# Towards a Framework for Engineering Smart-Grid-Specific Privacy Requirements

Christian Neureiter, Günther Eibl, Armin Veichtlbauer and Dominik Engel
Josef Ressel Center for User-Centric Smart Grid Privacy, Security and Control
Salzburg University of Applied Sciences
Urstein Sued 1, A–5412 Urstein/Salzburg, Austria
Email: {christian.neureiter, guenther.eibl, armin.veichtlbauer, dominik.engel}@en-trust.at

***Abstract*—Privacy has become a critical topic in the engineering of electric systems. This work proposes an approach for smart-grid-specific privacy requirements engineering by extending previous general privacy requirements engineering frameworks. The proposed extension goes one step further by focusing on privacy in the smart grid. An alignment of smart grid privacy requirements, dependability issues and privacy requirements engineering methods is presented. Starting from this alignment a Threat Tree Analysis is performed to obtain a first set of generic, high level privacy requirements. This set is formulated mostly on the data instead of the information level and provides the basis for further project-specific refinement.**

## I. Introduction

During the ongoing development of the smart grid, the issue of privacy turns out as an important concern. Particularly in the context of user acceptance this issue has to be dealt with. Various contributions have revealed a lack of trust on the end-user side towards smart grid technologies due to privacy concerns [1]. The need for privacy-preserving methods in the smart grid, e.g., in the area of smart metering, has been pointed out by numerous authors [2], [3], [4], [5]. Valuable work has already been done in the electrical engineering community by the postulation of privacy principles [6] derived from the "Fair Information Practices" proposed by the U.S. Department of Health, Education and Welfare and "privacy by design" [7], respectively.

From an engineering point of view, elaborating adequate privacy requirements in order to incorporate privacy is an important and not trivial task. Various approaches towards privacy requirements engineering are already existing in the field of software related systems. Beckers proposes a conceptual framework [8] for comparing various privacy requirements engineering approaches which differ in terms and notions. For this purpose, the author extends an existing framework [9] aiming at comparing security requirements engineering methods by adding privacy related terms and notions. The extended conceptual framework is then applied to current privacy requirements engineering processes. The LINDDUN approach proposed by [10] is based on a privacy threat analysis framework and an information flow oriented model with the focus on "personal information". It provides an extensive catalogue of privacy-specific threat tree patterns and appears to be very promising for real world projects.

In the field of smart grids architecture relevant work was done by the "Smart Grid Coordination Group" (SGCG). Following the EU mandate 490 (M/490) four working groups (WG) were established. The scope of these working groups were a smart grid reference architecture [11], a set of generic high-level use cases (WG "Sustainable Processes") [12], a first set of standards [13] and a document concerning "Information Security in the Smart Grid" [14]. Particularly the last document addressing information security is of special relevance in terms of engineering privacy requirements, as besides the security considerations which focus on "information assets" as working items, the need for privacy-preserving methods in the smart grid is addressed explicitly.

Besides these top-down approaches there are a number of contributions that do not focus on deriving requirements, but address challenges for privacy in the smart grid and suggest technological solutions. For example, subsumed as "Non-Intrusive Load Monitoring" (NILM) various studies investigate which information can be extracted from smart meter data like electrical load profiles, cf. [15], [16]. These publications point out that plain smart meter data can be used to gain various, also sensible, kinds of information. Even if a smart meter is originally intended for obtaining the information "energy consumption" or "voltage stability" the same data set can be used to gain privacy relevant information about a user. A number of methods have been proposed to balance the need for privacy with the information needed for correct operation of smart grids, e.g., through anonymization [17], homomorphic encryption [18] or multi-resolution conditional access [19].

The contribution of the work presented here is to deliver an approach on how to consider privacy requirements in the smart grid. To do so, a methodology is proposed how privacy requirements can first be aligned in context of dependability and can second be integrated in state of the art requirements engineering processes. Corresponding to this, a threat tree analysis is performed that delivers a classification of privacy specific threats. This classification is further used to elicit a basic set of "Generic High Level Privacy Requirements", analogously to the "Generic High Level Use Cases" from the WG "Sustainable Processes" [12].

The rest of this paper is organized as follows: In Section II two general approaches that seem suitable for privacy requirements engineering in the smart grid are mentioned. First, the compact framework, introduced by Beckers [8] and second, the LINDDUN approach [10] are briefly described. In Section III-A it is argued, why it could be useful to put the issue "privacy" into context with the quality requirements of the electrical grid. Next, it is described how minor extensions to the mentioned conceptual framework can reflect a separate

treatment of "information" and "data items" in Section III-B. In Section III-C a Threat Tree Analysis (TTA) is performed in order to identify and classify the causal faults leading to general privacy violations. This classification helps in identifying the causal faults that can be treated by one of the established privacy requirements engineering processes or security means. Moreover, causal faults needing further investigations can be detected. Section III-D introduces a basic set of generic, high level privacy requirements similar to the generic, high level use cases presented by [12]. These requirements can be applied to smart grid specific products and services by individual, proper refinements. The elicited privacy requirements subsequently can be fulfilled by privacy policies, by law, by dedicated counter-measures or serve as constraints for the smart grid related system itself. Finally Section IV discusses the obtained results and gives an outlook on future work.

## II. Related Work

Currently, a number of general approaches for engineering privacy requirements exist. In this section, we discuss two approaches in more detail, which are suitable to form the basis for engineering smart-grid-specific privacy requirements.

*1) Beckers' Conceptual Framework:* A comprehensive framework for comparing security requirements engineering processes is proposed by [9]. An extension of this framework, incorporating privacy requirements engineering is suggested by Beckers [8], as illustrated in Figure 1. This extended framework is not only suitable to compare various approaches for privacy requirements engineering, but also provides a feasible tool for supporting the process of privacy requirements engineering.

The conceptual framework consists of four building blocks. The *Stakeholder Views* building block considers the relation between a certain stakeholder, his or her personal information and his or her privacy goals. According to [8], privacy goals define how personal information can be distributed and used. Four privacy goals are listed: *anonymity*, *unlinkability*, *unobservability* and *pseudonymity*. A number of approaches, including [24], [25] and [26], are evaluated regarding their level of fulfillment of these goals. A further refinement of the high-level privacy goals delivers specific privacy requirements for each stakeholder. Since our specific focus is on the user domain within the smart grid context, the end-user is the only stakeholder to be considered in the context of the present contribution.

The second building block, *System Requirements*, reconciles all system-specific requirements, whereas the *Specification and Domain Knowledge* building block considers the requirements in context of the environment. In the context of smart grids privacy, the specific smart grid environment can be taken into account in these two blocks.

The fourth block, called *Threat Analysis*, is of special interest for our investigations because it introduces "Privacy Properties". These can be "privacy goals, personal information, privacy requirements and further more". Furthermore, it is stated that "violations of privacy properties imply potential harm to a stakeholder" [8, p. 577].

*2) The LINDDUN Approach:* Various privacy requirements engineering processes, like LINDDUN, realize the idea of threat analysis as depicted in the concerning building block.

The LINDDUN approach is based on an information flow oriented model with the focus on "personal information". It analyzes privacy related threats by the use of an extensive set of "Threat Tree Patterns" and the derivation of misuse cases. These misuse cases form the basis for the elicitation of privacy requirements. Basically, this approach is quite similar to the FTA, which is a commonly used technique in the field of dependability. Assuming an existing information model, this process is well-suited for privacy requirements engineering, yet it has not been applied to the smart grid domain so far.

## III. Smart Grid Specific Privacy Requirements Engineering

### A. Privacy in the Taxonomy of Dependability

The electric grid is a critical infrastructure which has to fulfill various non-functional requirements. These requirements should ensure that on the one hand a system delivers its intended functionality and on the other hand the risk of hazards, i.e., events causing harm to its environment, including human beings, is minimized. In literature these requirements are often termed *dependability requirements*.

In the field of dependability numerous very detailed approaches exist on how to deal with functional safety as can be seen in the IEC 61508 standard [21] and its associated requirements. Hereby, functional safety is related to the proper working of safety subsystems. In [22] the requirements *reliability*, *availability*, *maintainability* and *safety* are listed as issues to be considered. These requirements are subsumed under the acronym RAMS. As malicious attacks from outside also have the potential to cause harm, RAMS has been extended by the issue *security*, resulting in the acronym RAMSS. It is important to be aware that functional safety and security are rather abstract, high level requirements used to describe the dependability of a technical system, which can be broken down to concrete low level requirements like availability, which can be assessed also quantitatively by the definition of suitable metrics.

Some basic concepts and a corresponding taxonomy are delivered by [23]. Hereby the security issue is further detailed by the three elements *confidentiality*, *integrity* and *availability* (CIA). These dependability requirements are defined to be "dependability and security attributes". Beyond these attributes the introduced taxonomy includes the fault-propagation-chain (Fault – Error – Failure) as origin for specific threats and a classification for appropriate countermeasures, labeled as "means", see Figure 2. Note that security is mentioned implicitly by the three attributes confidentiality, integrity and availability (CIA).

The overall goal of dependability and security is to reduce the risk that a specific system delivers harm to its surrounding environment, which of course includes human beings. In addition to the abovementioned attributes, privacy violations also contain the potential of causing harm to humans. Keeping this in mind we extend the introduced acronym RAMSS to P-RAMSS with "P" representing the attribute *privacy*. Considering the conceptual framework discussed in Section

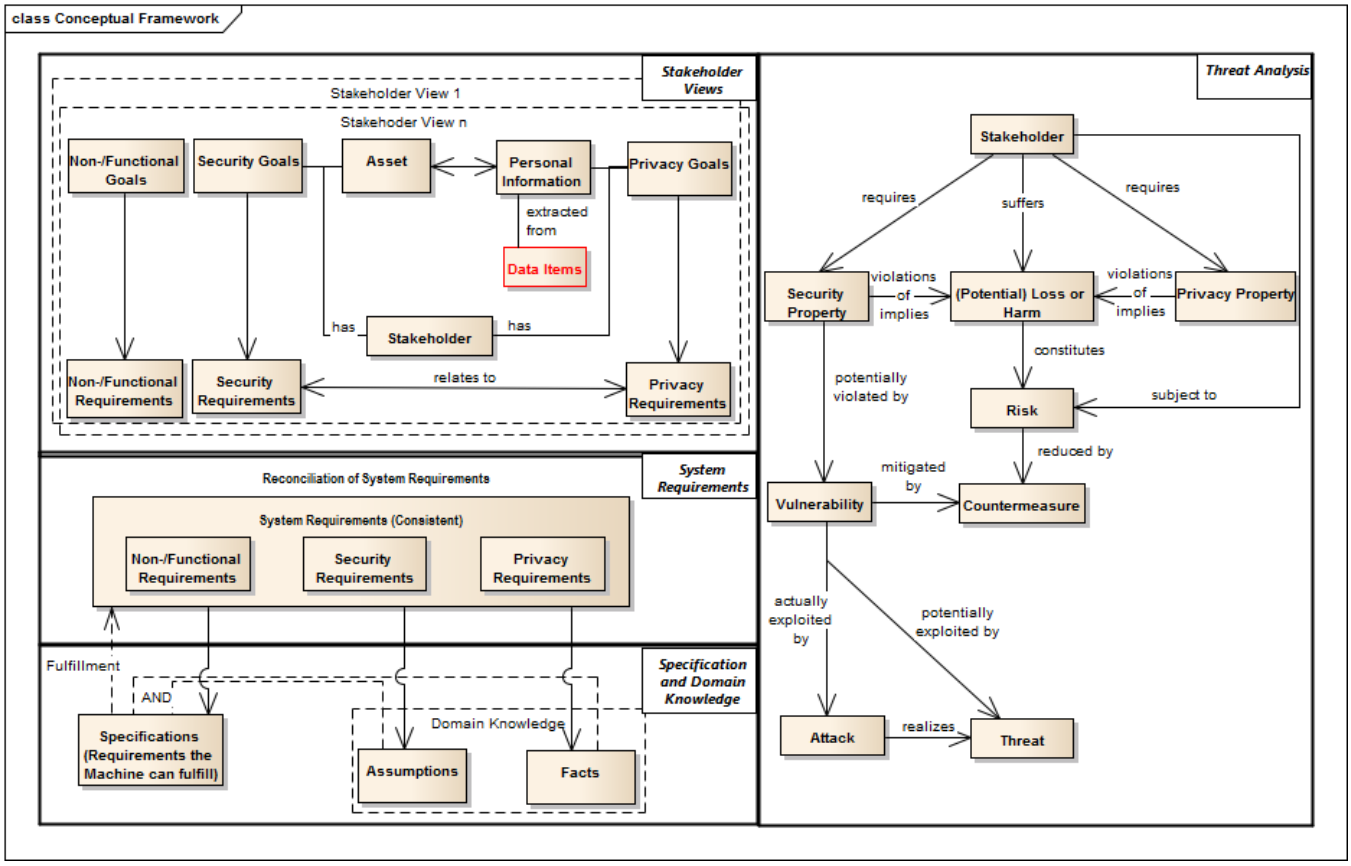


Fig. 1. Conceptual framework for privacy requirements engineering [8], extended by "data items"

II-1, the P-RAMSS related requirements are reflected by the *System Requirements* block.

The authors are aware of the fact that harms to persons due to privacy violations are "weaker" than usually considered harms in safety engineering, i.e., an analysis of "Safety Integrity Levels" (SIL) according to [21] would yield no safety requirements. Yet for user acceptance of smart grid systems also these "weaker" harms may have considerable effects. The point is that the methodology which is developed in safety engineering can be reused in the field of privacy, as we show by the example of an FTA for privacy issues. Whereas in safety engineering FTAs are used to assess the non-availability of safety functions, in the field of privacy FTAs can be used to assess privacy violations.

Using the methodology developed in safety engineering the high-level requirements safety and security are broken down to low level requirements, such as availability, which is itself dependent on reliability and maintainability. The elicitation of low level requirements is a non-trivial task, yet in the field of functional safety numerous analyzing methods and design concepts exist. As it will be helpful to apply them also to privacy investigations, the introduction of privacy to the dependability taxonomy turns out to be feasible. Following this reasoning, three main benefits can be listed that justify the introduction of *privacy* to the set of dependability requirements:

1) Privacy by design: Although the awareness for privacy is increasing, in real world projects privacy is considered in the end of the development phase for the first time. Treating privacy as a dependability requirement raises its importance and supports the chance for "privacy by design" [7], [6].
2) Privacy in context of systems engineering: Privacy is often treated as a software design issue only. As privacy analysis is based on data, in the smart grid domain privacy issues already appear on the electrical level during data acquisition (measurements). Therefore privacy should be considered in the context of systems engineering.
3) Principles of dependability: In the field of dependability numerous analyzing methods and design principles exist which can be used for considering privacy aspects.

### B. Adaptations to the Conceptual Framework

In contrast to pure software development for smart grid development, the close relation between information and communication technology (ICT) and the electrical network must be taken into account. Since electrical networks are critical infrastructures they have to meet stringent quality requirements. The intended operations in the smart grid (e.g., demand-side management) strongly rely on the created data sets as they for example serve as input to control systems performing specific grid operations. Hence, privacy considerations cannot be performed independently, as changes to the data sets (e.g., arising from data minimization) directly affect grid operations.

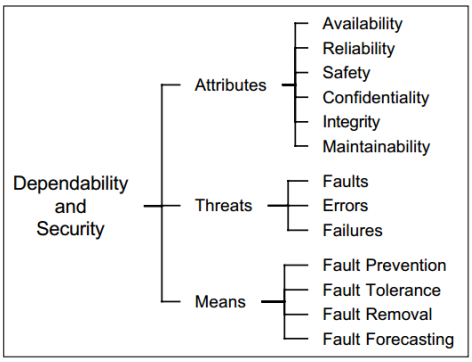


Fig. 2. The dependability and security tree [23]

It is important to take into account underlying data sets during the privacy requirements engineering process.

In contrast to other approaches we therefore start with data instead of the personal information and proceed from data to information in an additional step. In this step it must be investigated which information can be extracted from the data in addition to the intended information items. Additional complexity arises by considering smart-home based services delivered from third party stakeholders in addition to smart metering for billing purposes. Therefore, the link between smart-grid-related data, smart-grid-related information and user-specific (personal) information requires some dedicated investigations.

According to these considerations, the conceptual framework can be extended in a simple way by the addition of a "data items" block having an $n : m$ relationship to personal information (upper left part in Figure 1). The aim of this extension is to illustrate that various different (personal) pieces of information can be obtained from different data sets.

Similar to this extension of the framework, the requirements engineering process can be extended by a first step which elaborates the relation between data and information. There it is determined, which information is (also implicitly) included in data sets and can be obtained either in a straightforward way or by the application of data mining algorithms such as NILM analysis.

### C. Threat Tree Analysis

To figure out various threat scenarios with regard to the separation of information and data view, a simple, qualitative Fault Tree Analysis (FTA) has been performed. The analysis is scenario-based and the leaves are used to identify causal threats that lead to a privacy violation, as illustrated by Figure 3. Therefore, the term "Threat Tree Analysis" (TTA) can also be used for this kind of FTA.

The executed TTA is based on a scenario, where a third party delivers a specific, smart-grid-related service to an end-user.

To provide the desired service, the third party is in need of specific information about the end-user, and the end-user has to be willing to deliver this information. The delivery of this information is based upon access to some user-specific data. Based on these assumptions, the performed TTA (Figure 3) identifies the following six threats.

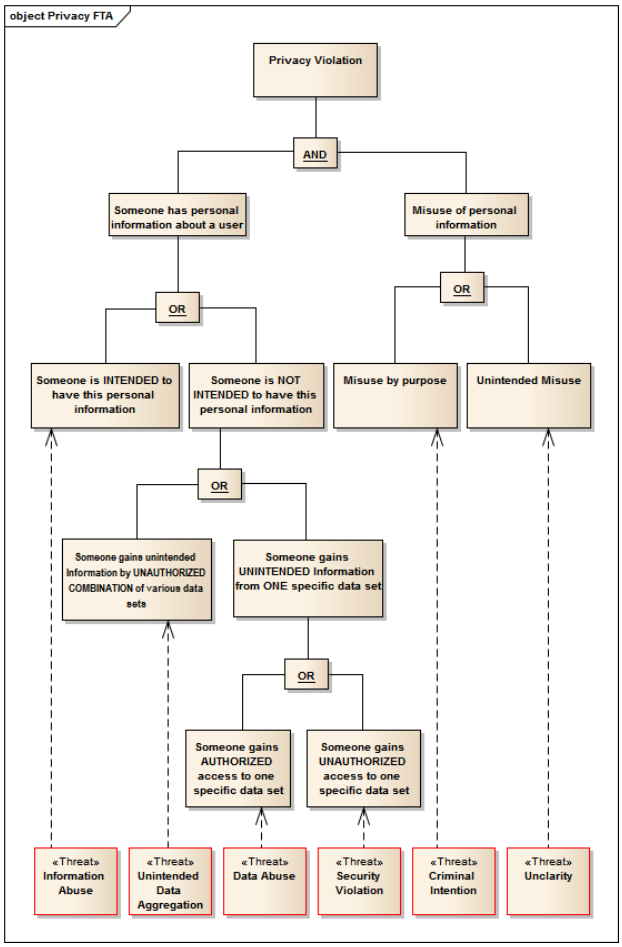


Fig. 3. Threat Tree Analysis

1) Information abuse: This threat considers the misuse of personal information, the third party is intended to have.
2) Data abuse: Hereby the end-user delivers some personal data to a third party in order to extract a specific information. The third party uses this data to extract additional information that is not intended to be released by the user.
3) Unintended data aggregation: This threat addresses scenarios, when a user releases two uncritical data sets to two different third parties. Indeed, both parties belong to one physical person or company and can be combined to a critical data set.
4) Security violation: In case of a security violation some third party illegally gains access to user-specific data.
5) Criminal Intention: Personal information, regardless of how it was obtained, is used intentionally for criminal purposes.
6) Unclarity: In this scenario, information is used in a way that was not intended by the user, regardless of how this information was obtained. However, this misuse does not happen by purpose, because the intended use of the information is not clear.

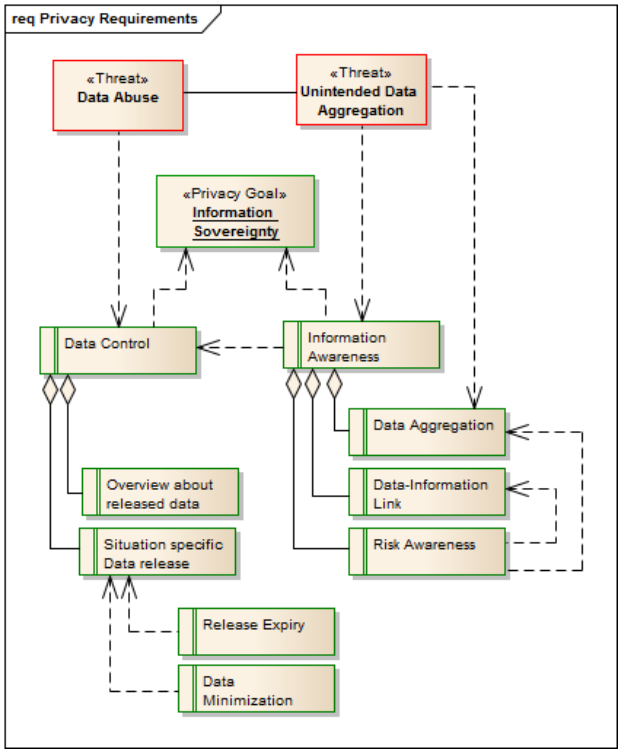


Fig. 4. Privacy Requirements

### D. Basic set of generic, high-level privacy requirements

In [13] a classification of smart grid use cases is developed. Use cases can either be classified based on their abstraction level or based on the project specificity. In the first case this relates to the distinction between "High Level Use Cases" describing the general idea of a function and "Primary Use Cases" describing a system-specific implementation. In the second case use cases are classified into use cases that are not project- or technology-specific, so-called "Generic Use Cases" and project-specific "Individual Use Cases". Following this classification, in this section the threats identified in section III-C are used to elicit a basic set of generic, high level privacy requirements. This initial set forms the basis for evaluation in real world projects, followed by adaptations and extensions, if necessary.

Since this work focuses on smart grids and data-based processes, threats related to this focus are discussed in more detail, whereas other threats are treated more superficially: The threats "Information Abuse" and "Security Violation" can be handled by means of established methods like PriS [20] or LINDDUN [10] and by adequate published security requirements engineering methods, respectively. Criminal intention must be treated mainly by legal concepts. "Unclarity" (of information) can be counteracted by measures clarifying the intended usage in an unambiguous way.

The two remaining threats "Data Abuse" and "Unintended Data Aggregation" have been subjected to requirements elicitation process in full detail, resulting in the model of generic, high level privacy requirements shown in Figure 4.

"Information Awareness" and "Data Control" are two important requirements that can directly be derived from the threats. According to the discussed conceptual framework we consolidate these requirements to a new privacy goal called "Information Sovereignty". Each of these two requirements consists of numerous other requirements with various relations among them, as detailed in Table I. The requirements are described similar to *user-stories* which are an established method in software engineering. This kind of description also emphasizes the end-user-centric perspective.

TABLE I. LIST OF REQUIREMENTS

| Requirement | Description |
|---|---|
| Information Awareness | I, as an end-user, want to be aware of the information that can be extracted from various data sets |
| Data Control | I, as an end-user, want to be able to control which data sets are released to which stakeholder |
| Data-Information link | I, as an end-user, want to be aware which information can be extracted from a specific data set |
| Data Aggregation | I, as an end-user, want to be aware which information can be extracted from various combinations of specific data sets |
| Risk Awareness | I, as an end-user, want to be aware which risk could arise by misuse of a specific information |
| Situation dependency | I, as an end-user, want to be able to release my data situation specific to dedicated stakeholders |
| Data Overview | I, as an end-user, want to have an overview about which data is released to which stakeholder |
| Data Minimization | I, as an end-user, want to release only as little data as necessary |
| Release expiry | I, as an end-user, want to have the expiry of specific data releases properly handled |

## IV. CONCLUSION AND FUTURE WORK

It has been shown that by combining approaches to privacy requirements engineering and integrating them into a smart-grid-specific perspective, the basis can be laid for a structured requirements engineering process for smart grids that is both data-based and user-centric.

As the electric network is part of a critical infrastructure, it is suggested to consider privacy in the context of other non-functional requirements. It has been illustrated, how state of the art approaches could be extended enabling a better adaption to smart-grid-specific scenarios. The key part of the extension is that the focus is put on data in addition to information. The data sets generated in smart grids form the basis for all privacy considerations. These data sets are closely related to the grid operations of the electrical network. A TTA has been performed to identify and classify causal threats. The main focus hereby is put on the relation between smart-grid-specific data and personal information. Outgoing from the derived threats a basic set of generic, high level privacy requirements especially suited for considerations on the data level have been introduced.

Further investigations are necessary to evolve the mentioned issues. More specifically, a detailed analysis on the relation between smart grid data and personal information is needed.

In addition, the presented ideas are to be applied to real life projects. To do so, they are integrated in the "SGAM Toolbox" which is currently implemented at the Josef Ressel Center.

The SGAM Toolbox is a Model-Driven-Architecture framework that incorporates the Smart Grid Architecture Model as introduced by [11]. By the usage of this toolbox for the development of real life projects further experiences are expected.

## ACKNOWLEDGEMENTS

The financial support of the Josef Ressel Center by the Austrian Federal Ministry of Economy, Family and Youth and the Austrian National Foundation for Research, Technology and Development is gratefully acknowledged.

Funding by the Austrian Federal Ministry for Transport, Innovation and Technology and the Austrian Research Promotion Agency (FFG) under Project 838793, "IntegrA", is gratefully acknowledged.

## REFERENCES

[1] M. A. Lisovich and S. B. Wicker, "Privacy concerns in upcoming residential and commercial demand-response systems," *IEEE Proceedings on Power Systems*, vol. 1, no. 1, 2008.

[2] E. L. Quinn, "Privacy and the new energy infrastructure," *Social Science Research Network (SSRN)*, Feb. 2009.

[3] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security Privacy Magazine*, vol. 7, no. 3, pp. 75–77, 2009.

[4] H. Khurana, M. Hadley, N. Lu, and D. Frincke, "Smart-grid security issues," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[5] S. Rohjans, C. Danekas, and M. Uslar, "Requirements for smart grid ICT-architectures," in *Proc. IEEE Int. Conf. Innovative Smart Grid Technologies (ISGT Europe)*, 2012, pp. 1–8.

[6] S. B. Wicker and D. E. Schrader, "Privacy-aware design principles for information networks," *Proceedings of the IEEE*, vol. 99, pp. 330–350, 2010.

[7] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation," *Identity in the Information Society*, vol. 3, pp. 275–294, 2010, 10.1007/s12394-010-0046-y. [Online]. Available: http://dx.doi.org/10.1007/s12394-010-0046-y

[8] K. Beckers, "Comparing privacy requirements engineering approaches," in *Seventh International Conference on Availability, Reliability and Security (ARES), 2012*, 2012, pp. 574–581.

[9] B. Fabian, S. Gürses, M. Heisel, T. Santen, and H. Schmidt, "A comparison of security requirements engineering methods," *Requirements Engineering Special Issue on Security Requirements Engineering*, vol. 15, pp. 7–40, 2010.

[10] M. Deng, K. Wuyts, R. Scandariato, B. Preneel, and W. Joosen, "A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements," *Requirements Engineering*, vol. 16, pp. 3–32, 2011.

[11] Smart Grid Coordination Group, "Smart grid reference architecture," CEN-CENELEC-ETSI, Tech. Rep., 2012.

[12] ——, "Sustainable processes," CEN-CENELEC-ETSI, Tech. Rep., 2012.

[13] ——, "First set of standards," CEN-CENELEC-ETSI, Tech. Rep., 2012.

[14] ——, "Smart grid information security," CEN-CENELEC-ETSI, Tech. Rep., 2012.

[15] G. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, Dec. 1992.

[16] M. Zeifman and K. Roth, "Nonintrusive appliance load monitoring: Review and outlook," *IEEE Transactions on Consumer Electronics*, vol. 57, pp. 76–84, 2011.

[17] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proceedings of First IEEE International Conference on Smart Grid Communications*, Gaithersburg, Maryland, USA, Oct. 2010, pp. 238–243.

[18] Z. Erkin, J. Troncoso-Pastoriza, R. Lagendijk, and F. Perez-Gonzalez, "Privacy-preserving data aggregation in smart metering systems: An overview," *Signal Processing Magazine, IEEE*, vol. 30, no. 2, pp. 75–86, March.

[19] D. Engel, "Wavelet-based load profile representation for smart meter privacy," in *Proc. IEEE PES Innovative Smart Grid Technologies (ISGT'13)*, Washington, D.C., USA, Feb. 2013, pp. 1–6.

[20] C. Kalloniatis, E. Kavakli, and S. Gritzalis, "Addressing privacy requirements in system design: the PriS method," *Requirements Engineering*, vol. 13, pp. 241–255, 2008.

[21] *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems*, International Electrotechnical Commission (IEC) Std., Apr. 2010.

[22] *Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit, Sicherheit (RAMS)*, Deutsches Institut für Normung (DIN) Std. DIN EN 50 126.

[23] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. Vol. 1 No.1, pp. 11–33, 2004.

[24] A. Pfitzmann and M. Hansen, "A terminology for talking about privacy by data minimization: Anonymity, unlinkability, unobservability, pseudonymity, and identity management - version v0.34," TU Dresden and ULD Kiel, Tech. Rep., 2011.

[25] *Common Criteria for Information Technology Security Evaluation*, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Std. ISO/IEC 15 408, 2009.

[26] H. Nissenbaum, "Privacy as contextual integrity," *Washington Law Review*, vol. 79, pp. 101–139, 2004.