Methodical Reference Architecture Development Progress

Beneficial Implications Developing a Secure Reference Architecture for Future Smart Grid Solutions in Austria

Marcus Meisel · Stefan Wilker · Joachim Fabini · Robert Annessi · Tanja Zseby · Markus Müllner · Wolfgang Kastner · Markus Litzlbauer · Wolfgang Gawlik · Christian Neureiter

Abstract – The *Reference Architecture for Secure Smartgrids Austria* (RASSA) project aims at developing a secure, interoperable reference architecture for Austrian smart grids. Building on the strength of the project's consortium, this architecture is being specified in close coordination with all relevant stakeholders in Austria. By instantiating parts of the reference architecture, secure, and compatible smart grid components can be implemented in a consistent and efficient way. This paper shows the progress of this effort and illustrates methodical consequential benefits, as well as the potential to integrate reactive and active security attributes into the reference architecture.

1. Motivation

A broad agreement of the energy sector concerning next steps for evolving the electrical grid into a smart grid, was a motivating starting point for developing a secure reference architecture for future smart grid applications in Austria. Triggered by the *Technology Roadmap for Smart Grids* [1], one of the most pressing concerns addresses the development of an overall ICT architecture for smart grids. These findings are the basis of the current development of the Austrian reference architecture. A first outlook on the attributes of the reference architecture, based on finding of the RASSA stakeholder process project was presented in [2].
In [3], the authors describe in detail for the first time a complete big-picture of the topic smart grid architecture modeling. This paper is describing the progress of the first steps implementing the described recipes.

M. Meisel · S. Wilker · J. Fabini · R. Annessi · T. Zseby · M. Müllner · W. Kastner · M. Litzlbauer · W. Gawlik
TU Wien, Gußhausstraße 27-29, 1040 Wien, Austria
marcus.meisel@tuwien.ac.at

Christian Neureiter
FH Salzburg, Urstein Süd 1, 5412 Puch/Salzburg, Austria
christian.neureiter@en-trust.at

2. Traceability in Modeling

Modelling RASSA with the freely available SGAM-Toolbox (www.en-trust.at/SGAM-Toolbox), a clear and traceable interconnection between RASSA, Österreichs Energien Domänenmodell.AT [4], and NIST Logical Reference Model (LRM) [5] has to be deposited in the model. In a fast-paced developing environment such as the smart grid, traceability is a cornerstone of RASSA since the changing security requirements, adding smart components, new market players, or the integration communication technology to previously "blind" components are not just happening once but constantly. A reference architecture has to be able to allow these changes and additions with minimal effort for the involved stakeholders.

2.1 Modeling Implications

The SGAM-Toolbox allows to satisfy the need to adapt the whole reference architecture to core changes, reflecting national or international development decisions, as well as allowing RASSA users inside the SGAM-Toolbox to model, using existing components and their predefined interfaces. As shown by one example component in Fig. 1, components in the original appearance of the NIST LRM Distributed Energy Resources (DER)-actor are visible in the upper part in the green box of NIST LRM. Due to the fact, that the Domänenmodell.AT model did not change the role of actors but adapted the naming of the components to match Austrian needs, the name of the component changed in the model. To visually distinguish the components, the Österreichs Energie (OE) logo was placed on the upper right corner of the DER-actor, as can be seen in the

light-red box. The RASSA role actor of "Erzeugung und Speicherung von Energie auf Kundenseite" was defined as a physical component during splitting of the NIST-LRM. A new visual representation is introduced, by having a cube as physical object with the RASSA logo on the upper right, to also provide a visual distinction for the actor role not to be mistaken as a DER-actor from either NIST-LRM or OE.

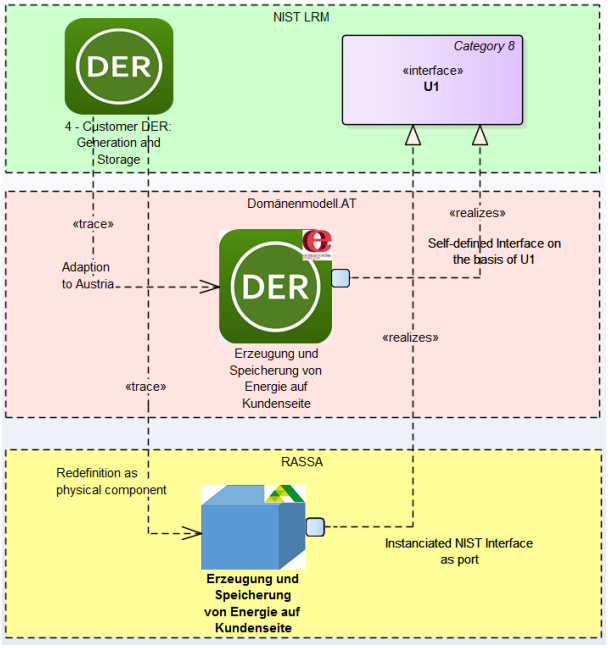

Fig. 1 Traceability of NIST-LRM, Domänenmodell.AT and RASSA in SGAM-Toolbox, own representation

2.2 Tracing Interfaces inheriting Security Requirements

The interface `U1` component in Fig. 1, placed in the NIST LRM box, is used by the `<<realizes>>` relationship in Domänenmodell.AT as well as by the RASSA model. This depiction emphasizes the benefit of reusing already existing knowledge, as well as the capability of the SGAM-Toolbox to include proven concepts from other sources, such as reactive security supervision methods for interfaces, possible attack vectors for interfaces, or active security threat analysis results for generic or instantiated specific components.

3. Modeling Progress

For exploring possible risks, it is necessary to describe (high level) use cases in detail. The SGAM-Toolbox already offers its ability to generate UML activity and sequence diagrams, linked to pre-existing RASSA/OE/NIST components in the model, merely through inserting their exact names in a sentence describing a behavior or a necessary action. For example, "`DSO` sends meter data request to `Smart Meter`" and "`Smart Meter` replies sending requested meter data to `DSO`" using `RASSA-Netzbetreiber` instead of `DSO` defines to inherit all interfaces of the differently modeled actor/component/entity that can be different from the NIST or OE one.

Working through use cases with stake holders or experts step by step, identifying involved services and components, can reveal potential errors in course of actions and are planned further steps in the modelling phase. Herewith, RASSA is attempting to set a state of the art description of a growing list of use cases relevant for critical infrastructures such as for smart grids in Austria.

Fig. 2 shows an automatically generated sequence diagram of five exemplary chosen use cases modelled by the SGAM-Toolbox. This is the most basic architecture view of any smart grid application, where one actor is connected to one final device, disregarding all intermediary connections and steps necessary in between.

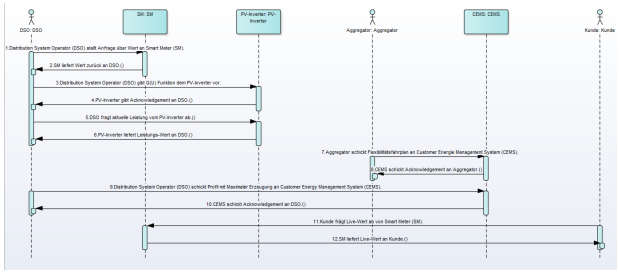

Fig. 2 First five basic system architecture representing Use-Cases modeled in SGAM-Toolbox, own representation

From this input, the SGAM-Toolbox will be further enabled to automatically generate all intermediary components and connections, suggesting all possible protocol or device instantiations, and exporting a complete system model specification within the existing electrical grid.

3.1 Patterns automating modeling

Patterns allow modeling engineers to automate a tedious manual process. A cyber-physical system such as the smart grid and future applications being modelled with RASSA is prone to human error if security-by-design stops at creating the model and does not consider the modeling process. SGAM-Toolbox assists the RASSA architecture modeling by offering the patterns for:

- communication security requirements
- network security requirements
- system security requirements

These patterns are the first attempt to increase security-by-design during the modeling phase.

3.2 Machine Readable Descriptions

Another benefit of using SGAM-Toolbox as modeling infrastructure for a reference architecture is its capability

to export a designed model as machine readable XML files. These files allow specialized software tools to provide additional functionalities such as risk management, using the descriptions provided within the components, connections, or actors.
Detailed descriptions (additionally to their position in the different SGAM layers) can include:

- complexity of the component
- status (approved, implemented, mandatory, proposed, validated)
- requirement specifications with status, difficulty, priority, and stability
- constraints like pre- or post-condition
- relation to risk analysis

The risk analysis schema allows comparison throughout various devices, interfaces, or services co-existing in a modeled smart grid application. For example, a resulting calculated higher estimated "Calculated Risk" value, aggregated over all the used components of the modelled smart grid application suggests, that more effort should be made to counter the possible risks.
To provide a set of risk and security attributes to entities being modelled is one of the benefits the reference architecture provides.

4. Security Attributes

The RASSA project investigates the use of reactive and active security for the detection of attacks on the smart grids.

4.1 Reactive Security in Smart Grids

One very challenging field is the detection and mitigation of data integrity attacks in wide area monitoring protection and control (WAMPAC) applications. Sensors supervise the power grid and their data can be used as input to control decisions. Any tampering with the input data can lead to wrong decisions with potentially critical effects on the power grid.
Classical WAMPAC structures consist of many different elements with different security levels. Sensors in the field (e.g., distributed phasor measurement units) are usually less protected and easier accessible than devices in the control center. Sensor also have to be cost efficient and therefore often do not provide sophisticated security measures.
A takeover of the control center provides the highest value for an attacker but may be hard to achieve. On the other hand, access to sensors in the field may be much easier and can provide a way to influence control decisions. Possibilities to influence higher level control elements depend on the structure of power grids and on ICT infrastructure. The impact of different grid structures to the distribution of malware is discussed in [6]
Other relevant element in WAMPAC structures are data aggregation points (e.g., phasor data concentrators) or classical ICT elements on the path (routers, middle boxes). Gaining access to those allows tampering with multiple sensor data flows.
Several methods have been already proposed to mitigate data integrity attacks in wide area monitoring. One possibility is checking sensor data for consistency with other types of sensor data or data from other locations. Based on static/dynamic state estimation, larger deviations can be identified. But it is difficult to detect small, slow changes (e.g., stealthy techniques by sophisticated attackers) and to detect deviations if multiple devices are compromised or attackers collude. Other possibilities are to secure the aggregation process to prevent any changes during aggregation. One example is to use homomorphic encryption to prevent aggregation devices needing access to cryptographic keys. A third method uses anomaly detection to notice unusual network behavior during an attack or attack preparation. With this it is also possible to detect new previously unknown attacks (e.g., due to zero-day exploits). An overview of potential attack vectors for wide area monitoring structures and on currently proposed mitigation strategies is provided in [7].
Currently protocols used for grid control are under investigation and further supervision methods for the WAMPAC communication network are being researched.

4.2 Active Security in Smart Grids

Currently threat modeling approaches connected to the first RASSA use cases are being evaluated. To base later security tests with real products on established standards, security auditing requirements have been defined, based on ISO/IEC 1508 (Common Criteria). The possible analysis methods range from general (high level analysis, attacker classification, low level analysis) such as passive sniffing of protocols and data or active port scan, replay attacks, or fuzz testing, up to advanced analysis techniques such as:

- probing
- side-channel attacks (e.g., power analysis)
- fault injection (e.g., voltage glitching)
- analysis of integrated circuits (e.g., decapsulation, delayering/deprocessing, microscope imaging, reverse engineering)

5. Summary and Outlook

This paper described the work in progress concerning the modeling of the RASSA system architecture based on the SGAM-Toolbox, taking into account potential security attributes for reactive and active security investigations.
Next steps will be to include the ENTSO-E market role model as potential business actors, matching e-control actors in the reference architecture, increasing the modelled components of the current energy system, and linking existing interfaces to all models to serve as a blueprint for stakeholders to model their new smart grid applications compatible to existing infrastructure, while relying on interface-wise defined requirements on all reference architecture components to provide security.

Acknowledgements

Findings presented are from project *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 (TPSGA): Technologieroadmap Smart Grids Austria - Die Umsetzungsschritte zum Wandel des Stromsystems bis 2020. Technical report, Technologieplattform Smart Grids Austria (April 2015), http://www.smartgrids.at/files/smartgrids/Dateien/Dokumente/05%20Roadmap_Management_Englisch.pdf
2. Meisel, M., Berger, A., Langer, L., Litzlbauer, M., Kienesberger, G.: The RASSA Initiative – Defining a Reference Architecture for Secure Smart Grids in Austria, Lecture Notes in Computer Science, vol. 9424, pp. 51–58. Springer International Publishing (2015), http://dx.doi.org/10.1007/978-3-319-25876-8_5
3. Neureiter, C., Engel, D., & Uslar, M. 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, S. 24.
4. E-Control, Oesterreichs Energie, Austrian Power Grid, Bundeskanzleramt, Bundesministerien (BMWFW, BMI, BMLVS), Kuratorium Sicheres Österreich, REPUCO Unternehmensberatung GMBH „RISIKOANALYSE FÜR DIE INFORMATIONSSYSTEME DER ELEKTRIZITÄTSWIRTSCHAFT unter besonderer Berücksichtigung von Smart-Metern und des Datenschutzes.“ *e-control.at.* 27.02.2014 (accessed: 9.09.2016) http://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7.
5. NIST - National Institute of Standards and Technology. 2010. Guidelines for Smart Grid Cyber Security: Vol. 1-3, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, Release 3.0. Technical Report, Gaithersburg, MD: NIST, 668.
6. P. Eder-Neuhauser, T. Zseby, J. Fabini: "*Resilience and Security: A Qualitative Survey of Urban Smart Grid Architectures*"; IEEE Access, **4** (2016), 839 – 848.
7. S. Paudel, P. Smith, T. Zseby: "*Data Integrity Attacks in Smart Grid Wide Area Monitoring*"; 4th International Symposium for ICS & SCADA Cyber Security Research 2016, Belfast, UK, August 2016.

Marcus Meisel, MSc. BSc. since 2007 is researching the Smart Grid domain in the Energy&IT Group at the Institute of Computer Technology at the TU Wien. His current projects additional to *RASSA* are *Spin.OFF*, applying neural networks to predict electrical loads and environmental data to optimize use of battery storages within buildings, and *iniGrid*, developing a secure automation network architecture for acting and sensing smart grid component prototypes.