POSITION PAPER FOR PRETSELS WORKSHOP JRZ

Stepping up: a methodological way from security models to security maturity for Smart Grids

Mathias Uslar[*][†], Julia Masurkewitz[†], Christine Rosinger[†] and Christina Delfs[†]

[*]Correspondence: uslar@offis.de
OFFIS- Institute for Information Technology, Escherweg 2, 26121 Oldenburg, Germany
Full list of author information is available at the end of the article
[†]Equal contributor

Abstract

Within this position paper, we motivate the use of doing assessment for risk analysis for the Smart Grid infrastructure using the so called NISTIR 7628 model in the very context with the SGAM model for Smart grid reference designation. Based on this work, risk, threats and mitigation can be assessed. Still, open questions remain in terms of how mature the chosen solution actually is. Within this contribution we address this very issue by proposing to use a hybrid capability model like the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) in the very context to properly start addressing the aspect of technical as well as organizational maturity for a critical infrastructure.

Keywords: SGAM; NISTIR 7628; SGMM

1 Overview on the position paper

The main idea of this contribution is to provide the reader with an overview on needed standards for assessing maturity to OT (operational technology) smart grid technologies. As of today, the SGAM has proven to be the most feasible solution to properly model individual aspects of Smart grid solutions and technology portfolios. It allows for identifying individual parts of a solution. In addition to this building block, domain knowledge from experts to address individual risk, threats and mitigation for certain system types (different applications like DMS, EMS; SCADA, EV Charging Pole, WAMS, etc. are in scope) and their generic interfaces in a typical utility can be re-used from the NISTIR 7628 series and its three parts. It can be used for security analysis [1] and [2]. The combination of those two methods can be regarded as the state-of-the-art in conceptual modeling for security analysis for smart grid architectures and solutions. Based on this work, the authors suggest adding the aspect of maturity models from pre-conditions of levels to the individual mitigations derived from NISTIR 7628 and SGAM models visualizing those levels. The sections will briefly discuss the individual building blocks and conclude with a proposal for a combination to be discussed at the workshop.

2 The Smart Grid Architecture Model (SGAM)

In the context of the European Commission's Standardization Mandate M/490 [3, 4], 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. The SGAM comprises five so called core viewpoint layers. The domains and zones support a holistic view on architecture including business processes which are usually regarded out of scope for standardization. In the following itemization the layers of the SGAM are explained:

- The Business Layer provides a Business viewpoint focusing on strategic and tactical goals and processes as well as regulatory aspects. For standardization purposes, this layer could be considered out of scope.
- The Function Layer is an IT-oriented, technology independent description of general use cases, its functions and used services.
- The Information Layer visualizes information about data and information models to support the exchange of business objects and data models of the Function Layer to enable interface interoperability.
- The Communication Layer provides a visualization for the specification of protocols and procedures for the data exchange between components based on the Information Layer.
- The Component Layer provides a physical and technical view on Smart Grids components. Besides power-system related infrastructure and equipment, ICT-infrastructure and -systems are also considered as possible items.

In summary, individual aspects and views on Smart grid solutions can be taken into account and security solutions assessed to individual parts- these will be derived from the NIST 7628 as described in [2].

3 US NISTIR 7628

Security is not just relevant for the operation of the Smart Grid as a critical infrastructure but also very important for user acceptance and general operation procedures. This particularly affects domains 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. [5] one of particular interest is the NISTIR 7628 series [6].

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 used to identify and define 22 logical interface (LI) categories within and across seven Smart Grid domains. Further, so called high-level security requirements for each of the logical interface categories are described. The first volume concludes with a discussion of technical cryptographic and key management issues across the scope of Smart Grid systems and devices.

The second volume from NISTIR 7628 focuses on privacy issues within customer premises. It provides awareness and discussion of such topics as the evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, mostly including their behavior within their premises, and whether these new types of information may contain privacy risks and challenges that have not been legally verified yet. Additionally, this volume of the overall series provides recommendations, based on accepted privacy principles, for entities that participate within the Smart Grid. These recommendations include concerns such as having entities develop privacy use cases that track data flows containing personal information in order to address and mitigate common privacy risks that exist within business processes within the Smart Grid.

The third volume is a compilation of supporting analyses and references used to develop the high-level security requirements and other tools and resources presented within the first two volumes of the NISTIR 7628 series.

These two include categories of vulnerabilities defined by the working group and a discussion of the bottom-up security analysis that it conducted while developing the guidelines.

4 Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

The ES-C2M2 [7] was developed by the US Department of Energy and the Department of Homeland Security. The objectives of this model are defined, to promote cybersecurity capabilities by sharing knowledge and best practices and to enable the distribution system operators to plan and coordinate their actions. Therefore, the ES-C2M2 was designed as a self-evaluation model with an adequate toolkit (of course, there are ES-C2M2 facilitators, who can be booked as consultants). As other maturity models, it is designed to fit all needs of different branches regarding its specific focus. Hence, industry subsectors can interpret the model regarding their concrete needs. To ensure an adaption, the model bases on existing cybersecurity standards (like NIST 7628, ISA 99, IEC 62351) and frameworks and takes into account the work of different programs and initiatives. The model consists of ten domains, which are divided into different objectives (like approach objectives and management objectives). The approach objectives are best described as domain-specific objectives, whereas the management objectives encompass all common objectives, which are similar in the different domains. Specific practices or practices for the management are pooled in each objective. Overall, four different maturity (indicator) levels (MIL) are applied in the model. MILs always refer to the domains separately. In order to reach a level, all assigned practices of a domain must be fulfilled. If an organization has risk management MIL1 that means that all practices are at least measured MIL1. The meaning of the different levels is as follows:

- MIL0: The practice does not reach MIL1.
- MIL1: It contains initial practices mostly on a case-by-case basis, depending on the skills and experiences of the acting person. Organizational guidance is not assumed.
- MIL2: Initial level of institutionalization of practices. The practices have to be performed according to a documented plan and all relevant stakeholders are identified and involved in the practices. Additionally, all necessary resources are provided. That includes that relevant standards or guidelines have been identified and implemented.
- MIL3: The institutionalization of the practices is further evolved and they are now being managed. The single practices are guided by ‘policies’ (including standards and guidelines). The employees and authority have each their responsibilities.

In practice, every organization should define a target MIL for each domain to best improve the actual state of the organization. In general, the achieved MILs, the business strategy and the cyber-security strategy of the organization should be harmonized. Thus, it is neither necessary nor useful always to achieve the highest MIL. The recommended process for applying the ES-C2M2 is structured into four steps (it is assumed that all preparations to use the model have already been conducted).

5 Conclusion of the position paper

5.1 Example: Use Case Scenario "Control of decentralized power plants"

We assume a simple scenario. Within a so called virtual power plant, different, mostly small distributed energy resources (DER) are combined to achieve a critical mass of generation 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 other market participants and create a schedule 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 or by providing incentives to the owners to behave appropriately. Applying the aforementioned methods, the following steps have to be taken to assess security requirements from NISTIR 7628 to this use case.

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

We start using the basic description from the previous paragraph as use case specification. The identified actors are: DER, VPP operator and Control Unit for DER. Additionally, at this step a sequence diagram is normally useful to get an overview about the communication between the actors and identify interfaces. Please refer to [2] for a more detailed description on this case.

5.3 Identification and mapping of LI, communication links and interface categories

The identified actors and communication links have to be mapped in the NISTIR 7628 descriptions. The DER is a Customer DER (CDER) in the very NISTIR system classes sense, is is usually controlled via the Customer EMS and the VPP operator gets involved in the control process using 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. The colors reflect the domains as in the LI diagrams. For the communication and interfaces, this means the following: The system with number 32 LMS/DRMS (Domain Operations) sends two different signals to the system No. 5 Customer EMS (CEMS) (Domain Customer). Then, appropriate ramp-up time, tariffs and schedules are submitted. If the time being for the schedule is reached, real-time measurements are used to check if the schedule is fulfilled and how it is met if there are changes in operation. If this is not the case, direct control using a control signal for the individual DER is initialized. Both signals are sent to the CEMS. The CEMS decides how to react based on predefined and engineered rule sets and sends control signals to the Customer DER. CDER can be mainly generators like Micro CHP, fuel cells, or battery storage.

LI	C	I	A	Smart Grid Cyber Security Requirements
10	Low	High	Medium	AC-14, IA-04, SC-05, SC-06, SC-07, SC-08, SC-26, SI-07
15	Low	Medium	Medium	AC-14, IA-04, SC-03, SC-05, SC-06, SC-07, SC-08, SC-09, SC-26, SI-07
Result	**Low**	**High**	**Medium**	**AC-14, IA-04, SC-03, SC-05, SC-06, SC-07, SC-08, SC-09, SC-26, SI-07**

Table 1 CIA Analysis for SG-CySecReq

5.4 Integration of the LI onto the SGAM Functional layer

Within this step of the methodology, the mapping onto the SGAM layers is conducted. For this example, it is done at functional level. Figure 1 provides an overview of the mapped actors as well as the corresponding communication links. Utilizing this kind of graphical representation makes it is easier to check which domains are covered by which actors as well as to recognize the hierarchical zone they reside in. The next step for the security analysis consists of using the SG-CySecReq for assessing the protection goals as CIA analysis for the use case as well as the individual high-level requirements. Based on the identified interfaces, the requirements are given in Table 1. In addition, security requirements from other standards can be used from the annex lookup tables of the NISTIR 7628 report. The individual high-level requirements are the very basis to integrate the new concept of the maturity model.

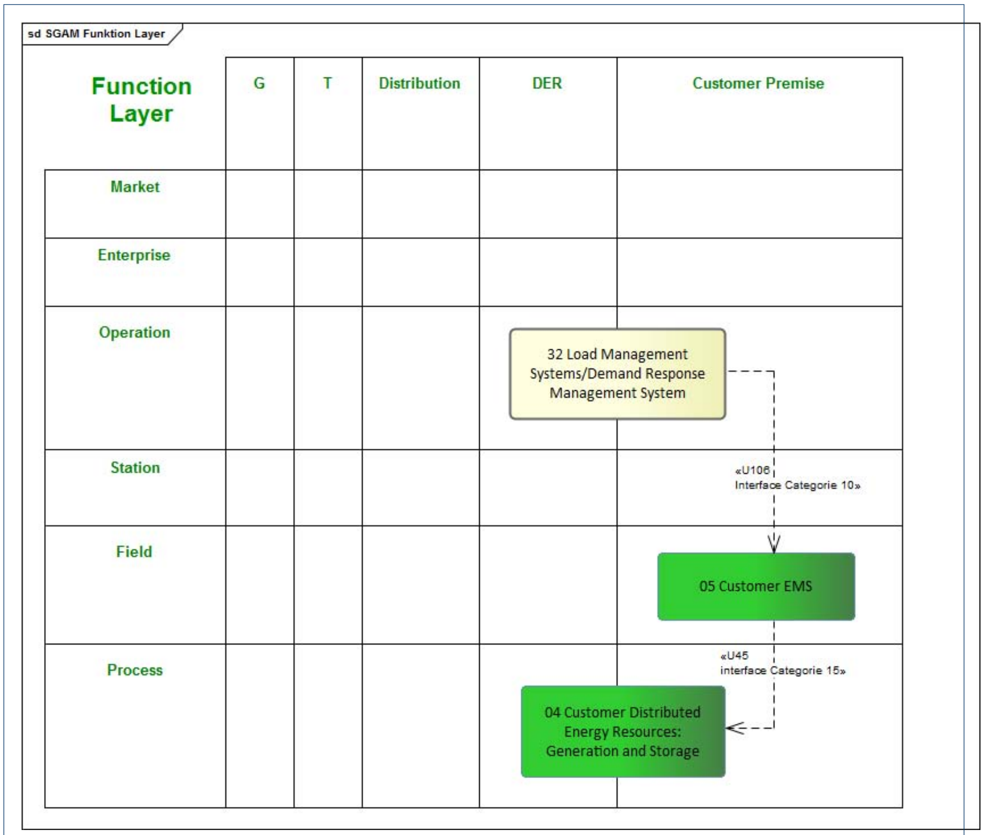
sd SGAM Funktion Layer
Function Layer
G
T
Distribution
DER
Customer Premise
Market
Enterprise
Operation
Station
Field
Process
32 Load Management Systems/Demand Response Management System
«U106 Interface Categorie 10»
05 Customer EMS
«U45 interface Categorie 15»
04 Customer Distributed Energy Resources: Generation and Storage

Figure 1 SGAM Mapping of the Interfaces

To properly align the state-of-the-art with the new concepts developed in the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), it is necessary to look at the individual systems addressed in the ten domains of the ES-C2M2, provide and analysis on the individual cyber-security requirements. In Table 1, individual aspects like AC-14 (Permitted Actions without Identification or Authentication) can be mapped onto the ten individual domains from the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) based on the work to be presented in the workshop. Within the work conducted in the context of the FP7 ELECTRA project, all of the more than 190 SG-CySecReq have been classified for both the ES-C2M2 domains as well as the individual levels. Based on the domains, the sub-objectives have detailed maturity levels defined. The CySecReqs have been mapped onto the maturity with their individual objectives levels. According to the SGIP, there is a defined process to assess the CySecReqs to individual solutions. Based on this, solutions shall be assessed for. In addition to the common pareto-principle security analysis assessment for a smart grid solution, the proposed look-up for combining the three methods leads to an maturity assessment for the solution and, by combining the results from multiple solutions, a maturity assessment for the organization itself is created. The next step to come up with a meaningful dashboard solution for a smart grid has to cover the aspect of the dependencies between the individual smart grid technologies building upon each other. Based on those technical dependencies, migration strategies can be developed which can also cover in-depth the aspect of security maturity. This work will be presented as an outlook at the workshop discussions.

Acknowledgements
The authors would like to thank their colleagues from the projects In2VPP, GreenAccess and ELECTRA for their input to this work.

References

1. Neureiter, C., Eibl, G., Engel, D., Schlegel, S., Uslar, M.: A concept for engineering smart grid security requirements based on SGAM models. Computer Science - Research and Development, 1–7 (2014). doi:10.1007/s00450-014-0288-2
2. Uslar, M., Rosinger, C., Schlegel, S.: Security by design for the smart grid: Combining the sgam and nistir 7628. In: Computer Software and Applications Conference Workshops (COMPSACW), 2014 IEEE 38th International, pp. 110–115 (2014). doi:10.1109/COMPSACW.2014.23
3. European Commission: M/490 Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment (2011)
4. Uslar, M., Specht, M., Dänekas, C., Trefke, J., Rohjans, S., González, J.M., Rosinger, C., Bleiker, R.: Standardization in Smart Grids. Springer, Berlin, Germany (2013)
5. International Electrotechnical Commission (IEC): IEC 62351 part 1 – 11, Power systems management and associated information exchange - Data and communications security (2007 - 2013)
6. The Smart Grid Interoperability Panel Cyber Security Working Group: NISTIR 7628 - Guidelines for Smart Grid Cyber Security vol. 1-3 (2010)
7. DoE: Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) (2013)