Contract No 608224

1st Stakeholder Workshop
20th May, 2014
Graz, Austria

AIT Austrian Institute of Technology • Fraunhofer AISEC • The Queen's University Belfast
Energieinstitut an der Johannes Kepler Universität Linz • EMC Information Systems International Ltd
Kungliga Tekniska högskolan (KTH) • Landis + Gyr
United Technologies Research Centre • SWW Wunsiedel GmBH

Workshop Overview and Goals

Ensuring the cybersecurity and resilience of the smart grid is of paramount importance and the target of the SPARKS project – Smart Grid Protection Against Cyber Attacks. The SPARKS project has a strong remit to engage with stakeholders in the smart grid area, in order to collect requirements and disseminate the project's outcomes. As a basis for this engagement, the project has created a stakeholder group that has privileged access to the project's results and steers the research direction of the project.

To initiate this engagement, the 1st SPARKS stakeholder workshop was held on the 20th May, 2014 at the premises of Energie Steiermark in Graz, Austria. The workshop was attended by members of the stakeholder group, representing a number of different types of organisation in the smart grid area. These included Distribution System Operators (DSOs), equipment and hardware vendors, solutions providers, research institutes and policy makers.

The workshop was held over a full day, and involved presentations on the major activities that will be carried out in the project. The programme included time slots for guided discussions. This document provides a brief summary of the presentations and discussions that took place at the workshop.

Smart Grid Security Architectures and Standards

Lucie Langer, AIT Austrian Institute of Technology

The SPARKS project will investigate baseline security reference architectures for smart grids, and provide guidance with respect to security standards in this area. Dr Lucie Langer from AIT Austrian Institute of Technology presented the CEN-CENELEC-ETSI Smart Grid Architecture Model (SGAM) reference architecture as a starting point for this activity. The purpose of the three-dimensional SGAM architecture includes the development of smart grid use cases and the identification of areas in which further standards are required. Dr Langer highlighted how the SGAM reference architecture had been used in a nationally-funded project, called $(SG)^2$, to develop a smart grid reference architecture for Austria. She then went on to discuss a number of relevant security standards, including IEC 62351 and IEC 62443. Furthermore, she highlighted important guidelines from organisations, such as the European Network and Information Security Agency (ENISA).

During an open discussion session a number of important points were raised by the SPARKS stakeholders. The stakeholders called for **support in organising the myriad of smart grid security standards that are available**, with respect to the different smart grid sub-systems or use cases. A likeness was drawn with an activity being led by the IEC in this regard. Furthermore, there were concerns that related to the fact the smart grid is an evolving infrastructure, and **legacy systems**, with an expected lifetime of 20 to 30 years, **must be considered when developing security architectures and solutions**.

Smart Grid Security Analysis

Paul Smith, AIT Austrian Institute of Technology

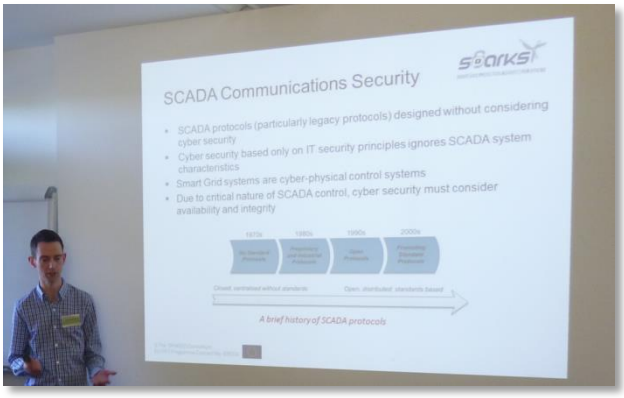
Understanding the cybersecurity risks to a smart grid are important, in order to enable appropriate security investment decisions to be made. This point was picked up by Dr Paul Smith from AIT Austrian Institute of Technology, when he discussed the security analysis activities that are to undertaken in the project. The project will innovate in three main areas: *(i)* risk assessment methods for smart grids; *(ii)* novel tools to support the implementation of this method; and *(iii)* simulation tools that can be used to understand the impact on a power grid of a cyber-attack – an important consideration when considering risks. Dr Smith highlighted the importance of considering the smart grid as an evolving infrastructure, when understanding risks, and the need to understand risks from new targeted attacks to smart grids.

Product certification and supply chain security was discussed after the presentation; the discussion touched on whether equipment vendors could provide information about their products to support customers, such as DSOs, when they carry out risk assessment activities. Additionally, it was discussed how existing **safety assessment techniques should be integrated with those from the security domain**. This has the dual benefit of leveraging existing expertise in the energy sector and supporting the co-analysis of safety (e.g., fault- and natural phenomena-driven) and security (i.e., threat-driven) aspects.

Intrusion Detection for SCADA Systems

Kieran McLaughlin, Queen's University Belfast (CSIT)

Supporting the implementation of advanced energy services that the smart grid promises to bring are Supervisory Control and Data Acquisition (SCADA) systems, which can be used to monitor and issue commands to remote devices, such as those found in energy substations. Dr Kieran McLaughlin from the Centre for Secure Information Technologies (CSIT) at Queen's University Belfast discussed how the communication protocols that support SCADA activities have evolved over time from closed proprietary protocols into more open protocols that make use of TCP/IP. The use of open standards and the increased connectedness of systems in a smart grid introduce a higher risk of cyber-attacks.

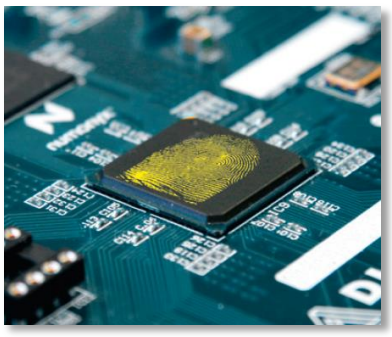


Therefore, the aim of this research is to detect the misuse of SCADA protocols by attackers, for example, as part of an attack to ex-filtrate sensitive data about the operation of plant or in order cause intentional damage to infrastructure. The research builds on previous work that was carried out in the EU-funded PRECYSE project, which aimed to detect attacks to the IEC 60870-5-104 – a SCADA protocol that is widely used in the energy sector for telecontrol operations. The SCADA intrusion detection system that has been developed by researchers at CSIT can be used to detect when the values of protocol fields in the IEC 104 packet headers are outside normal bounds, using so-called "deep-packet inspection." Furthermore, stateful detection can be used to determine when IEC 104 messages are being sent out of order, for example. Moving forward, in SPARKS existing work will be extended to look at emerging smart grid protocols, such as IEC 61850, which is used for intelligent substation automation. Initial plans involve conducting experiments using the AIT SmartEST laboratory (see below).

Discussion on this topic focused on **how operators might respond to detected attacks, in a safe way** that does not cause the operational function of a grid to be compromised, e.g., via blocking ports that critical network traffic uses. Furthermore, it was highlighted the **sensitivity of Remote Terminal Units (RTUs) to external probing, which can cause them to fail**, for example, as part of a vulnerability assessment. Finally, it was discussed how the **normal behaviour of SCADA systems and protocols can be learned**, from an operational perspective, and **whether machine learning approaches might support this process**.

Smart meter (gateway) authentication and key management using hardware PUFs

Martin Hutle, Fraunhofer AISEC



Smart meters, and metering gateways, are one of the core components of the smart grid. They support finer-grain energy consumption and generation measurement, which can form the basis of demand-response management schemes and the measurement input to various grid control strategies. However, they are at risk from a range of attacks, including being particularly exposed to physical tampering. Therefore, it is important to have suitable solutions in place to secure them, and in particular, to be able to reliably authenticate them. This is the target of this activity in the project, which was described by Dr Martin Hutle from Fraunhofer AISEC. The approach that SPARKS will take is to develop a so-called **Physical Unclonable Function (PUF)** for smart meters and metering gateways. A PUF can be used to uniquely identify hardware (such as a smart meter) by using discrepancies in the microchip manufacturing process. Leveraging these discrepancies, a function can be created that, when presented with a particular challenge, produces the same random result that cannot be mathematically predetermined

and cloned. The benefits of using PUFs for smart meters and gateways include the ability to authenticate a device without the need for any secret information to be stored on the device, and tampering with the PUF destroys the information that it stores.

Discussions were largely focused on the challenges of implementing PUFs for smart meters. These included aspects such as **developing PUFs with consistent behaviour in environments with highly variable temperatures and electric fields, and that are robust to aging** – all challenges that are relevant to smart meters and gateways.

Smart grid security information analytics

Robert W. Griffin, RSA an EMC Company

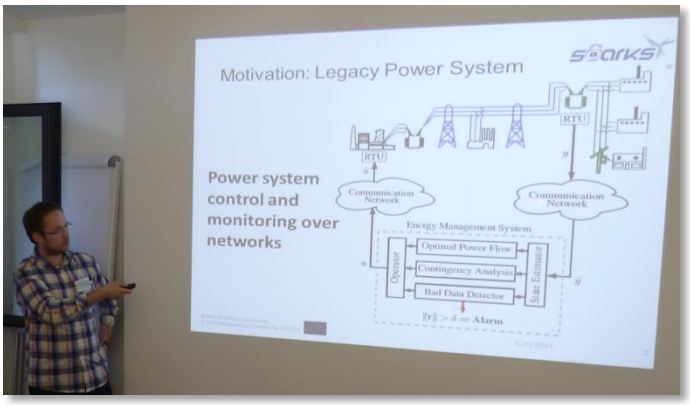
Like many other complex and large-scale information infrastructures, the smart grid is susceptible to new forms of *targeted attacks*. Such attacks can implement a number of stages in order to realise some nefarious objective, and in many cases infiltrate an organisation's ICT infrastructure using social engineering attacks. Targeted attacks are particularly challenging to address because they can operate in a stealthy manner, as they traverse an infrastructure to reach some target system. This motivates the need for new security analytics approaches for the smart grid. In his talk, Dr Robert Griffin from RSA (and EMC company) outlined how security analytics should draw on security and operational data, to address attacks in three primary ways: via capturing attacks, in a way that is analogous to tripwires; using analytics approaches in a streaming-based manner that draws on multiple big data sources to identify complex multi-stage targeted attacks; and finally determining longitudinal trends using historical data. Key benefits of using security analytics include being able to more effectively respond to incidents, such as a targeted attack, and improved knowledge that can be used when performing risk assessment activities.

Much of the discussion regarding the use of security analytics techniques focused on **privacy issues** that stem from, for example, correlating various sources of operational and security data. It was mentioned that privacy (or data protection) issues are important when *personally identifiable information* is used, and that in many cases aggregation techniques can be used to remove such information from data sets. However, it was acknowledged that privacy concerns should be addressed in the SPARKS project, as part of this research activity.

Cyber-attack resilient control systems

André Teixeira, Royal Institute of Technology (KTH)

The monitoring and control of power systems makes use of wide-area communication networks. In the smart grid, it is anticipated there will be a greater number of control loops that interact with smart devices, for example, in secondary substations. To support these new control loops, more communication networks will be required that transmit a greater

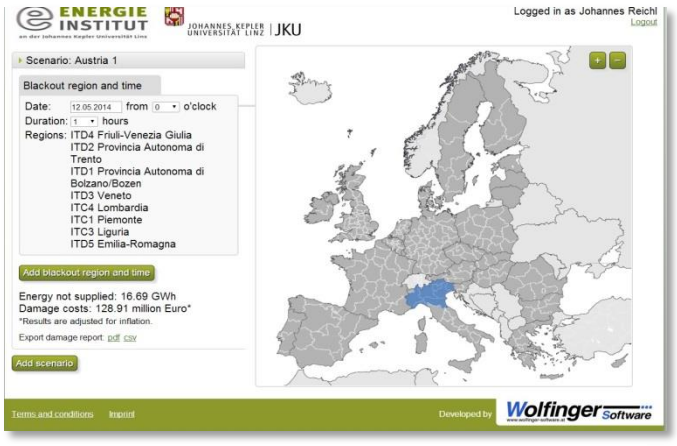


amount of critical monitoring and control data. This leads to an increased vulnerability to cyber-physical threats, because of the many new potential attack points. In this environment, traditional ICT security strategies and tools are not sufficient. Therefore, new tools are required to understand these cyber-physical attacks so that we can address a number of questions, such as which threats should we care about, what impact could they have on the smart grid, and which resources should we protect? Mr André Teixeira from the Royal Institute of Technology (KTH) in Sweden described techniques that can be used to quantify how resilient control systems are to cyber-attacks that manipulate measurement data. Furthermore, he discussed a security metric that can be used to determine the minimum number of signals an attacker must be able to manipulate, in order to remain undetected. This metric can be used as a benchmark for identifying where security improvements should be made to make such attacks harder to implement.

As a way of focusing this activity, it was discussed what the key control algorithms are (or will be) in the smart grid. It was suggested that this is an open questions at this stage of smart grid development, but it was likely the most **critical algorithms will relate to Volt-Var Control (VVC) in the distribution grid**, which are, for example, necessary to support the widespread deployment of renewable energy sources.

Smart grid security legal, economic and social issues

Michael Schmidthaler, Energy Institute at the J. Kepler University Linz



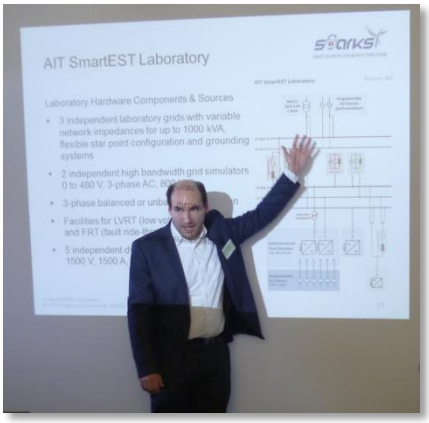
The blackout simulator: www.blackout-simulator.com

The security technologies that are developed in the SPARKS project will be subjected to a cost-benefit analysis. The basis for this analysis will be an understanding of the economic costs associated with blackouts that could be caused by cyber-attacks. To evaluate these costs, tools such as the blackout simulator, developed by Dr Michael Schmidthaler and his colleagues at the Energy Institute at the J. Kepler University Linz, will be used. Based on an understanding of the costs of a cyber-attack, business cases will be developed that show the benefit of using the SPARKS technologies. In addition to this economic analysis, the societal acceptance of the technologies that are developed in the project will be assessed. This will primarily take two forms: a *foresight process*, wherein workshops are used to explore hypothetical attack scenarios and their impact relative to the introduction of novel security technologies, and a quantitative analysis that suggests the conditions under which

the introduction of new technologies could be motivated. Underpinning SPARKS's technology development will be a clear understanding of the legal directives and regulations, which will be surveyed and reported on in a deliverable that is due towards the end of the project. Again, as stated before, **privacy issues** were highlighted in discussions as being important to consider when understanding the societal acceptance of security technologies.

SPARKS demonstration activities

Friederich Kupzog, AIT Austrian Institute of Technology



The research outcomes from the SPARKS project will be demonstrated using three facilities, namely the AIT SmartEST laboratory, the Nimbus microgrid, and the infrastructure from SWW Wunsiedel GmbH. An overview of these facilities was presented by Dr Friederich Kupzog from AIT. The Nimbus microgrid incorporates, amongst other items, a 10kW wind turbine, a 35 kWh Li-Ion battery, a 50kW electrical/82kW thermal combined heat and power unit (CHP), and a feeder management relay that is used to manage the point of coupling between the microgrid and the rest of the building it serves. Associated with the Nimbus microgrid is a sophisticated building management system. We foresee the Nimbus facility supporting our research activities on security analytics and resilient control systems. Meanwhile, the SWW Wunsiedel infrastructure represents a rich and varied state-of-the-art smart grid deployment, which includes a smart metering deployment, a number of sites in the Wunsiedel region that use a range of renewable energy sources, and an underlying fibre-optic network that can be used to support communications. We foresee the SWW Wunsiedel infrastructure being an interesting case study for the project's novel risk assessment methods and tools. Finally, Dr Kupzog presented the AIT SmartEST laboratory, which is typically used to carry out conformance testing of smart grid equipment, such as large-scale power inverters. The SmartEST laboratory can be used to flexibly combine novel smart grid equipment with power grid simulators, which are controlled by an open-source SCADA system. Ongoing work is investigating how the SmartEST laboratory can be used to support the demonstration of the intrusion detection system for SCADA systems, focusing on the IEC 61850 protocol.

Summary

In addition to the specific points outlined above, based on the discussions that were held during the stakeholder workshop, it was clear to see the importance of the different research activities the SPARKS project is investigating, and that much work still needs to be done to realise a secure and resilient smart grid. Furthermore, it was evident that a number of different stakeholder groups must engage effectively to realise this vision – the relationship and interface between equipment (and solutions) providers and DSOs was highlighted as being of particular importance by the group.

Moving forward, the SPARKS project will take on board the issues that were raised at the stakeholder workshop when shaping their research direction. The next stakeholder workshop is scheduled to take place in the Spring of 2015, when the project will highlight the importance of its research activities by demonstrating a cyber-attack to a smart grid. Details regarding this workshop will follow, in due course. The slides that were presented at the

workshop are available on the SPARKS project website, along with a blog entry that summarises some of the major outcomes from the day. If you have any further comments or questions about the project, then please do contact us.