RASSA Reference Architecture for Secure Smart Grids in Austria

Marcus Meisel, marcus.meisel@tuwien.ac.at
Stefan Wilker, stefan.wilker@tuwien.ac.at
Joachim Fabini, joachim.fabini@tuwien.ac.at
Robert Annessi, robert.annessi@tuwien.ac.at
Tanja Zseby, tanja.zseby@tuwien.ac.at
Markus Müllner, mmuellner@auto.tuwien.ac.at
Wolfgang Kastner, wolfgang.kastner@tuwien.ac.at
Markus Litzlbauer, markus.litzlbauer@tuwien.ac.at
Wolfgang Gawlik, wolfgang.gawlik@tuwien.ac.at
Christian Neureiter, christian.neureiter@en-trust.at

Methodical Reference Architecture Development Progress

Introduction

The *Reference Architecture for Secure Smart Grids in 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 poster 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.

Methods

Modeling in SGAM-Toolbox (www.en-trust.at/SGAM-Toolbox)

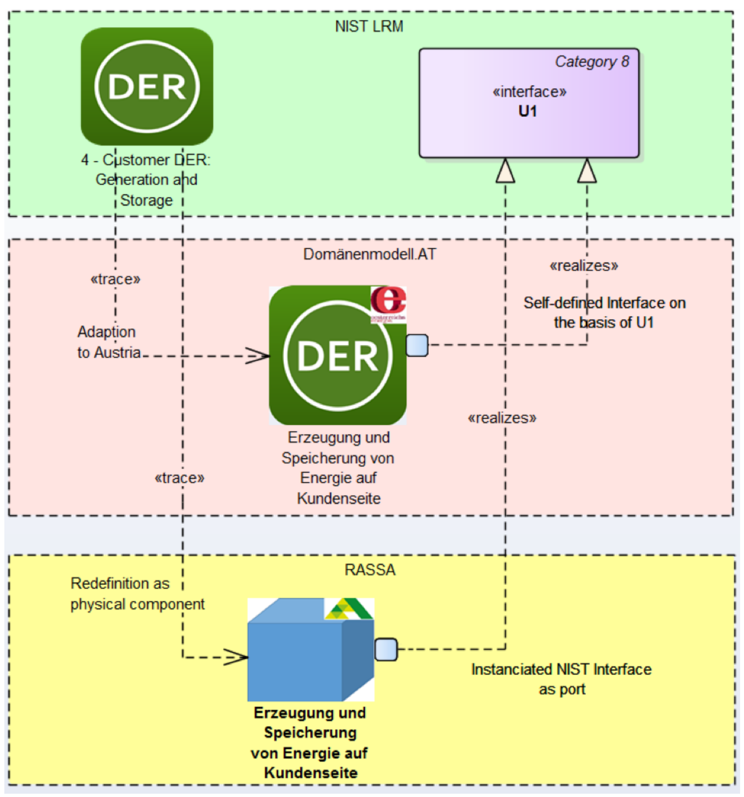

Fig. 1 Traceability of NIST-LRM, Domänenmodell.AT and RASSA in SGAM-Toolbox

Traceable interconnection:
- RASSA
- *Österreichs Energien (OE) Domänenmodell.AT* [1]
- *NIST Logical Reference Model* (LRM) [2]

Prioritization:
- generic basic use cases
- testing toolbox as documentation method
- extensive use cases (e.g., Smart Metering)

Risk Attributes:
- SGAM layer position
- complexity of component
- status of specification (e.g., difficulty, priority, stability)
- constraints (pre- or post-condition)
- risk analysis (e.g., importance)

Reactive Security:
- traffic observation (observation points, filter/sampling strategies)
- signature detection (machine learning, statistics)
- anomaly detection

Active Security:
- sniffing, port scan, replay attacks, fuzz testing
- side-channel attacks (e.g., power analysis)
- probing, fault injection (e.g, voltage glitching)
- analysis of integrated circuits (e.g., decapsulation, delayering/deprocessing, microscope imaging, reverse engineering)

Results

SGAM-Toolbox can generate UML activity and sequence diagrams, linked to pre-existing RASSA/OE/NIST components in the reference architecture model, by using exact names in a sentence describing a behavior or a necessary action: "`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 entity, different from the NIST or OE one, but all are interlinked and can inherit/realize/trace security requirements and attributes.

Fig. 2 is an automatically generated sequence diagram of the most basic architecture view of any smart grid application. One actor is connected to one final device, disregarding all intermediary connections and steps necessary in between.

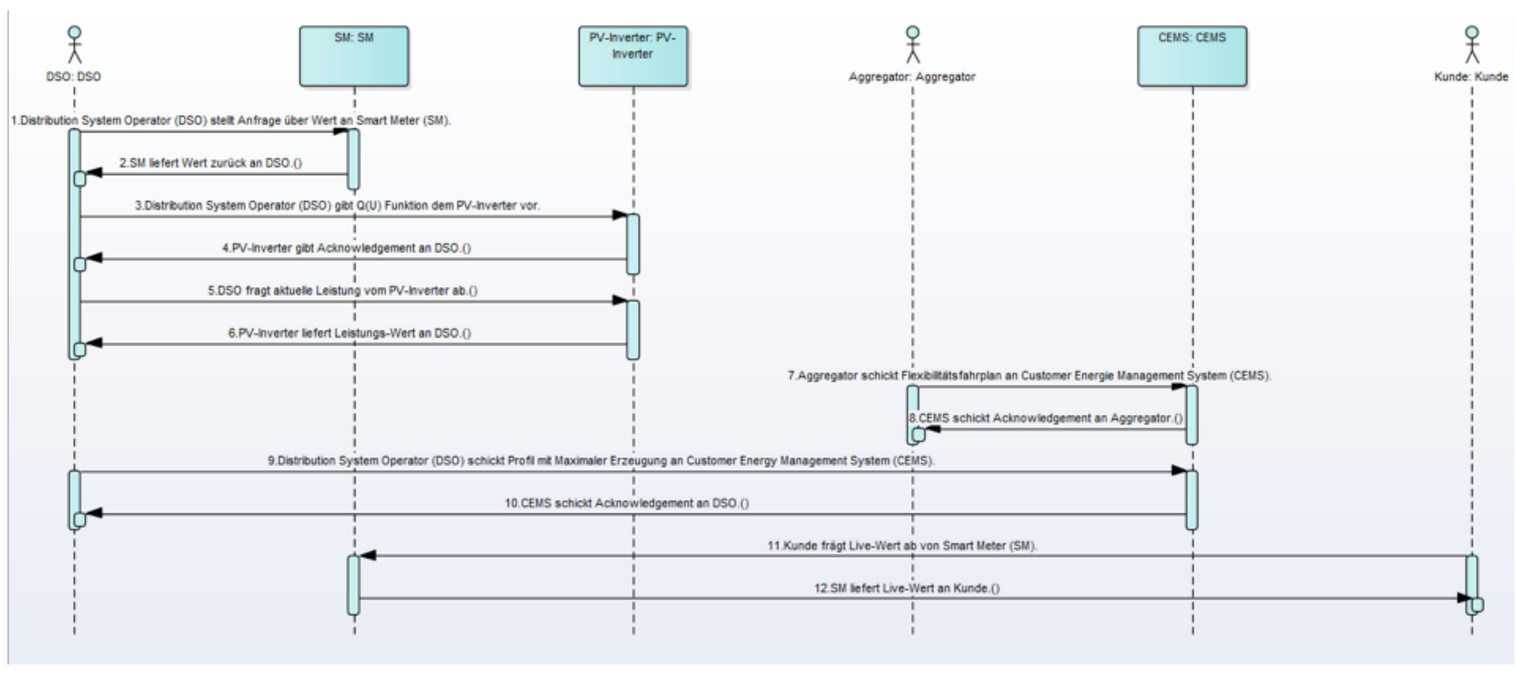

Fig. 2 First five basic system architecture representing use cases modeled in SGAM-Toolbox

Conclusion

Modeling of the RASSA system architecture ist a work in progress. Taking into account potential security attributes for reactive and active security investigations is the next step. Following steps are:
- including interconnection of ENTSO-E market role model
- adding active and reactive security attributes
- evaluating and setting attributes with stakeholders

[1] 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.
[2] 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.

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*.