Reference Architecture as Foundation for Risk and Threat Analysis

Marcus Meisel · Stefan Wilker · Markus Kammerstetter · Markus Müllner · Dominik Fasthuber · Wolfgang Kastner · Wolfgang Gawlik

Abstract – The project "*Reference Architecture for Secure Smart Grids Austria"* (RASSA) is developing a foundation for secure, interoperable architecture components dedicated for future smart grids in Austria. A key feature of this blueprint is its tool supported model driven design approach, enabling users to estimate the risk of components introduced into the models as a decision base for a deeper threat analysis. The design of this architecture is carried out in close coordination with all relevant stakeholders from Austria through an established stakeholder process supported by "*Technologieplattform Smart Grids Austria"* (TPSGA). During the RASSA-architecture project, parts of the reference architecture will be instantiated to validate relevant smart grid components. This paper shows the progress of this undertaking and illustrates the potential of integrating reactive and active security attributes within a reference architecture.

1. Motivation

One of the urgent needs in the *Technology Roadmap for Smart Grids* [1] is the development of an overall ICT architecture driving the development of an Austrian reference architecture. Its model driven design approach is described in [2] and allows attributes of a multitude of extendible sources, first presented in [3], to create a solid foundation for automated risk and threat analysis.

2. Modeling Progress

As shown in Fig. 1, a preliminary model of an Austrian harmonized market role model was created, based on the *entso-e* market role model [4]. To shift the model based (document-) approach to a model driven approach it was decided to use and eventually extend the *SGAM-Toolbox*[1] (see Fig. 2).

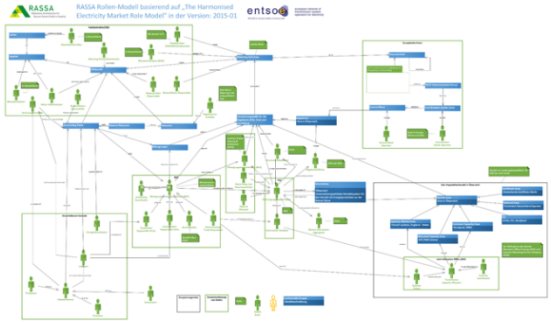

Fig. 1 entso-e market role model for Austria overview

[1] SGAM-Toolbox https://www.en-trust.at/downloads/sgam-toolbox/ (accessed: 27.01.2017), a Sparx Systems Enterprise Architect Plugin

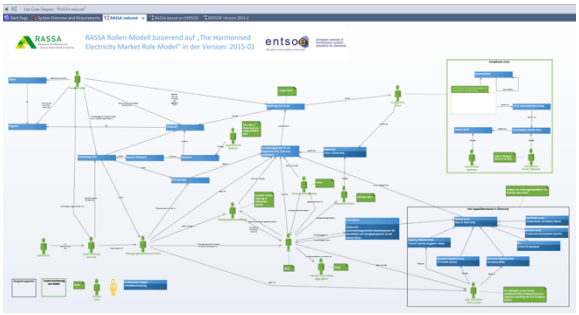

Fig. 2 entso-e market role model for Austria modelled in SGAM-Toolbox compact

2.1 Integrating entso-e Market Role Model

The modeled version allows to reduce complexity for users, since actors assuming multiple roles in Austria can be displayed as one actor, while their linked roles are still modelled separately. Fig. 3 shows a detailed view of multiple roles of one actor, including their respective links to the original modelled *entso-e* actors of a particular *entso-e* version. Users can decide which actor and role they want to model within their business case, inheriting all provided, possibly varying security requirements, threats, and risks. Including the *entso-e* market role model allows to identify business actors that are matching nationally to e-control actors [5], as well as internationally to actors inside the *NIST-LRM* as described in [2]. Within the *SGAM-Toolbox* this increases the modelled components of the current energy system, and links existing interfaces to all models to serve as a blueprint for stakeholders to model new smart grid services, applications, and components, compatible with an existing infrastructure. The interface-based approach taken inside the *SGAM-Toolbox* is additionally providing defined requirements on all reference architecture components, enabling automated risk estimation on a system level.

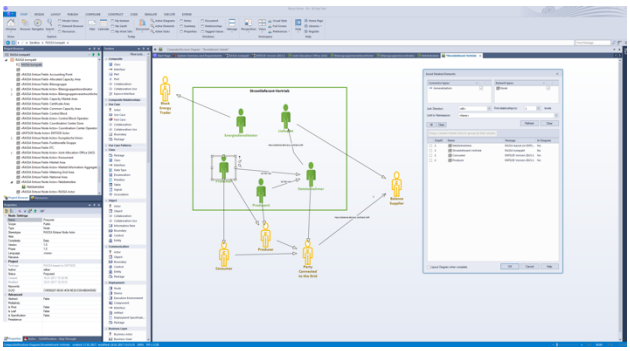

Fig. 3 Detail of SGAM-Toolbox modelled entso-e market role model for Austria, linked with modelled original entso-e

2.2 Integrating Importance, Risk, Threats

Technical security audits are an important tool for companies to harden their devices and systems in the field. This is especially true for systems and devices in a critical infrastructure such as the smart grid. It is expensive and time consuming to thoroughly audit devices or systems even on a surface level, whereas technology to hack for example wireless communication is cheap and readily available. Automated analysis of models estimating risks and threats allows users of the reference architecture to identify hotspots of a smart grid component within a complete system architecture. The foundation enabling this automated analysis is a multitude of security survey results [6], risk and catalogues of measures such as [7], component or protocol relevant attacks [8], active and reactive, as well as threats [9]. Just as measures and security risks weights for different roles can be added, based on surveys done in RASSA-architecture, to finally calculate security metrics. In Fig. 4, some of the parameters (weights) are exemplary illustrated in one of the physical components and protocols.

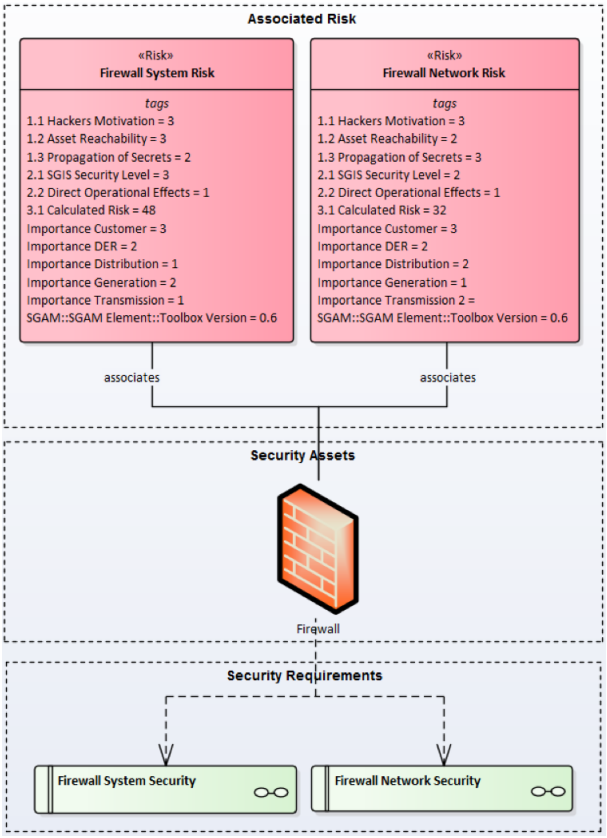

Fig. 4 Associated Risks and importance parameters modelled in SGAM-Toolbox, used for automated risk evaluation

This way, users of the reference architecture model are supported to evaluate newly introduced components, protocols, actors or connections within a complex infrastructure of many different networked devices.

3. Summary and Outlook

This paper presents risk and threat analysis relevant parts of the ongoing research of the project RASSA-architecture. As part of the project, first steps in modeling international reference architecture frameworks, such as the *entso-e* market role model have already been addressed and the extendibility of the used framework inside the *SGAM-Toolbox* shown.

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. 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.
3. 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
4. entso-e – THE HARMONISED ELECTRICITY MARKET ROLE MODEL entso-e Version 2015-01, 2015, Entso-E, 33 p. (accessed: 27.01.2017) https://www.entsoe.eu/Documents/EDI/Library/HRM/2015-September-Harmonised-role-model-2015-01.pdf
5. 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: 27.01.2017) http://www.e-control.at/documents/20903/-/-/3f89d470-7d5e-433c-b307-a6443692d8f7.
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. L. Langer, J. Göllner, M. Tischlinger, M. Kammerstetter et al. (Hrg.): "Smart Grid Security Guidance - (SG)²: Sicherheitsmaßnahmen für Stromnetzbetreiber in Österreich"; Schriftenreihe der Landesverteidigungsakademie, Wien, 2016, ISBN: 978-3-902944-98-6; 253 S.
8. 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.
9. M. Kammerstetter, L. Langer, F. Skopik, W. Kastner: "Architecture-driven smart grid security management"; Vortrag: 2nd ACM workshop on Information hiding and multimedia security, Salzburg; 11.06.2014 - 14.06.2014; in: "2nd ACM workshop on Information hiding and multimedia security", (2014), ISBN: 978-1-4503-2647-6; S. 153 - 158.