FP7 Grant Agreement N° 607109

Security for smart Electricity GRIDs

D6.3 Report on dissemination activities

Due date of deliverable: 01/10/2016
Actual submission date: 30/09/2016
Workpackage: WP6 Dissemination
Number of pages: 15
Revision: Version 1
Classification level: Public

Project type:	Collaborative project – small or medium scale focused research project
Thematic Priority:	FP7-SEC-2013-1
Start date of project:	October 1st, 2014
Duration:	36 months

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

Author(s)	Reinder Wolthuis (TNO)
Contributor(s)	Frank Fransen (TNO) Rolf Blom (SICS) Mathias Ekstedt (KTH) Antonio Silva Moriano (INCODE) Maarten Hoeve (ENCS) Sander Kruese (Alliander) Gunnar Björkman (ABB) Nuno Neves (FFCUL) Nuno Medeiros (EDP) Exabier Bilbao Hernández (ZIV)

TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 4
1.1 The SEGRID Project 4
1.2 Work Package 6 : Dissemination 5
1.3 Deliverable D6.5: second report on dissemination activities 6
2 DISSEMINATION INSTRUMENTS 7
2.1 SEGRID website 7
2.2 SEGRID Advisory Board (SAB) 7
2.3 SEGRID white paper 7
2.4 Combined CPSR- SG 2016 workshop with SPARKS and SALVAGE 8
2.5 SEGRID presentations 9
2.6 Journals and magazines 10
2.7 SEGRID gadgets 11
2.8 SEGRID banner 11
2.9 Planned events 12
3 SEGRID LIAISON ACTIVITIES 13
3.1 EU projects 13
3.2 Standardisation bodies 13
4 DISSEMINATION TO TARGET GROUPS 13
4.1 General public 13
4.2 Policy makers and national CERTs 14
4.3 Security research community 14
4.4 Standardization bodies 14
5 CONCLUDING REMARKS 15

1 Introduction – Rationale of this document

1.1 The SEGRID Project

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. In the coming years, the level of automation in electricity distribution grids will grow substantially. Smart meters will be deployed at home premises, and remote terminal units (RTUs) will be placed in distribution substations. The increased automation should provide a better view of how electricity flows to the medium and low voltage grids, and provide grid operators increased control to influence that flow. But the increased automation also has major consequences for the cyber security posture of the electricity grid. By nature, automation adds new attack vectors through which cyber attackers can enter and attack the networks of grid operators, and offers other possibilities to cause physical damage to the electricity grid itself. Moreover, there is an increased risk of physical damage to the electricity grid due to inadvertent events in the cyber domain of Smart Grids (e.g. malware, technical dependencies, and human errors).

From a technical point of view, it is not sufficient to only consider all the different components in a Smart Grid separately; they will together form a truly integrated system-of-systems and the Smart Grid will neither be completely owned, nor completely controlled, by a single power system operator. There will be many Smart Grid services and components that are operated by other organisations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new methods for connecting with various Smart Grid applications using a diverse set of communication channels, such as local connection interfaces, distributed web access, and smart apps on smart phones. A number of new cyber security issues become critical in this context.

This new utility-wide system(-of-systems) will not come into existence overnight; the Smart Grid will be composed of a mix of old, even legacy, and new components. Therefore, we look upon the Smart Grid as a gradually evolving system in which new functionalities are added to accommodate new use cases with the challenge to maintain security, privacy and dependability of the Smart Grid as a whole. The required security solutions to cope with this situation range from improvements in current security, privacy and operational solutions and procedures to the introduction of new security and privacy paradigms.

The term 'Smart Grid' is used for a wide variety of developments related to the automation of electricity grid. Focusing on the efforts of the project, SEGRID will work on five concrete use cases, shown in Figure 1. These have been further elaborated in the deliverable D1.1 of the project. The five SEGRID use cases are:

1. Smart meters used for on-line reading of consumption and technical data;
2. Load balancing renewable energy centrally;
3. Dynamic power management for smart homes, smart offices, and electric vehicles;
4. Load balancing renewable energy regionally (substation automation);
5. Automatic reconfiguration of the power grid.

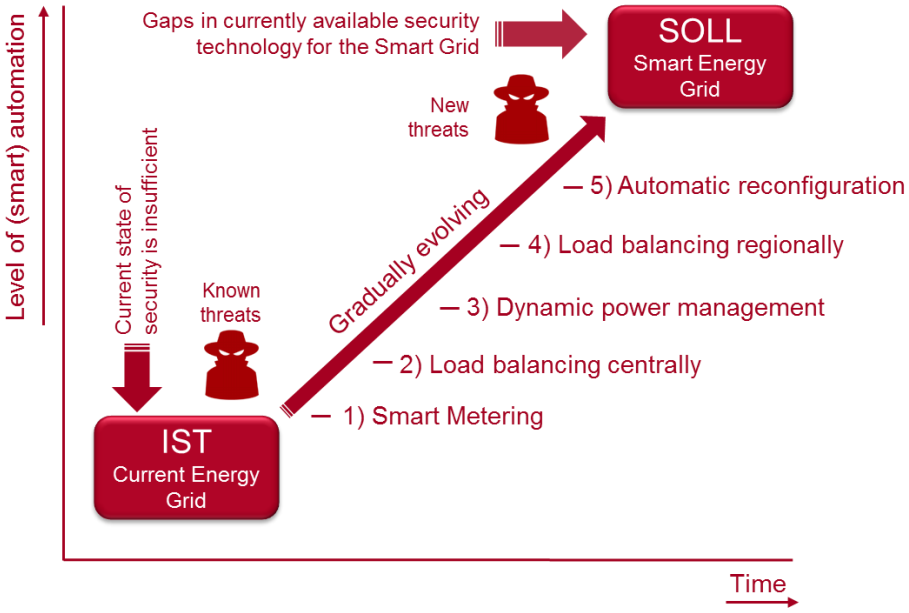

Figure 1: SEGRID storyline

The SEGRID use cases reflect important steps of Smart Grid developments until 2020 and beyond, and will cover the most relevant security and privacy issues that will arise from the increasing complexity of Smart Grids.

SEGRID will formulate privacy and security goals for the use cases defined (WP1) and perform a risk analysis of these use cases (WP2). Vulnerability assessment frameworks and tools to identify these risks in real systems will be developed (WP3) and gaps in the currently available security solutions will be identified (WP2). Solutions for some of these gaps will be developed in WP4. Selected vulnerability assessment tools and novel security solutions will then be tested in SITE (WP5).

1.2 Work Package 6 : Dissemination

The SEGRID dissemination objectives are:

- To inform the user community, involving citizens, companies and public authorities about developments in the protection of Smart Grids.
- To raise awareness among all relevant stakeholders (e.g. policy makers, regulatory bodies, utility companies and Smart Grid equipment manufacturers) of the risks of cyber-attacks on Smart Grids and how to addresses these risks;
- To develop the SEGRID Smart Grid security white paper composed of project results specifically targeted to raise awareness among policy makers and higher management of stakeholders;
- To organise and/or publish results in international event(s) to inform the scientific and business community (i.e. utility companies and Smart Grid equipment manufacturers) as well as policy makers and decision makers about the project, its goals and achievements and to gather valuable information on related issues;
- To develop and implement an interactive and user friendly web site to inform the general public and relevant stakeholders about the project;

- To produce an exploitation plan which will include a list of opportunities that arise from the project's achievements and a detailed analysis of benefit and impact for the consortium as a whole as well as for the results of individual participants.

SEGRID dissemination activities are conducted in Work package 6.

1.3 Deliverable D6.5: second report on dissemination activities

This report lists the dissemination activities that have been carried out in the second year of SEGRID.

Section 2 describes the use of the SEGRID dissemination instruments. Section 3 describes the SEGRID liaison activities. Section 4 describes the dissemination to specific target groups, while some concluding remarks are made in section 5.

2 Dissemination instruments

2.1 SEGRID website

The SEGRID website (www.segrid.eu) is the general communication channel for SEGRID. The website shows general information of the SEGRID project, the project approach and its partners. The (non-classified) deliverables that are finished were published on the website and the website has been kept up-to-date with the project activities and results. Several requests have already been made through the website contact mechanisms (mail, phone number).. Recently we have a implemented a new release to facilitate the information provisioning and registration for the SEGRID workshop. See Figure 2 for an impression of the website

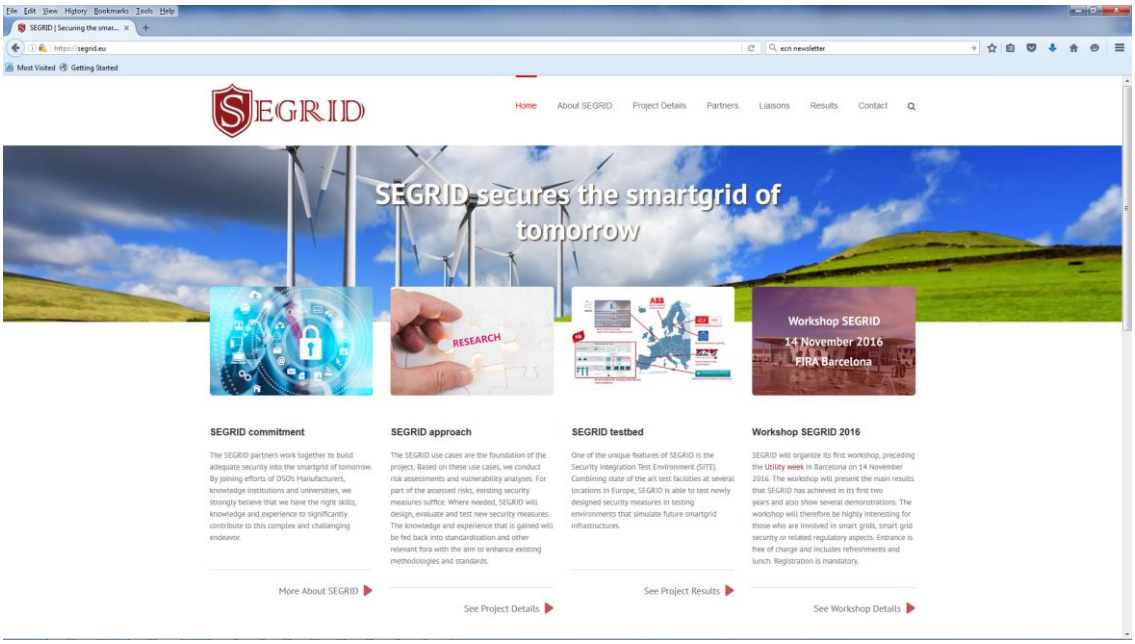

Figure 2 – SEGRID website

2.2 SEGRID Advisory Board (SAB)

The SEGRID Advisory Board (SAB) is an independent proactive review group of external experts within the areas of IT security, privacy and power system control that will review the SEGRID technical direction, assumptions, progress, and deliverables. SEGRID has organized the second SAB meeting in Lisbon on March 8th 2016. Two members were present and the other members were informed of the results afterwards. SEGRID presented the current status and plans to the SAB members and the SAB commented on these and provided valuable feedback to the project.

2.3 SEGRID white paper

The SEGRID white paper originally was planned to be delivered on October 1st, 2016. With approval of the PO, this date was postponed to December 31st 2016, in order to be able to include the results of deliverables that were due on October 1st 2016.

2.4 Combined CPSR- SG 2016 workshop with SPARKS and SALVAGE

The three projects SEGRID, SPARKS and SALVAGE have organized a joint workshop preceding the CPS week in Vienna, April 12th 2016: *The Joint International Workshop on Cyber-Physical Security and Resilience in Smart Grids: CPSR-SG 2016*. The organization of the workshop was facilitated by the CPS week organization. Program chairs were the coordinators of the three projects and a program committee was formed from the people of each of the three projects. See Figure 3 for the workshop agenda. And Figure 4 for a workshop impression.

7:45-8:15	Registration
8:15-9:30	8:15-8:30 Opening: Johannes Fröhlich, TU Wien Rectorate 8:30-9:30 Keynote: Rajeev Alur
9:30-9:45	Coffee Break
9:45-10:00	Anna Magdalena Kosek, Reinder Wolthuis and Paul Smith. *Welcome to the Joint International Workshop on Cyber-Physical Security and Resilience in Smart Grids: CPSR-SG 2016*
10:00-12:00	Paper Session I (Chair: Anna Magdalena Kosek) **10:00-10:30** Judith E. Y. Rossebø, Frank Fransen and Eric Luiijf. *Including Threat Actor Capability and Motivation in Risk Assessment for Smart Grids* **10:30-11:00** Rikard Blom, Matus Korman, Robert Lagerström and Mathias Ekstedt. *Analyzing Attack Resilience of an Advanced Meter Infrastructure Reference Model* **11:00-11:30** J.K. Wang and Christian Moya. *Attack Path Reconstruction from Adverse Consequences on Power Grids- with a focus on Monitoring-Layer attacks* **11:30-12:00** Tudor B. Ionescu and Gerhard Engelbrecht. *The Privacy Case: Matching Privacy-Protection Goals to Human and Organizational Privacy Concerns*
12:00 - 13:30	Lunch
13:30 – 14:15	*Cyber Security Landscape from a Vendor's Perspective* Bart de Wijs (Head of Cyber Security at ABB b.v. from Power Grids Division)
14:15 – 15:45	Paper Session II (Chair: Paul Smith) **14:15-14:45** Robert Czechowski and Anna Magdalena Kosek. *The Most Frequent Energy Theft Techniques and Hazards in Present Power Energy Consumption* **14:45-15:15** Rajesh Kavasseri, Yinan Cui and Nilanjan Ray Chaudhuri. *A Supervisory Approach towards Cyber-Secure Generator Protection* **15:15-15:45** Justyna Chromik, Anne Remke and Boudewijn R. Haverkort. *What's under the hood? Improving SCADA security with process awareness*
15:45 - 16:00	Coffee Break
16:00 - 18:00	Paper Session III (Chair: Reinder Wolthuis) **16:00-16:30** Anibal Sanjab and Walid Saad. *On Bounded Rationality in Cyber-Physical Systems Security: Game-Theoretic Analysis and Application to Smart Grid Protection* **16:30-17:00** Jin Wei and Gihan J. Mendis. *A Deep Learning-Based Cyber-Physical Strategy to Mitigate False Data Injection Attack in Smart Grids* **17:00-17:30** Anna Magdalena Kosek. *Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model* **17:30-18:00** Volker Turau and Christoph Weyer. *Cascading Failures Caused by Node Overloading in Complex Networks*

Figure 3 – Agenda of joint workshop at CPS week

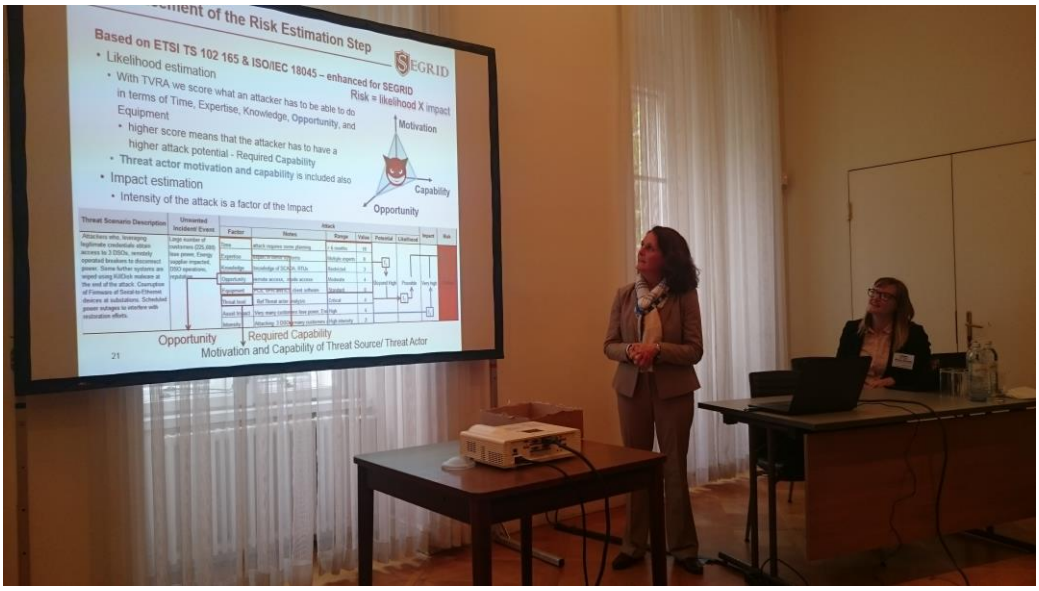

Figure 4 – Judith Rossebø (ABB) presenting at the CPS –SG-2016

A total of 15 submitted papers were each reviewed by three members of the program committee and 11 were accepted, of which two from outside Europe. Bart de Wijs of ABB was invited to provide a keynote speech. The workshop was a great success. It was attended by quite some people during the day and there were some very good discussions. All presentations and papers were distributed to the conference attendants on a USB stick.

The accepted papers will be published by IEEE, in the IEEE Conference Publication Program (CPP).

2.5 SEGRID presentations

SEGRID members have given presentations on the project at the following conferences:

- Presentation of SEGRID and member of panel discussion (Reinder Wolthuis) on a workshop called 'Talking Smart Grids' on Cybersecurity in Electricity Distribution Grids, 15 October 2015 in Brussels. A joint initiative from EURELECTRIC and the IEA.
- Summarizing the SEGRID project and the addressed work domains at the 2nd Stockholm international summit on cyber-security in SCADA and Industrial Control Systems, (4SICS), October 20-22, 2015, Stockholm, Sweden. (https://4sics.se)
- Presentation of SEGRID at the Digital Utilities Europe in London (Reinder Wolthuis) on May 12th 2016.
- Presentation "Improving the Resilience of SCADA in Critical Infrastructures" (Nuno Neves), at the European Security Conference, Lisboa, Portugal, June 2016.
- Presentation "Tolerância a faltas para SmartGrid" (Nuno Neves), at the Workshop in Security for Smart Grids, Curitiba, Brasil, July 2016.
- Presentation "A Data-centric Approach for Scalability and Fault-tolerance of SDN Controllers" (Alysson Bessani), at the International Workshop on Dependability Issues on SDN and NFV, Toulouse, France, July 2016.
- Presentation "Improving the resilience of SCADA in Critical Infrastructure" (Nuno Neves), at the 70 Meeting of the IFIP 10.4 Working Group on Dependable Computing and Fault Tolerance, Toulouse, France, July 2016.
- Presentation of Threat and Risk Assessment in SEGRID (Judith Rossebø) at SPARKS workshop, Centre for Secure Information Technologies, Queen's University Belfast, August 26th 2016.

- 11th Future Security – Sensor Systems for Safety and Security, (Marcial Valmorisco) the 11th Future Security, Berlin on September 13 – 14 , 2016.

2.6 Journals and magazines

SEGRID partners have made publications as shown in the table below in the second year of the project:

Partner	Title	Title of magazine/conference
FFCUL	Equipping WAP with WEAPONS to Detect Vulnerabilities,	IEEE Conference on Dependable Systems and Networks
FFCUL	JITeR: Just-in-time application-layer routing	Computer networks
FFCUL	SieveQ: A Layered BFT Protection System for Critical Services,	IEEE Transactions on Dependable and Secure Computing
FFCUL	Photons with Electrons to Reduce the Energy Footprint of IPTV Networks,	IFIP Networking 2016
FFCUL	Hacking the DBMS to Prevent Injection Attacks	ACM Conference on Data and Applications Security and Privacy
ABB/TNO	Including Threat Actor Capability and Motivation in Risk Assessment for Smart Grids	CPSR-SG2016 workshop, to appear in IEEE proceedings
ABB	A Framework for MAC Layer Wireless Intrusion Detection & Response for Smart Grid Applications	Accepted in the 14th IEEE International Conference on Industrial Informatics (INDIN), Poitiers, France, July 2016
SICS	On Improving Resistance to Denial of Service and Key Provisioning Scalability of the DTLS Handshake,	International Journal of Information Security, Springer, 2016 (To appear)
SICS	GREP: a Group REkeying Protocol Based on Member Join History"	Proceedings of the twenty-first IEEE Symposium on Computers and Communications (ISCC 2016), pp 326-333, Messina (Italy), 2016
SICS	Robust and scalable DTLS Session establishment	ERCIM News, number 106, July 2016, special theme: Cyber security
SICS	Performance and Security Evaluation of SDN Networks in OMNeT++/INET	OMNeT++ Community Summit 2016
KTH	Automatic Probabilistic Enterprise IT ArchitectureModeling: a Dynamic Bayesian Networks Approach	20th IEEE International Enterprise Distributed Object Computing Conference Workshops, 2016.
KTH	pwnPr3d: an Attack Graph Driven Probabilistic Threat Modeling Approa	Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES), IEEE, Salzburg, Austria, 2016
KTH	Analyzing Attack Resilience of an Advanced Meter Infrastructure Reference Model, in Proceedings of the 2016	Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG) 2016).
TNO	SEGRID introductory article	The European CIIP Newsletter (ECN)

2.7 SEGRID gadgets

For PR reasons, we have ordered two types of gadgets with the SEGRID logo (see Figure 5) .

- A ‘camcover’
- A ‘USB syncstop’

Figure 5 – SEGRID gadgets

The camcover is meant to provide privacy against unwanted use of the built in camera of a laptop. It is glued over the camera and has a small panel that can be slided in order to use the camera. When done, the panel can be slided back in order to cover the camera.

The USB syncstop can be put between a device (such as a smartphone) that has to be powered and an untrusted power-outlet, that can be found on most airports. The syncstop prevents data going through, it only passes power and power negotiation protocols.

Both gadgets were a great success and useful to make people familiar with what SEGRID does. We already have ordered a second batch of the camcovers.

2.8 SEGRID banner

We have produced a SEGRID banner (see Figure 6), that provides a high level overview of the SEGRID project and already served on some occasions, were it proved to be a very useful tool.

Figure 6 – SEGRID banner

2.9 Planned events

The following dissemination events are currently in the planning phase. The list is non-exhaustive, we will strive for more dissemination opportunities.

- First SEGRID workshop, November 14th in Barcelona, preceding the utility week. Target audience:
  - Utility companies + Smart Grid equipment manufacturers
  - Security people
  - Management level
  - Operational staff
  - SEGRID SAB
  - Regulators (National/EU level)
  - EU staff
- Second Joint workshop SPARKS/SLAVAGE/SEGRID – Follow-up of CPSR-SG-2016, during the CPS week.
- Workshop with SPARKS and maybe SALVAGE, to present project results, to be organised in February 2017 (exact date to be determined).
- Submit article on SEGRID Risk Management Methodology in special issue on security risk assessment for the IEEE Computer magazine

3 SEGRID liaison activities

3.1 EU projects

There already is a liaison agreement with SPARKS, the other project that was funded in FP7 call SEC-2013.2.2-3. Several activities have been conducted:

- The CPSR-SG-2016 workshop (also with SLAVAGE, see above)
- Presenting on events that were organized by the respective projects
- Discussions on content, such as risk management methodology

Several events are scheduled or will be scheduled together with SPARKS.

3.2 Standardisation bodies

SEGRID is active or has liaisons with the following bodies:

- (KTH) Cigré working group: Cigré Study Committee D2 Work group D2.40 Cyber risks and cyber security for the next generation of digital systems in Electric Power Utilities (EPUs).
- (TNO, Alliander) have joined the liaison request for CEN-CENELEC JWG 8 (Privacy management in products and services). This is the established by the European Standardisation Organisations CEN/CENELEC, to answer Commission request M/530. Submitted a document describing the work on privacy by design within SEGRID to the CEN-CENELEC JWG8 meeting of February 2016 (Doc. Number: N 0058).
- SEGRID (ABB, TNO) have contacted ETSI TC Cyber to submit a CR for TS 102 165 Part 1: *"Method and proforma for Threat, Vulnerability, Risk Analysis (TVRA)"*. A Work Item (RTS/CYBER-0018) was opened to enable modifications. The ETSI TC Cyber workgroup meeting in Sorrento Italy, is visited to present the proposed changes to the ETSI TVRA as proposed by SEGRID. The proposed CR **has been submitted and is accepted** at the ETSI TC Cyber meeting, Sorrento, 21-23 September 2016.
- Alliander is working on a presentation of SEGRID during a SGIS meeting
- EDP is working a presentation of SEGRID during a PLC Prime meeting
- ABB has been and continues to be active in International Standardization activities, both on a regional level (EU) and on an International level (IEC). In particular, ABB is actively contributing to the IEC 62351 series and ISA99/IEC 62443 series. In the context of the International standards development, ABB benefits from the work in SEGRID on threat and risk assessment, the work on security and privacy, and the work on the gap analysis (with proposed solutions to close the gaps). In particular, when reviewing Committee drafts, the expertise in these areas gained from participation in the SEGRID project has helped identify gaps and areas for improvements in the draft international standards that are under development. Comments and proposals have therefore been submitted accordingly to the Committee (e.g., ISA99 /IEC 62443-4-2, ISA99/IEC 62443-3-2)

4 Dissemination to target groups

The SEGRID dissemination activities are targeted at different stakeholders and audiences. Below we will briefly describe each target group.

4.1 General public

The website of SEGRID has provided information for the general public.

4.2 Policy makers and national CERTs

SEGRID WP1 has conducted a questionnaire to national policy makers and national CERTs. We will do a second questionnaire, with different questions, to be issue at the end of September 2016. The results of this survey will be included in D1.6 - Report with recommendations of improving Smart Grid security policies.

4.3 Security research community

Several scientific papers have been published (see section 2.6).

4.4 Standardization bodies

Several meetings have been attended and presentations and meetings are planned (see section 3.2). A successful result of SEGRID was the CR that was proposed to and accepted by TC CYBER, to enhance the ETSI TVRA.

5 Concluding remarks

During the first year of the SEGRID project, dissemination activities have mainly focused on making the project visible and accessible in the research community as well as in the Smart Grid industry. The second year we have tried to gain more attention and to disseminate the Y2 results of SEGRID. As can be read in this report, several instruments were used to this end.
Dissemination during the second year of the SEGRID project can be seen as successful. The project has gained more visibility within the scientific community, both through publications, presentations and demonstrations and through cooperation with other projects and organisations and liaisons with standardization bodies. Also we have organized the second advisory board (SAB) meeting.
The third year of dissemination will be even more focussed toward the dissemination of results. At the end of Y2, the first demonstrations will be finished and we will use these a.o. for dissemination at e.g. the first SEGRID workshop. Also we will focus in Y3 on impact an exploitation plans of partners.