FP7 Grant Agreement N° 607109

Security for smart Electricity GRIDs

D6.7 Final report on dissemination activities

Due date of deliverable: 30/11/2016
Actual submission date: 01/12/2016
Workpackage: WP6 Dissemination
Number of pages: 26
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:	39 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) Marco Tiloca (RISE SICS) Mathias Ekstedt (KTH) Marcial Valmorisco (INCODE) Maarten Hoeve (ENCS) Sander Kruese (Alliander) Gunnar Björkman (ABB) Nuno Neves (FCIENCIAS.ID) Nuno Medeiros (EDP) Exabier Bilbao Hernández (ZIV)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	30/11/2017
Remarks	None

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 D6.7: Final report on dissemination activities 6
2 DISSEMINATION INSTRUMENTS 7
2.1 SEGRID website 7
2.2 SEGRID flyer 7
2.3 SEGRID Advisory Board (SAB) 8
2.4 SEGRID white paper 9
2.5 Combined CPSR- SG 2016 workshop with SPARKS and SALVAGE 2017 9
2.6 Combined CPSR- SG 2017 workshop with SPARKS and SALVAGE 11
2.7 Symposium on Innovative Smart Grid Cybersecurity Solutions in Vienna 13
2.8 SEGRID summit 14
2.9 SEGRID presentations 17
2.10 Journals and magazines 18
2.11 SEGRID gadgets 21
2.12 SEGRID banner 22
3 SEGRID LIAISON ACTIVITIES 22
3.1 EU projects 22
3.2 Standardisation bodies 23
4 DISSEMINATION TO TARGET GROUPS 24
4.1 General public 24
4.2 Policy makers and national CERTs 24
4.3 Security research community 25
4.4 Standardization bodies 25
5 CONCLUDING REMARKS 26

Classification level: Public

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.

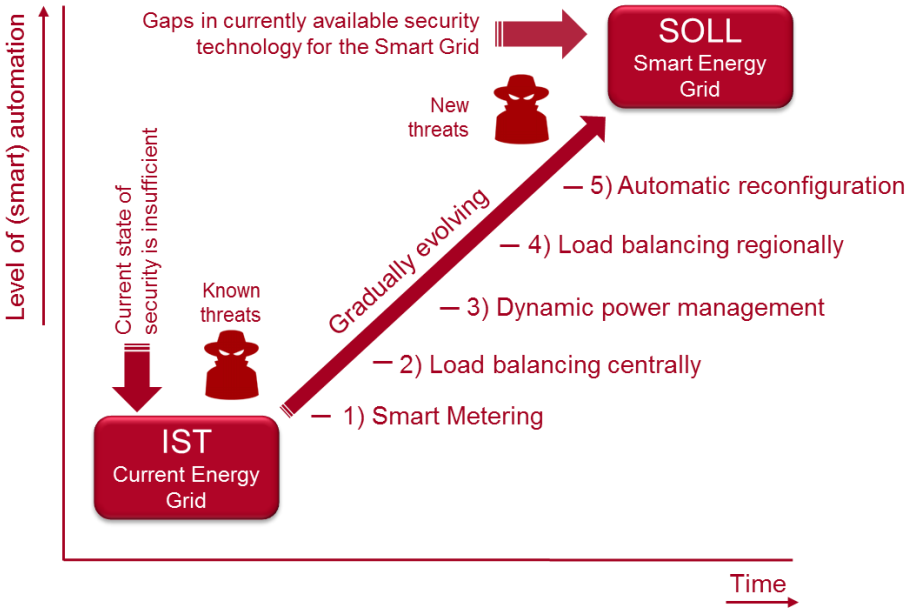

Figure 1: SEGRID storyline

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 D6.7: Final report on dissemination activities

This report lists the dissemination activities that have been carried out during the lifetime of the SEGRID project. It also includes the activities already reported in the first year dissemination report (D6.2) and the second year dissemination report (D6.5), to provide a complete overview. Where relevant, the specific year where a dissemination activity took place will be mentioned.

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

This chapter provides an overview of the dissemination instruments that SEGRID used throughout the project.

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

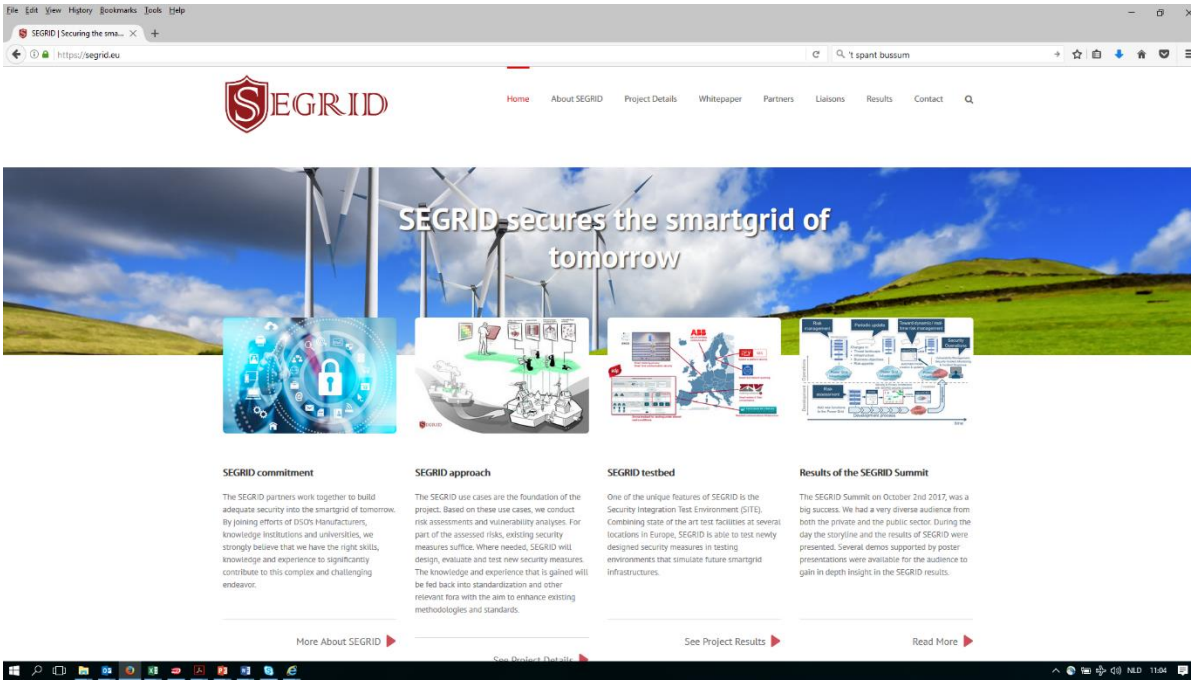

Figure 2 – SEGRID website

2.2 SEGRID flyer

The SEGRID flyer has been distributed at events and conferences. We intend to devote even more attention to this in year2 and year3. It is a one-page (A5) double printed paper flyer, offering information about the SEGRID project and its partners and it contains contact information. The flyer can also be downloaded at the SEGRID website. See Figure 3 for an impression of the SEGRID flyer.

Figure 3 – front page of SEGRID flyer

2.3 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 three SAB meetings:

- A first SAB meeting in Lisbon on March 4th 2015. 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.
- 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.
- The third SAB meeting in Lisbon on March 9th 2017 in Porto. Three 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.

The SAB members were also invited to join the SEGRID workshop in Barcelona in 2016 and the SEGRID summit in Amsterdam in 2017. A SAB delegation has indeed joined these meetings.

During the project, two members have indicated that they had to leave the SEGRID SAB. We have successfully replaced one of the members.

2.4 SEGRID white paper

The SEGRID white paper was delivered in May 2017 and distributed as a physical booklet and published on the SEGRID website as downloadable PDF.

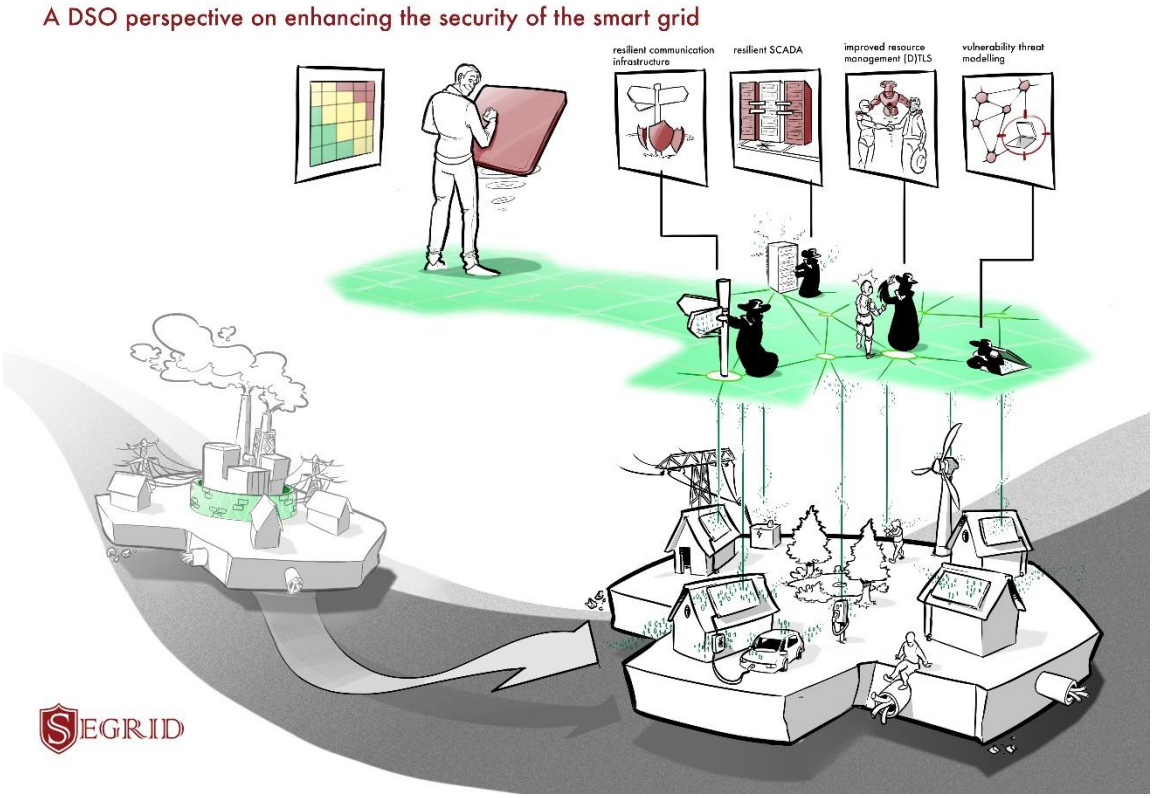

Figure 4 The centerfold of the SEGRID whitepaper

It was also actively distributed to interested parties and send with invitations for the SEGRID summit. In Spain, it was actively distributed to a.o. Gas Natural Fenosa (a private Spanish company dedicated to the marketing of natural gas and electricity), Enagás, S.A. (the main carrier of natural gas in Spain and technical manager of the gas system espanol), Iberdrola S.A. (a group of companies based in Bilbao and dedicated to the production, distribution and energy marketing).

2.5 Combined CPSR- SG 2016 workshop with SPARKS and SALVAGE 2017

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 5 for the workshop agenda. And Figure 6 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 5 – Agenda of joint workshop at CPS week 2016

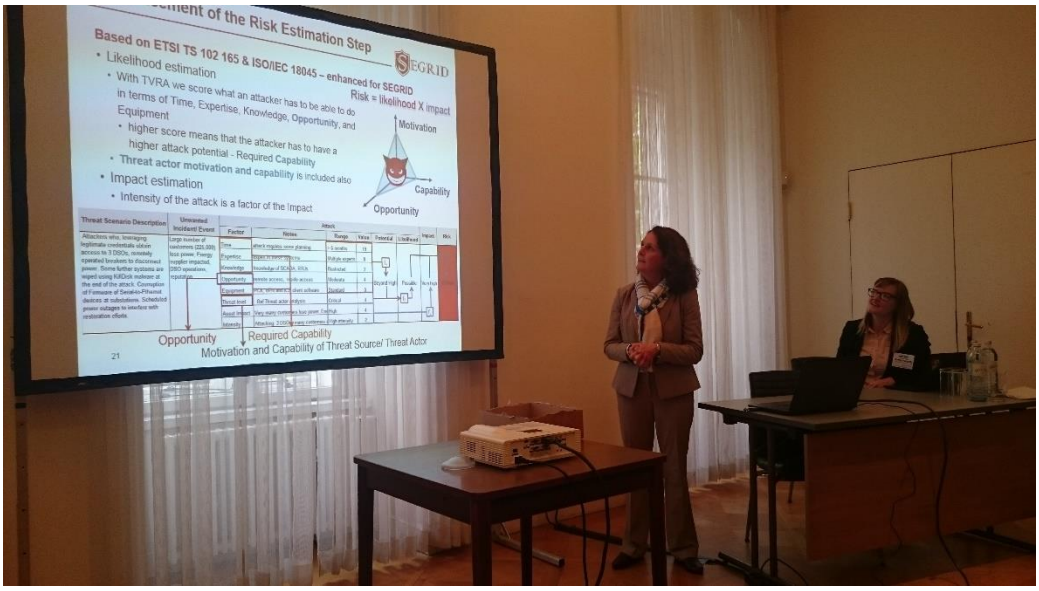

Figure 6 – Judith Rossebø (ABB) presenting at the CPS –SG-2016

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 have been published by IEEE, in the IEEE Conference Publication Program (CPP), ISBN 978-1-5090-1164-3 (http://ieeexplore.ieee.org/document/7684093/).

2.6 Combined CPSR- SG 2017 workshop with SPARKS and SALVAGE

The three projects SEGRID, SPARKS and SALVAGE have organized a second joint workshop preceding the CPS week in Pittsburgh, April 21st 2017: *Second Workshop on Cyber-Physical Security and Resilience in Smart Grids: CPSR-SG 2017*. 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 7 for the workshop agenda. and Figure 8 for a workshop impression.

Time	Item
9:00-9:15	Oliver Gehrke and Reinder Wolthuis. *Welcome to the Joint International Workshop on Cyber-Physical Security and Resilience in Smart Grids: CPSR-SG 2017*
09:15-11:15	Paper Session I (Chair: Oliver Gehrke) **09:15-09:45** Jaap-Henk Hoepman. *Fault Tolerant Aggregation of Smart Meter Readings When Meters Crash* **09:45-10:15** Abdallah Farraj, Eman Hammad, and Deepa Kundur. *Performance Metrics for Storage-Based Transient Stability Control* **10:15-10:45** Christian Moya and Jiankang Wang. *Cyber-Attacks to Voltage Con-*

	trol Applications viaWide AreaMonitoring, Protection and Control System **10:45-11:15** Jue Tian, Rui Tan, Xiaohong Guan, Ting Liu. *Hidden Moving Target Defense in Smart Grids*
11:30 – 12:15	**Key note**: *Securing the Grid of the Future* - **Joe Doetzl**, Cyber Security Practice Leader at ABB Inc., Business Unit Grid Automation, Power Grids division
13:30 – 15:30	Paper Session II (Chair: Oliver Gehrke) **13:30-14:00** Abdallah Farraj, Eman Hammad, and Deepa Kundur. *Impact of Cyber Attacks on Data Integrity in Transient Stability Control* **14:00-14:30** Chenglu Jin, Lingyu Ren, Xubin Liu. *Mitigating Synchronized Hardware Trojan Attacks in Smart Grids* **14:30-15:00** Ajay Chhokra, Amogh Kulkarni, Saqib Hasan, Abhishek Dubey, Nagabhushan, Mahadevan, Gabor Karsai. *A Systematic Approach Of Identifying Optimal Load Control Actions For Arresting Cascading Failures In Power Systems* **15:00-15:30** Margus Välja, Matus Korman, Robert Lagerström. *A study on software vulnerabilities and weaknesses of embedded systems in power grids*
16:00 – 18:00	Paper Session III (Chair: Reinder Wolthuis) **16:00-16:30** Oliver Gehrke, Kai Heussen, Matus Korman. *Integrated multi-domain risk assessment using automated* *hypothesis testing* **16:30-17:00** Sarita Paudel, Paul Smith, Tanja Zseby. *Attack Models for Advanced Persistent Threats in Smart Grid Wide Area Monitoring* **17:00-17:30** J.K. Wang, Chunyi Peng. *Analysis of Time Delay Attacks against Power Grid Stability* **17:30-18:00** Matus Korman, Margus Välja, Gunnar Björkman. *Analyzing the Effectiveness of Attack Countermeasures in a SCADA System*
18:00 – 18:15	**Best paper award, workshop Summary and closing**

Figure 7 The CSPR2017 workshop agenda

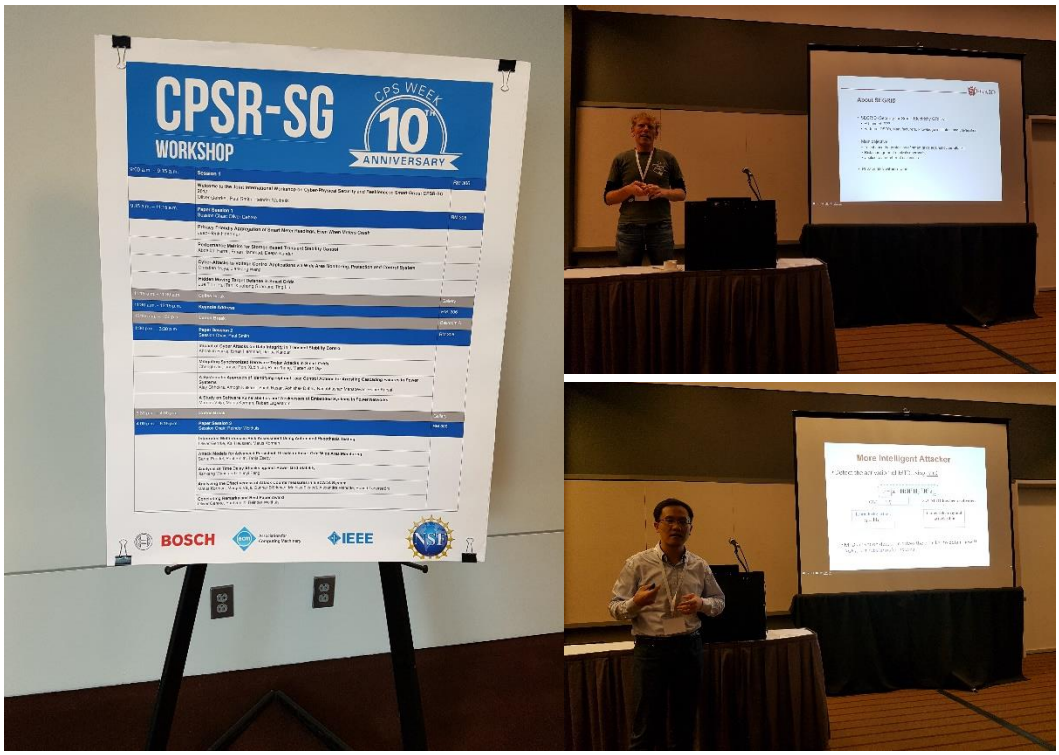

Figure 8 – Impression of the CSPR 2017 workshop

A total of 12 submitted papers were each reviewed by three members of the program committee and 12 were accepted, of which two from outside Europe. Joe Doetzl (Cyber Security Practice Leader Business Unit Grid Automation 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 have been be published by ACM, ISBN: 978-1-4503-4978.

2.7 Symposium on Innovative Smart Grid Cybersecurity Solutions in Vienna

On Monday March 13 and Tuesday March 14th 2017, a joint workshop was organized by the projects HyRim, IRENE, SALVAGE, SPARKS, SUCCESS and SEGRID, kindly hosted by AIT in Vienna. The intention was to show the results of the participating projects to a broader audience by presentations and demonstrations. The participating projects were introduced and there were five sessions:

- Smart Grid Security Risk Management – chaired by Reinder Wolthuis and a Judith Rossebø presented the SRMM
- Security Analytics and Situational Awareness – Maarten Hoeve presented the DSO oriented Security capability model
- Session: Smart Grid Resilience (I)
- Session: Smart Grid Resilience (II) – Nuno Neves presented the Intrusion-Tolerant Eclipse SCADA
- Social, Legal and Policy Aspects – Nuno Medeiros presented A DSO Perspective on Future Cybersecurity and Privacy Policies

In the panel session: 'Reflections on the Symposium and Future Directions', Jaap Henk Hoepman and Nuno Medeiros were participating experts.

SEGRID participated with the 'Denial-of-service attack against the DTLS server' by Hamid Rahmouni and Marco Tiloca in the demo session.

The symposium was very successful with a large audience and very good discussions. It provided an excellent platform to disseminate the SEGRID results.

Figure 9 – Impression of the joint symposium in Vienna

2.8 SEGRID summit

On October 2nd 2017, the SEGRID summit was organized in Amsterdam, preceding the Utility week. It was the concluding event of the SEGRID project and was a huge success. We were able to attract a considerable audience, including some members of our Advisory Board and during the day there was much interest in SEGRID and many good discussions. The Agenda for the day is shown in Figure 10 and some impressions are shown in Figure 12. We have used our use case 2, scenario 2 as a storyline during the day to highlight the SEGRID results. There were 5 demos that showed the practical results and 9 posters explained the SEGRID innovations. We have discussed privacy issues in smart grids in a panel session.

Time	Title	Who
9:30	Registration and coffee	

10:00	Welcome and overview	Reinder Wolthuis
10:10	SEGRID Smart Grid (load balancing centrally)	Nuno Medeiros & Frank Fransen
10:40	Cyber Attack's on the Power Grid + *demo*	Maarten Hoeve
11:10	**Coffee break**	
11:30	SEGRID Risk Assessment – UC2.2	Judith Rossebø & Reinder Wolthuis
12:00	Security & Privacy Architecture Design (SPADE) – UC2.2	Marco Tiloca
12:30	**Lunch Break**	
13:15	Vulnerability Analysis – SecuriCAD + *demo*	Mathias Ekstedt & Alexandre Vernotte
14:00	Resilient Communication Infrastructure + *demo*	Nuno Neves & Ricardo Fonseca
14:45	**Coffee + Poster & Demo Session**	
15:45	Cost Assessment	Eldine Verweij
16:15	Operational Security Capability for DSOs	Maarten Hoeve
16:45	Panel Discussion – **Privacy and Smart Grid**	Nuno Medeiros, Johan Rambi, Jaap Henk Hoepman, Frank Fransen
17:30	**Food and beverages + Poster & Demo**	

Figure 10 – Agenda of the SEGRID summit

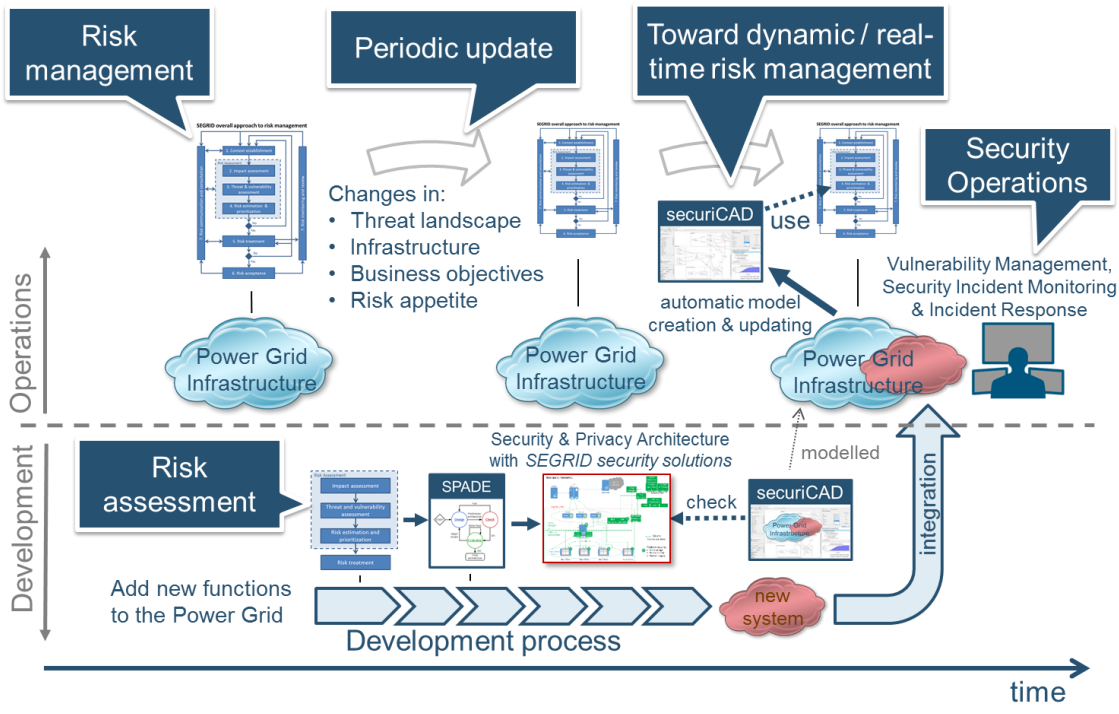

Figure 11 - View on how SEGRID innovations fit together

Figure 12 – Impression of the SEGRID summit

2.9 SEGRID presentations

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

Year 1:

- (FFCUL) IFIP Working Group 10.4 meeting, Bristol UK, January 22nd – 26th, 2015
- (TNO) European Smart Grid and Cyber Security 2015, London, March 9th and 10th
- (ABB) NFA - Norwegian Society of Automatic Control - Information Security Conference, Oslo, September 16th – 17th, 2015
- (ABB) SINTEF Information Security Seminar – Estimation of Security from an Interdisciplenary Perspective, Oslo, September 29th, 2015

Year 2:

- (TNO) 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.
- (RISE SICS)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)
- (TNO) Presentation of SEGRID at the Digital Utilities Europe in London (Reinder Wolthuis) on May 12th 2016.
- (FCiencias.ID) Presentation "Improving the Resilience of SCADA in Critical Infrastructures" (Nuno Neves), at the European Security Conference, Lisboa, Portugal, June 2016.
- (FCiencias.ID) Presentation "Tolerância a faltas para SmartGrid" (Nuno Neves), at the Workshop in Security for Smart Grids, Curitiba, Brasil, July 2016.
- (FCiencias.ID) 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.
- (FCiencias.ID) 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.
- (ABB) 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.
- (Incode) 11th Future Security – Sensor Systems for Safety and Security, (Marcial Valmorisco) the 11th Future Security, Berlin on September 13 – 14 , 2016.

Year 3:

- (TNO) Presentation of SEGRID at a lunch meeting of the security group at Radboud University, Nijmegen, The Netherlands (Frank Fransen), 17 February 2017.

- (TNO) Presentation of SEGRID at the opening of the new Hybrid Energy System Integration (HESI) lab of TNO, Groningen, The Netherlands (Reinder Wolthuis), January 31st 2017
- (TNO) SEGRID presented by Reinder Wolthuis at EDSO conference June 26/27 2017
- (Alliander) Johan Rambi presented SEGRID at a DG HOME Community of Users for Safe Secure and Resilient Societies CoU session in May
- (FCiencias.ID) Presentation and demonstration "Demonstrating a Tool for Injection Attack Prevention in MySQL" (Ibéria Medeiros), at the International Conference on Dependable Systems and Networks (DSN), Denver, USA, June 26-29 2017
- (FCiencias.ID) Presentation "Detection of Vulnerabilities broken by Circular Dependencies in Static Analysis" (Ibéria Medeiros), at the Workshop of the IFIP Working Group 10.4 Dependable Computing and Fault Tolerance, Longmont, USA, June 22-25 2017
- (ENCS) The SEGRID roadmap was presented by Maarten Hoeve as one of the research highlights of 2016 at the ENCS Assembly on 7 February 2017. Representatives of nine DSOs were present at CIO or CISO level. A printed version of the roadmap was given to them as part of a hand-out package.
- (ENCS) April 4, 2017: Presentation of work on the DSO operational security capability model in the face-to-face meeting to the E.ON PIT Security Community. This community gathers people working on the security of industrial control systems within the E.ON group.
- (ENCS) April 5, 2017: Presentation of work on the DSO operational security capability model in the contact group on OT-IT security of Netbeheer Nederland. This contact group is a meeting of people working on industrial control system security at Dutch grid operators.
- Several presentations at the Symposium on Innovative Smart Grid Cybersecurity Solutions, Vienna, 13-14 March; see paragraph 2.7.
- (TNO) Frank Fransen presented SEGRID in a project session at the CRITIS2017 conference in Lucca, Italy on October 10th 2017

2.10 Journals and magazines

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

Year 1

Partner	Title	Title of magazine/conference
FFCUL	Detecting and Removing Web Application Vulnerabilities with Static Analysis and Data Mining	Special issue of IEEE Transactions on Reliability
FFCUL	Fault-Tolerant Precision Time Protocol for Smart Grids	INFOFORUM

ENCS	Klaus Kursawe and Christiane Peters: Structural Weaknesses in the Open Smart Grid Protocol.	To appear in the proceedings of the Tenth International Conference on Availability, Reliability and Security, ARES 2015, Toulouse, France, August 24-28, 2015. IEEE Computer Society 2015.
FFCUL	Securing Passive Replication Through Verification	SRDS 2015
KTH	Working time between vulnerability disclosures: A measure of software product vulnerability	Computers & Security
KTH	A Requirements Based Approach for Automating Enterprise IT Architecture Modeling Using Multiple Data Sources	International Workshop on Methodical Development of Modeling Tools (ModTools15)
FFCUL	Towards Secure and Dependable Authentication and Authorization Infrastructures	2014 IEEE 20th Pacific Rim International Symposium on Dependable Computing (PRDC)
FFCUL	SITAN: Services for Ad Hoc Networks with Unknown Participants	The 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2014)
SICS	Simulative evaluation of security attacks in networked critical infrastructures	2nd International Workshop on Reliability and Security Aspects for Critical Infrastructure Protection (ReSA4CI 2015)

Year 2:

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	GREP: a Group REkeying Protocol Based on Member Join History"	Proceedings of the twenty-first IEEE Symposium on Computers and Communications (ISCC 2016), 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)

Year 3:

Partner	Title	Title of magazine/conference
ABB, EDP, TNO	An Enhanced Risk Assessment Methodology for Smart Grid	IEEE Computer, special issue on Risk assessment, Volume 50, issue 4, page 62 - 71
TNO	'Smart grids: And the bad news is?'	In the international journal of critical infrastructure protection 18 (2017) 34–36
TNO	SEGRID introduction	European eneegy innovation magazine issue of summer 2017
KTH	In-Depth Modeling of the UNIX Operating System for Architectural Cyber Security Analysis	proc. of the 9th International Workshop on Vocabularies, Ontologies and Rules for the Enterprise, co-located with the 21st IEEE International EDOC Conference, 2017.
KTH	A Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Grids	Proc. of the 2nd Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), 2017
KTH	Analyzing the Effectiveness of Attack Countermeasures in a SCADA System,	Proc. of the 2nd Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), 2017
TNO	Privacy Friendly Aggregation of Smart Meter Readings Even When Meters Crash	Proc. of the 2nd Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG), 2017
RISE SICS	On Improving Resistance to Denial of Service and Key Provisioning Scalability of the DTLS Handshake	International Journal of Information Security, Springer, vol. 16, issue 2, 2017

FCiencias.ID	Secure Network Monitoring Using Programmable Data Planes	Proceedings of the Third International Workshop on Security in NFV-SDN (SN), Berlin, Germany, November 2017
FCiencias.ID	Resolução de Dependências Circulares em Inclusão de Código em Análise Estática de Código	INFORUM - Simpósio de Informática (INFORUM), Aveiro, Portugal, October 2017
FCiencias.ID	Demonstrating a Tool for Injection Attack Prevention in MySQL	Proceedings of the International Conference on Dependable Systems and Networks (DSN), Denver, USA, June 2017
FCiencias.ID	DEKANT: A Static Analysis Tool that Learns to Detect Web Application Vulnerabilities	Proceedings of the International Symposium on Software Testing and Analysis (ISSTA), Saarbrücken, Germany, July 2016

2.11 SEGRID gadgets

For PR reasons, we have ordered two types of gadgets with the SEGRID logo (see Figure 13) .

- A ‘camcover’
- A ‘USB syncstop’

Figure 13 – 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.

2.12 SEGRID banner

We have produced a SEGRID banner (see Figure 14), 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 14 – SEGRID banner

3 SEGRID liaison activities

3.1 EU projects

Liasons with other projects:

- Smart Grid Protection Against Cyber Attacks (SPARKS, the other project that was funded in FP7 call SEC-2013.2.2-3)
- SALVAGE
- Critical Infrastructure Preparedness and Resilience Research Network (CIPRNet)

Several activities have been conducted:

Year 1

- Coordination of activities on risk management, including a workshop (by conference call with go2meeting facilities over two separate days, June 16th, 2015 and August 13th, 2015)

- SEGRID provided input to a questionnaire exclusively targeted towards EU (co-) funded research projects on Smart Grid Security related issues, to inventory these projects.
- SEGRID presented at SPARKS 2nd stakeholder workshop, March 25th, 2015
- A joint meeting between SPARKS and SEGRID was organized, in Bilbao on September 8th, just after the SEGRID general meeting

Year 2

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

Year 3

- 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

Together with other EU projects, SEGRID organized a smart grid security symposium in 2017 hosted by AIT in Vienna. See paragraph 2.7 for more information.

There are plans to write a white paper on Risk Management in smart grids, jointly with SPARKS and HyRIM. The EE-ISAC has agreed to publish this white paper on behalf of the EE-ISAC. This will probably delivered after SEGRID has ended.

3.2 Standardisation bodies

SEGRID is active or has liaisons with the following bodies:

Year 1:

- (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).
- (KTH) secretary of WG D2.31 (Security architecture principles for digital systems in Electric Power Utilities (EPUs)
- (TNO, Alliander) have joined the liaison request for 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

Year 2:

- (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. It will be included in the next version of the standard

- 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)

Year 3:

- (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).
- (RISE SICS, ENCS) The work on (D)TLS improvement led to a proposal to improve the (D)TLS IETF standard. A first version of an Internet Draft was submitted to IETF 99 held in Prague in July 2017 (see https://tools.ietf.org/html/draft-tiloca-tls-dos-handshake-00). The Internet Draft got a **positive and constructive review from Eric Rescorla**, **namely Security Area Director of the IETF**. An updated version of the draft has been submitted to IETF 100 held in Singapore in November 2017 (see https://tools.ietf.org/html/draft-tiloca-tls-dos-handshake-01), and has been presented there in the TLS Working Group meeting.

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 sent a two questionnaires to national policy makers and national CERTs. The results of this survey are included in D1.5 Report on analysis of policies regarding smart grid security and D1.6 Report with recommendations of improving Smart Grid security policies.

Some of the SEGRID partners have actively approached smart grid policy makers and regulators to inform them about the SEGRID progress. In Spain for example, the following stakeholders were actively informed by SEGRID partner Incode in periodic meetings.

ORGANISATION	DESCRIPTION

CNPIC	Centro Nacional de Protección de las Infraestructuras Críticas (CNPIC) is responsible for the direction, coordination and supervision of the protection of national critical infrastructures. For this reason, CNPIC will lead the implementation of the National Plan for the protection of critical infrastructure and will act as national contact point with the Commission and other States which are owners or managers of critical infrastructure.
INCIBE	The Spanish National Cybersecurity Institute (INCIBE), formerly National Institute of Communication Technologies is a subsidiary of the Secretary of State for the Information Society and Digital Agenda (SESIAD) and consolidated as a reference entity for cybersecurity development and digital trust of citizens, academic and research network, professionals, companies and especially for strategic sectors. INCIBE activity is based on research, service delivery and coordination with the competent agents in the matter, INCIBE contributes to building cybersecurity at the national and international levels.
Sevilla Council	Seville a municipality and a city of Spain, capital of the homonymous province and of the autonomous community of Andalusia account with 690 566 inhabitants in 2016,6 by the ' s after the largest city in Andalusia, the espana of the Madrid, Barcelona and Valencia fourth and 32. the European Union Rd
Malaga Council	Malaga is a city and a municipality of Spain, capital of the province of same name and located in the autonomous community of Andalusia. With a population of 569 009 people in 2016,8 Málaga is the sixth most populous city in Spain, the second of Andalusia and the forty-six number in the European Union, as well as the largest among them are not autonomous capital

4.3 Security research community

Several scientific papers have been published (see section 2.10). On top of that:

- In year 1, SICS organized an “Open house" event, where SEGRID was presented to colleagues, customers and other interested parties overviewing SEGRID and SICS activities within SEGRID. (see also https://www.sics.se/events/sics-open-house-2015 and https://www.youtube.com/watch?v=gYZ6XaeXO9Y)

4.4 Standardization bodies

Several meetings have been attended and presentations and meetings are planned (see section 3.2).

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.
The third year of dissemination has even more been focussed on dissemination of results and showed many activities, including the successful SEGRID summit.

Overall, we see the SEGRID dissemination results as successful. We have had two successful standardization contributions (ETSI TVRA and IETF TLS), we have published many articles, we have organized many events and showed a number of demonstrators. We have reached a large audience doing all these activities and gained visibility within the relevant communities, such as the scientific community, standardization, regulators and DSOs.

The follow up of the SEGRID results is described in D6.6- The SEGRID partner exploitation plans.