Smart Grid Security Analysis: The (SG)² Approach

L. Langer, M. Kammerstetter, F. Skopik, T. Hecht, and P. Smith

(SG)² Smart Grid Security Guidance

AUSTRIAN INSTITUTE OF TECHNOLOGY

Introduction

Future energy grids will make extensive use of the integration of ICT technologies. Thus, cybersecurity risks become a threat even for energy suppliers. Numerous security issues are completely unsolved today, because these special environments require novel security mechanisms and processes.

The aim of the Austrian (SG)² project is to perform a systematic study of ICT security issues in smart grid technologies, and to define suitable countermeasures. Based on a comprehensive risk assessment of the national power grid's ICT architecture and a thorough security analysis of available smart grid components, (SG)² explores security measures that can support power grid operators in securing the ICT systems deployed in future power grids.

The (SG)² consortium consists of experts with ICT security and energy systems knowledge, coming from leading national distribution grid operators (DSOs), equipment manufacturers, research organisations, and national authorities. As such, the practical applicability and scientific dissemination of the project results is ensured.

ENERGIE AG Data · IKB Innsbrucker Kommunalbetriebe · ENERGIE INSTITUT an der Johannes Kepler Universität Linz · LINZ AG STROM · SIEMENS · BM.I · SEC Consult · TU WIEN · bmlvs.gv.at

ICT Architecture of Austrian Smart Grids

In order to define a national ICT architecture for smart grids, we surveyed the ICT architectures of past and ongoing smart grid pilot projects and model regions in Austria. Overall, 45 different national projects were identified and prioritised according to size and relevance, out of which seven were selected for a closer review and mapped to the **Smart Grid Architecture Model (SGAM)** [1]. In addition, the participating DSOs were asked to map their local smart grid systems and foreseeable developments to SGAM.

The resulting architecture sketches were combined into a **holistic ICT architecture model for Austrian smart grids**, which reflects the current power grid ICT technology, as well as its short- to mid-term extension towards future smart grid functionalities (see Fig. 1). The (SG)² architecture model serves as an anchor point for further analysis, and as a common document of energy, IT, and security experts.

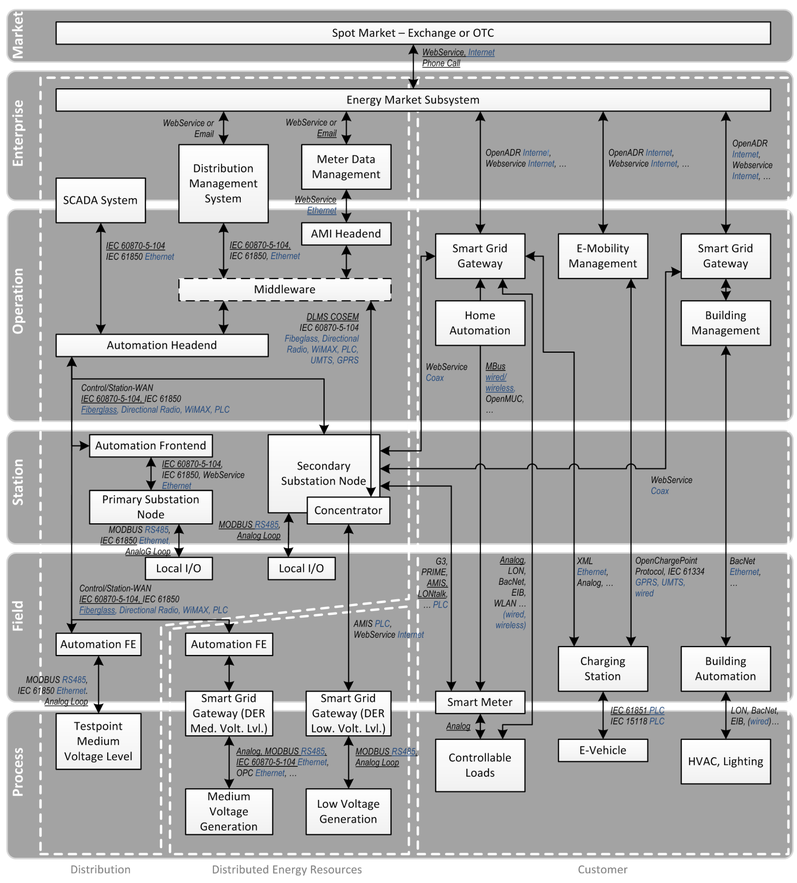

Fig. 1: (SG)² architecture model

Risk Assessment Methodology

To allow for a comprehensive smart grid risk assessment, a catalogue of relevant cybersecurity threats was defined, taking into account existing works by BSI and ENISA [2,3,4]. The relevance of each threat to each cluster of architecture components (see blue boxes in Fig. 2) was then assessed by developing possible attack scenarios, resulting in a **threat matrix**.

Next, the risk was assessed for each element of the threat matrix by estimating probability and impact, following a semi-quantitative approach. The probability was expressed by the number of cybersecurity incidents p.a., while the impact of a successful attack was determined by monetary loss, customer impact, and geographic range of effects. In several workshops, the consortium members' ratings were discussed and consolidated to ensure the validity of the resulting **risk matrix**. Currently, **mitigation strategies** addressing the identified risks are being developed.

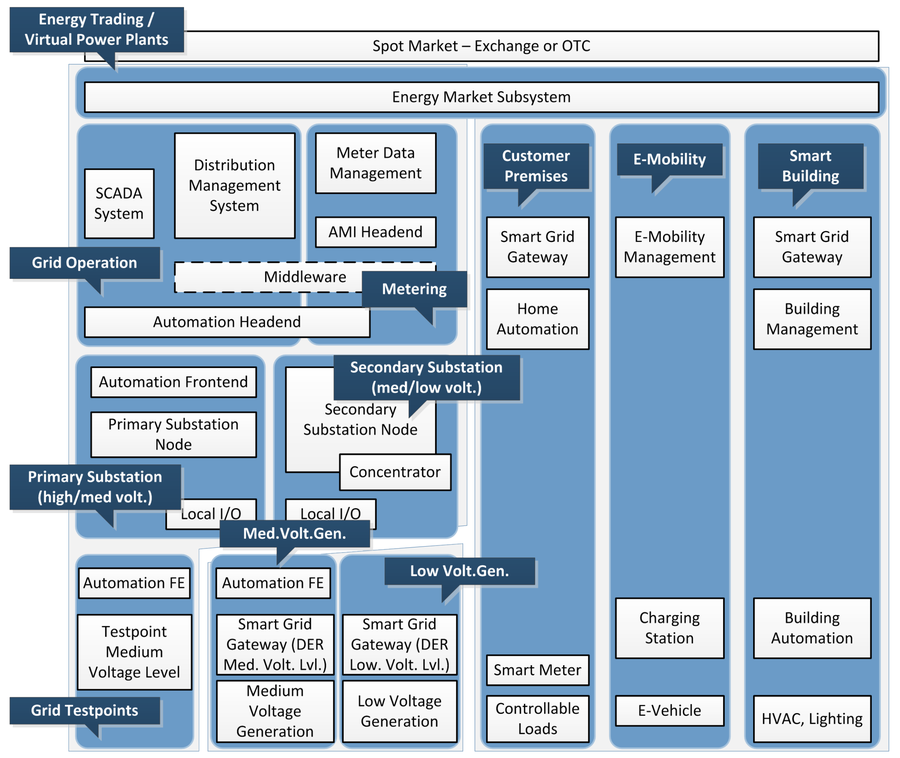

Fig. 2: Clusters of architecture components for risk assessment

Fig. 3: Substation test system

Security Audit

Based on the previous risk assessment and the testability of devices, two different subsets of the architecture model were selected for the System-Under-Test (SUT): **Secure Substation Automation (SSA)** and **Advanced Metering Infrastructure (AMI)**, see Fig. 3. Considering implementation & configuration details and functionalities of the SUT, we explored potential attack vectors and vulnerabilities, and determined those parts of the SUT which should undergo an in-depth security analysis in addition to the light-weight security audits performed on on all devices in the SUT.

The light-weight tests focused on network communication and involved both passive and active tests, such as creating network stimuli and intercepting the network traffic, or performing replay attacks. For the in-depth security audit, we used deep firmware analysis methods, involving the disassembly of the devices under test followed by deep firmware code analysis techniques, like dynamic instrumentation in a debugging environment.

Key Findings

Apply effective encryption and authentication. Applying state-of-the-art authentication and encryption standards is of paramount importance for the security of smart grids. The two main challenges are to employ mechanisms that will remain safe for years while keeping maintenace costs low, and to address interoperability issues between devices from different vendors and/or different generations.

Reducing the attack surface. Reducing the attack surface of individual components is vital for achieving strong security in critical infrastructures like power grids. Therefore, any ancillary services that are not required, and might expose additional security vulnerabilities, should be disabled.

Improve embedded systems security analysis. Embedded systems in critical infrastructures have very high security requirements. However, state-of-the-art embedded security and firmware analysis techniques are much less mature than those available for commodity PC systems. Without adequate tools and techniques, performing security audits on smart grid devices will remain challenging in the future.

References

1. CEN-CENELEC-ETSI Smart Grid Coordination Group, "Reports in response to Smart Grid Mandate M/490," 2012.
2. BSI, "Protection Profile for the Gateway of a Smart Metering System," BSI-CC-PP-0073, 2013.
3. BSI, "Protection Profile for the Security Module of a Smart Metering System (Security Module PP)," BSI-CC-PP-0077, 2013.
4. ENISA, "Smart grid threat landscape and good practice guide," Dec 2013.

FFG · KIRAS Sicherheitsforschung · bmvit Bundesministerium für Verkehr, Innovation und Technologie