# Aligning IT Architecture Analysis and Security Standards for Smart Grids

Stefanie Schlegel[1], Christine Rosinger[1], Mathias Uslar[1]

## Abstract

In this paper, an approach using the European Smart Grid Architecture Model (SGAM), in the context of the NISTIR 7628, is presented. Research has shown that both models and methodologies have particular impact, but have not yet been put into mutual context. The combination of these models makes it possible for US smart grid experts to re-use the SGAM model and its benefits, and vice versa European stakeholders are encouraged to use the security analysis framework from NIST. Within this paper, we briefly introduce the methodologies including their strengths and fallbacks. We outline the necessity to make them interoperable and aligning them. Finally, the logical interface framework from NISTIR 7628 is mapped onto the SGAM and its planes, domains and zones, bridging the previous gap.

## 1. Introduction

One particular important aspect of a future smart grid, being a system-of-a-system, is the growing need for using ICT for communication between the various components, involved in the processes. Particular goals, to be achieved by the smart grid, may be related to aspects like the optimization and coordination of the various elements and their operation in the transmission as well as the distribution grid [1].

The importance of the aspect of (system) availability and uptime for the electric power distribution system is high. Furthermore, the dependability of the infrastructure, as well as of its basic components, is the focus of system and interfaces at design-time. Additionally, interoperability and interchangeability have to be taken into account to ensure a meaningful analysis of both, technical and non-technical requirements [2]. To achieve this goal, one particular way is to standardize technical solutions like data models, interfaces, processes and communication protocols at both international and national level. [3].

After the first standardization, initiatives were raised by both IEC and NIST, the very idea, that standards without being applied as best-practice in real-world applications are not the solution per se, became very apparent [4]. The NIST framework and roadmap for interoperability, as well as the European initiatives derived from the M/490 Smart Grid mandate [5], focuses on properly using, expanding and adopting so called IEC core standards as well as various related ones. To realize this, in 2012 the *Smart Grid Coordination Group* (SG-CG) initiated four different groups, that should develop a report for their corresponding topic, which are *"Sustainable processes"*, *"(First) Set of Consistent Standards"*, *"Reference Architecture"* and *"Smart Grid Information Security"* [6].

## 2. Security Architecture Development in the Smart Grid

Within this section, we highlight the existing work, which is relevant to the ideas, and preliminary work presented in this paper. First, the scope of the M/490 mandate motivates the need for a common architectural viewpoint in order to foster better component and system interoperability. This section concludes with a short overview on the NISTIR 7628 document series and a

[1] OFFIS – Institute for Information Technology, Escherweg 2, 26121 Oldenburg, Germany. forename.surname@offis.de

motivation why the various models should be combined for a better security-by-design methodology.

## 2.1. The SGAM

In the context of the European Commission's Standardization Mandate M/490 [7], [8], a holistic viewpoint of an overall smart grid infrastructure named Smart Grid Architecture Model (SGAM) is developed. This work is based on existing previous approaches and subsumes the different perspectives and methodologies of the smart grid concepts. Figure 1 depicts the SGAM structure with its layers; the subclasses of the domains and zones are also outlined in Figure 1.

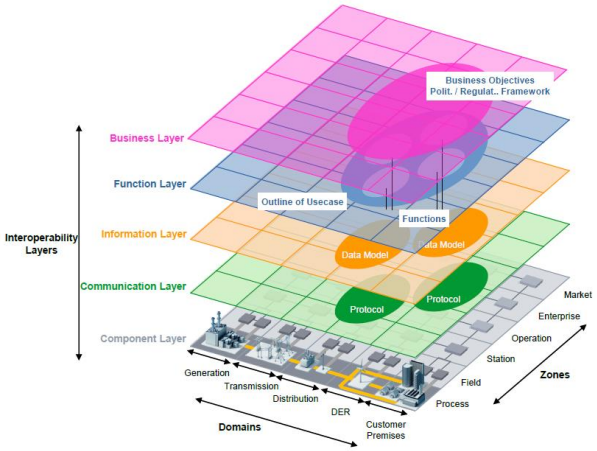


*Figure 1: The SGAM cube*

The SGAM comprises five so-called core viewpoint layers which support energy architecture design of different domain experts. Additional, the domains and zones support a holistic view on an architecture, including the business processes, which usually are out of scope for standardization. These layers were adopted from the Gridwise Alliance Architecture Council (GWAC) stack and context-setting framework [9].

## 2.2. Security Standards for Smart grids

Information security is not just relevant for the operation of the smart grid as a critical infrastructure, it is also very important for user acceptance and general operations. This particularly affects technologies like smart metering, especially in the part of privacy issues. Many different standards exist in the IEC TC57 portfolio, among them there are standards especially designed for end-to-end security; see e.g. [10] – one of particular interest is the NISTIR 7628 series [1]. Following the executive summary, the first volume of this internal report describes the overall approach, including the so-called risk assessment process, used by the CSWG to identify so called high-level security requirements. It also represents a high-level architecture, followed by a sample logical interface reference model with a composite view of 46 actors, distributed among the seven energy domains (transmission, bulk generation, marketing, operations, service provider, distribution and customer). This model is used to identify and define 22 logical interface (LI) categories within and across the domains. For these LI categories, so called high-level security requirements are described.

## 2.3. Linking Architecture and Security

As stated beforehand, combining the two state-of-the-art models from Europe and the US should lead to a better security analysis possibility for the current SGAM cube methodology. Later, this

should lead to a better dependability analysis for SGAM models as well as a proper linking of logical interfaces (LI) from the NISTIR 7628 to a domain and zonal oriented viewpoint. Additionally, there is potential to crosscheck the NISTIR 7628 with the latest IEC Smart Grid Mapping Tool and, thus, enhancing the possibility to properly assess security standards for Smart Grids to the logical interfaces from NIST. Round-tripping between the various methodologies, tools and models will become possible. The Smart Grid Information Security (SGIS) group from the M/490 mandate currently focuses on privacy and data protection issues, therefore only complements the work done by NIST. Part of this work was a mapping of the logical interfaces and their systems from the NISTIR 7628 onto the SGAM functional plane. This implies that with the logical reference model, mapped onto the SGAM, even the logical interface categories with its *Smart Grid Cyber Security Requirements* (SG-CySecReq) can be transferred onto the SGAM model. The example, shown in this paper, will cover a part of this work. To properly use this model, the authors suggest a canonical model using five individual steps to integrate the methodology into the development to use it as security assessment, which can be seen in Section 3 of this paper. Normally, the use case itself typically covers 10-15 pages in the IEC PAS 62559 template, with an additional ten pages for the SGAM and NISTIR 7628 security analysis, so the description is limited to the very necessary aspects.

## 3. Example Use Case "Control of DER"

We assume a very simple scenario for this example that can be seen in **Fehler! Verweisquelle konnte nicht gefunden werden.**. Within a so called virtual power plant, different, mostly small *distributed energy resources (DER)* are combined to achieve a critical mass of generating capacity and, thus, to act as if they were a bigger single unit. Trading of energy at markets or providing various ancillary services is one focus of this virtual power plant (e.g. frequency control, voltage control, grid recovery or contingency planning). Based on their individual generation forecasts, *virtual power plant (VPP) operators* contract with market participants and create schedules to operate their individual units for a so-called combined product. To realize such a plan at operational level, generation and load has to be adapted to the needs of the market bid. Typically, this is done by direct control of the individual plants (*control unit for DER*) or by providing incentives to the owners to behave appropriately. In Figure 2, the communication and data exchange of the actors in this use case is displayed in a so-called UML sequence diagram that is explained in the following paragraphs.

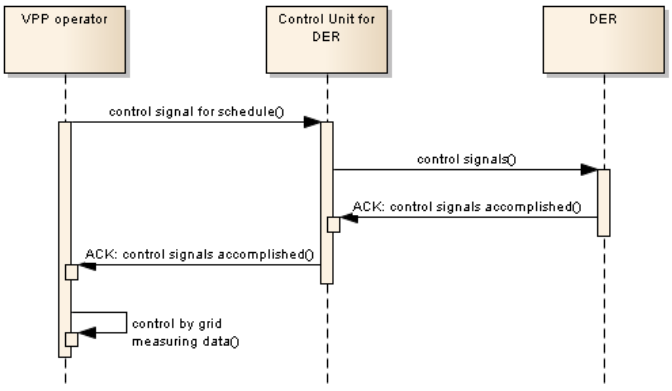


*Figure 2: Example use case sequence diagram*

Applying the aforementioned methodology, the following five steps have to be taken to assess security requirements from NISTIR 7628 to this use case.

**(1) Identifying and (formally) specifying the use case in PAS 62559 templates**

We start using the IEC PAS 62559 template and specify the use case of the former paragraph. Because of the limitation of pages in this paper the definition of the use case is here reduced to the identified actors and sequence diagram. The identified actors are: *DER, VPP operator* and *Control Unit for DER*. The sequence diagram of Figure 2 is useful to get an overview about the communication between the actors and to identify interfaces.

**(2) Identification and mapping of LI, communication links and interface categories**

The identified actors and communication links have to be mapped on the NISTIR 7628 descriptions. Figure 3 shows the scenario as a so-called high-level diagram from NISTIR 7628. The DER is a Customer DER (CDER). It is controlled via the Customer EMS and the VPP Operator gets involved in the control process via the LMS/DRMS system. The communication links, U106 and U45 from the NISTIR 7628 annex, and their corresponding interface categories, 10 and 15, are identified using the generic blueprint from the authors.

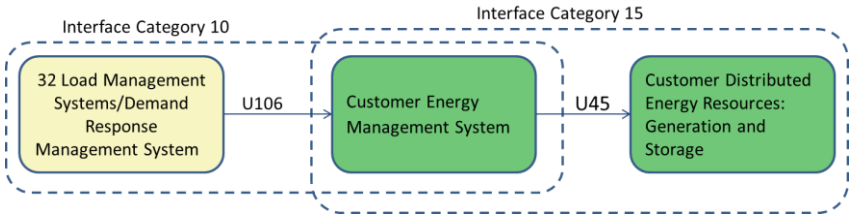


*Figure 3: Interface categories and systems*

The colours, used in Figure 3, reflect the domains of the LI diagrams. The system with number 32 LMS/DRMS (= yellow, domain operations) sends two different signals to the system number 5 Customer EMS (CEMS) (green = domain customer). After an appropriate ramp-up time the two signals, of tariffs and schedules, are submitted. If the time of the schedule is reached, real-time measurements are used to check the fulfilment. If the schedule is not satisfied, direct control, using a control signal for the Customer DER, is initialized. Once the signals are sent to the CEMS, the CEMS decides how to react, based on pre-defined and engineered rule sets, and sends control signals to the CDER. After accomplishing the tasks, first, the CDER acknowledges to the CEMS and the CEMS acknowledges to the LMS/DRMS, as can be seen in Figure 2.

**(3) Integration of the LI onto the SGAM Functional Layer**

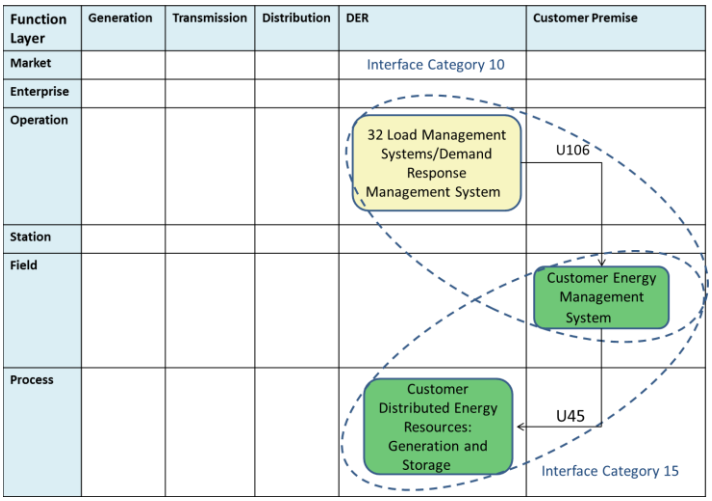


*Figure 4: Mapped actors and interfaces*

Within this step of the methodology, the mapping onto the SGAM layers is conducted. For this example, it is done in the Function Layer. Figure 4provides an overview of the mapped actors as

well as the corresponding communication links. Utilizing this kind of graphical representation makes it easier to check which domains are covered by which actors as well as to recognize the hierarchical zone they reside in.

### (4) Using the SG-CySecReq annex from NISTIR 7628

In the NISTIR 7628 the interfaces are categorized and for the different categories protection goals, like CIA analyses and high-level security requirements, are determined. Based on the previous identified interfaces and categories, Table 1 shows the corresponding SG-CySecReq and the resulting sum of these to obtain requirements for the communication from the LMS/DRMS to the CDER. In addition, security requirements from other standards can be used from the annex lookup tables of the NISTIR 7628 report, volume 1 and 3.

| **Logical Interface Category:** | **10** | **15** | **Result:** |
|---|---|---|---|
| **Confidentiality:** | Low | Low | **Low** |
| **Integrity:** | High | Medium | **High** |
| **Availability:** | Medium | Medium | **Medium** |
| **Smart Grid Cyber Security Requirements:** | AC-14 (Permitted Actions without Identification or Authentication) | AC-14 | **AC-14** |
| | IA-04 (User Identification and Authentication) | IA-04 | **IA-04** |
| | SC-05 (Denial-of-Service Protection) | SC-05 | **SC-05** |
| | SC-06 (Resource Priority) | SC-06 | **SC-06** |
| | SC-07 (Boundary Protection) | SC-07 | **SC-07** |
| | SC-08 (Communication Integrity) | SC-08 | **SC-08** |
| | SC-26 (Confidentiality of Information at Rest) | SC-26 | **SC-26** |
| | SI-07 (Software and Information Integrity) | SI-07 | **SI-07** |
| | | SC-03 (Security Function Isolation) | **SC-03** |
| | | SC-09 (Communication Confidentiality) | **SC-09** |

*Table 1: CIA and SG-CySecReq analysis for the example*

### (5) Mapping additional SGAM layers

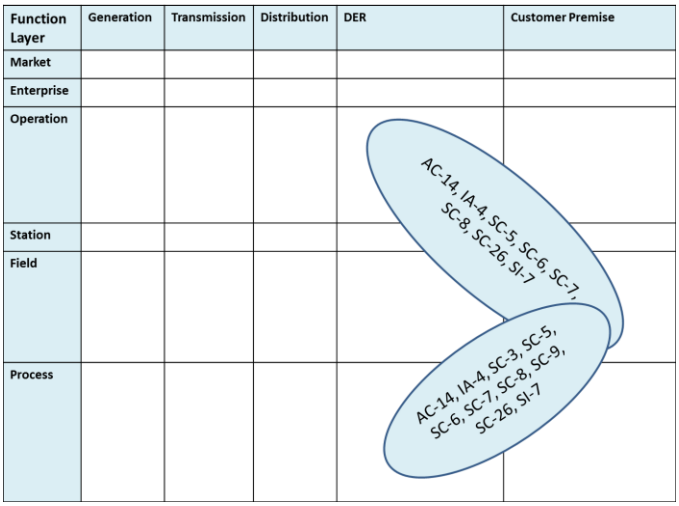


*Figure 5: NIST 7628 requirements*

In this step, the identified SG-CySecReq and their actors and communication links are mapped onto the individual further SGAM planes. Figure 5 shows where the high-level requirements are placed on the Business Layer. Figure 6 shows the corresponding SG-CySecReq, from the SG-

CySecReq classes. Additional aspects can be identified and assessed to the responsible architects for the individual layer.

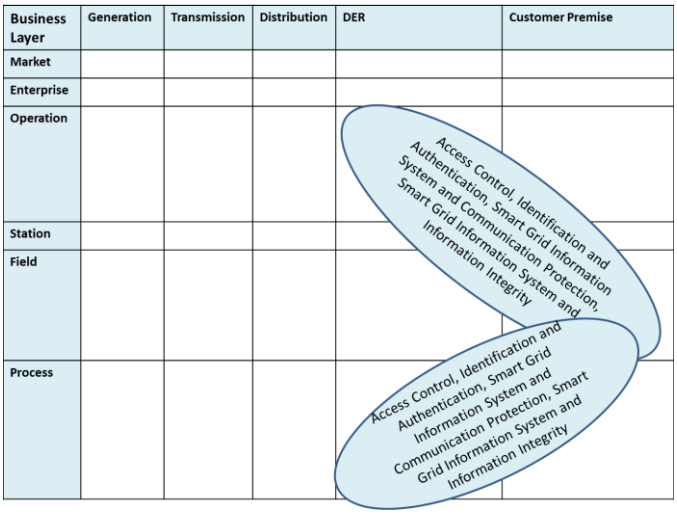


*Figure 6: high-level security requirements*

## 4. Conclusion and future work

Because of the very need of integrating security into the development process of smart grid architectures from the very beginning, the preliminary work, presented in this paper, shows a combined European and American approach, whereby the advantages of both facilitate a secure architecture development in the smart grid domain.

In the future, additional standards should be mapped to the SGAM to obtain a comprehensive model for the development of smart grid architectures.

## References

[1] The Smart Grid Interoperability Panel Cyber Security Working Group, "NISTIR 7628 - Guidelines for Smart Grid Cyber Security vol. 1-3," August 2010.

[2] Suhr, A., Rosinger, C., and H. Honecker, "System Design and Architecture Essential Functional Requirements vs. ICT Security in the energy domain," Proceedings of Internationaler ETG-Kongress 2013, 2013.

[3] Uslar, M., Schmedes, T., Lucks, A., Luhmann, T., Appelrath, H.-J., and Winkels, L., "Interaction of EMS related systems by using the CIM standard," In (Marx-Gomez, J., and Rautenstrauch, C. (Edt.)) Proceedings of the ITEE 2005, 2005.

[4] SMB Smart Grid Strategic Group (SG3), "IEC Smart Grid Standardization Roadmap," June 2010.

[5] Rohjans, S., Uslar, M., Bleiker, R., Gonzalez, J., Specht,M., Suding, T., and Weidelt, T., "Survey of smart grid standardization studies and recommendations," 2010.

[6] CEN, CENELEC, and ETSI, "Final report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids," May 2011.

[7] European Commission, "M/490 Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment," March 2011.

[8] Uslar, M., Specht, M., Dänekas, C., Trefke, J., Rohjans, S., Gonzalez, J. M., Rosinger, C., and Bleiker, R., "Standardization in Smart Grids". Berlin, Germany: Springer-Verlag, 2013.

[9] CEN, CENELEC, and ETSI, "Smart Grid Reference Architecture," November 2012.

[10] International Electrotechnical Commission (IEC), "IEC 62351 part 1 – 11, Power systems management and associated information exchange - Data and communications security," 2007 - 2013.