# Smart Grid Reference Architecture, an Approach on a Secure and Model-Driven Implementation

Stefan Wilker*, Marcus Meisel*, Ewa Piatkowska‡, Thilo Sauter*† and Oliver Jung‡
*TU Wien – Institute of Computer Technology, 1040 Vienna, Austria
Email: {first.lastname}@tuwien.ac.at
‡AIT – Austrian Institute of Technology, 1210 Vienna, Austria
Email: {first.lastname}@ait.ac.at
†Danube University Krems – Center for Integrated Sensor Systems, 2700 Wiener Neustadt, Austria
Email: {first.lastname}@donau-uni.ac.at

***Abstract*—Up to date new devices for electrical power systems are introduced and used on every level. There is a myriad of documents related to those devices ranging from vendor requirements to checklists for the maintenance crew. This paper presents the results of creating an Austrian Reference Architecture for Smart Grids, not only being able to handle all these documents but also manage their versioning and automated security requirement list generation. Furthermore the architecture allows a role based focus on specific viewpoints as well as interoperability to third-party tools, for instance for external security evaluations. The main contribution of the project is the creation of the reference architecture on an available modeling framework plugin while keeping all stakeholders on board of the process to form a common understanding of its growing importance in the future. The exemplary steps of creating a reference architecture for Austria are introduced in this paper. These steps are internationally applicable and present a substantial move in this domain going from a document based procedure towards a model-based and digitized example resulting in a model-driven engineered implementation.**

## I. Introduction

Technological revolutions such as blockchain are happening, cyber-physical energy networks are about to become smart grids, digital information and communication technologies are growing more prevalent in new, semiconductor including devices. Furthermore, advances of combining different energy sources (electricity with gas or heat) are taking place all at once with goals of achieving ambitious climate goals, enabling more volatile renewables, and allowing decentralized multitudes of prosumers to participate in new business models.

Understanding the (inter-)national electricity market and available products in order to create new business models, revenue streams, or applications with special regard to a secure realization can be a challenging task for established companies as well as start-ups in this ever-changing environment. In Austria, one noteworthy outcome of the *Reference Architecture for Secure Smart Grids in Austria* (RASSA)-Initiative [1] was a stakeholder process, which strengthened early-on participation. In continuation of the efforts of the EU Mandate M/490 [2], to allow stakeholders of different domains to understand the same taxonomy when modeling new smart grid applications, a *Smart Grid Architecture Model* (SGAM) [3] based approach was used in RASSA. The use of a model-driven design approach through the use of the SGAM Toolbox [4] was an essential enabling technology decision especially due to the fact that SGAM has become a standard way of describing smart grid systems. Modelling the systems architecture in the SGAM Toolbox offers a possibility to interface it with other tools that require detailed knowledge about the system as input, e.g., security or privacy risk assessment tools.

The *Unified Modeling Language* (UML) based model-driven design as described in [5], allows the definition of components, systems, and roles in the Austrian electricity market to the fullest extent, enabling the comparison with internationally corresponding counterparts. The model-driven design approach and the aforementioned detailed definitions enable the inclusion of national [6] as well as international [7] security- and privacy-by-design efforts already undertaken or planned [8], on all levels of new smart grid application use cases.

Current workflows are often document-based, containing tables with version numbers or dates in the file names. Approaching the modeling of an application for the smart grid, with a tremendous amount of security-sensitive components can get complicated swiftly and not maintainable in document-based approaches. Furthermore, large manually drawn use case definitions and dependencies are often discussed on flip charts and afterward digitized. They are better maintainable, but version conflicts and limited screen estate usually limit complex interactions. Initially, the handling of modeling with the toolbox has a steep learning curve [9]. Nevertheless, we will show in this paper that the advantages outweigh the disadvantages in the long run. The goal of RASSA is to provide an accessible and up-to-date version of use cases, their components, definitions, elements, and notably security requirements in a model, thriving towards a model-driven approach according to [10], allowing highly complex interactions, combinations of standards, protocols, components, actors, functions, and business objectives. This modeling environment and the provided model from the SGAM Toolbox enables users to collaborate and have less workload on the maintenance of file-versioning since these features are provided in the tool. Furthermore, it enables to link source documents (in terms of product descriptions or technical specifications) to every relevant component or actor within the digital models. Additionally, specialized third-party services can be integrated or import such models for further analysis and development of new business models. Attributes for models and elements can be added dynamically. Together with specified components, actors, interfaces, and security requirements, a model-driven approach allows a trusted set to serve as the foundation of a manageable blueprint for a reference architecture [1]. This work focuses on the contribution of handling documentation processes and security guideline issues in a growing domain of smart grid architecture development.

Section III of this work provides the methodology used in RASSA. Afterwards, we give an example of a created use cases using our methodology in Section IV which is followed by a small scale excerpt for demonstration. In Section V we explore the generation of security-related generated documents from a model-driven diagram. Afterwards, we use the data from the presented approach in an external tool for Data Protection Impact Assessment in Section VI. Finally, we present our conclusions to our current findings in Section VII and provide prospects of development and implementation in Section VIII.

## II. Motivation

The amount of threats to electronic devices is on a constant increase, as well as the accompanying countermeasures and strategies for closing possible vulnerabilities. Keeping the operating system as well as the working environment up to date and secure is a resource-intensive task. Furthermore, applying the correct countermeasures requires a well-designed access towards the needed knowledge for the responsible persons in a compressed but understandable way. So-called knowledge databases are an option of providing the necessary platform for sharing and accessing know vulnerabilities.

One of the greatest challenges relies on granting the right amount of useful information for the person in charge, preferably attuned to his level of expertise. A common understanding of the type and functions of the device or system in question is therefore crucial. The design and proof of concept of an adjustable user or group specific knowledge-transfer database access (or similar technological approaches) or knowledge-transfer process that enables integration into everyday working situations while enhancing the overall security situation even for small companies, is recommendable. The correct treatment and containment of vulnerability need to be accessible and practical regarding available resources, which are inevitably connected to the user or technician, carrying out the task of keeping the operating system alive and secure. This comes hand in hand with bringing together different levels of domain knowledge or varying terminologies for the very same object exposing the vulnerability in question. The accessibility of the right information, the avoidance of finding redundant solutions, and furthermore the ongoing documentation in order to avoid common errors are approached that are not limited to the domain area of security. New approaches or methods need to prove themselves valuable among different levels of the company, ranging from small to large scale. One of these new approaches is the model-driven engineering approach in the Smart Grid domain as described by the author of [11] in which one of the goals is also to raise awareness on possible vulnerabilities in cyber-physical systems. A similar model-driven engineering strategy has also been applied to the field of Industry 4.0 by the authors of [12], unmanned aircraft systems [13] and healthcare [14] for validation purposes and handling the complexity of todays quick developments. Establishing processes or software for reducing information floods for the end-user is going to be more important than ever considering the importance of Big Data, whereas the yearly collected data and information surpasses all previous accumulated volumes of data collected in human history.

## III. Methodology

Initially, in the RASSA-Architecture project technical, juridical-regulatory, and user-centered requirements towards a reference architecture were collected and organized by the consortium, which afterward consolidated the requirements with external stakeholders as part of an established stakeholder process [15][16] within the RASSA-Initiative.

Technical requirements focus on the areas of proactive and reactive ICT-security, personal, and facility security, and interfaces towards a semi-automatic risk management system. Furthermore, components include renewable energy sources, decentralized energy storages, linkage of other energy carriers (like gas, thermal and cooling), as well as novel consumers (e.g., electrical vehicles, or flexible processes).

Regarding user-oriented requirements, we pursue a user-centered and value-centered design approach. This approach mandates an ongoing involvement of potential users (as clients), inquiring their needs for the development process and therefore improve the acceptance of the developed system and model and its provided functionalities. Requirements and concerns are raised through qualitative as well as quantitative methods to reach a broad foundation for ensuring the development of the created architecture and its features.

The requirement elicitation is based on selected use cases that have high relevance for the Austrian market. A small excerpt of these use cases is listed in alphabetical order as follows:

- Automatic fault detection and rapid restoration of power (power-system protection)
- Coordinated charging of electric vehicles
- Distribution grid automation
- Distribution grid monitoring
- Incrementation of hosting capacity through active regulatory approaches

Throughout RASSA, these use cases are mapped onto the SGAM and used to serve as an initializing framework for developing the most relevant parts of the reference architecture for Austria. Key aspects are therefore security and privacy requirements. For a detailed taxonomy of the reference architecture, the technical and user-oriented requirements are compared and formulated as precisely as possible. Industrial partners were encouraged to widen their focus on far-reaching applicable solutions and not concentrating solely on their short-term development strategies.

While use cases are initializing the models, in parallel, the juridical-regulatory framework conditions of pertinent union directives, a summary and analysis of the implementation of intelligent sensor systems (e.g. in directive 2009/72/EG, directive 2012/27/EU) is made, as well as security analysis in the area of this critical infrastructure (for example the directives 2005/89/EG, 95/46/EG, 2008/114/EG, 2013/40/EU).

A comparison with longterm implementation and expansion goals of the European Commission for the future-oriented embodiment of the reference architecture ensures contacts and correspondence with opinion-leaders within strategic committees on the European level (e.g., ETIP SNET [17]), as well as respective research discussions.

## IV. Example of Power-System Protection Use Case

As an example, we apply our presented approach by modeling a small line current differential protection use case. The illustrations given are intentionally chosen as a small show case to keep the complexity to a minimum. As the first example, we chose the line current differential protection, which is a scheme for protecting high-voltage transmission lines. Two protective relays, which are represented as intelligent electronic devices (*Intelligente, elektronische Übertragungsgeräte*) in Fig. 2, are monitoring the current on different parts of a transmission line. If the current flowing into the line and the current flowing out of the line do not match, the protective relay trips.

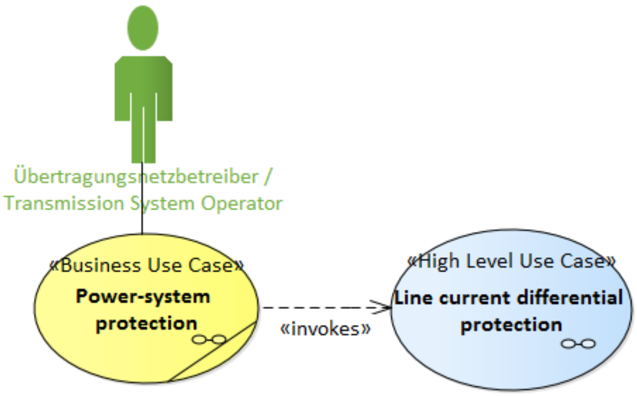

Übertragungsnetzbetreiber /
Transmission System Operator
«Business Use Case»
Power-system protection
«invokes»
«High Level Use Case»
Line current differential protection

Fig. 1. Business Layer: line current differential protection

Fig. 1 shows a diagram in the SGAM Business Layer. The figure includes the business actor *Übertragungsnetzbetreiber / Transmission System Operator* that is pursuing the business case grid protection. This business case invokes the use case line current differential protection. The SGAM Communication Layer diagram consists of two intelligent electronic devices that communicate current measurements using IEC 61850 protocols (see Fig. 2).

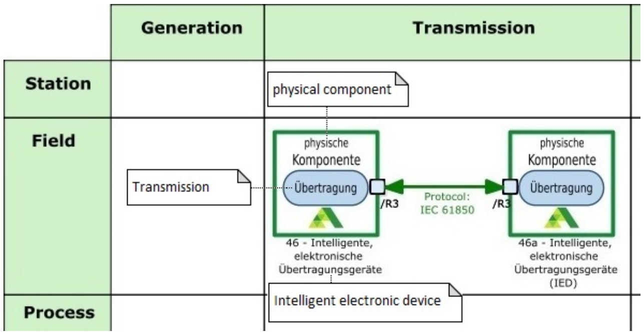
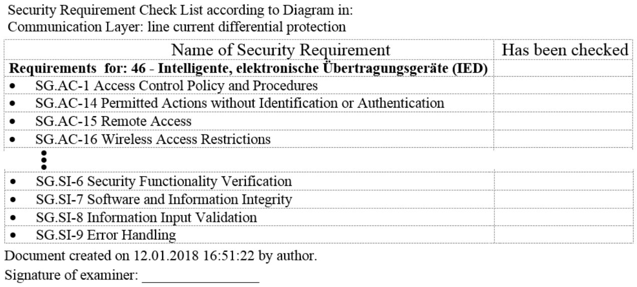


Fig. 2. Communication Layer: line current differential protection

## V. Generation of Security Related Documentation for the Power-System Protection Use Case

Dealing with the huge amount of security risks, countermeasurements and the necessity of keeping a comprehensive view on already implemented or still open measures can quickly be burdensome for the responsible person. As a result of the RASSA project, the SGAM-Toolbox embedded template report named *SGAM Project - Section (detailed)* generates a text file of the created reference architecture, containing 1125 DIN A4 pages and nearly 125.000 words. The numbers indicate that employees could not specify this amount of highly precise descriptions in manual labor within a reasonable time-frame. Furthermore, upon investigation of these numbers, it shows the advantages of a model-driven approach for the processing and the deposition of data over otherwise recorded spreadsheet applications or text documents.



Security Requirement Check List according to Diagram in:
Communication Layer: line current differential protection

| Name of Security Requirement | Has been checked |
|---|---|
| **Requirements for: 46 - Intelligente, elektronische Übertragungsgeräte (IED)** | |
| • SG.AC-1 Access Control Policy and Procedures | |
| • SG.AC-14 Permitted Actions without Identification or Authentication | |
| • SG.AC-15 Remote Access | |
| • SG.AC-16 Wireless Access Restrictions | |
| ⋮ | |
| • SG.SI-6 Security Functionality Verification | |
| • SG.SI-7 Software and Information Integrity | |
| • SG.SI-8 Information Input Validation | |
| • SG.SI-9 Error Handling | |

Document created on 12.01.2018 16:51:22 by author.
Signature of examiner: ________________

Fig. 3. Excerpt of device specific checklist with derived security requirements

In special regard to the above-mentioned huge amount of pages and text, a far more reduced and specific view on the necessary information is desirable, such as for the activity of working through a catalog of security requirements for a defined use case. The rules for report generation can be individualized to the specific needs of the end users or target groups, ranging from simple checklists up to uniform specifications in corporate design. In Fig. 3 we show such an informal checklist for the equipment shown in Fig. 2. The generated file contains a list of 66 bullet points with security requirements, which have been derived from the NIST *Logical Reference Model* (LRM).

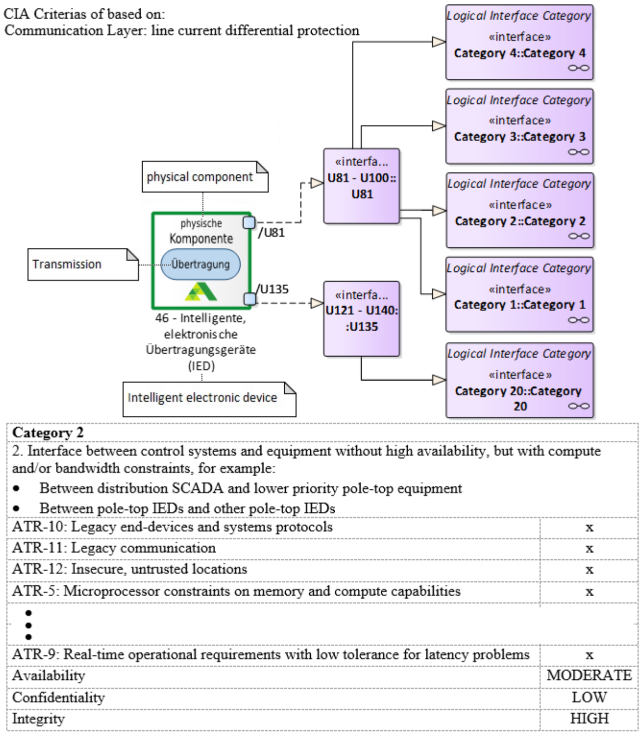
Even though, the example from Fig. 3 is just for a single device, the extension towards checklist descriptions for entire use cases is applicable. The pieces of information are listed as defined in the document generation schema for each element used within the use case diagram. Enterprise Architect offers all kinds of options and filter possibilities for the adaption of the document generation. However, they require a training period and an understanding of the used data types and structures that are defined by the Enterprise Architect software, to achieve a proper outcome. Another example for a different data-subset of elements from a use case is depicted in Fig. 4. The representation of information is linked with the associated attributes and *CIA* (Confidentiality, Integrity, Availability) criteria from the interfaces and categories of each element in the use case, which have been derived from the NIST LRM. We present those in a tabular format and as a detail view diagram in the following. In the table shown in Fig. 4, the description of the involved category (in the example shown: Category 2) is listed, as well as the associated *Security Requirements* which starts with the requirement *ATR-10: Legacy end-devices and systems protocols*. The detailed description of this *Security Requirement* is not generated for the sake of enhanced transparency, but can be enabled easily in the documentation template for the document generation. In the case of *ATR-10*, the description is “Older end-devices and protocols may constrain the types, thoroughness, or effectiveness of different security technologies which may be employed” [7], which is also derived from the NIST LRM due to the nature of the RASSA project. The aforementioned *CIA* criteria that are also depicted in the table with their assessment of having a *LOW*, *MODERATE* or *HIGH* potential impact, are defined and summarized as follows by [7]:

- *Confidentiality*: A loss of confidentiality is the unauthorized disclosure of information.
- *Integrity*: A loss of integrity is the unauthorized modification or destruction of information.
- *Availability*: A loss of availability is the disruption of access to or use of information or an information system.

Throughout the project, this feature of documentation generation is considered as a helpful tool by our partners for formulating official requirements for certain installations or devices in future public tenders made by distribution system operators. By following the presented approach with a common defined set of devices/roles/actors, as proposed by our reference architecture, the different legal partners could exchange a standardized form and guarantee (as well as control) that legal or technical requirements have been implemented or checked.

## VI. Data Protection Impact Assessment

However, currently quite a lot of effort is being put into ensuring compliance with the new European General Data Protection Regulation (GDPR) [18], which states that all services that collect or process personal data are subject to Data Protection Impact Assessment (DPIA). Since smart metering data also falls into this category, all smart grid services are required to have DPIA in place.


CIA Criterias of based on:
Communication Layer: line current differential protection
physical component
physische
Komponente
Transmission
Übertragung
/U81
/U135
46 - Intelligente, elektronische Übertragungsgeräte (IED)
Intelligent electronic device
«interfa...
U81 - U100::
U81
«interfa...
U121 - U140:
:U135
Logical Interface Category
«interface»
Category 4::Category 4
Logical Interface Category
«interface»
Category 3::Category 3
Logical Interface Category
«interface»
Category 2::Category 2
Logical Interface Category
«interface»
Category 1::Category 1
Logical Interface Category
«interface»
Category 20::Category 20

| **Category 2** | |
|---|---|
| 2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example:<br>• Between distribution SCADA and lower priority pole-top equipment<br>• Between pole-top IEDs and other pole-top IEDs | |
| ATR-10: Legacy end-devices and systems protocols | x |
| ATR-11: Legacy communication | x |
| ATR-12: Insecure, untrusted locations | x |
| ATR-5: Microprocessor constraints on memory and compute capabilities | x |
| ⋮ | |
| ATR-9: Real-time operational requirements with low tolerance for latency problems | x |
| Availability | MODERATE |
| Confidentiality | LOW |
| Integrity | HIGH |

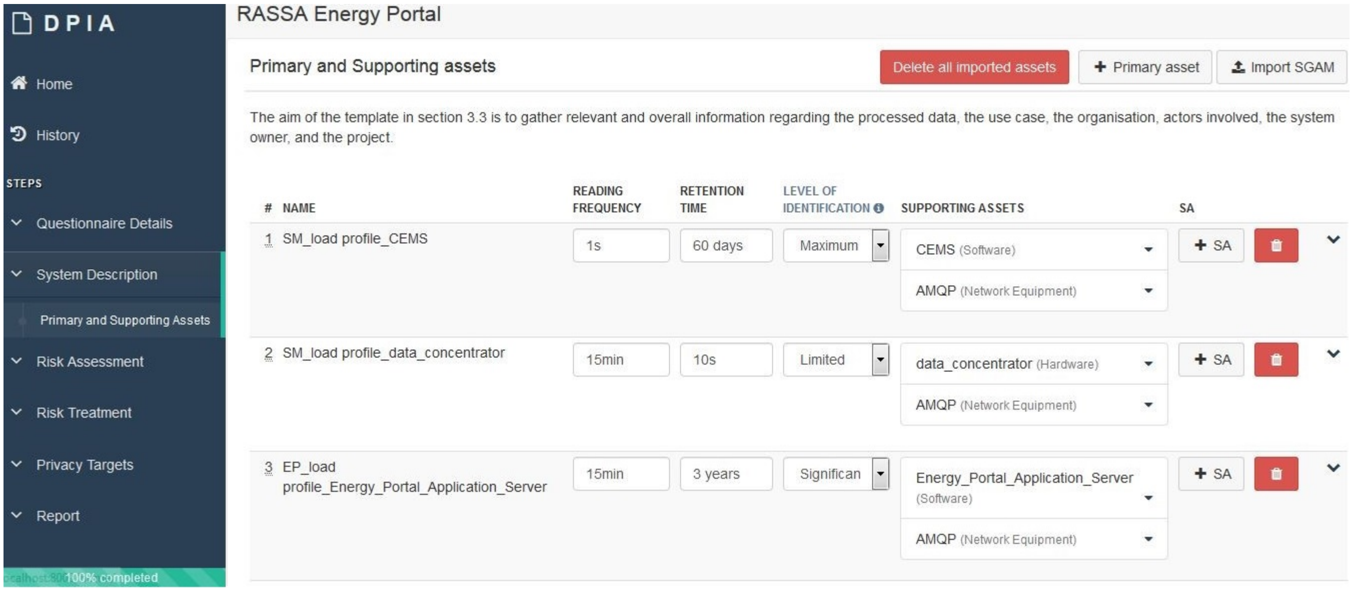
Fig. 4. Exemplary outline of a generated category information with CIA criterias and additional attributes

In the RASSA project we have performed a DPIA exercise for a *Customer Energy Portal* use case to identify any potential privacy risks associated with the portal deployment. We have implemented the assessment with support of the DPIA tool[19], which enables an automatic import of the SGAM model. As presented in Figure 5 three types of information are extracted from the model:

1) primary assets, i.e., information items, including personal data, exchanged or stored in a system
2) supporting assets, which represent all the components within systems infrastructure, such as software, hardware or network equipment
3) associations between primary and supporting assets, e.g., load profile information stored in the Customer Energy Management System (CEMS) will be associated with CEMS hardware and software.

Primary assets are further described with information about the data reading frequency, retention time and level of identification. These are specific for the DPIA and are used to determine the impact level if assets confidentiality gets compromised.

Through the compatibility with tools like the DPIA Tool as well as the aforementioned document generation feature, we are able to demonstrate the different ways of extracting security or privacy related aspects from the proposed reference architecture model and outlined their added value.



RASSA Energy Portal

Primary and Supporting assets

The aim of the template in section 3.3 is to gather relevant and overall information regarding the processed data, the use case, the organisation, actors involved, the system owner, and the project.

| # | NAME | READING FREQUENCY | RETENTION TIME | LEVEL OF IDENTIFICATION | SUPPORTING ASSETS | SA |
|---|---|---|---|---|---|---|
| 1 | SM_load profile_CEMS | 1s | 60 days | Maximum | CEMS (Software)<br>AMQP (Network Equipment) | + SA |
| 2 | SM_load profile_data_concentrator | 15min | 10s | Limited | data_concentrator (Hardware)<br>AMQP (Network Equipment) | + SA |
| 3 | EP_load profile_Energy_Portal_Application_Server | 15min | 3 years | Significan | Energy_Portal_Application_Server (Software)<br>AMQP (Network Equipment) | + SA |

Fig. 5. Exemplary snippet of the DPIA Tool, with opened system description step and imported data of SGAM elements from RASSA use cases.

## VII. Conclusion

As stated in Section III, one focus throughout the project is security. While this work describes the approach for creating a secure and model-driven implementation of a use case in the smart grid domain and the communication between stakeholders and formal documentation steps, the verification of the presented strategy plays a significant role in the RASSA project. This verification is based on the use cases that have been defined in RASSA and are checked against the extracted specifications of the presented reference architecture blueprint model. For this, a specific testing hardware setup has been build in order to undergo in-depth analysis procedures and penetration tests. Based on the results (which are subject to confidentiality agreements and therefore are not discussed further within this work), feedback towards the reference architecture model is made in the final step of the RASSA project. The results show a high coverage of the considered security requirements that are proposed by the reference architecture. We also discovered some highly product-specific issues, that are only partly covered by the extracted data as it is presented in this work. A generalization in terms of the *Category* association or *Category* definition would not be applicable in a general way. Therefore we propose to introduce a new modeled layer, which inherits product-specific or producer-specific catalogs of requirements to enhance the overall security even further.

With further convenient features and additional information sources for the presented model-driven approach, the model developed in the RASSA project can be used as a foundation for creating smart grid application use cases that are applicable in other countries as well. Great benefits can be derived when European regulations or requirements could be integrated into such a model, making them accessible for all the involved parties. It can be a structural foundation model for other countries that are coupled with Austria in order to support the dialog, security and exchange of information between the various (grid-) connected neighboring countries, facilitating a common terminology and criteria that are fully compatible with the SGAM. All information that is publicly available, can be accessed online [1], [22] with the a clickable browser version of the reference architecture published at [23].

Further improvements regarding plugin compatibilities or exchange possibilities for current software solutions in use (e.g., one of them namely CRISAM) in corresponding formats will enhance the spread and acceptance of the presented approach. CRISAM is widely used in Austrian companies [20] for information risk management, enterprise risk management or industrial control systems and supervisory control and data acquisition with a wholesale of functionalities for operational business.

## VIII. Outlook

At the current state, the SGAM Toolbox is depended on the Enterprise Architecture software, which already itself offers great extendability. One project among them is described in the work of [21]. The authors demonstrate a show-case, in which they use “the Common Information Model (CIM) which describes terms in the energy sector and relations between them” [21] and model CIM UML specifications. The authors showed successfully the usage of the CIM data to make first steps into the direction of *round-trip engineering* possible [21] through demonstration of C++ code generation according to their CIM UML diagrams. To close the gap to the *round-trip engineering*, they showed that they can modify the CIM UML accordingly, when code structures are changed and played back into the system. The proposed reference architecture could benefit by using similar approaches in the future:

One potential benefit would be, that the code generation according to (DIM) UML specifications could enhance the definition of interfaces and deliver testbeds for them. With this feature, the overall interoperability can be improved while incorporating the vast amount of defined security requirements.

Another beneficial aspect can be an automated code snippet generation for surface security tests, which are applicable for the components in the defined UML diagram.

## IX. ACKNOWLEDGEMENTS

Findings presented are from the project *RASSA Architecture* as part of the Initiative *Reference Architecture for Secure Smart Grids Austria*, which was commissioned by the Austrian Climate and Energy Fund and supported by the Austrian Research Promotion Agency (FFG project number 848811) as part of the 1st Call *Energieforschungsprogramm* in the main area *Intelligente Netze*.

## REFERENCES

[1] Technologieplattform Smart Grids Austria, "Reference Architecture for Secure Smart Grids Austria". [Online]. Available: http://www.smartgrids.at/plattform-aktivitaeten/rassa-initiative.html. [Accessed: 19-Jan-2018]

[2] European Commission, EU Mandate M/490. [Online]. Available: https://ec.europa.eu/energy/sites/ener/files/documents/2011_03_01_mandate_m490_en.pdf. [Accessed: 19-Jan-2018]

[3] Smart Grid Coordination Group: "Smart Grid Reference Architecture", Technical Report, CEN-CENELEC-ETSI, (Nov. 2012). [Online]. Available: http://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx. [Accessed: 12-Jan-2018]

[4] Josef Ressel Center for User-Centric Privacy, Security and Control, SGAM-Toolbox Setup (AddOn for *Enterprise Architect* from Sparx Systems), [Online]. Available: https://www.en-trust.at/downloads/sgam-toolbox-2-0/sgam-toolbox-2-0-download/. [Accessed: 12-Jan-2018]

[5] C. Neureiter, D. Engel, M. Uslar, Domain Specific and Model Based Systems Engineering in the Smart Grid as Prerequesite for Security by Design. MDPI Electronics – Special Issue on Smart Grids Cybersecurity, 2016, 5. Jg., Nr. 2, p. 24.

[6] E-Control, Oesterreichs Energie, Austrian Power Grid (APG), Bundeskanzleramt (BKA), Bundesministerien (BMWFW, BMI, BMLVS), Kuratorium Sicheres Österreich (KSÖ), REPUCO Unternehmensberatung GMBH. 2014. "Risikoanalyse für die Infoermationssysteme der Elektrizitätswirtschaft unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes. [Risk analysis for the information systems of the electricity sector with particular focus on smart meters and data privacy protection]". [Online]. Available: http://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7. [Accessed: 22-May-2017]

[7] Smart Grid Interoperability Panel: Guidelines for Smart Grid Cyber Security. Technical Report 7628, Cyber Security Working Group, (NIST) (September 2010). [Online]. Available: http://www.nist.gov/smartgrid/upload/nistir-7628_total.pdf. [Accessed: 22-May-2017]

[8] Technologieplattform Smart Grids Austria (TPSGA),Technologieroadmap Smart Grids Austria - Die Umsetzungsschritte zum Wandel des Stromsystems bis 2020 [Technology Roadmap Smart Grids Austria - The implementational steps towards the transition of the power system until 2020], Technical Report, Technologieplattform Smart Grids Austria (April 2015). [Online]. Available: http://www.smartgrids.at/files/smartgrids/Dateien/Dokumente/05Roadmap_Management_Englisch.pdf. [Accessed: 22-May-2017]

[9] S. Wilker, M. Meisel and T. Sauter, "Smart Grid Architecture Model Standardization and the Applicability of Domain Language Specific Modeling Tools," 2017 IEEE 26th International Symposium on Industrial Electronics (ISIE), Edinburgh, 2017, pp. 152-157.

[10] C. Neureiter, M. Uslar, D. Engel and G. Lastro, "A Standards-based Approach for Domain Specific Modelling of Smart Grid System Architectures", in: *11th System of Systems Engineering Conference (SoSE)*, IEEE, pages 1-6, 2016.

[11] Christian Neureiter, " A Domain-Specific, Model Driven Engineering Approach for Systems Engineering in the Smart Grid ", Doctoral Thesis, MBSE4U, 2017, pp. 1-272., ISBN: 978-3-9818529-2-9

[12] M. Weyrich and C. Ebert, "Reference Architectures for the Internet of Things, (2016)", published in IEEE Software, vol. 33, no. 1, pp. 112-116, 2016.

[13] E. Denney, G. Pai and I. Whiteside, "Model-Driven Development of Safety Architectures", 2017 ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS), Austin, TX, 2017, pp. 156-166.

[14] H. Gannud, H. Wu and J. Timoney, "Applying a MDE approach to a Healthcare Environment: A Case Study of an AE Dept",2017 28th Irish Signals and Systems Conference (ISSC), Killarney, 2017, pp. 1-7.

[15] M. Meisel, A. Berger, L. Langer, M. Litzlbauer, G. Kienesberger, The RASSA Initiative  Defining a Reference Architecture for Secure Smart Grids in Austria, Lecture Notes in Computer Science, vol. 9424, pp. 5158. Springer International Publishing (2015), http://dx.doi.org/10.1007/978-3-319-25876-8_5

[16] A. Berger, M. Meisel, L. Langer, M. Litzlbauer and M. Uslar, RASSA-Stakeholderprozess, Technical Report for Bundesministerium für Verkehr, Innovation und Technologie; Report-Nr. 12, 2015; 79 p.

[17] The European Technology and Innovation Platform Smart Networks for Energy Transition. [Online]. Available: http://www.etip-snet.eu. [Accessed: 15-Jan-2018]

[18] Official Journal of the European Union "General Data Protection Regulation", May 2016. [Online]. Available: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf. [Accessed: 30-Jan-2018]

[19] E. Piatkowska, A. Bajraktari, D. Chhajed, and P. Smith, "Tool Support for Data Protection Impact Assessment in the Smart Grid", e&i Elektrotechnik und Informationstechnik, February 2017, Volume 134, Issue 1, pp 2629.

[20] Calpana Business Consulting Gmbh, CRISAM Software Reference List. [Online]. Available: https://www.crisam.net/de/referenzliste. [Accessed: 10-Feb-2018]

[21] L. Razik, M. Mirz, D. Knibbe, et al. "Automated Deserializer Generation from CIM Ontologies: CIM ++ an Easy-to-Use and Automated Adaptable Open-Source Library for Object Deserialization in C ++ from Documents Based on User-Specied UML Models Following the Common Information Model (CIM) Standards for the Energy Sector", Computer Science - Research and Development 2017, Springer Berlin Heidelberg, https://doi.org/10.1007/s00450-017-0350-y

[22] AIT Austrian Institute of Technology and Technologieplattform Smart Grids Austria (TPSGA), "RASSA Official Website". [Online]. Available: https://rassa.at. [Accessed: 08-Apr-2018]

[23] AIT Austrian Institute of Technology and Technologieplattform Smart Grids Austria (TPSGA), "RASSA Reference Architecture - Clickable Version". [Online]. Available: https://rassa.at/referenzarchitektur. [Accessed: 08-Apr-2018]