reference model providing an end-to-end support for cybersecurity by design in the electricity sector. The objective of this paper is to provide the foundations for the reference model, in terms of setting out requirements, providing a first partial sketch of a model, and offering its first validation. Our research project can be categorized as design science (Hevner, March, Park, et al., 2004), and we follow the stages from the well-established engineering cycle (Wieringa, 2014, p. 28). Particularly, this paper covers the following phases of the cycle, and is structured accordingly: During problem investigation, by means of conceptual argumentative exploration (as per the introduction), as well as a confrontation of our vision and goals to the state of the art, we first identify a research gap to which our reference model is a response. During treatment design, on the basis of driving goals (section 2) and an illustrative scenario, we identify a set of requirements which our reference model should fulfill. During treatment implementation we provide a first sketch of a multi-level reference model and implement it in a supporting tool (section 4). Finally, during treatment evaluation we provide a first evaluation of our approach by means of a confrontation to the requirements, as well as feedback gathered from expert interviews (section 5).

2 Vision and Motivating Scenario

2.1 Vision and Goals

Due to the importance of cybersecurity and the challenges of a cybersecurity by design analysis, our aim is to provide organizations with a reference model that supports them through different stages of creating secure systems. Our target organizations are therefore companies, active in the smart grid domain, interested in digitalizing their processes, and valuing security aspects in the design of the new architecture, both to ensure the functionality of their processes and to protect the sensible data of their customers.

A broad variety of knowledge is needed to accomplish this task, such as knowledge about the power grid, the related IT components as well as an understanding of cybersecurity (Sun, Hahn, and Liu, 2018). Therefore, we aim to provide a solution that enables also experts in one of the fields only, and just basic knowledge in the others, to design secure systems (Goal 1). Thus, the targeted reference model should provide support during all phases of an undertaking: starting from the identification of (security) requirements, through identification of relevant assets, risk assessment, identification of countermeasures, and finally design of a supporting architecture.

It is not solely of importance for companies to design secure systems, but also to create sufficient trust of their stakeholders into their system. One way to achieve this, is to implement best-practices and follow acknowledged standards. Often, these allow certification easing the communication of the invested efforts. In line with this, we desire our solution to incorporate established best-practices or standards (Goal 2). The power grid is a complex system, and issues in one segment can have significant influence on other segments. Therefore, it is of high importance that the entire system is designed in a robust fashion. In line with this, security knowledge should be generalizable, so that others can also benefit from it. Consequently, our solution should be generalizable and extensible to other participants in the power grid (Goal 3).

2.2 Exemplary Scenario

To illustrate our goals and targeted outcomes, consider the following exemplary scenario. A utility company, ACM-e, wishes to digitalize their processes. They have deployed classical analog meters at their customers' side, which are supposed to be exchanged with modern smart meters to enable, inter alia, a fully digitalized billing process. Simultaneously, ACM-e is aware that security aspects are important for the new architecture, both to ensure the functionality of their processes and protect the sensible data of their customers.

Therefore, the use case of interest refers to the billing in smart grids, which relate to the capturing and processing of time-based energy consumption data from customers' smart meters (Brown et al., 2008). The automated data collection enables ACM-e to transform their billing processes and to offer time-based rates to their customers. Further, they are able to remotely initiate or terminate services without sending a technician. Finally, the more detailed available data can ease the optimal planning, design, and maintenance, as well as the development of tailored services.

However, this digitalization enables attackers to penetrate the infrastructure, which was previously not possible. To address this, we propose to follow a three stepped approach following well-established approaches (Morana and Uceda Vélez, 2015; NIST Smart Grid Cybersecurity Panel, 2010):

Firstly, we *select a scenario* (i.e., a use case in the NISTIR terminology), in which we apply our reference model. Here, we consider ACM-e, which desires to reduce its costs associated with meter reading, as well as increasing its billing accuracy and distribution planning. Accordingly, the key elements for the following risk assessment are determined. In our case, these are reading the meters and the concluding validation, as well as the customer bill generation.

Secondly, a *risk assessment is performed*. We combine a top-down and a bottom-up approach, as the top-down approach ensures that the overall process is considered, and we ensure a sufficient depth on

security threats for single assets in the bottom-up approach. To realize the top-down approach, we may, e.g., rely on the NISTIR standard and identify NISTIR interfaces (NIST Smart Grid Cybersecurity Panel, 2010), which are relevant for the respective use case. In case of ACM-e, we recognize that the NISTIR interfaces 13 and 14 (NIST Smart Grid Cybersecurity Panel, 2010) are of relevance, due to their focus on advanced metering infrastructure for billing purposes. These interfaces point us to relevant assets (i.e., smart meters and customer gateways), and relevant security requirements including a prioritization. Following these prioritization, the interfaces 13 and 14 solely differ in their perception of availability. As the use case is related to billing, the availability is not of high importance (especially relative to confidentiality and availability of metering data (NIST Smart Grid Cybersecurity Panel, 2010)), and we opt for a low priority of availability.

Next, we perform a bottom-up analysis by identifying involved assets and their interconnection. On the one hand, we can identify different assets that are involved in the described use case (Coelho, Gomes, and Moreira, 2019; Kumar et al., 2019; NIST Smart Grid Cybersecurity Panel, 2010): a smart meter, a customer gateway, and a metering data management system. Additionally, we reveal the communication between these assets along different types of networks (Coelho, Gomes, and Moreira, 2019; Kumar et al., 2019): Home Area Network (HAN) and Wide Area Network (WAN). Now, we determine threats to these assets and networks that are categorized along the different threat categories (confidentiality, integrity, availability, CIA). For example, the confidentiality for a customer gateway is threatened by a traffic analysis (Procopiou and Komninos, 2015), its integrity by replay attacks (Namboodiri et al., 2013), and its availability by Denial of Service (DoS) (Procopiou and Komninos, 2015). Similarly, the confidentiality for the WAN is threatened by eavesdroppping (Procopiou and Komninos, 2015), while man-in-the-middle (MITM) attacks (Procopiou and Komninos, 2015) are a threat to both confidentiality and integrity.

Thirdly, we *design the security architecture*. Therefore, we identify countermeasures to the found threats. For example, cryptography addresses (or at least complicates) MITM, eavesdropping, and replay attacks (Nam- boodiri et al., 2013), while a comprehensive set of measures like ingress/egress filtering can serve as mitigation for DoS (Zeb, Baig, and Asif, 2015). Given the previous steps and the mitigations, we assess the impact upon initially designed infrastructure. For ACM-e, we conclude to apply encryption to increase confidentiality and integrity, while countermeasures for availability are not further considered.

2.3 Resulting Requirements

Considering the vision and goals we identify the following requirements (R).

R1: The reference model should provide support during all phases of cybersecurity by design, and thus, account for threats, attacks, assets involved, as well as effects, among others. *Rationale:* In-line with Goal 1, the reference model should provide support during all phases of cybersecurity by design: starting from the identification of (security) requirements, through the identification of relevant assets, risk assessment, the identification of countermeasures, and finally the design of a supporting architecture. It follows that the reference model should adhere to well-established domain-specific concepts and rules of cybersecurity domain, as used in existing standards and norms. To foster understandability of the reference model, the terminology used by the community (Frank, 2013) should be applied. In turn to ease its adoption, also good practices and state of the art should be considered (Kelly and Tolvanen, 2008) (Goal 2).

R2: The reference model shall be scenario driven. *Rationale*: Organizations are usually change driven. A driver for such changes can be scenarios, which determine a function desired from a system for a certain business demand like billing. Consequently, the scenarios provide a basis for security requirements and their prioritization. As mentioned in the description of the targeted vision, for instance, in their process for developing a cybersecurity strategy, NISTIR 7628 (NIST Smart Grid Cybersecurity Panel, 2010, pp. 8–12) start with use cases (scenarios, i.e., a function desired from a system, like billing), as a basis for security requirements and their prioritization. Subsequently, these scenarios, to a considerable extent, drive the identification of involved assets and threats (Goal 2).

R3: The reference model shall provide both high-level, generic security-related, as well as threat- or asset- specific information; and, at the same time, the reference model shall consider both concepts generally relevant to security, as well as security concepts specific for the electricity sector. *Rationale*: To support the targeted vision, the reference models should encompass information at different level of granularity, from high-level, generic information to specific information relevant to a specific threat or effect. The top-down approach enables non-experts to benefit from pre-defined templates and, thus, compensates missing knowledge (Goal 1). In addition, the general concepts of cybersecurity are the same among different domains (security requirements, e.g., CIA triad, concepts of threats, and assets). At the same time, on the concrete level of implementation, concrete concepts for the domain under study are needed (Goal 3), e.g., in the smart grid other assets are used than in a hospital. Thus, the reference model should provide information at varying level of abstraction, both horizontally and vertically, i.e., it should cover both general security concerns, and concerns specific to the electricity sector, as well as it should cover different types of threats/assets etc., and dependencies among those. It follows, cf. (Kinderen and Kaczmarek-Heß, 2019, 2021), that the language architecture used to design the targeted reference model shall (1) allow for the natural modeling of domain hierarchies and allow for expressing both generic, as well as specific knowledge; as well as (2) allow for incorporating domain knowledge into the reference model. Regarding the latter, as considerable expertise regarding assets, threats etc., is available (Xiong and Lagerström, 2019), therefore, there should be a possibility to express current knowledge about requirements, possible threats, countermeasures, effects, as well as assets, and incorporate it into the model. Please note that it requires assigning state to classes, which is not supported by conventional language architectures for meta modeling, cf. (Kinderen and Kaczmarek-Heß, 2019, 2021).

R4: The reference model and its underlying language architecture shall support (semi-)automated security analysis, e.g., it should be possible to run computations and simulations. *Rationale*: To provide semi-automated support for a variety of security analysis, next to supporting a static perspective on the domain at hand, the language architecture shall also support a functional perspective. Such semi-automated simulations would also enable non-security experts to assess the security of their systems (Goal 1).

3 Cybersecurity by Design Approaches and Their Integration

3.1 Related Approaches

Previously, we have elaborated on the vision and requirements for our work. Our research is grounded in existing work on other approaches supporting cybersecurity by design and its phases (i.e., on the abstract level, gathering security requirements, analysing existing risks, and designing secure systems). Conceptual modeling in general, and domain-specific modeling languages in particular, have proven themselves to be useful instruments to support those analyses. Indeed, different approaches have been proposed that can be used to support different phases of the cybersecurity by design process. For instance, to support the engineering of security requirements one can employ, e.g., STS-ml, an actor- and goal-oriented requirements modeling language for socio-technical systems (Paja, Dalpiaz, and Giorgini, 2015) or ModelSec (Sánchez et al., 2009) to relate security requirements to assets, threats and contingency plans. Nevertheless, identification of security requirements, as well as further stages, even if supported by dedicated modeling languages, are not trivial to conduct and require substantial knowledge on the domain under study, as well as cybersecurity relevant concepts (Morikawa and Yamaoka, 2011). Here additionally, reference models and standards focusing on cybersecurity come into play. In the following, we discuss only selected ones, being the most relevant to the goals of our research.

The most widely-known reference model for smart grids cybersecurity is the NIST reference model for cybersecurity, NISTIR 7628 (NIST Smart Grid Cybersecurity Panel, 2010), which offers concepts, cybersecurity requirements, and guidelines. Those elements are specific for the energy sector in terms of, e.g., considered actors, and IT infrastructure types. For example, NISTIR distinguishes different

equipment types, among others, a smart meter or a customer gateway[1]. NISTIR 7628 has been widely touted for providing guidance on cybersecurity concerns in smart grid projects (Abercrombie et al., 2013; Chan and Zhou, 2013; Kotut and Wahsheh, 2016; Neureiter et al., 2016), but its adoption and maintenance is partially hampered by various challenges, among others, a lack of systemacy in relating the generic security requirements to the specific smart grid (Kinderen and Kaczmarek-Heß, 2019).

In turn, an example of a source of threat intelligence, perceived as a reference model by many, is ATT&CK, published by MITRE (Strom et al., 2018). It provides a taxonomy and instance knowledge for adversary tactics and techniques curated from real-world observations (Strom et al., 2018). Nevertheless, ATT&CK is not integrated with other cybersecurity information and operational data (Kurniawan, Ekelhart, and Kiesling, 2021), and it does not support querying and automated processing. In order to deliver other required information other sources of information have been proposed, e.g., the Unified Cybersecurity Ontology (UCO) (Syed et al., 2016), the SEPSES Cybersecurity Knowledge Graph (Kiesling et al., 2019), and different domain-specific languages (DSLs), such as enterpriseLang, being based on the MITRE ATT&CK Matrix (Xiong, Legrand, et al., 2021).

When it comes to threat modeling and attack simulations, supporting risk assessment and the design of secure architectures, DSLs have been proposed that are based on the Meta Attack Language (MAL) framework (Johnson, Lagerström, and Ekstedt, 2018). MAL is a meta-meta language, which combines probabilistic attack and defense graphs with object-oriented modeling. It is used to create DSLs that provide a meta language, which can be used to create models for attack simulations. The most prominent concept in a MAL DSL is *asset*, which represents the main elements of a domain under study. An *asset* contains *attack steps*, which represent the actual attacks an attacker is able to perform on them. An *attack step* can be connected with other *attack steps*, resulting in an attack path that an attacker can take. Based on these paths an attack graph can be created that is then used for attack simulations. Additionally, each *attack step* can be related to specific types of risks such as confidentiality (C), integrity (I), and availability (A). Further, *defenses* are entities that do not allow connected *attack steps* to be compromised, if they are enabled. *Assets* have relations between them, which are called *associations*. For a detailed overview see (Johnson, Lagerström, and Ekstedt, 2018).

There are already different attempts to apply MAL in the power domain. For instance, S. Hacks, A. Hacks, et al. (2019) proposed a method that automatically creates a MAL DSL based on given enterprise architecture models. To illustrate their approach, they facilitated examples from the power domain, i.e., the model of a power plant and from a substation. To ease the modeling on substations based on existing standards, SCL-lang was suggested (Rencelj Ling and Ekstedt, 2021), which provides the capabilities for attack simulations on the common assets of a substation. However, organizations related to the power domain are complex and cover greater parts than just substations. To address this complexity, powerLang (S. Hacks, Katsikeas, et al., 2020) was developed, which covers the infrastructure of substations as well as the classical office IT. Moreover, powerLang provides assets that link the office IT to the Operational Technology of substations and, thus, provides a comprehensive view of cybersecurity concerns in the light of cyber-physical systems.

Complementary to initiatives mentioned above, different efforts have been conducted to reuse existing information and enrich it with security relevant information. As such, Jiang et al. (2018) used models describing the power infrastructure and performed attack simulations on them. The results of the simulations were then used to suggest an optimized infrastructure towards the reduction of lost energy in case of an attack. Alternatively, researchers reused other well-known concepts to assess the security of organizations. For example, Manzur et al. (2015) enhanced ArchiMate to xArchiMate to perform simulations, experiments, and analyze Enterprise Architectures (EA) by an extension to the ArchiMate meta-model. Similarly, Xiong, Carlsson, and Lagerström (2019) used EA repositories to predict effects of failing components on the entire architecture, without making actual changes to the used notation. In

[1] A customer gateway is an (embedded) piece of equipment on the customer side, which acts as a communication interface towards other parts of the smart grid (like the service provider), and which can take care of computationally intensive tasks, like encrypting sensitive metering data prior to transmission

addition, process models can be used for similar purposes. For instance, Zareen, Akram, and Ahmad Khan (2020) leveraged the extension mechanism provided in BPMN 2.0 to model threat-based security requirements and introduced graphical components for BPMN. Contrary, Rodriguez, Fernandez-Medina, and Piattini (2007) proposed a non-compliant BPMN meta-model extension including predefined set of high-level cybersecurity requirements, enabling business analysts to express their security needs.

3.2 Discussion

As the above selective overview indicates, although different approaches exist, no single approach supports the complete cybersecurity by design process (cf. R1). In addition, either the existing approaches provide general, abstract information, or quite specific ones, however, not both at the same time (cf. R3). They also do not usually support a scenario-driven approach (cf. R2). While one has to take heed of pre-empting the risks inherent to composing a language out of existing ones (Karsai et al., 2009), the reuse by means of an integration of existing languages comes with a variety of prospects like avoiding the labor intensive construction of a language from scratch, or the reliance on presumably well established domain rules encoded in the language. Therefore, to support our vision, there is a need to integrate and use in tandem existing approaches in order to reach the desired domain coverage (both vertically and horizontally). However, integrating various approaches and being able to apply them in tandem requires reconstructing them using the same language architecture. Taking into account identified requirements, in line with our previous work (Kinderen and Kaczmarek-Heß, 2019, 2021), application of multi-level modeling seems to be particularly promising.

Multi-level modeling (MLM) allows for an arbitrary number of classification levels, which are represented within a single body of model content, cf. (Atkinson and Kühne, 2001). Partly as a response to the limitations of conventional meta modeling (Atkinson and Kühne, 2001, 2008), MLM refers to approaches which share the following core ideas, cf. (Neumayr, Schrefl, and Thalheim, 2011): (1) one can define an arbitrary number of classification levels in one and the same body of model. This means that one can employ as many classification levels as needed for expressing the domain knowledge at hand (Atkinson and Kühne, 2008). This is opposed to the two classification levels (M2 and M1) from conventional meta modeling; (2) one can defer instantiation, meaning that one can constrain the instantiation to a model element residing at a specific classification level (Frank, 2014). This is opposed to shallow instantiation for conventional meta modeling, whereby one can instantiate only to the directly proceeding level; (3) one can relax the strict separation between type and instance (Atkinson and Kühne, 2001), allowing one to populate and use a model with instance level data. This is again opposed to conventional meta modeling which adheres to a strict type-instance dichotomy. As we argue in (Kinderen and Kaczmarek-Heß, 2019, 2021), those features make MLM promising for the design and use of reference models.

4 A Reference Model for Smart Grid Cybersecurity

4.1 Approach Followed

By providing the targeted reference model, we seek to increase the overall security of systems because requirements, threats, and countermeasures are made explicit and are traceable across an entire development lifecycle. Therefore, the reference model involves the integration of different well-established approaches from academia and practice for a comprehensive coverage of security by design (cf. R1). As a starting point, we select two fragmented, but complementary approaches, namely: the NISTIR 7628 and powerLang based on MAL. Additionally we rely on the taxonomy and instance knowledge for adversary tactics and techniques provided by ATT&CK (Strom et al., 2018). Next to that, to structure and represent the smart grid specific concepts, we benefit from the Smart Grid Architecture Model (SGAM), being a product of the standardization process in the EU Mandate M/490 (SGAM, 2012), which provides a set of concepts, viewpoints, and a method for standardized decomposition of

smart grid systems with a focus on interoperability (SGAM, 2012). SGAM allows to classify smart grid elements according to smart grid specific dimensions, such as the transmission grid, distribution grid, or end customers, and to analyze them according to a set of interrelated viewpoints, such as information, communication or business (Gottschalk, Uslar, and Delfs, 2017; SGAM, 2012).

From existing multi-level modeling approaches, taking into account identified requirements and reported practical experiences, cf. (Kinderen and Kaczmarek-Heß, 2019, 2021), we select the Flexible Meta Modeling and Execution Language (FMML^x) (Frank, 2014) for our project. FMML^x appears to be the only approach with a meta modeling editor (XModeler, Frank, 2014) that has an integrated language execution engine. This allows for, among others, running computational analyses and simulations on reference models (cf. R4).

4.2 Multi-Level Reference Model

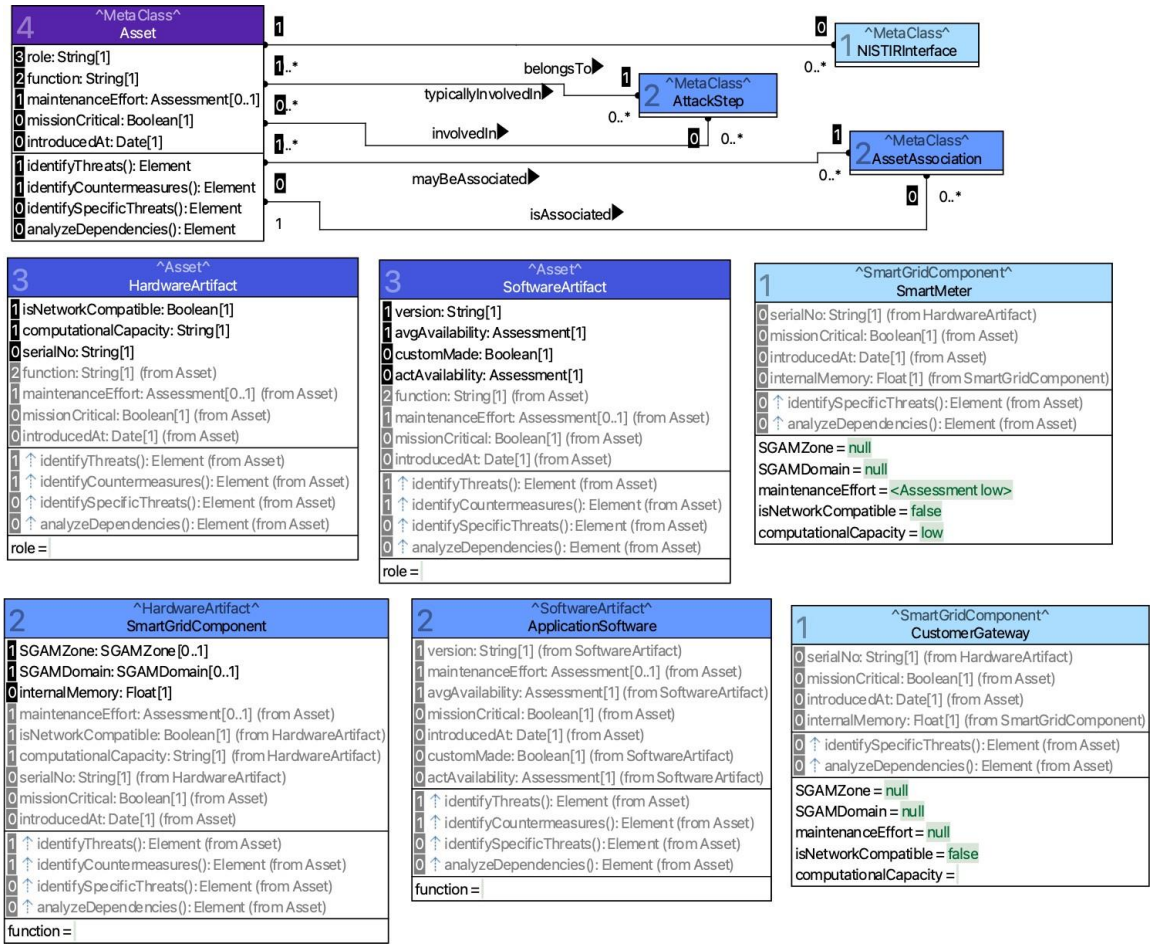

Figure 1. Focus: Asset's hierarchy.

Figs. 1–3 present selected excerpts from the designed and implemented, using the XModeler, multi-level reference model. It encompasses the main concepts from the reference models and approaches selected, i.e., ***UseCase***, ***Asset***, ***Requirement***, ***AttackStep***, or ***Countermeasure*** (cf. R1). Please note that for readability purposes we present only selected concepts, selected attributes and selected operations assigned to different levels of classification. For a detailed description of FMML^x we refer to (Frank, 2014, 2018). Apart from the "traditional" modeling constructs such as classes, attributes, operations and relationships, it is possible to defer an instantiation of all modeling constructs by assigning them a so called level of intrinsicness, which dictates at which level of classification a given property will be instantiated.

Let us have a look at the hierarchy of assets, as presented in Fig. 1. By supporting multiple classification levels, FMML^x offers the possibility to define and use concepts that correspond directly with the desired level of detail (cf. R3). Thus, we have a possibility to account for the fact that a concept such as ***Asset*** spans multiple levels of classifications with categories, types and instances. At each level of classification, we have the possibility to express relevant information, making the model semantically rich (thus, we support the productivity of modeling and enable various analyses), and at the same time to facilitate its reuse (cf. R3). Regarding the latter, consider, e.g., attributes, operations and relationships defined for the concepts of ***SoftwareArtifact*** or ***HardwareArtifact*** (on Level 3 (L3), as indicated by the number "3" next to the concept name). Please note that a majority of those characteristics will be instantiated (i.e., assigned with values) only a few classification levels below (cf. the assigned level of intrinsicness). For example, the attribute ***serial number*** for a ***HardwareArtifact*** will be known only for a specific instance on the level L0. Now, while we move along the created hierarchy (e.g., the chain starting from ***Asset*** via ***HardwareArtifact*** up to a specific ***CustomerGateway*** and its instances, cf. also (R3), on the one hand, we instantiate the concepts, i.e., the relevant attributes are assigned with values (e.g., the function performed) and we can execute relevant operations for aggregating, calculating, or acquiring data from external sources (e.g., identification of types of attacks possible) (R4). On the other hand, we specialize those concepts, i.e., additional attributes, operations and relationships may be added to make concepts more specific (cf. additional attributes defined for the concepts specific for Smart Grids).

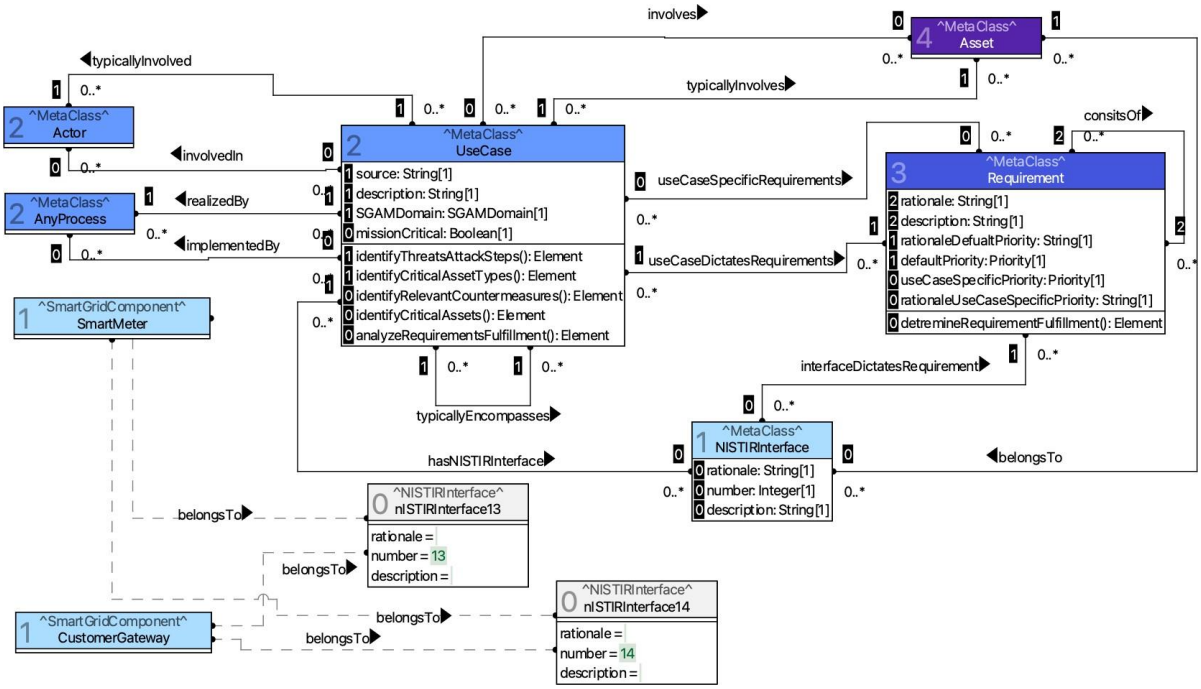

Figure 2. Multi-level Reference Model – Focus: Use Cases and Requirements.

The excerpt presented in Fig. 2 focuses on ***UseCases*** (cf. R2), their characteristics and relations with other concepts, as well as the concept of a (security) ***Requirement*** (cf. R1). This fragment of the reference model supports the first part of the scenario as described in Section 2. A ***UseCase*** in this case should be understood as a situation, a process or activity, which is (or is to be) supported by IT. So taking into account running or planned processes within some organization, the reference model allows to model properties of the ***UseCase***, point to involved ***Actors***, and a ***Process*** realizing it, as well as state security-related ***Requirements*** and their priorities (R2). Please note here how multi-level modeling supports both descriptive as well as prescriptive aspects of a reference model. The meta class ***UseCase*** is defined at the L2 classification level, and encompasses attributes and operations that will be instantiated/obtain values at L1 or L0 (as indicated by the intrinsicness value next to the attribute or

operation). So, whereas the reference model may provide us with the instance of a ***UseCase*** on L1 level, e.g., ***Billing***, cf. Fig. 2, and provides us information on the smart grid domain it belongs to (through the attribute ***SGAMDomain***), main types of ***Actors*** involved, etc.; it also provides us with information (by instantiating the association ***hasNISTIRInterface***) what ***NISTIR Interface*** is relevant, what security ***Requirements*** there are, and the prioritisation of the security requirements (R3). The Billing use case may be further instantiated, e.g., into ***BillingAtACME*** (L0) where the given organization may benefit from already stated information (cf. R3). At the same time the given organization can make decisions regarding how the given ***UseCase*** will be implemented in the given setting. The provided excerpt also shows how *a risk assessment* may be performed. The organization may decide to follow the priorities suggested by NISTIR, or to adjust them.

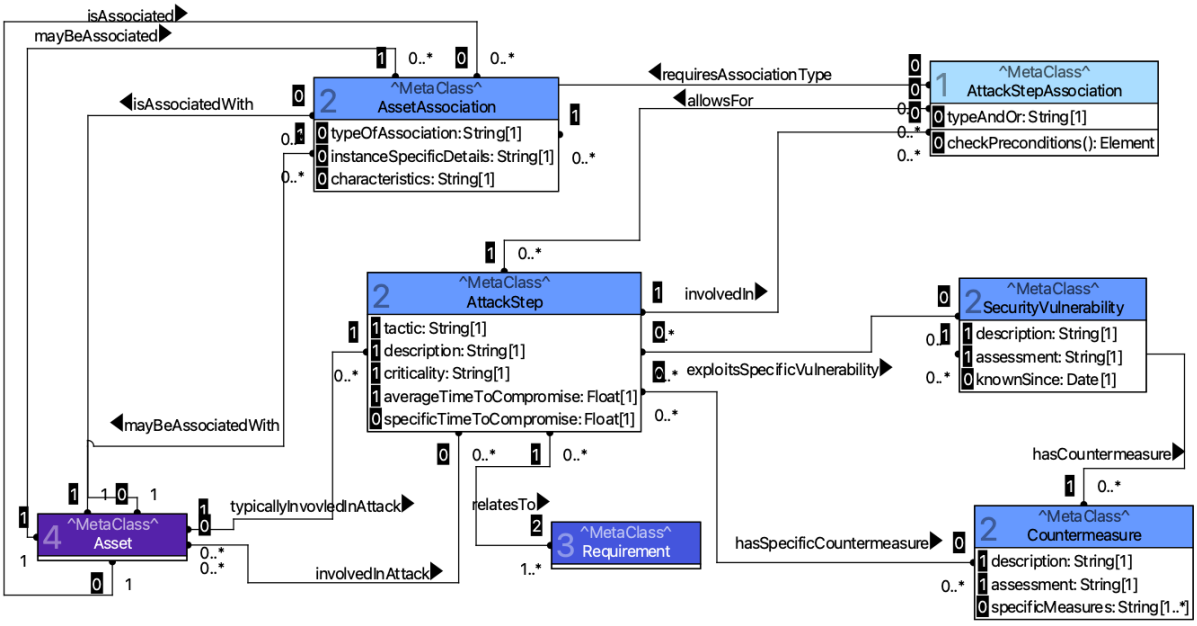

Figure 3. Multi-level Reference Model – Focus: Attack Steps, Countermeasures and Assets.

The discussed excerpt of the reference model also allows us to support the first phase of the risk assessment and identify which assets (***Asset***, L4) are involved by the ***UseCase***, but also what ***Assets*** belong to a given ***NISTIR interface*** (cf. Fig. 2). Knowing the types of assets involved, allows us to investigate the threats (***AttackSteps***), as well as analyse possible ***Countermeasures***, cf. Fig. 3 (R1). Indeed, the excerpt of the reference model represents the characteristics and dependencies among Attack[2] steps (***AttackStep***, L2), involved Assets (***Asset***, L4), ***Countermeasures*** (L2) and ***Vulnerabilities*** (L2) (R1). The domain-specific knowledge regarding the above mentioned aspects, e.g., in-line with ATT&CK providing a taxonomy and instance knowledge for adversary tactics and techniques curated from real-world observations (Strom et al., 2018), can be stated by instantiating the enumerated meta classes and associations between them (R3). Please also note that relevant constraints have been defined to make the model semantically richer and exclude the not well-formed instances along different levels. For instance, a constraint has been defined stating that only ***Assets*** on L0 being instantiated from ***Assets*** on L1, having a link to an ***AttackStep*** (***typicallyinvolvedIn***), may have a link (***involvedIn***) to instances of this ***AttackStep*** on L0.

[2] An attack is a set of actions of someone to reach a certain point in the network.

5 Evaluation

We employ semi-structured expert interviews to gain a feedback on the first version of our multi-level reference model, as well as the overall goals and vision of our project. The feedback thus gained through semi-structured interviews is rich and in-depth feedback (Miles and Huberman, 1994; Oates, 2005). Combined with the broad coverage of expert backgrounds (two experts from the security and electricity sector respectively, and one expert for security in the electricity sector), this provides us with substantial feedback for further development of our reference model during the next engineering cycle.

5.1 Interview Setup

Procedure and Materials. The interview setup consists of three parts (next to an elicitation of the participant's background): (i) an elicitation of reference documents the participant typically uses for guidance (standards, guidelines, etc.) on the basis of describing experiences in a recent project, (ii) a scenario walk through of the reference model, (iii) questions on the basis of the scenario walk through. Here the questions pertained to understandability of both the concepts, and the reference model, perceived utility, and limitations or suggested additions.

In terms of materials, each participant was shown a slide deck with the reference model, and the ACM-e billing use case to provide a scenario walk through[3]. The interviews lasted from around one hour to an hour and a half. The interviews were recorded and transcribed, and were analyzed with the support of software tools for qualitative research (maxqda, nvivo).

Participants. As a mix of convenience sampling and purposive sampling (Oates, 2005), we sourced three participants from our professional network: two experts active in one domain each, respectively, IT security and the electricity sector, and one expert active in both domains. Further details of the participants are provided in Table 1.

Study limitations. For a first, qualitative, in-depth, feedback on our reference model, we deem semi-structured interviews with three domain experts appropriate. However, for further steps, when extending and consolidating the reference model, a wider sample would be appropriate. In addition, carrying out quantitative assessment, e.g., using questionnaires, will be considered.

Characteristics	Participant 1 (P1)	Participant 2 (P2)	Participant 3 (P3)
Job and responsibilities	Cybersecurity expert; advising, analyzing, project management	Engineer for telecommunication; consultancy for and operations of cybersecurity	Visiting assistant professor, working on smart infrastructure
Years of job experience, and educational background	10 years in job with a focus on security, studied computer science	5 years experience in cybersecurity and power grids, studied electrical engineering	10 years of experience in the electricity sector, studied computer science
Organization character and size	EU institution, not for profit, about 950 personnel	European Transmission System Operator (TSO), more than 2,000 personnel	private university, not for profit, around 250 personnel
Modeling experience	formal ontologies, UML, enterprise architecture modeling	UML, BPMN, ARIS	process modeling, enterprise (architecture) modeling, UML

Table 1. Background of the three interview participants.

[3] The materials, including the accompanying interview guide, can be found online via https://www.dropbox.com/sh/6cmuxfa6ak71z25/AACvgdLq-i7Oag8kiss0eIvja?dl=0

5.2 Interview Results

We discuss the interview results in accordance with the order mentioned in the interview procedure: currently used reference documents, a scenario walk through of the reference model, and questions pertaining to reference model in terms of understandability, perceived utility, and limitations.

Currently used reference documents. As a cybersecurity expert for a large European institution, P1 often works with the ISO 2700x series of IT security standards. Additionally, P1 works with a guiding document called the ITSRM 2, which offers specialized guidance for security issues in the European public sector, but has a strong basis in ISO standards as well. P2, meanwhile, as a security expert for the electricity sector declared a use of, mostly, the NISTIR 7628. P2 added that NISTIR 7628 is the only document that is concrete enough to be useful (instead of, e.g., the SGAM (for SGAM, see section 4)). Finally P3, for his different projects in the electricity sector, often relies upon domain-specific communication standards like MODBUS or IEC 61850. Additionally, he partly takes cues from I-REC, having to do with the standardization, and finally also certification of renewable energy.

Interestingly, the participants often adjust the reference documents to regional and/or project specific circumstances. P1 discussed how, in a recent project, he had to closely collaborate with domain stakeholders to design a security architecture which allows lawyers external to the EU institutions suitable access to legal documents. The reference documents simply did not provide sufficient detail for this project. P3, meanwhile, discussed how I-REC was not fully suitable for Mexico, the region he was active in. This is because I-REC officially certifies renewable energy installations above a certain electricity production threshold only, whereas in Mexico many renewable energy installations fall below this threshold. So, while providing guidance on the installation and management of renewables, I-REC cannot be used as such for some functions of interest, specifically official certification.

Understandability. In terms of the used concepts, the understandability appears to vary across the participants. P1 and P3 were largely familiar with the concepts close to their domain of expertise, and declared that – after explanation – they could also largely follow along with the concepts not directly related to their domain. As a minor point, P3 declared that the concept of a ***NISTIRInterface*** was confusingly named, especially since the way it is used in the NISTIR 7628 differs from his everyday (software/programming) use of the interface concept. P2, meanwhile, pointed out potential language barriers, in terms of, both, (i) personnel at Distributed Systems Operators[4] speaking a language other than the English of the reference model, as well as (ii) in terms of concepts which he understands, but would name differently (e.g., using "business process" instead of "use case"). In terms of understandability of the reference model itself, as presented to the participants: firstly, moderation by a someone familiar with MLM appears to have been a necessity. For one, based on the models in slidedeck alone P3 initially equated the abstraction levels to the importance of concepts. P1, meanwhile, based on the slidedeck alone did not fully grasp the idea that the concepts related to specific use cases are monotonic extensions of the expertise encoded in concepts provided on a higher level of abstraction. In the same spirit, P2 labeled the reference model as a "bit too complicated", and that training might be required for employees to use it. This training, he remarked, might induce costs, which could be a barrier to establishing the reference model – at least in the manner in which we presented it.

Utility. The participants generally expressed potential use for the reference model, but did so in different ways. P1 considered the reference model to be a useful knowledge base for non-domain experts. Meaning, he deemed that a security architect, also without specific expertise of the electricity sector, can use the reference model to spot potential gaps or weak spots, even when some have been missed in the discussion with the domain experts. A similar sentiment was expressed by P3. Particularly, he was recently involved in the development of a platform for collecting and aggregating data coming from different solar panel inverters, which resulted in a technically feasible prototype. He remarked that our reference model has the potential to inform the roll-out of such prototypes, especially when it comes to securing the "last mile", in terms of the connection from the customer premises to the distribution grid.

[4] Distributed Systems Operators are responsible for the infrastructure associated with the low to medium voltage grid. As such, they typically deal (in-)directly with the kind of billing and metering use cases described in this paper.

Additionally P1 remarked on the potential of having a computerized tool, e.g., allowing him to query the model, thus adding systemacy to the analysis – especially when compared to textual reference documents he typically works with.

P2 equally considered the reference model to have potential. However, partly in line with his motivations for using the NISTIR 7628 only (see the discussion under understandability), he did remark that the utility of the reference model depends on its concrete and up-to-date coverage of assets, and mitigations.

Finally, of note is a feedback of P1, the cybersecurity expert, on the proposed metering and billing architecture for ACM-e. Namely based on the designed architecture alone, i.e., assets and their interconnection only, P1 spontaneously discussed a notable weak spot: the LAN on the customer premises, which is used to transmit metering data from the smart meter to the customer gateway. This is mainly interesting as it shows that experts can conduct their security analysis over different parts of the reference model: not only specific attacks and countermeasures are considered interesting, but also weak spots in the designed architecture by itself, and how to deal with that by changing the architecture.

Perceived limitations. P1 remarked upon the need for a procedural model for using the reference model. P1 and P3, meanwhile, emphasize the need for further considering also existing infrastructure. Often, they remarked, what is in place partly influences the security design. Sometimes, P1 points out, all one can do is to focus on patching, rather than putting into place what one would ideally like to have. Furthermore, P3 emphasized the need for a different visualization. Indirectly, the need for a different visualization is also emphasized by the discussion with P1. Namely, while P1 discussed potential weaknesses in the proposed architecture, we discussed the proposed architecture based on a different visualization accompanying the reference model. While the information in this different visualization is very much grounded in the multi-level reference model, the spontaneous discussion by P1 on the designed architecture was primarily triggered by the different visualization, which we speculate was more accessible to him. This further highlights the need for further visualization mechanisms to accompany the multi-level reference model.

6 Conclusions

In this paper, we discussed the foundations of a reference model to support end-to-end security by design for the electricity sector. Particularly, we reported on a first full engineering cycle, in terms of discussing the problems the reference model is supposed to address, the requirements the reference model should fulfil, and a first sketch of the reference model, which uses multi-level modeling as the underlying language architecture. Finally, we discussed feedback from domain experts on our reference model.

The expert feedback constitutes valuable input for the next engineering cycle of our research project. For one, we learned that a procedural model for using the reference model is deemed important, as well as a different visualization to make the reference model more accessible. Going forward, this feedback is expected to at least influence (i) the solution design, especially in terms of relevant requirements. For example, the requirements are currently less aimed at a procedure for using the reference model; and (ii) the solution implementation, in terms of artefact development. Furthermore, apart from the expert feedback, we deem it relevant to cover further specific use cases next to the ones being in the focus of this paper. Next to increasing the applicability of our reference model, such wider coverage of specific use cases is also expected to further solidify the concepts which reside on a high level of abstraction, and – in line with the promises of MLM – to assess their utility in terms of a reuse, e.g., across multiple use cases. Finally, a full prototypical implementation of the reference model for a more comprehensive scenario should take place, accompanied by the possibility to conduct various simulations, so that also a more comprehensive evaluation of the reference model could take place.

References

Abercrombie, R. K., F. T. Sheldon, K. R. Hauser, M. W. Lantz, and A. Mili (2013). "Risk assessment methodology based on the NISTIR 7628 guidelines." In: *System Sciences (HICSS), 2013 46th Hawaii International Conference on*. IEEE, pp. 1802–1811.

Atkinson, C. and T. Kühne (2001). "The Essence of Multilevel Metamodeling." In: *Proceedings of the 4th International Conference on The Unified Modeling Language, Modeling Languages, Concepts, and Tools*. London, UK, UK: Springer-Verlag, pp. 19–33.

— (2008). "Reducing accidental complexity in domain models." *SoSyM* 7 (3), 345–359.

Brown, B., B. Singletary, B. Willke, C. Bennett, D. Highfill, D. Houseman, F. Cleveland, H. Lipson,
J. Ivers, J. Gooding, et al. (2008). "AMI system security requirements." *AMI-SEC TF*.

Chan, A. and J. Zhou (2013). "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628." *IEEE Communications Magazine* 51 (1), 58–65.

Coelho, P., M. Gomes, and C. Moreira (2019). "Smart metering technology." In: *Microgrids Design and Implementation*. Springer, pp. 97–137.

Fang, X., S. Misra, G. Xue, and D. Yang (2012). "Smart Grid — The New and Improved Power Grid: A Survey." *IEEE Communications Surveys Tutorials* 14 (4), 944–980.

Frank, U. (2013). "Domain-Specific Modeling Languages: Requirements Analysis and Design Guidelines." In: *Domain engineering*. Springer, pp. 133–157.

— (2014). "Multilevel Modeling - Toward a New Paradigm of Conceptual Modeling and Information Systems Design." *BISE* 6 (6), 319–337.

— (2018). *The Flexible Multi-Level Modelling and Execution Language (FMMLx). Version 2.0: Analysis of Requirements and Technical Terminology*. Tech. rep. 66. ICB-Research Report.

Geismann, J., C. Gerking, and E. Bodden (2018). "Towards Ensuring Security by Design in Cyber-Physical Systems Engineering Processes." In: *Proceedings of the 2018 International Conference on Software and System Process*. ICSSP '18. Gothenburg, Sweden: Association for Computing Machinery, pp. 123–127.

Gottschalk, M., M. Uslar, and C. Delfs (2017). *The Use Case and Smart Grid Architecture Model Approach: The IEC 62559-2 Use Case Template and the SGAM Applied in Various Domains*. 1st. Springer. ISBN: 3319492284, 9783319492285.

Gunduz, M. Z. and R. Das (2020). "Cyber-security on smart grid: Threats and potential solutions." *omputer Networks* 169, 107094.

Hacks, S., A. Hacks, S. Katsikeas, B. Klaer, and R. Lagerström (2019). "Creating Meta Attack Language Instances using ArchiMate: Applied to Electric Power and Energy System Cases." In: *EDOC*, pp. 88– 97.

Hacks, S., S. Katsikeas, E. Ling, R. Lagerström, and M. Ekstedt (2020). "powerLang: a probabilistic attack simulation language for the power domain." *Energy Informatics* 3 (1), 1–17.

Hevner, A. R., S. T. March, J. Park, et al. (2004). "Design Science in Information Systems Research." *MIS Quarterly* 28 (1), 75–105.

Jiang, Y., M. Jeusfeld, Y. Atif, J. Ding, C. Brax, and E. Nero (2018). "A Language and Repository for Cyber Security of Smart Grids." In: *2018 IEEE 22nd International Enterprise Distributed Object Computing Conference (EDOC)*, pp. 164–170.

Johnson, P., R. Lagerström, and M. Ekstedt (2018). "A Meta Language for Threat Modeling and Attack Simulations." In: *Proceedings of the 13th International Conference on Availability, Reliability and Security*. ARES 2018. Hamburg, Germany: Association for Computing Machinery. ISBN: 9781450364485.

Kelly, S. and J.-P. Tolvanen (2008). *Domain-Specific Modeling: Enabling Full Code Generation*. John Wiley & Sons.

Kiesling, E., A. Ekelhart, K. Kurniawan, and F. J. Ekaputra (2019). "The SEPSES Knowledge Graph: An Integrated Resource for Cybersecurity." In: *The Semantic Web - ISWC 2019 - 18th International Semantic Web Conference, Auckland, New Zealand, October 26-30, 2019, Proceedings, Part II*. Ed. By C. Ghidini, O. Hartig, M. Maleshkova, V. Svátek, I. F. Cruz, A. Hogan, J. Song, M. Lefrançois, and F. Gandon. Vol. 11779. Lecture Notes in Computer Science. Springer, pp. 198–214.

Kinderen, S. de and M. Kaczmarek-Heß (2019). "Multi-level Modeling as a Language Architecture for Reference Models: On the Example of the Smart Grid Domain." In: *21st IEEE Conference on Business Informatics, CBI, Moscow, Russia, July 15-17, Volume 1 - Research Papers*. Ed. by J. Becker and D. A. Novikov. IEEE, pp. 174–183.

— (2021). "Making a Case for Multi-level Reference Modeling – A Comparison of Conventional and Multi-level Language Architectures for Reference Modeling Challenges." In: *Wirtschaftsinformatik 2021 Proceedings*. aisnet.

Karsai, G., H. Krahn, C. Pinkernell, B. Rumpe, M. Schindler, and S. Völkel (2009). "Design Guidelines for Domain Specific Languages." In: *Domain-Specific Modeling Workshop (DSM'09)*. Techreport B-108. Helsinki School of Economics, pp. 7–13.

Kotut, L. and L. A. Wahsheh (2016). "Survey of cyber security challenges and solutions in smart grids." In: *2016 Cybersecurity Symposium*. IEEE, pp. 32–37.

Kumar, P., Y. Lin, G. Bai, A. Paverd, J. S. Dong, and A. Martin (2019). "Smart grid metering networks: A survey on security, privacy and open research issues." *IEEE Communications Surveys & Tutorials* 21 (3), 2886–2927.

Kurniawan, K., A. Ekelhart, and E. Kiesling (2021). "An ATT&CK-KG for Linking Cybersecurity Attacks to Adversary Tactics and Techniques." In: *Proceedings of the ISWC 2021 Posters, Demos and Industry Tracks: From Novel Ideas to Industrial Practice co-located with 20th International Semantic Web Conference (ISWC 2021), Virtual Conference, October 24-28, 2021*. Ed. by O. Seneviratne, C. Pesquita, J. Sequeda, and L. Etcheverry. Vol. 2980. CEUR Workshop Proceedings. CEUR-WS.org.

Luthra, S., S. Kumar, R. Kharb, M. F. Ansari, and S. Shimmi (2014). "Adoption of smart grid technologies: An analysis of interactions among barriers." *Renewable and Sustainable Energy Reviews* 33, 554–565.

Manzur, L., J. M. Ulloa, M. Sánchez, and J. Villalobos (2015). "xArchiMate: Enterprise Architecture Simulation, Experimentation and Analysis." *Simulation* 91 (3), 276–301.

Miles, M. B. and A. M. Huberman (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Mohassel, R. R., A. Fung, F. Mohammadi, and K. Raahemifar (2014). "A survey on Advanced Metering Infrastructure." *International Journal of Electrical Power & Energy Systems* 63, 473–484.

Morana, M. M. and T. Uceda Vélez (2015). *Risk centric threat modeling: Process for attack simulation and threat analysis*. Hoboken, New Jersey: John Wiley & Sons.

Morikawa, I. and Y. Yamaoka (2011). "Threat Tree Templates to Ease Difficulties in Threat Modeling." In: 2011 14th International Conference on Network-Based Information Systems, pp. 673–678.

Namboodiri, V., V. Aravinthan, S. N. Mohapatra, B. Karimi, and W. Jewell (2013). "Toward a secure wireless-based home area network for metering in smart grids." *IEEE Systems Journal* 8 (2), 509–520.

Neumayr, B., M. Schrefl, and B. Thalheim (2011). "Modeling Techniques for Multi-level Abstraction." In: *The Evolution of Conceptual Modeling*. Ed. by R. Kaschek and L. Delcambre. Berlin: Springer, pp. 68–92.

Neureiter, C., M. Uslar, D. Engel, and G. Lastro (2016). "A standards-based approach for domain specific modelling of smart grid system architectures." In: *System of Systems Engineering Conference (SoSE), 2016 11th*. IEEE, pp. 1–6.

NIST Smart Grid Cybersecurity Panel (2010). *NISTIR 7628-Guidelines for Smart Grid Cyber Security vol. 1-3*.

Oates, B. J. (2005). *Researching information systems and computing*. Sage.

Paja, E., F. Dalpiaz, and P. Giorgini (2015). "Modelling and reasoning about security requirements in socio-technical systems." *Data & Knowledge Engineering* 98, 123–143.

Procopiou, A. and N. Komninos (2015). "Current and future threats framework in smart grid domain." In: *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*. IEEE, pp. 1852–1857.

Rencelj Ling, E. and M. Ekstedt (2021). "Generating Threat Models and Attack Graphs Based on the IEC 61850 System Configuration Description Language." In: *AT-CPS '21*. ACM, pp. 98–103.

Rodriguez, A., E. Fernandez-Medina, and M. Piattini (2007). "A BPMN Extension for the Modeling of Security Requirements in Business Processes." *IEICE Trans. Inf. Syst.* 90-D (4), 745–752.

Sánchez, O., F. Molina, J. Garcia-Molina, and A. Toval (2009). "ModelSec: a generative architecture for model-driven security." *Journal of Universal Computer Science* 15 (15), 2957–2980.

SGAM (2012). *Smart Grid Reference Architecture*. Tech. rep. Date last accessed 11-02-2020. CEN-CENELEC-ETSI Smart Grid Coordination Group. URL: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf.

Strom, B. E., A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas (2018). *Mitre ATT&CK: Design and Philosophy*. Technical Report. The MITRE Corporation.

Sun, C.-C., A. Hahn, and C.-C. Liu (2018). "Cyber security of a power grid: State-of-the-art." *International Journal of Electrical Power & Energy Systems* 99, 45–56.

Syed, Z., A. Padia, T. Finin, M. L. Mathews, and A. Joshi (2016). "UCO: A Unified Cybersecurity Ontology." In: *Artificial Intelligence for Cyber Security, Papers from the 2016 AAAI Workshop, Phoenix, Arizona, USA, February 12, 2016*. Ed. by D. R. Martinez, W. W. Streilein, K. M. Carter, and A. Sinha. Vol. WS-16-03. AAAI Workshops. AAAI Press.

WG15, I. T. (2016). *IEC 62351 Security Standards for the Power system Information Infrastructure*. Wieringa, R. J. (2014). *Design science methodology for information systems and software engineering*. Springer.

Xiong, W., P. Carlsson, and R. Lagerström (2019). "Re-using Enterprise Architecture Repositories for Agile Threat Modeling." In: *EDOCW*, pp. 118–127.

Xiong, W. and R. Lagerström (2019). "Threat modeling–A systematic literature review." *Computers & security* 84, 53–69.

Xiong, W., E. Legrand, O. Åberg, and R. Lagerström (2021). "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix." *Software and Systems Modeling*.

Zareen, S., A. Akram, and S. Ahmad Khan (2020). "Security requirements engineering framework with BPMN 2.0. 2 extension model for development of information systems." *Applied Sciences* 10 (14), 4981.

Zeb, K., O. Baig, and M. K. Asif (2015). "DDoS attacks and countermeasures in cyberspace." In: *2015 2nd World Symposium on Web Applications and Networking (WSWAN)*. IEEE, pp. 1–6.