SPARKS

SMART GRID PROTECTION AGAINST CYBER ATTACKS

Contract No 608224

Deliverable D.1.6
Overview of Research Projects in the area of Smart Grids

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

Document control information	
Title	D1.6 Overview of Research Projects in the area of Smart Grids
Editor	Michael Schmidthaler (EI)
Contributors	Michael Schmidthaler (EI), Johannes Reichl (EI), Paul Smith (AIT)
Description	This short deliverable contains a directory of projects, finished and currently running, that relate to smart grid security that are operating at a European level, for example, in the context of Framework Programme 7, and national research initiatives. This includes short description of the project's objectives and expected results. Using the consortium's international reach, this deliverable also attempts to summarise the research activities outside of Europe. An update of this deliverable will appear in the project's final report.
Requested deadline	31st March, 2015

Executive Summary

This report entails a summary of SPARKS' engagement and interaction activities with related smart grid and cyber security research projects. In addition to a summary of relevant projects in this area, D.1.6 describes the assessment steps which were carried out in order to collect information on research activities at the European and national level which – for the most part – received funding through the European 7th framework programme as well as country-specific funding authorities.

The empirical assessment of the existing research landscape w was carried out by means of a structured questionnaire from November 2014 until February 2015. In addition to gathering of information on parallel scientific activities, it aimed at interacting with the European research community. The questionnaire was distributed – among other relevant researcher and industry representatives – to members of the SPARKS stakeholder advisory board, to decision makers in administration and business as well as to external contacts in the European smart grid research community. The empirical methodology is presented briefly in section 1 of this report.

One key finding of the empirical research carried out is that the relationship between SPARKS and other projects needs to be further enhanced due to content overlap in certain –specific and heterogeneous – areas. This is particularly relevant for the SEGRID project which in addition to highly sophisticated research sets out to analyse use cases for security measures. The joint outcome can be enhanced – and thus redundancies be avoided – if fundamental research from SPARKS is transferred successfully to other projects such as SEGRID.

Summarizing the activities in D.1.6, this report presents the interaction activities of the SPARKS project with researchers in the field of smart grids, cyber security and critical infrastructure. In order to do so, a comprehensive assessment of the research landscape in this area was conducted and awareness for the SPARKS project has been raised.

Table of Contents

1 Engagement with Related European and National Projects

This report relates to one of SPARKS' core objectives namely raising awareness of ongoing activities among stakeholders in the European smart grid community. This is particularly necessary as research addressing cyber security and privacy concerns associated with the accelerated development of innovative smart grid solutions has become more important and needs to provide effective protective mechanisms.

D.1.6 conducted literature-based analysis of existing projects. This report contains the main findings as well as the results of a survey among the SPARKS stakeholder advisory board and additional research projects. To this end, a questionnaire was developed in conjunction with the SEGRID project. This was done to achieve two main goals: (a) identifying and assessing projects with direct involvement of the partner and activities which are known to the partners and; (b) raising awareness of the SPARKS project which is highly useful for dissemination purposes.

Special emphasis has been put on interacting with other research groups within and outside the SPARKS consortium. This correlates with SPARKS' ambition to intensively interact with related project such as HyRim and SEGRID, which are presented subsequently. The mutual project focus and subsequent draft of the questionnaire significantly benefited both projects and improved the empirical process.

2 Methodology and Empiric Assessment

SPARKS aims to avoid parallel research by pro-actively interacting with other projects and consortia. This was done in D.1.6 in which research activities related to smart grids and cyber security have been contacted and detailed information as regards the way of conduct, the consortia, relevant funding bodies, the project duration and other attributes of these related projects has been acquired.[1]

In a first step a target group was defined. On this basis, a list for contacting each person with special knowledge of a project (i.e. project lead) was compiled. Subsequently a specific questionnaire and invitation letter was developed according to the characteristics of each project in question. These questionnaires – for which a template is presented in the appendix – were sent out to approximately 70 involved research groups. Contacted persons were kindly reminded to reply within a month. Reminders were sent out 4 weeks after the initial contacts. Despite significant – partly telephone-based – interaction, replies of only 13 research groups were received and could be incorporated. These are presented subsequently. [2]

Adding to the assessment of transnational (European) research activities, the focus was put on trans-national (i.e. EU funded) regional research activities and endeavours. The aim was to enhance the existing project interactions and to show the involvement of SPARKS at the level of individual researchers who pursue activities in the field of Smart Grids security and privacy. Furthermore, this helped to raise the awareness for SPARKS among projects and the research community.

In addition to smart grid projects, research endeavours from the broader field of critical infrastructure protection have been accounted for. Consequently, outreach of the SPARKS project was achieved for selected projects in this research field as well. As critical infrastructure protection is investigated in various – quite heterogeneous – research activities, their incorporation was considered useful for SPARKS.

---

[1] Nevertheless, the focus here has been put on cyber security projects.
[2] In order to present the main objectives to survey participants, two separate invitation letters were distributed in German and English.

3 Research Projects with special relation to SPARKS

In order to provide a holistic summary of the research landscape as regards smart grid and cyber security, this section presents research activities which pursue similar objectives as SPARKS does.

Table 1 entails a selection of current and past research projects which were gathered by means of the described survey.

Table 1: Summary of participating European Research projects in the SPARKS survey

Short title	Long title	Type	Project Duration	Link	Budget
CIPRNet	Critical Infrastructure Preparedness and Resilience Network	FP 7	2013-2017	www.ciprnet.eu	1.6 m. €(EU), 2,6 m €total
VIKING	Vital Infrastructure, Networks, Information, and Control Systems Management	FP7	Completed in 2011	www.vikingproject.eu	27 m. €(EU), total 54 m. €
Grid4EU	Large-Scale Demonstration of Advanced Smart Grid Solutions with wide Replication and Scalability Potential for Europe	FP 7	2011-2016	www.grid4eu.eu	2.03 m. € (EU), total 3.15 m. €
CRUTIAL	CRitical UTility InfrastructurAL resilience	FP6	2006-2009	http://crutial.rse-web.it/	0.17m. € (EU), total 0.52 m. €
SoES	Security of Energy Systems	EPCIP	2012-2014	www.soes-project.eu	3.48m. €(EU), total 4.9 m. €
SmartC2Net	Smart Control of Energy Distribution Grids over Heterogeneous Communication Networks	FP7	2012-	www.smartc2net.eu	2.9 m. €(EU), 4.29 m. total
C-DAX	Cyber-secure Data And Control Cloud for Power Grids	FP7	2009-2012	http://www.cdax.eu/	1.188.501,-
SG²	Smart Grid Security Guidance	KIRAS	2013-	http://www.kiras.at/projects/?L=1	0.78 m. €total
CIIS	Cyber Incident Information Sharing	KIRAS	2013-	http://www.ait.ac.at/	4.7 m. € (EU), 7,9 m. € total
DISCERN	Distributed Intelligence for Cost-effective and Reliable Solutions	FP7	2013-2016	http://www.discern.eu/project/partners.html	1.6 m. €(EU), 2,6 m.€total
CRISALIS	Cyber-attacks against critical infrastructures – capability project	FP7	2012-2015	http://www.crisalis-project.eu/	3.426m€(EU) 5.322m total

SEGRID	Security for Smart Electricity GRIDs	FP7	2014-2017	http://www.segrid.eu/	3 m. €total
AFTER	A Framework for electrical power systems vulnerability identification, defence and restoration	FP7	2011-2014	http://www.after-project.eu/Layout/after/	3.473m€(EU) 5 m. €total
HyRiM	Hybrid Risk Management for Utility Providers	FP7	2014 – 2017	https://hyrim.net	3.387m€(EU) 4.657m€total

Although the goal of achieving a significantly higher number of replies was difficult to achieve, the results of the empiric assessment have proven to be highly valuable for the SPARKS project and its stakeholders. As further information could be obtained via the online presence of most projects, it was possible to present each project, their objectives and merits step-by-step. This is provided subsequently.

4 Detailed Assessment Smart Grid Research Activities

The following section includes a set of relevant projects in the smart grid and cyber security research area. Project-specific information was obtained from the described survey methods as well as facts from online presences of these projects. These projects are described step-by-step following a standardized format.

4.1 CIPRNet

The EU-sponsored project *Critical Infrastructure Preparedness and Resilience Research Network* (CIPRNet) works towards establishing a European infrastructures simulation and analysis centre (EISAC). The research network will integrate knowledge and technologies to create added-value decision support capabilities for national and multi-nation emergency management. In this way, CIPRNet will provide substantial improvements for fast and adequate responses by authorities and critical infrastructure owners to complex emergencies affecting or originating from critical infrastructures. The purpose of the projected EISAC is sustaining the new capabilities and providing further innovations to end-users and stakeholders beyond the duration of CIPRNet.

The following partners collaborated in the project:

- Fraunhofer IAIS (DE)
- ENEA Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (IT)
- TNO (NL)
- UIC International Union of Railways (FR)
- CEA Commissariat à l'énergie atomique et aux énergies alternatives (FR)
- JRC Joint Research Center – Institute for the Protection and Security of the Citizen (EU)
- Deltares Enabling Delta Life (NL)
- UCY (CY)
- UTP University of Science and Technology (PL)
- UCBM University Campus Bio-Medico of Rom Italy (IT)
- UBS University of British Columbia, CA (CA)
- ACRIS GmbH (CH)

The project was carried out under the Network of Excellence (NoE) initiative.

Further information is available under www.ciprnet.eu

4.2 VIKING

The overall goal of the VIKING project is to make SCADA systems robust against attacks and operational errors. The project's main goals are to investigate the vulnerability of SCADA systems and the cost of cyber-attacks on society, to propose and test strategies and technologies to mitigate these weaknesses and to increase the awareness for the importance of critical infrastructures and the need to protect them.

Specifically, the project aimed at achieving the following core objectives:

- Increase understanding of vulnerabilities of integrated control systems.
- Evaluate potential consequences and cost for society of misbehaving control systems that can be used as a base for evaluating control system design solutions.
- Propose solutions to eliminate or counteract these vulnerabilities.
- Develop new technical security and robustness solutions.
- Demonstrate solutions on a test bed. Increase the public awareness of the dependencies and vulnerabilities of cyber-physical systems in the power industry.

The following partners collaborated in the project:

- ABB AG (DE)
- ETH Zürich Eidgenoessische Technische Hochschule Zürich (CH)
- E.ON AG (DE)
- Astron Informatics Ltd, Kungliga (HU)
- Tekniska Högskolan (KTH) (SE)
- Univeristy Systems of Maryland Foundation (US)
- MML Analys & Strategi (SE)

Activities were carried out under the EC FP7 framework.

Further information is available under www.vikingproject.eu

4.3 Grid4EU

The Grid4EU project is an innovative smart grid project proposed by a group of distribution system operators from Czech Republic, France, Germany, Italy, Spain and Sweden, in close partnership with a set of electricity retailers, manufacturers and research organisations. Adopting a systemic approach and organised around large-scale demonstrations networks located in six different countries, its structure is built to facilitate dynamic knowledge sharing, technical assistance and review.

Designed in response to a call for projects from the European Commission, the project lays the groundwork for the development of tomorrow's electricity grids. Financed to the tune of €25 M by the European Commission, and costing €54 M overall, it is the biggest smart grid project to be funded by the European Union.

GRID4EU brings together a consortium of six European energy distributors, namely ERDF, Enel Distribuzione, Iberdrola, CEZ Distribuce, Vattenfall Eldistribution and RWE.

It will test the potential of smart grids in areas such as renewable energy integration, electric vehicle development, grid automation, energy storage, energy efficiency and load reduction.

GRID4EU consists of six demonstrators, which will be tested over a period of four years in each of the European countries represented in the consortium. The emphasis will be on fostering complementarity between these projects, and on promoting transversal research and sharing results between the different energy distributors involved.

GRID4EU also draws on the know-how of other industrial and scientific partners, thereby bringing together thirty partners from around ten different EU countries.

The project will run over a 51 month period. Grid4EU aims at testing in real size some innovative system concepts and technologies in order to highlight and help to remove some of the barriers to the smart grids deployment and the achievement of the 2020 European goals. These barriers may be technical, economic, societal, environmental or regulatory barriers. It focuses on how distribution system operators can dynamically manage electricity supply and demand, which is crucial for integration of large amounts of renewable energy, and empowers consumers to become active participants in their energy choices. Ultimately, these innovative concepts and technologies should cost-effectively increase the network's reliability, flexibility, and resiliency.

The following partners collaborated in the project:

- RWE (DE)
- Vattenfall (SE)
- Iberdrola (ES)
- ENEL S.p.A. Ente nazionale per l'energia elettrica (IT)
- CEZ (CZ)
- ERDF Électricité réseau distribution france (FR)
- 21 other beneficiaries (vendors, universities, research organisations, etc.)

Being a major project, activities were carried out under the EC FP7 framework.

Further information is available under www.grid4eu.eu

4.4 SoES

SoES aims at facing the ICT security demand of Energy Smart Grids on a three-dimensional plan: technical plan, policy plan, inter-national / inter-organiational plan with the following specific objectives:

- Identification of vulnerabilities, threats and countermeasures relevant for the Smart Grid architectures.
- Creation of a comprehensive knowledge base grouping together reference architectures, international standards, vulnerabilities and countermeasures of the Smart Grids.
- Definition of ICT security best practices for Energy Smart Grids.
- Establishment of an information sharing platform, named Hub for Smart Grid Cyber Security (H4SGCS), to improve the security know-how of Smart Grid actors.

The following partners collaborated in the project:

- RSE - Ricerca Sistema Energetico SpA (IT)
- Global Cyber Security Center (GCSEC) (IT)
- Engenharia e Sistemas EFACEC (PT)
- ENEL S.p.A. Ente nazionale per l'energia elettrica (IT)

Activities were carried out under the EC FP7 framework.

Further information is available under www.soes-project.eu.

4.5 SmartC2Net

The future energy grids will face a widespread participation of distributed energy resources and have the need for customer-side applications that support the energy balancing in the low and medium voltage grids. Adding intelligence to the power grid requires communication and computation infrastructure, requiring additional investments. To be cost efficient, it is therefore essential to leverage existing communication infrastructures for intelligent power grid operations. The SmartC2Net project will develop, implement and validate robust solutions that enable smart grid operation on top of heterogeneous off-the-shelf communication infrastructures with varying properties.

The objectives are:

- to provide a reliable energy infrastructure at low infrastructure costs;
- to position the capabilities of telecommunication operators and energy system integrators in the smart grid value chain creating benefits for all stake-holders;
- to strengthen European research and industrial innovation in the area of Smart Grids.

The following partners collaborated in the project:

- FTW Forschungszentrum Telekommunikation Wien GmbH (AT)
- Aalborg Universitet (DK)
- Technische Universität Dortmund (DE)
- Resiltech SRL (IT)
- Ricerca Sul Sistema Energetico - RSE SPA (IT)
- Vodafone Omnitel N.V (NL)
- Efacec Engenharia e Sistemas - EFACEC (PT)

Activities were carried out under the EC FP7 framework.

Further information is available under www.smartc2net.eu .

4.6 CRUTIAL

CRUTIAL addresses new networked information and communication technology (ICT) systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet.

The project will: a) identify and describe control system scenarios; b) provide modelling approaches for understanding and mastering the various interdependencies; c) develop a test bed integrating the electric power system and the information infrastructure; d) investigate fault-tolerant architectural configurations; e) provide qualitative and quantitative support for the identification, analysis and evaluation of the scenarios identified. The results will be validated against test beds of Electric Power Systems.

CRUTIAL's innovative approach resides in modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks.

The objectives of the project are:

- investigation of models and architectures that cope with the scenario of openness, heterogeneity and evolvability endured by electrical utilities infrastructures;
- analysis of critical scenarios in which faults in the information infrastructure provoke serious impacts on the controlled electric power infrastructure;
- investigation of distributed architectures enabling dependable control and management of the power grid.

The project's results will help in designing and assessing new Electric Power systems and information infrastructures. Thus, they will enable to reduce the current (unfortunately repetitive) blackouts, in terms of frequency, duration and extent, and provide insights to Electric Power companies and standardisation bodies for exploiting resilience in critical utilities infrastructures.

The following partners collaborated in the project:

- Ricerca di Sistema - CESI RICERCA (IT)
- Faculty of Sciences of the University of Lisboa, FCUL (PT)
- Italian National Research Council - NR-ISTI, CNR (IT)
- French National Organisation for Academic Scientific Research - LAAS, CNRS, (FR)
- K.U.Leuven - ELECTA division (BE)
- Consorzio Nazionale Interuniversitario per le Telecomunicazioni – CNIT (IT)

Activities were carried out under the EC FP6 framework.

Further information is available under http://crutial.rse-web.it/

4.7 C-DAX

C-DAX, Cyber-secure Data and Control Cloud for Power Grids, proposes a Cyber-secure Data and Control Cloud for future power distribution networks as an integrated communication and information infrastructure. C-DAX exploits the properties of novel, information-centric networking (ICN) architectures that are by design more secure, resilient, scalable, and flexible than conventional information systems. Further, C-DAX will provide added value to current protocols and data models used within the power systems domain for monitoring and control purposes.

The following partners collaborated in the project:

- Alcatel-Lucent (FR)
- Alliander (NL)
- Eberhards Karl Universität Tübingen (DE)
- École Polytechnique Fédérale de Lausanne (CH)
- iMinds (NL)
- National Instruments (AT)
- Radboud Universiteit Nijmegen (NL)
- University College London (GB)
- University of Surrey (GB)

Activities were carried out under the EC FP7 framework.
Further information is available under http://www.cdax.eu

4.8 SG²

Being a purely national – i.e. Austrian – research project in the area of smart grid and Cyber Security, SG² is the exception to the rule in this collection of European activities. This project is important since a variety of interconnections with SPARKS exist in terms of content, partner structure, scale and scope effects and dissemination platforms.

In terms of investigated research questions, SG² addresses issues associated with the implementation of innovative SG technologies with a special focus to the Austrian infrastructure. As future energy grids will make extensive use of the integration of ICT technologies, cyber security 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 project (SG)² is therefore a systematic study of smart grid technologies in terms of ICT security issues and the research of countermeasures. Based on a thorough threat and risk analysis from a state-level perspective and security analysis of smart grid components, (SG)² explores measures for power grid operators that serve to increase the security of computer systems deployed in the future critical infrastructure of energy.

The following partners collaborated in the project:

- AIT Energy Department (AT)
- Technische Universität Wien (AT)
- SECConsult Unternehmensberatung GmbH (AT)
- Siemens AG - Corporate Technology Österreich (AT)
- LINZ STROM GmbH, Energie AG Oberösterreich Data GmbH (AT)
- Innsbrucker Kommunalbetriebe AG (AT)
- Energieinstitut an der JKU Linz GmbH (AT)
- Bundesministerium für Inneres (AT)
- Bundesministerium für Landesverteidigung und Sport (AT)

Activities were carried out under the AUSTRIAN KIRAS framework.

Further information is available under http://www.ait.ac.at/research-services/research-services-digital-safety-security/ict-security/reference-projects/sg2-smart-grid-security-guidance/?L=1

4.9 CIIS

The smooth operation of critical infrastructures, such as telecommunications or electricity supply is essential for our society. In recent years, however, operators of critical infrastructure have increasingly struggled with cyber security problems. Through the use of ICT standard products and the increasing network interdependencies, the attack surfaces and channels have multiplied. Therefore, the goals in CIIS are twofold:

- the development of mechanisms for information correlation, aggregation, and fingerprinting of status and attack data, as well as;
- the development of methods and technologies for the exchange of information on cyber incidents to better defend against cyber-attacks and to streamline the analysis of the current threat.

As a result, the resilience of systems to be improved (e.g., operators of critical infrastructures) both between organiations and between organiational units within large organiations (e.g., within ministries) and increased regarding cyber-attacks in sensitive areas.

The following partners collaborated in the project:

- Energie AG Oberösterreich Data GmbH (AT)
- T-Systems Austria (AT)
- VRVis Forschungs GmbH (AT)
- Bundesministerium für Inneres (BM.I) (AT)
- Bundesministerium für Landesverteidigung und Sport (BMLVS) (AT)
- Institut für Rechts- und Kriminalsoziologie (AT)
- Netelligenz e.U (AT)

Activities were carried out under the AUSTRIAN KIRAS framework.

Further information is available under http://www.ait.ac.at/research-services/research-services-digital-safety-security/ict-security/reference-projects/ciis-cyber-attack-incident-information-sharing/?L=1 and project lead Florian Skopic.

4.10 DISCERN

The target of DISCERN is to assess the optimal level of intelligence in the distribution networks and to determine the replicable technological options that will allow a cost-effective and reliable enhancement of observability and controllability of the future distribution networks in Europe.

Specific objectives of DISCERN:

- establish a family of demonstration projects focused on the MV/LV network and develop an assessment framework based on KPIs that allows the comparison of technical solutions for monitoring and controlling the distribution network;
- identify, assess and compare the technological options for monitoring and control systems in the distribution network;
- test and validate optimal technological solutions by means of real time simulations (e.g. Real Time Digital Simulator [RTDS]) and small scale field tests;
- facilitate the knowledge exchange with innovative European projects testing various smart grid functionalities in the area of network operation, monitoring and control;
- develop recommendations for the cost-effective application of advanced distributed sensors, monitoring and control systems to increase the intelligence of electricity distribution networks based on KPIs;
- map relevant standards and contribute to standardisation activities.

The following partners collaborated in the project:

- RWE Deutschland AG (DE)
- ABB (SE, CH)
- CIRCE (Research Centre for Energy Resources and Consumption) (ES)
- Gas Natural Fenosa (ES)
- Iberdrola (ES)
- DNV KEMA Energy & Sustainability (NL)
- OFFIS (Oldenburg Research and Development Institute for Information Technology Tools and Systems) (DE)
- The Royal Institute of Technology (Kungliga Tekniska högskolan in Swedish, KTH) (SE)
- Southern Electric Power Distribution (SEPD) (GB)
- Vattenfall Eldistribution (SE)
- ZIV (ES)

Activities were carried out under the EC 7th framework programme.

Further information is available under http://www.discern.eu/project/partners.html

4.11 Crisalis

The CRISALIS project aims at providing new means to secure critical infrastructure environments from targeted attacks, carried out by resourceful and motivated individuals.

CRISALIS focuses on the following two aspects: detection of vulnerabilities and attacks in critical infrastructure environments. The focus is put on two different, yet interlinked, use cases that are typical for the power grid infrastructure: control systems based on SCADA protocols and the Advanced Metering Infrastructure. CRISALIS leverages the unique characteristics of critical infrastructure environments to produce novel practical mechanisms and techniques for their security assessment and protection. This is achieved by pursuing three main research objectives: (i) providing new methodologies and techniques to secure critical infrastructure systems; (ii) providing new tools to detect intrusions; (iii) developing new, more effective, techniques to analyse infected systems. Particular attention is paid to ensure the practical implementation of these techniques in real-world environments, and to minimise the impact on operations, goals which are attainable thanks to the direct involvement in the process of end users and device manufacturers who provide expertise and realistic test environments to validate the proposed methodologies.

CRISALIS develops tools to facilitate the automated analysis of critical infrastructure environments and the discovery of possible threat vectors, and embeds these techniques into a comprehensive and practical methodology for vulnerability discovery.

The following partners collaborated in the project:

- Symantec (IE)
- Eurecom (FR)
- University of Twente (NL)
- University of Chalmers (SE)
- University of Ulm (DE)
- Security Matters (NL)
- Alliander (NL)
- ENEL S.p.A. Ente nazionale per l'energia elettrica (IT)
- Siemens (DE)

Activities were carried out under the EC 7th framework programme.
Further information is available under http://www.crisalis-project.eu/

4.12 SEGRID

SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks. We do this by applying a risk management analysis approach to a number of smart grid use cases (the SEGRID use cases), which will define security requirements and determine gaps in current security technologies, standards and regulations. The identified gaps and the analysis itself will give input to the enhancement of risk assessment methodologies and the development of novel security measures for smart grids.

We are convinced that SEGRID will deliver a major contribution to the protection of smart grids of 2020 against cyber-attacks by:

- identifying threats and potential future cyber-attack pathways, for the SEGRID use cases;
- determining the gap between currently available security standards, methods and measures for smart grids in order to derive which additional security methods and measures are required for the SEGRID use cases;
- developing the necessary new security methods and measures for privacy, communication and system security in smart grids, to mitigate the threats found in the SEGRID use cases, evaluate and test them;
- building up a realistic test environment (Security Integration Test Environment, SITE) to test and verify new security methods and measures;
- evaluating and improving current risk management methodologies in order to make them optimally suited to identify and address the key risk factors of smart grids of 2020;
- feeding the established results from the SEGRID project into European and global standardisation bodies, industry groups and smart grid suppliers and make sure that the project results fit the needs of those communities and raise awareness among stakeholders.

The following partners collaborated in the project:

- Organisatie voor toegepast natuurwetenschappelijk onderzoek, TNO (NL)
- Swedish Institute of Computer Science (SE)
- Kungliga Tekniska högskolan (SE)
- Instituto Consultivo para el Desarrollo (ES)
- European Network for Cyber Security (NL)
- Liander NV (NL)
- ABB AS corporate research (NO)
- Foundation of the Faculty of Sciences of Lisbon University (PT)
- Energias de Portugal (PT)
- ZIV smart grid solutions by CG (ES)

Activities were carried out under the EC 7th framework programme.

Further information is available under http://www.segrid.eu

4.13 HyRiM

Risk management is a core duty in critical infrastructures as operated by utility providers. Despite the existence of numerous risk assessment tools to support the utility providers in estimating the nature and impact of possible incidents, risk management up till now is mostly a matter of best practice approaches. Risk management tools are mostly focused on one of two major topics:

- the utility network physical infrastructure, consisting of, e.g. gas, water pipes or power lines
- the utility's control network including SCADA (Supervisory Control and Data Acquisition) networks and business and information systems.

The main objective of this project is to identify and evaluate 'Hybrid Risk Metrics' for assessing and categorizing security risks in interconnected utility infrastructure networks in order to provide foundations for novel protection and prevention mechanisms.

The project will provide utility network providers with a risk assessment tool that – in adherence with, e.g., the BSI or ICNC recommendations – supports qualitative risk assessment based on numerical (quantitative) techniques. For that matter, our method will explicitly account for the infrastructure's two-fold nature in terms of the utility network and the control network alongside it. The expected impact is thus a movement away from best practice only, towards the treatment of risk in utility networks based on a sound and well-understood mathematical foundation. The project will take an explicit step towards considering security in the given context of utility networks, ultimately yielding a specially tailored solution that is optimal for the application at hand.

The following partners collaborated in the project:

- Ait Austrian Institute Of Technology Gmbh
- Universität Passau
- Lancaster University
- Etra Investigacion Y Desarrollo Sa
- Akhela Srl
- Suministros Especiales Alginetenses Coop. V.
- Linz Ag für Energie, Telekommunikation, Verkehr und kommunale Dienste

Activities were carried out under project number EU Project Number 608090.

Further information is available under https://hyrim.net//

4.14 AFTER

The AFTER project aims at increasing the TSO capabilities in creating, monitoring and managing secure interconnected electrical power system infrastructures, being able to survive major failures and to efficiently restore service supply after major disruptions.

These objectives are to be met with the definition of a framework, methodologies, tools and techniques to evaluate and to enhance the security and resilience of complex energy systems, in particular for:

- risk assessment (hazard, vulnerability and impact analysis) of the interconnected and integrated electrical power and ICT systems;
- design and assess of global defence and restoration plans;
- AFTER gives great importance to TSOs requirements and point of view.

AFTER proposes a new framework for vulnerability and risk assessment and contingency planning of power systems, whose development requires:

- the analysis of vulnerabilities, failures and the identification of cause-effects relationships (dependency models), within the power system and from the ICT to the power system;
- the definition of appropriate risk assessment methods and risk indices;
- the definition of physical security methods and techniques;
- the definition of criteria and techniques for defence and restoration.

The following partners collaborated in the project:

- RSE Ricerca sul Sistema Energetico - RSE S.p.a. (IT)
- ENEA Agenzia nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile (IT)
- SINTEF - EN (NO)
- SINTEF - ICT (NO)
- UNIGE Universita degli studi die Genova (IT)
- UCD University College Dublin (IE)
- CU City University London (GB)
- ALSTOM (FR)
- SIEMENS (DE)
- JRC Joint Research Center (BE)
- ELIA (BE)
- TERNA Trasmissione Elettricità Rete Nazionale S.p.A (IT)
- CEPS (CZ)

Activities were carried out under the EC 7th framework programme.

Further information is available under http://www.after-project.eu/Layout/after/

5 International Smart Grid Research

In addition to the responses gathered by means of the described survey, a variety of international research projects has been included based on a secondary literature assessment.

This is split in two sections: Part one focuses on non-European research projects that are related to root the activities carried out in SPARKS into an international research agenda and a part two, which contains the opposite, namely a strictly regional research overview in the field of smart grid technologies.

Thus, in the following and firstly, projects with a strong international focus are being presented. As national funding bodies have prioritised smart grid related projects, a variety of research emphases have emerged touching on issues of smart grid security, renewable energy integration, consumer interaction and others. Table 2 includes a brief overview of relevant research projects in the USA with high visibility in the scientific community and the broader public.

Table 2: International Smart Grid Technology Projects – Activities in the US

Long title	Countries	Short title	Project Status	Partners	Abstract	Contact
Guidebook for ARRA Smart Grid Program Metrics and Benefits	USA		completed: 2010	United States Department of Energy (DoE)	DOE determines what information is required and how best to gather it for developing and reporting metrics and benefits. This Guidebook serves as a way to begin a dialogue.	https://www.smartgrid.gov/sites/default/files/pdfs/sgdp_rdsi_metrics_benefits.pdf
ElEctricity SubSEctor cybErSEcurity capability Maturity MoDEl(ES-c2M2)	USA	MoDEl(ES-c2M2)	completed: 2012	United States Department of Energy (DoE), University Software Engineering Institute - CERT Program	This project describes the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). The goal of this model is to support ongoing development and measurement of cybersecurity capabilities within the electricity subsector.	http://energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf https://www.naseo.org/Data/Sites/1/documents/committees/energysecurity/webinars/2013-03-05/hoffman-c2m2.pdf
A Preliminary Estimate of the Investment Requirements and the Resultant Benefits of a Fully Functioning Smart Grid	USA		completed: 2011	Electric Power Research Institute (EPRI)	The primary goal of this report, which is a partial update to an earlier report (EPRI 1011001), is to initiate a stakeholder discussion regarding the investment needed to create a viable Smart Grid. To meet this goal, the report documents the methodology, key assumptions, and results of a preliminary quantitative estimated of the required investment.	http://www.rmi.org/Content/Files/EstimatingCostsSmartGRid.pdf
Demand Response and Open Automated	USA		completed: 2010	Lawrence Berkeley National Laboratory	This study examines data centre characteristics, loads, control systems, and technologies to identify demand response (DR) and automated DR (Open Auto-DR) opportunities and	http://eetd.lbl.gov/sites/all/files/demand_response_and_open_automated_demand_response_opportunities_for_data_centers_lbnl-3047e_0.pdf

Demand Response Opportunities for Data Centers					challenges. The study is performed in collaboration with technology experts, industrial partners, and data centre facility managers and existing research on commercial and industrial DR is collected and analysed.	
The Road to Maximizing Smart Grid 's Environmental Benefit	USA		completed: 2009	The GridWise® Architecture Council by E Source	The focus of this report is to demonstrate the environmental benefits of smart-grid interoperability. Resource optimisation, decreased emissions intensity, and carbon productivity are the primary conduits by which environmental benefits can be achieved.	http://www.gridwiseac.org/pdfs/environmental_interoperability.pdf
Smart Meter Demonstration Project	USA	gridS MAR T	started: 2009, completed: 2013	"BKW Energie AG, ewz (Elektrizitäts werk der Stadt Zürich), Supercomput ing Systems AG, Bacher Energie AG, The project is co-funded by:	This project built a secure, interoperable, and integrated smart grid infrastructure that demonstrates the ability to maximise distribution system efficiency and reliability, and consumer use of demand response programs to reduce energy consumption, peak demand costs, and fossil fuel emissions. The demonstration area includes 150 square miles including approximately 110,000 meters and 70 distribution circuits. AEP Ohio implements smart grid technology over 58 13kV circuits from 10 distribution stations and 12 34.5kV circuits rom six distribution stations. Included in this project is a redistribution management system, integrated volt-VAR control, distribution automation, advanced meter infrastructure, home area networks, community energy storage, sodium sulfur battery storage, and renewable generation sources. These technologies are combined with two way consumer communication and information sharing, demand response, dynamic pricing, and	https://smartgrid.gov/sites/default/files/doc/files/Smart_Meters_First_Step_into_Tomorrow_201007.pdf https://www.aepohio.com/global/utilities/lib/docs/save/gridsmartphase2/FAQs.pdf http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-23192.pdf http://energy.gov/sites/prod/files/15_Recovery_Act_AEP_Ohio_gridSMARTSM_Demonstration_Project.pdf http://www.gridsmartohio.com/docs/AEPohioGridSmart_CommunityEnrichment.pdf

				consumer products, such as plug-in hybrid vehicles.	
Enhanced Distribution and Demand Management Regional Demonstration	USA		started: 2010; completed: August 2014	Swiss Federal Office of Energy SFOE"	This project demonstrates smart grid technologies with 27 cooperatives in 11 states. NRECA conducted studies in advanced volt/volt-ampere reactive for total demand; generation and transmission-wide (G&T) demand response over advanced metering infrastructure (AMI); critical peak pricing over AMI; water heater and air conditioning load control over AMI; advanced water heater control; consumer Internet energy usage portal pilots; consumer in-home energy display pilots; time-sensitive rates pilots and self-healing feeders for improved reliability.	http://energy.gov/sites/prod/files/20_Recovery_Act_Enhanced_Demand_and_Distribution_Management_Regional_Demonstration.pdf https://www.smartgrid.gov/sites/default/files/pdfs/project_desc/OE0000222_NRECA_Fact%20Sheet_3.0_0.pdf

Table 3 includes a summary of European and International Smart Grid projects with a broader focus.

Table 3: Additional Smart Grid research projects

Long title	Countries	Short title	Project Status	Partners	Abstract	Contact
EcoGrid	DK		In operation since 2011	Energienet.dk, SINTEF, Oestkraft, DTU, IBM, Siemens, landys+gyr, elia, eandis, ttu, ecn, tno, edp, tecnaliam AIT	The objective of the EcoGrid EU project is to illustrate that modern information and communication technology (ICT) and innovative market solutions can enable the operation of a power system with more than 50% renewable energy sources (RES) such as wind, biomass and photovoltaic (PV).	http://www.eu-ecogrid.net/
Smart Area Aachen	DE		Various steps until 2016	STAWAG, ABB, FGH, TU Dortmund, FGH, Nexans, IFHT (RWTH), MR, SAG, Kisters, VDE|DKE, BET, PSI, IAEW (RWTH)	Smart Area Aachen develops new holistic concepts and methods based on new equipment for future smart grid solutions. In this context, innovative technical solutions are identified, optimised and eventually verified in pilot trials. Moreover, new business models are developed for the different stakeholders and harmonisation aspects are addressed in accompanying standardisation activities.	http://smartarea.de/verbundprojekte/kommunikation/ http://www.eneff-stadt.info/fileadmin/media/News/Dateien/Vortraege_Kongress_2014/TOP_11-4_Nolde_SmartArea.pdf http://www.berliner-energietage.de/fileadmin/user_upload/2014/Tagungsmaterial/Vortragsfolien/Berliner_Energietage_2014_VA_1.04_7_Zimmer.pdf http://www.bine.info/themen/energiesysteme/news/smart-grid-im-modellversuch/?type=123&filename=Smart%2520Grid%2520im%2520Modellversuch&cHash=803223cd48f76cd2c89ec519826ae827

Stockholm Royal Seaport – Urban Smart Grid	SWE		completed: 2011	"ABB, Fortum, KTH, Ericsson, Electrolux, Interactive Institute	The pre-study for Stockholm Royal Seaport - an urban smart grid area, delivers a concept description including market models and description of technical solutions ready for implementation and testing as a new project phase.	https://www.energimyndigheten.se/Global/Forskning/Kraft/NDS%20f%C3%B6rstudie%20ENG%20final%20_public.pdf
Flexible Approaches for Low Carbon Optimised Networks	GBR	FALCON	started: 2011 (bis Sept. 2015)	NCC, HSB, JM, ByggVesta, Stockholm Hamn"	Project FALCON aims to investigate how new 11 kV network techniques work in practice and, by simulating their use in different scenarios, will determine the best ways to manage the network problems expected to arise from increased low carbon technologies and generation.	http://www.westernpowerinnovation.co.uk/Falcon.aspx http://www.westernpower.co.uk/docs/Innovation-and-Low-Carbon/Falcon-Customer-Data-Protection-Plan-v1-20121213.aspx
Ontario Smart Meter Initiative	CAN		In operation since 2008	Western Power Distribution, Thameswey Energy	Smart meters are installed in residences and small businesses across Ontario along with a "time-of-use" electricity price structure. A smart meter system opens up the opportunity for new kinds of conservation and demand management programs. In the future, smart meters could allow the introduction of different time-based incentive programs, or the opportunity to control energy use through energy management devices or smart appliances. Smart meter data also provides comprehensive, detailed information for electricity system planning, allowing us to identify where future generation, transmission and distribution investments are required. Time-of-use pricing encourages Ontarians to shift some electricity use to offpeak hours. The aim is to lower peak demand and lowering costs for all Ontarians.	http://esr.degroote.mcmaster.ca/documents/1A-1.pdf
Puducherry	IND			"Ontario Smart	Pilot covers 87,031 no. of consumers with dominant being domestic consumers. The module of	http://electricity.puducherry.gov.in/css/smart%20grid.pdf http://www.pace-

				Metering Initiative (SMI), Ontario Ministry of	automated metering infrastructure (AMI) for residential consumers and industrial consumers is proposed to be implemented to assist with consumer issues like event management & prioritising, billing cycle review and revenue collection efficiency for energy auditing and AT&C loss reduction. The AMI system shall aid in knowing real time energy input from DT as well as energy consumption by consumers that can instantly help to know losses in the system. Common Meter Data Management System is proposed that shall take data from MDMS of different meter manufacturer/solution provider and integrate the information for use. The pilot project also proposes developing a mature model of "time of use tariff and net metering."	d.com/wp-content/uploads/2014/04/Puducherry-Smart-Grid-Pilot-Project-PowerGrid.pdf http://www.kalkitech.com/wp-content/files/CS_%20Enabling%20the%20Smart%20Grid%20in%20India-Puducherry%20Pilot%20Project.pdf http://www.npti.in/Download/Distribution/Article%20on%20Smart%20Grid%20Pilot%20Project%20in%20India.pdf
Presentation of Energy Usage Information (Smart Billing, Mandated In Home Display and Customer Web Interface)	IRL		started : 2007	Energy and Infrastructure, Ontario Energy Board, Measurement Canada, "	The project assesses: the impact of Time of Use pricing and billing/information stimuli on the customer behaviour; and the available technologies for AMI roll out in an Irish context. The outcomes of both are factored into the cost benefit analysis for the full roll out of AMI in Ireland.	http://www.cer.ie/docs/000117/cer13164-presentation-of-energy-usage-information.pdf http://www.cer.ie/docs/000117/Smart%20Metering%20High%20Level%20Design%20Proposed%20Decision%20(CER13286).pdf
Open real-time distribution grid control system	CH	GridBox			GridBox proposes a novel grid management system which provides solutions to the new energy system requirements for handling the growing infeed of distributed electricity generators (PV, wind, CHP, biomass), the increased flexibility of active electricity consumption and the use of distributed storage. GridBox provides a strongly coordinated, distributed, low cost, small form factor solution for	http://download.nachhaltigwirtschaften.at/edz_pdf/events/20140522_sgw14_poster_25_gridbox_open_real-time_distribution_grid_control_system.pdf

					guaranteeing a secure operation of the distribution grid while at the same time allowing (local) market participation also for prosumers, i.e. consumers with their own electricity generation and storage. GridBox is adaptable and open to new grid technology and business models.	
Stockholm Royal Seaport – Urban Smart Grid	SWE		completed: 2011	CER	The program specifies, develops, tests and evaluates both business and market models, new technical solutions and concepts, information and communications technology (ICT) as well as aspects of data security. The first phase of the program and this application is focus on scenarios related to active end-customers and reliability of the future grid, where the urban smart grid in a new way creates opportunities for interaction with the end customer. Also, scenarios for increased reliability and availability in a future urban smart grid are tested.	https://www.energimyndigheten.se/Global/Forskning/Kraft/NDS%20f%C3%B6rstudie%20ENG%20final%20_public.pdf
A report on the economic benefits of smart grid	UK		completed: 2012	Ernst & Young	Understanding the full economic case for smart grid is therefore vital and it is why we commissioned Ernst & Young to work with SmartGrid GB to develop this report. We want a better understanding of what the advantages would be for Britain if we pushed ahead with smart grid development and what will be needed to make it happen.	https://www.smartgrid.gov/sites/default/files/doc/files/Smart_Grid_Race_Worth_Winning_Report_on_Economic_Benefits_201209.pdf

6   Regional Smart Grid-related Research Projects

The following section includes a set of regional Smart Grid research projects whose focus is broader than in terms of security relevance. They are largely based on work by Kollmann et al. (2015) and allow an insight into the European smart grid research landscape.[3]

These projects are only partly related to security aspects, but nevertheless shed some light on the research activities in this highly dynamic research area. Table 4 presents the summary of regional research with regards to Smart Grid technology and also includes research projects with direct involvement of EI-JKU.

Understanding the involvement of national and regional governments in Smart Grid and cyber security related projects helps fine tune research questions to the end-user level. In accordance with the WP management in SPARKS this is done by involving stakeholders from a variety of research and business activities to mutual workshops and events. The following list includes a set of mostly German and Austrian activities with direct involvement of SPARKS partners and the objective to include them into the stakeholder process in the SPARKS.

---

[3] Work in this area was mainly done as part of the ISGAN work group (Kollmann et al., 2015).

Table 4: Regional Smart Grid Projects

Long title	Countries	Short title	Project Status	Partners	Abstract	Contact
Smart Grids Modellregion Salzburg - Consumer to Grid	AT	SGMS-C2G	completed: 2012	Salzburg AG für Energie, Center for Usability Research & Engineering (CURE); TU Wien – ICT; AIT; Salzburg Wohnbau GmbH	This study examines how information about potential energy savings is best presented to consumers in order to reduce energy consumption in a smart grid. C2G focuses on basic research, which investigates whether, how, when and which feedback to consumers is required to save energy. The feedback should also take account of a social, demographic and cultural background.	http://www.smartgridssalzburg.at/fileadmin/user_upload/downloads/C2G_Endbericht.pdf
Smart-Efficiency - CO2-Reduktion auf Basis automatisierter Effizienz- und Energieanalyse für Haushalte mit Hilfe von Smart Metern	AT	Smart Efficiency	completed: 2012	TU Graz Institut für elektrische Anlagen	The aim of this project is to develop a method for automated energy analysis; the consumer provides a visually processed method for power consumption reduction, evaluation and monitoring.	http://www.energieinformatik2012.org/docs/pt/Praesentation_Meisel_EI2012.pdf
Schlüsselfaktoren für einen effektiven und akzeptablen Einsatz von Smart Meters	AT	Smart New World	completed: 2012	IIFZ; Austrian Academy of Science ÖAW; ITA;, e-commerce monitoring GmbH	The project team develops scenarios for a successful and acceptable introduction of smart meters. For this, a participatory process is designed with the involvement of various stakeholder groups.	http://noest.line.at/news/docs/28620_Smart_New_World_Energy_Lunch_27-10-2011.pdf
Persusasive End-User	AT	PEEM	completed: 2012	CURE; University	The objective of the proposed PEEM Project is to research and develop new strategies and tools	http://www.smartgridssalzburg.at/fileadmin/user_upload/downloads/PEEM_Endber

Energy Management				Salzburg - (ICT&S Center); Salzburg AG	for the home context that provide energy-saving related feedback in a persuasive and unobtrusive way and thereby have the potential to help to reduce energy consumption without loss of comfort. Tailored persuasive approaches overcoming limitations of existing solutions are developed, prototyped and experimentally validated with real user in realistic long-term settings.	icht.pdf
Energieabrechnungs-Optimierung zur Endverbraucher motivation	AT	e-Motivation	completed: 2012	Energieinstitut an der JKU Linz; Forschungsgruppe Energie- und Kommunikationstechnologien EnCT GmbH	Innovative energy bills based on intelligent measurement and counting systems (Smart Billing) can motivate the end users to an efficient and climate-friendly energy use. The project e-MOTIVATION examines and tests for which energy sources innovative payment systems are useful as an efficiency point of view as optimal as possible billing system should look like, what energy savings can be achieved and what is needed in order to involve energy suppliers, equipment manufacturers and enhanced consumers behaviour.	http://www.energyefficiency.at/dokumente/upload/Endbericht_E-Motivation_Energieinstitut_EnCT_November_2011.pdf http://www.energyefficiency.at/index.php?menuid=2&downloadid=164&reporeid=22 http://www.energyefficiency.at/index.php?menuid=1&downloadid=151&reporeid=58
Entwicklung Pilot Smart Metering Privatkunden & Gewerbe und monatliche Abrechnung	AT	Smart Metering HH IND	completed: 2011	EVN; Austrian Energy Agency (AEA)	In this pilot project, smart meters are installed in about 300 households, service companies and public buildings. It examines how a smart metering system shall be designed that is accepted by the end customer and can lead to an efficient change in energy-related behaviour	EVN AG https://www.klimafonds.gv.at/foerderungen/gefoerderte-projekte/detail/?plistcall=1&pid=182781&merken=1
Entwicklung eines zentralen Visualisierungsgeräts für den Energie- und	AT	ZENVIS	completed: 2009	ÖGUT; Die umweltberatung; VKI;, Gemeinnützige Industrie	The research project provides information on whether a central display unit of energy demand can serve an effective tool for reducing energy consumption.	http://www.oegut.at/downloads/pdf/ZENVIS-Endbericht.pdf

Ressourcenverbrauch in Haushalten				Wohnungs AG (GIWOG)		
Inwieweit vermögen Smart Grids die wirtschaftliche Entwicklung ländlicher Regionen zu stärken?	AT	INSPIRED Regions	completed: 2012	Pöyry Energy GmbH; Österreichisches Institut für Raumplanung (ÖIR)	The research project determines the potential impact of "smart grids" in the economic development of rural regions of Austria.	http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/reports/endbericht_201413_smart_grids_inspired_regions.pdf http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/events/20140311_fti_smartgrids2020_expws_smarte_energie_regionen_03_kropiunigg_etal.pdf
Smart Grids Modellregion Salzburg – Building to Grid	AT	SGMS-B2G	completed: 2013	Salzburg AG; AIT; Salzburg Wohnbau; TU Wien; Siemens AG	The project assess how and to which extent the intelligent and collaborative integration of buildings into the smart grid infrastructure can reduce load peaks, mitigate problems in the power grid and enhance energy efficiency?	http://www.smartgridssalzburg.at/fileadmin/user_upload/downloads/Endbericht_Building_2_Grid.pdf
Integral Resource Optimization Network Concept	AT	IRON Concept	completed: 2008	TU Wien; - Institut für Computertechnik	The project investigates who an integral automation infrastructure for a more efficient use of the resource "electrical energy" ought to be conceptualised. It provides a concept for new, innovative services based on the use of the latest developments of modern information and communication technologies.	http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/reports/endbericht_201413_smart_grids_inspired_regions.pdf http://www.nachhaltigwirtschaften.at/e2050/e2050_pdf/events/20140311_fti_smartgrids2020_expws_smarte_energie_regionen_03_kropiunigg_etal.pdf http://www.salzburg-ag.at/?eID=download&uid=1379
Smart Response - Demand Response for Austrian Smart Grids	AT	Smart Response	completed: 2013	TU Wien Institut für Computertechnik (ICT)	The project aims to conduct a critical analysis of consumption oriented energy management solutions. The focus of analysis will be consumer-side energy management and its potential to contribute to overall energy efficiency of future smart grids in the best possible way.	http://link.springer.com/content/pdf/10.1007%2Fs00287-012-0667-7.pdf http://www.researchgate.net/profile/Marcus_Meisel/publication/257394211_Erfolgsversprechende_Demand-Response-Empfehlungen_im_Energieversorgungssystem_2020/links/00b4952f89c8fcdf11000

						000 http://www.energieinformatik2012.org/docs/pt/Praesentation_Meisel_EI2012.pdf
The potential of smart meter enabled programs to increase energy and systems efficiency: a mass pilot comparison	FI	Empower Demand	completed; 2011	VaasaETT, Global Energy Think Tank	Analysis of case studies in various countries The aim of the research whose results are presented in this report are to discover the potential and limitations of a range of feedback and dynamic pricing programs enabled through smart metering technologies.	VAASA, http://smartgridcc.org/resauth/vaasaett
Blackouts in Österreich, Teil 1 und Blackoutprävention und -intervention	AT	Black Ö.1 Black Ö.2.	2011-2015	Energieinstitut an der JKU Linz; TU-Wien; Linz Strom Netz GmbH; WIEN ENERGIE Stromnetz; APG; IV; WKO; BKA	„Blackouts in Austria" analyses the economic and social consequences of large-scale blackouts within the Austrian electricity network. The aim of the project is to create a comprehensive database which provides a basis for political decision concerning infrastructure, economics and security (Part I) and to develop strategies to ensure the current level of security and for the prevention of large-scale blackouts in Austria.	http://www.energyefficiency.at/dokumente/upload/Endbereicht-Blackoe_e544f.pdf http://www.prokamin.at/fileadmin/PROKAMIN/downloads/Kampagne-Sicherheitskamin/Dokumente/Studie-JKU-Blackouts-in-Oesterreich.pdf
Guidelines for conducting a cost-benefit analysis of Smart Grids projects	EU		completed: 2012	European Commision, Joint Research Centre	The recent EC Communication on Smart Grids [EC 2011a] explicitly states that the Commission intends to come up with guidelines on the CBA to fulfil the provisions in Annex I of Directives 2009/72/EC and 2009/73/EC for roll-out of smart metering systems. In a second step, the Commission also intends to release guidelines for a CBA for the assessment of smart grid deployment.	http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20120427_smartgrids_guideline.pdf

7 Overlap with existing projects

A selection of the presented projects investigates similar research questions, though differences in the geographic focus, the project's scope and time dimension exist. As regards the possible interaction with other research groups, particularly strong ties exist with SEGRID and HyRim, which is coordinated by AIT as well.[4]

In terms of similarities of research objectives/approach, SoES and VIKING included relevant research for SPARKS. Interaction with the key researchers has been fostered so as to make sure that relevant information is shared across different research projects. SPARKS is actively pursuing the connection with projects which aim to address critical infrastructure aspects. This is the case for instance for the CRISALIS project.

The summary provided in Table 5 includes a – personal – interpretation of connections between the analysed projects with SPARKS in terms of various attributes. This helps to obtain a better picture of the research landscape and ensures the appropriate interpretation of merits and limits of each projects included in the list. The – qualitative – assessment is based on a 1-10 scale with the latter being the highest figure the relevant attributes.

---

[4]A particular presentation of this project is available upon request; it is related to Sparks however and thus to be mentioned in addition to the presented projects.

Table 5: Summary of project connection to SPARKS, personal interpretation of project highlights

Project/Category	Project runtime (in years)	Research on Cyber Security and Privacy (index 1-10)	Partner structure (number of partners)	Partner structure overlap (number of partners in both consortia)	Budget compared to SPARKS (in % of total budget not restricted to funding)
SPARKS	3	9	9	-	100%
CIPRNet	4	7	12	0	53%
VIKING	3	3	7	1	1109%
Grid4EU	5	2	6+21	0	65%
CRUTIAL	3	5	6	0	11%
SoES	2	5	4	0	101%
SmartC2Net	3	6	7	0	88%
C-DAX	3	6	9	0	24%
SG²	2	7	9	2	16%
CIIS	2	6	7	0	162%
DISCERN	3	5	11	1	53%
CRISALIS	3	7	9	0	109%
SEGRID	3	6	10	0	62%
AFTER	3	5	13	0	103%
HyRiM	3	7	7	1	96%

Figure 1 presents the interaction and overlap of SPARKS with the projects presented. The budget of Grid4eu is more than 10 times larger that of SPARKS and is thus omitted from the graphic due to enhanced readability. Interestingly, though some differences with regards to the presented characteristics exist, the majority of research projects are comparable in terms of "technical" attributes such as runtime, budget and partner structure. The interpretation of "Research on Cyber Security and Privacy (index 1-10)" is based on a qualitative – and personal – of interpretation of the contents.
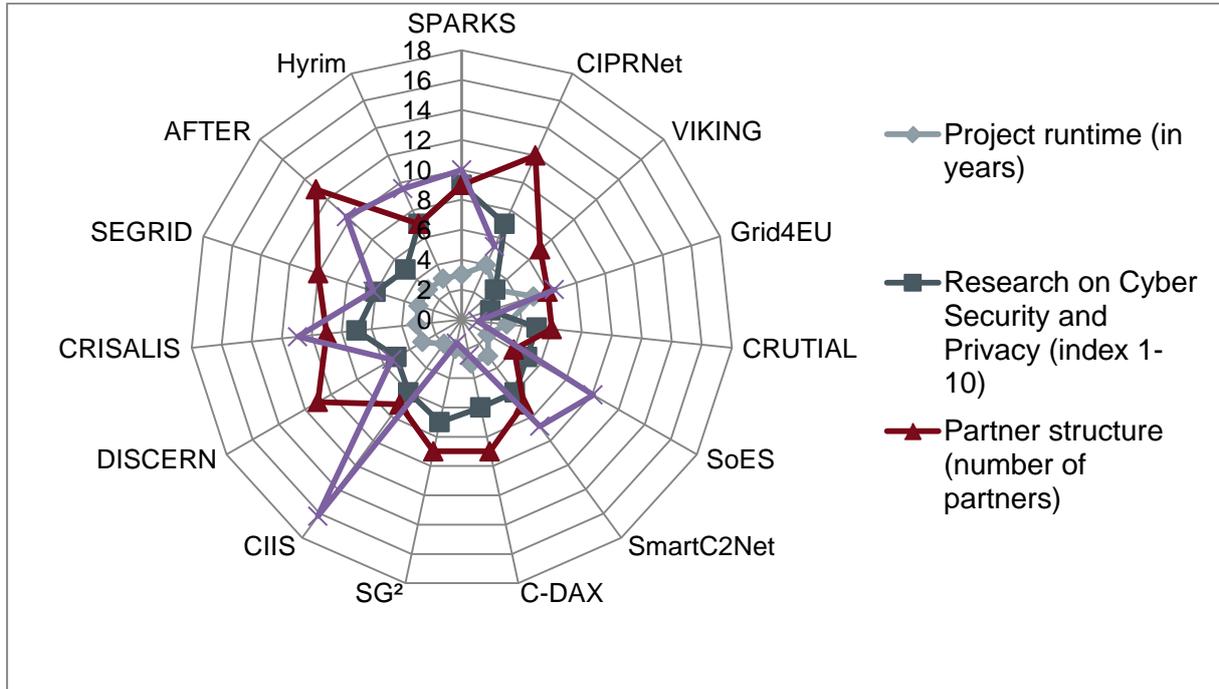
Figure 1: Summary of relevant projects' interaction with SPARKS

As presented in the three subsections on international, EU funded and national/regional projects, including stakeholders at various levels is paramount in order to ensure that the outcomes of SPARKS are perceived at different levels of policy as well. Thus, the overlap with other projects – while being limited to specific aspects of Smart Grid and cyber security technology is a chance to bringing together researchers from various backgrounds.

In addition to the presented research activities here, milestone projects such as Grid4EU are important with regards to the research carried out in SPARKS. Though being different in scope and size, overlap in various areas exists. For instance this is the case regarding ongoing activities around security and privacy related research questions. Overall the exchange of mutually relevant activities is important for a variety of reasons, which SPARKS aims to support in a best possible manner.

8 Conclusion and Synopsis

This report presents major activities of SPARKS to engage, interact and exchange with other related research projects and activities in the field of smart grid technologies. To this end, a survey was conducted in collaboration with the SEGRID project. It was enriched by a literature based review of existing scientific activities in the field of Smart Grid security and privacy. Information was mainly gathered from project websites and official funding bodies.

Overlap with other – mainly EU funded – projects exist, though the focus of SPARKS is unique in the sense that technical, social and legal aspects of Smart Grid Security and Privacy initiatives are considered in conjunction.

This is relevant as the best technological solutions remain academic if the acceptance of the public or the legal frameworks needed to implement them are missing. The outlined approach of SPARKS incorporates these important aspects and provides a highly valuable contribution of how to make the future Smart Grid safe, accepted and well established in European and national legislation.

In addition to the assessment of related projects, SPARKS has been actively engaging with the running projects with related emphases. Thus, this report helps the interested reader to obtain a fuller picture of present and past research activities. The main finding is that the existing research landscape shows a great variety. Projects as well as consortia and funding differ significantly among projects. In terms of making best use of available funds, it is important to enhance the outreach activities to existing projects and consortia also with special regard to the maximisation of SPARKS' impact.

9 Outlook and Future Research

Currently, various smart grid technology aspects are intensively researched. The fact that different emphases are being pursued brings about the possibility of parallel activities and loss of efficiency. A comprehensive assessment of conducted work is needed. This deliverable aimed at shedding some light on different approaches, but can only initiate a broader debate.

In the future, a stronger interconnection between different research entities and projects is desirable which can among others foster collaboration and enhance efficiency in the European smart grid research landscape.

While being desirable, it remains difficult to interconnect national research agendas with European funded projects. Though major funding authorities very actively pursue the internationalisation of their national research areas, it remains unclear how the needed interconnection and collaboration can be enhanced.

10 References

Anonymised personal communication with stakeholders and survey during the SPARKS project

Kollmann et al (2015). Project excerpt from ISGAN working group, available online in March 2015.

11 Appendix

This section contains the questionnaire as it was used during the empiric assessment which led to the development of this report.

Questionnaire Smart Grid Security & Privacy

Please return the completed questionnaire by e-mail **by 30 November 2014**

Contact details:
Institution/company: Energy Institute at the Johannes Kepler University
Contact: Schmidthaler Michael, Dr., Reichl Johannes, Dr.
Address & country: Altenberger Strasse 69 ; 4040 Linz, Austria
Phone: +43 732 2468 5665
E-mail: Schmidthaler@energieinstitut-linz.at
Website: www.energieinstitut-linz.at

> First of all I want to thank you very much for your participation in this research project.
>
> Please bear in mind that the aim of this research is to create a review of the major literature/projects in the field of the security & privacy of smart grids and electricity supply security in Europe.
>
> Please send us information about all relevant projects you have done or collaborated. A section is defined below with associated points and boxes to be filled in. Please send us several of this form (one per project) and if available additional information/reports.
>
> **We thank you for your cooperation!**

Project title (e.g. SG Essences - Elaborated Assessment of Competing Smart Grid Solutions)

Long title (e.g. Elaborated Assessment of Competing Smart Grid Solutions)

Short title (e.g. SG-Essences)

Country (e.g. Austria or European Union)

Project status (e.g. Started: 2009, ~~In Progress~~/Finished: 2012)

Started: In Progress/Finished:

Project Consortium (<u>e.g.</u> Energieinstitut an der JKU Linz,…)

Project Type (report, <u>research project</u>, <u>field test</u>,…)

☐ report   ☐ research project

☐ field test   ☐ …………………

Research issues, goals, ideas and visions (<u>e.g.</u> The Smart Grid valuation is based on technical ecological and economic…)

Project link, Homepage (<u>e.g.</u> http://www.nachhaltigwirtschaften.at/e2050/e2050-_pdf/reports/endbericht_201420_sg_essences.pdf)

Project costs and EU funding (only used for aggregation purposes in terms of SG-, privacy- and security-related research in the EU).