FP7 Grant Agreement N° 607109

Security for smart Electricity GRIDs

D6.2 Dissemination plan

Due date of deliverable: 31/03/2015
Actual submission date: 01/04/2015
Workpackage: WP6 Dissemination & Exploitation
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:	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)	Frank Fransen (TNO) Reinder Wolthuis (TNO)
Contributor(s)	Rolf Blom (SICS) Mathias Ekstedt (KTH) Antonio Silva Moriano (INCODE) Chistiane Peters (ENCS) Bart Luijkx (Alliander) Gunnar Björkman (ABB) Nuno Neves (FFCUL) Nuno Medeiros (EDP) Miguel Ángel Alvarez Cabanes (ZIV)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	31/03/2015
Remarks	None

TABLE OF CONTENTS

1 INTRODUCTION 4
2 DISSEMINATION STRATEGY AND OBJECTIVES 5
2.1 The SEGRID project objectives 5
2.2 The SEGRID dissemination objectives 6
2.3 Classified information 7
3 TARGET AUDIENCE AND STAKEHOLDERS 8
3.1 General public 8
3.2 Policy makers 8
3.3 National CERTs and agencies related to homeland security and energy 8
3.4 Security research community 8
3.5 Smart grid community 8
3.6 (EU) smart grid security innovation projects 9
4 DISSEMINATION ORGANISATION AND SCOPE 10
5 COMMUNICATION CHANNELS, LIAISON AND MEDIA 12
5.1 SEGRID logo 12
5.2 SEGRID website 12
5.3 SEGRID flyer 13
5.4 SEGRID white paper 13
5.5 SEGRID workshop 13
5.6 SEGRID Advisory Board (SAB) 14
5.7 Conferences 14
5.8 Journals and magazines 16
5.9 SEGRID liaison activities 16
5.10 Press releases 16
5.11 Demonstrations 17
5.12 Social media 17
5.13 Give-aways 17
5.14 Video 17
6 EXPLOITATION 18
7 DISSEMINATION WORK PLAN 19
7.1 Ongoing dissemination activities 19
7.2 Planned dissemination activities 19
7.3 To-be-planned dissemination activities 20
ANNEX A: SEGRID PARTICIPATION IN TECHNOLOGY PLATFORMS AND INDUSTRIAL ASSOCIATIONS 22
ANNEX B: INITIAL EXPLOITATION IDEAS 24

1 Introduction

This document is the dissemination plan for the SEGRID project. The Dissemination Plan (DP) describes the approach of SEGRID regarding dissemination objectives, plans, activities target audience and results.

Section 2 describes the dissemination strategy and measurable dissemination objectives, while section 3 identifies the SEGRID stakeholders and the target audience for the dissemination activities, considering their specific information needs.

Section 4 provides details on the organization of the dissemination activities and the specific scope of the activities. Section 5 lists the channels and media that SEGRID intends to utilize in the dissemination activities, including a detailed list of messages and hints tailored according to the category of the audiences and stakeholder groups, in terms of content, format, style and support. Also in section 5 are the projects, organizations and standardization activities that SEGRID aims to liaise with. Finally in chapter 6, the work plan is laid down, describing the planning for all dissemination activities and their intended results.

2 Dissemination strategy and objectives

2.1 The SEGRID project objectives

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. In a Smart Grid, it is not sufficient to consider all the different components separately; they will together form a truly integrated system-of-systems. 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 organizations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new channels, such as local connection interfaces, distributed web access, and smart apps on smart phones to connect with various Smart Grid applications.

This new utility-wide system (-of-systems) will not come into existence overnight. Therefore, the Smart Grid will be composed of a mix of old, even legacy, and new components. This is why we introduce the concept of a gradually evolving system in which a number of use cases reflect newly added functionalities, with the challenge to maintain the security (and privacy) of the Smart Grid as a whole. We will apply a risk management analysis approach to these 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.

The SEGRID approach is based on 6 main objectives:

- 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.

We have selected five use cases that clearly demonstrate this gradual evolving system concept. The SEGRID use cases have been selected based on the work already done by ENISA

along with the working parties involved in the EC Mandates M/441 and M/490 as well as based on the work and competence of the project partners.

The five SEGRID use cases are:

1. Smart meter 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.

We believe that the SEGRID use cases reflect important steps of Smart Grid developments until 2020 and beyond (SEGRID storyline, see Figure 1). Moreover, the SEGRID use cases will cover the most relevant security and privacy issues that will arise from the increasing complexity of Smart Grids.

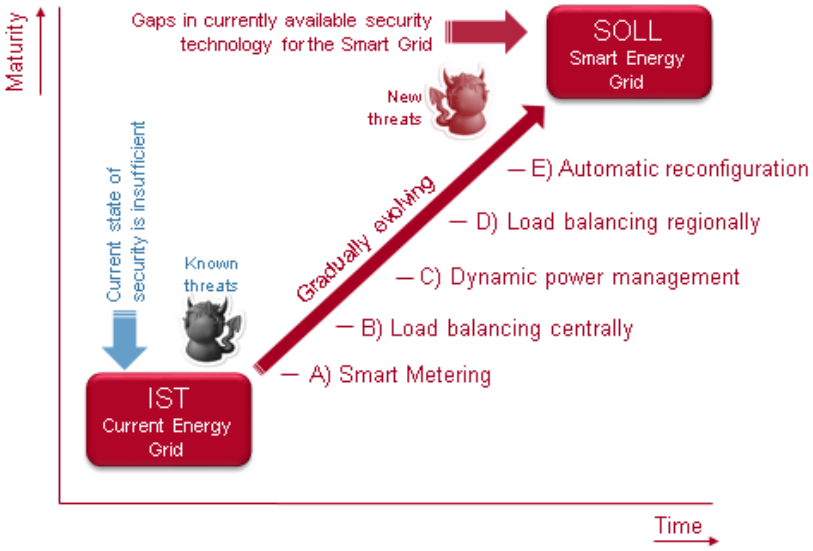

Figure 1: SEGRID Storyline

2.2 The SEGRID dissemination objectives

SEGRID will only be valuable if the results are adequately disseminated. This is even reflected in one of the SEGRID project objectives, that describes the feedback of SEGRID results into European and global standardisation bodies, industry groups and smart grid suppliers.

The objective for the dissemination activities is to create strong awareness of the SEGRID results at European level, multiplying its impact and subsequent exploitation opportunities. 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.

2.3 Classified information

Some of the deliverables of SEGRID are classified as 'EU restricted'. Where necessary, before actual dissemination activities will be effectuated, the SEGRID Security Advisory Group (SAG) will be consulted to be sure that no restricted information is published. The SEGRID SAG has drawn up procedures to this end.

3 Target audience and stakeholders

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

3.1 General public

The 'general public' or citizens of Europe form one of the target groups for SEGRID, focussing on generic high level information regarding security issues of smart grids. The website of SEGRID is one of the main tools to achieve this goal and also the public deliverables of SEGRID will be available for download at the SEGRID website.

3.2 Policy makers

Dissemination towards policy makers is aimed at making the policy makers aware of the SEGRID results and experiences, which might be important for future smart grid security policies. Dissemination will be conducted both on a European (e.g. Directorate-general Energy (ENER) and a national level (e.g. Agentschap NL). Main partner for the European level is INCODE, while each SEGRID partner will conduct dissemination activities towards its own national policy makers.

3.3 National CERTs and agencies related to homeland security and energy

SEGRID research and results can be of interest to the Computer Security Incident Response community. If needed, SEGRID will contact national CSIRTs (such as CERT-EU, CERT-SE, CERT.PT, CCN-CERT, NorCERT or NCSC-NL) to inform them about SEGRID findings. SEGRID will also strive to invite national CSIRT staff to SEGRID events.

3.4 Security research community

One important dissemination target group for SEGRID is the scientific research community, such as universities with a strong security group. We will reach this community by the contacts with research projects, by participating in scientific conferences and publishing in scientific magazines. The security research community will mainly be reached by our scientific partners KTH and University of Lisbon (FFCUL) and by research institutions TNO, ENCS and SICS.

3.5 Smart grid community

The smart grid community is very large, involving players from industry, government, standardization bodies, service providers, energy distributors, transport operators and many more.

They are in principle all relevant for SEGRID dissemination purposes, but SEGRID cannot approach all of these players individually. This is why SEGRID will focus its dissemination activities on technology platforms, standardization bodies and industrial associations.

The aim of the dissemination towards these technology platforms, standardization bodies and industrial associations is to inform them about SEGRID results and provide them with the opportunity to embed SEGRID results and experiences in e.g. updated versions of standards.

Dissemination activities towards technology platforms, standardization bodies and industrial associations will be done by partners that are participating in these technology platforms, standardization bodies and industrial associations or by contacting them directly. SEGRID will focus technology platforms, standardization bodies and industrial associations as shown in Annex A: SEGRID participation in technology platforms and industrial associations.

Also, as many people from the smart grid community as possible will be invited for the SEGRID events.

3.6 (EU) smart grid security innovation projects

SEGRID will keep contact with relevant (EU) smart grid security innovation projects, in order to exchange results and learn from each other. This will be done by all partners, coordinated by TNO. A non-exhaustive current list of these projects:

- MAS2TERING - Multi-Agent Systems and Secured coupling of Telecom and EnErgy gRIds for Next Generation smart grid services
- CAPITAL - Cyber security research Agenda for PrIvacy and Technology chAL-lenges
- TCLOUDS - Trustworthy Clouds – Privacy and Resilience for Internet-scale Critical Infrastructure
- MODESEC - Model-based Design of Secure Cyber-Physical Systems
- SMART-NRG - Industry-academia partnership for the design and implementation of an efficient, reliable and secure smart energy network
- EU ERA-Net project SALVAGE (Cyber-phySicAl security for Low-VoltAGE grids)
- TRESPASS http://www.trespass-project.eu
- SYSSEC http://www.syssec-project.eu

4 Dissemination organisation and scope

TNO is the coordinator of the dissemination activities, that are managed in WP6. The other workpackages provide input for the dissemination activities, see also Figure 2.

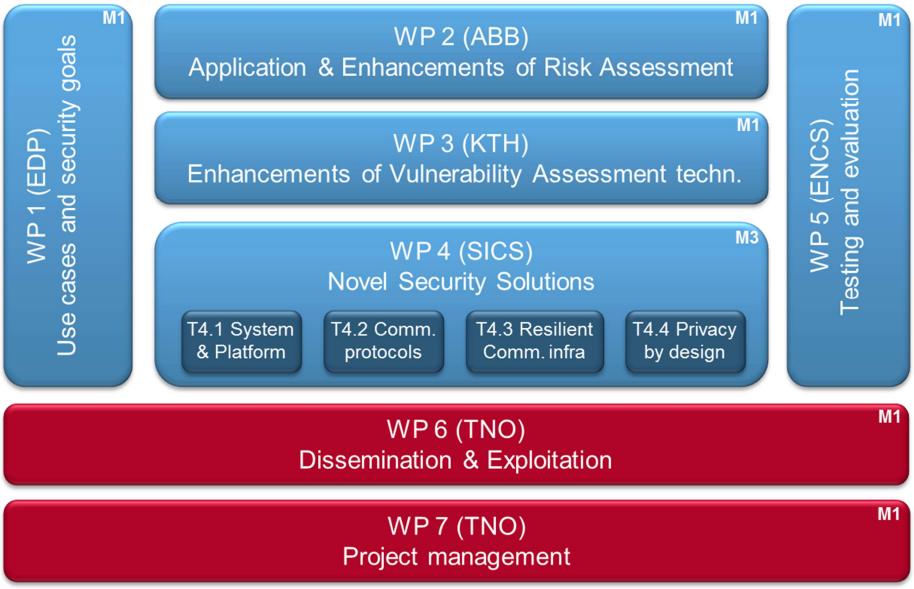

Figure 2 SEGRID Workpackage structure

Work package 6 is organized according to the following tasks:

- T6.1 Develop and maintenance of the SEGRID web site.
- T6.2 Develop the SEGRID smart grid security white paper
- T6.3 Dissemination towards policy makers and higher management
- T6.4 Contribution to standardisation and other fora
- T6.5 Preparation and realisation of SEGRID workshops
- T6.6 Dissemination activities towards the scientific community
- T6.7 Exploitation

Work package 6 will deliver the following results:

Table 1 - WP6 results

Deliverable number	Deliverable title	Dissemination level	Delivery date
D6.1	Project flyer and website	PU	6
D6.2	Dissemination plan	PU	6
D6.3	Report on dissemination activities	PU	12

D6.4	SEGRID smart grid security white paper	PU	24
D6.5	2nd report on dissemination activities	PU	24
D6.6	Partner exploitation plans	PU	34
D6.7	Final report on dissemination and standardisation activities	PU	36

One key purpose in the project is boosting the impact of its results. That is why SEGRID employs a clear dissemination approach. The graph below shows this dissemination approach.

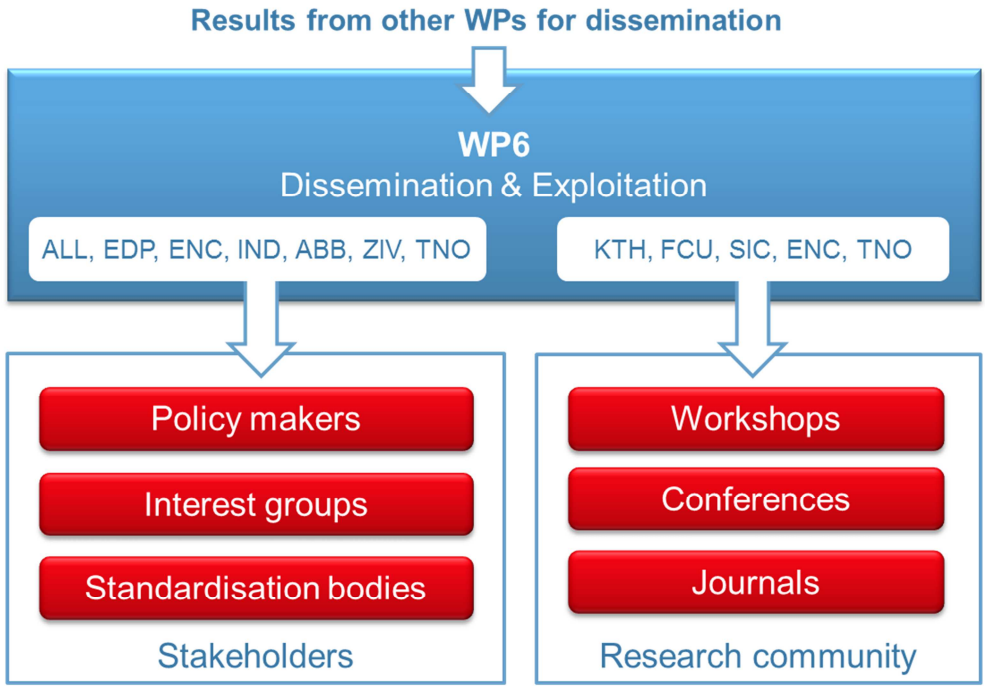

Figure 3 – SEGRID dissemination approach

The activities are distributed among the SEGRID project partners, but each partner will have a specific focus.

5 Communication Channels, liaison and media

This section describes the dissemination channels, liaison activities and dissemination means and media that SEGRID will utilize.

5.1 SEGRID logo

The SEGRID logo will be used consistently throughout all communications of the SEGRID project. See below in Figure 4 for the logo and its different appearances.

Figure 4 The SEGRID logo and its appearances

5.2 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. Also it offers the possibility to download (non-classified) deliverables and it offers the opportunity to contact the project. The website will be refreshed with actual information as often as possible. See Figure 5 for an impression of the website.

Figure 5 – SEGRID website start page

5.3 SEGRID flyer

The SEGRID flyer is meant to be distributed at events and conferences. 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 web-site. See Figure 6 for an impression of the SEGRID flyer.

Figure 6 – front page of SEGRID flyer

5.4 SEGRID white paper

The SEGRID white paper is composed of project results and is specifically targeted to raise awareness among policy makers and higher management of stakeholders. It will contain results of all RTD work packages, clarifying what has been achieved and putting the SEGRID results in the perspective of the SEGRID stakeholders.

5.5 SEGRID workshop

Two public dissemination workshops will be organised, possibly in collaboration with other conferences and/or projects. The first workshop will take place just before the second project review, the second at the end of the project. The goal of these workshops is to inform utility companies and smart grid equipment manufacturers about the project's results and to stimulate feedback. With this timing of the first workshop the consortium still has the possibility to adjust specific system aspects, methods or tools based on the feedback. These events will be

public and timely advertised to convey a large audience. The SEGRID Advisory Board will also be invited for those workshops.

5.6 SEGRID Advisory Board (SAB)

The SEGRID Advisory Board (SAB) will form 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. The members of SAB are not directly involved in the project work in order to ensure evaluation independence. SEGRID will use the SAB as a means to verify the technical direction of the project, but also utilize the SAB as a dissemination channel, taking profit of the extensive network of the individual SAB members.

5.7 Conferences

SEGRID will take a flexible approach towards conferences. When it is in the interest of SEGRID, the project will strive to attend or if possible present at relevant conferences. Although a complete and comprehensive list cannot be given for the whole project lifetime, at least the following list of conferences is considered to be important for SEGRID and active presence will be sought at these conferences.

- IFIP Working Group 10.4 meeting, Bristol UK, January 22nd – 26th, 2015
- European Smart Grid and Cyber Security 2015, London, March 9th and 10th
- Cyber- Physical Systems week, Vienna, April 10-14, 2016
- IEEE/IFIP Internatinal Conference on Dependable Systems and Networks
- IEEE Symposium on Reliable Distributed Systems
- USENIX Security Conference
- IEEE Symposium on Security and Privacy Conference
- Network and Distributed System Security Symposium
- ACM Conference on Computer and Communications Security

SEGRID will also strive to participate in the annual conferences as shown in Table 2 below.

Table 2 Overview of annual conferences

Conferences	About	Target audiences
European Smart Grid Cyber and SCADA Security	Annual conference on European Smart Grid Cyber and SCADA Security organised by SMi Group.	stake holders
IEEE Smart gridComm	IEEE International Conference on Smart Grid Communications (Smart gridComm) is centred on all communi-	research community, stake holders

	cations aspects that are relevant to the Smart Grid and aims at bringing together researchers from Academia, Industry, and National Labs to exchange novel ideas, explore enabling technologies, discuss innovative designs, and share field trial experiences and lessons learnt.	
ICS Cyber-Security	The conference where industrial control systems users, ICS vendors, system security providers and government representatives meet to discuss the latest cyber-incidents, analyse their causes and cooperate on solutions.	stake holders
CRITIS	CRITIS Conference on Critical Information Infrastructures Security is set to presenting innovative research and exploring new challenges for the protection of critical infrastructures.	research community
ENERGY	ENERGY is a large event focusing on Green approaches for Smart Grids and IT-aware technologies. It addresses fundamentals, technologies, hardware and software needed support, and applications and challenges (incl. cyber-security).	stake holders
SANS SCADA & Process summit	SANS is a well renowned company that specialises in information security training and certification. Among their many knowledge domains they also have SCADA and ICS security with a large number of successful conferences and courses. Within this area yearly conferences are organised annually in both the US and EU.	stake holders
IEEE PES Innovative Smart Grid Technologies (ISGT) Europe	ISGT is organised annually by IEEE Power & Energy Society. It has since its start been recognising the topic of cyber security with papers and panels on the topic.	research community
European Utility Week	A big yearly conference and exhibition (perhaps the biggest in the domain) targeting all topics from transmission to end users in electric power. (http://www.european-utility-	stake holders

	week.com/conference) It is well-known for its market leading conference programme, featuring over 300 high level speakers and covering all the major value streams	
ARES	http://www.ares-conference.eu/conference/	research community
FSE (Fast Software Encryption)	http://light-sec.org/fse2015/index.php/event/program	research community
CIRED (International Conference and Exhibition on Electricity Distribution)..	This series of biennial conferences began in 1971 and we are now at the 23rd edition	stake holders

5.8 Journals and magazines

Journals and magazines are a very suitable channel to publish SEGRID results. SEGRID has identified the following list of journals and magazines as relevant for the project dissemination objectives and will strive to publish SEGRID results in those magazines. This does not exclude any other opportunity that might arise to publish SEGRID results in other magazines or journals. Journals/magazines where SEGRID has published or plans to publish are:

- IEEE Transactions on Reliability
- IEEE transaction on dependable and secure computing
- Elsevier Computer and Security

5.9 SEGRID liaison activities

5.9.1 EU projects

SEGRID aims to liaise with a limited number (4-6) of projects that have comparable objectives as SEGRID. There already is a liaison agreement with SPARKS, the other project that was funded in FP7 call SEC-2013.2.2-3.

5.9.2 Standardisation bodies

Where possible, SEGRID will set up liaisons with relevant standardization bodies. One reason is the dissemination of SEGRID results into standardization bodies, another reason is the improved availability of standards for the SEGRID project.

5.10 Press releases

SEGRID does not foresee the publication of press releases. But if necessary, this channel will be utilized, after consultation of the PO and preserving the classification of information.

5.11 Demonstrations

One of the most visible results of SEGRID is the test-environment, Security Integration Test Environment (SITE). SITE will be built across several countries (Netherlands, Portugal, Spain, Sweden). When SITE is built, it is possible to give local demonstrations and site visits to show the test-environment and the implemented security solutions. Site visits and demonstrations will be on request only and will have to take into account the classification level of SEGRID results.

5.12 Social media

SEGRID will implement a Linked-In account to provide the Linked-In community with results of SEGRID.

5.13 Give-aways

If budget allows, SEGRID will order some simple give-aways with the SEGRID logo, to distribute at conferences and events.

5.14 Video

If budget allows, SEGRID will produce a short (animated) film with a simple explanation of the SEGRID approach and results, to present the SEGRID results to a broader public.

6 Exploitation

The SEGRID partners all will strive to maximally exploit the SEGRID results. These results will be exploited by all individual partners, after the project. The way of exploitation will be addressed in individual partner exploitation plans, that will be made in the last phase of the project. In the exploitation of the project results, SEGRID will take into consideration different scenarios depending on the maturity of the technologies under research and development. The exploitation plans will be based upon the initial ideas (see Annex B: Initial exploitation ideas) that were already drawn up during the proposal phase of SEGRID.

7 Dissemination Work Plan

This section provides a comprehensive plan for the SEGRID dissemination activities. These activities can be divided in three categories:

- Ongoing activities – these are activities that will be ongoing during project life-time, such as maintaining the website
- Planned activities – these are activities that can be planned beforehand, either at a specific date or in a timeframe (e.g. Q4 of 2016)
- To-be planned activities these are activities that cannot be planned at this moment. They will be listed and where possible, the activities are planned at specific dates during the project, but not every activity can be planned beforehand.

After each year, a concise report of the SEGRID dissemination activities will be made.

7.1 Ongoing dissemination activities

A number of dissemination activities are ongoing and are listed in Table 3 below.

Table 3 - Ongoing dissemination activities

Dissemination activity	Responsible partners
Maintaining the SEGRID website	TNO
Distributing the SEGRID flyer (pdf download and physical copies)	All partners
Maintaining the Linked-In account	TNO
Responding to questions of interested people (through website or Linked-in)	All partners
Set up liaisons with other projects and standardization bodies	All partners

7.2 Planned dissemination activities

The table below shows the planned dissemination activities for the SEGRID project.

Table 4 – planned dissemination activities

Dissemination activity		Planned date	Responsible partners
IFIP Working Group 10.4 meeting	2015	Q1, 2015	FFCUL
First SAB meeting		Q1, 2015	TNO
European Smart Grid and Cyber Security 2015 (London)		Q1, 2015	TNO
SPARKS stakeholder's workshop (Cork)		Q1, 2015	TNO
CIRED (Lyon)		Q2, 2015	TBD
ARES conference (Toulouse)		Q3, 2015	ENCS
CRITIS Conference on Critical Information Infrastructures Security 2015 (Berlin)		Q4, 2015	TNO

IEEE PES Innovative Smart Grid Technologies (ISGT) Europe (Warsaw)		Q4, 2015	TBD
European Utility Week 2015 (Vienna)		Q4, 2015	TBD
European Smart Grid and Cyber Security 2016 (London)	2016	Q1, 2016	TBD
SEGRID first workshop (NL)		Q1, 2016	TNO
Second SAB meeting (TBD)		Q1, 2016	TNO
CIRED (TBD)		Q2, 2016	TBD
A SEGRID Session at SICS Security Seminar 2016 (Stockholm)		Q2, 2016	SICS
A workshop or panel session (in cooperation with SPARKS and SALVAGE) during Cyber-Physical Systems week (Vienna)		Q2, 2016	TNO
IEEE/IFIP International Conference on Dependable Systems and Networks (TBD)		Q2, 2016	FFCUL
ARES conference (Toulouse)		Q3, 2016	ENCS
Third SAB meeting (TBD)		Q3, 2016	TNO
SEGRID white paper publication		Q4, 2016	TNO
CRITIS Conference on Critical Information Infrastructures Security 2016 (Berlin)		Q4, 2016	TNO
IEEE PES Innovative Smart Grid Technologies (ISGT) Europe (TBD)		Q4, 2016	TBD
European Utility Week 2016 (Vienna)		Q4, 2016	TBD
European Smart Grid and Cyber Security 2017 (London)	2017	Q1, 2017	TNO
Fourth SAB meeting (SITE demo, TBD)		Q2, 2017	EDP, ENCS
CIRED (TBD)		Q2, 2017	TBD
Publishing exploitation plans		Q3 2017	All partners
SEGRID final workshop (SAB invited, TBD)		Q3 2017	TNO

7.3 To-be-planned dissemination activities

The following table contains an overview of dissemination activities that cannot be planned at this moment. This also includes annual conferences that are organized outside of Europe. SEGRID budget does not include travels outside of Europe, unless the SEGRID PO gives permission. So SEGRID can only be disseminated at these conferences after permission of the PO.

Table 5 – To-be-planned dissemination activities

Dissemination activity	Responsible partners
Dissemination towards standardization bodies (2015-2017)	All partners
Publishing papers in the context of conference presentations or in magazines and journals (2015-2017)	All partners
Informing policy and decision makers ((2015-2017, EU and national level)	All partners
Visits and demonstrations to SITE locations for interested parties	ENCS, Alliander, EDP, ZIV, KTH
Publishing press release(s) if relevant and needed	TNO
Producing a short (animated) video	TNO
Attending conferences if feasible:	
USENIX Security Conference	TBD
IEEE Symposium on Security and Privacy Conference	TBD
Network and Distributed System Security Symposium	TBD
ACM Conference on Computer and Communications Security	TBD
IEEE International Conference on Smart Grid Communications	TBD
ICS Cyber-Security	TBD
SANS SCADA & Process summit	TBD
FSE (Fast Software Encryption)	TBD

Annex A: SEGRID participation in technology platforms and industrial associations

Table 6 - SEGRID participation in technology platforms, stnadardization bodies and industrial associations

Industrial associations, technology platforms, standardisation working group	Main partners involved
Working Group Smart Grid Information Security (SGIS) under EU Mandate M/490	ALL ENC
Smart Metering Coordination Group (SM-CG) under EU Mandate M/441	ALL ENC
EU DG ENERGY Task Force Smart Grid Expert Group 2	ALL EDP
International Electrotechnical Commission (IEC) TC57 WG15 - Power systems management and associated information Exchange - Data and communication security	ALL, ABB, ZIV
IEC TC57 WG09; IEC TC57 WG10; IEC TC57 WG17; IEC TC57 WG19; IEC TC57 WG20	ZIV
CENELEC TC13 WG02 (privacy & security smart meter)	ALL
IEC TC65 WG 10 - Security for industrial process measurement and control - Network and system security	ALL, ABB
DLMS User Association	ALL, ABB, ZIV
ISO JTC1 SC27 – IT Security Technologies	TNO
European Research Network on CIP (ERNCIP) Thematic Group on ICS and Smart Grids	TNO, ALL
ENISA	ENC, ABB
EU DG Connect – Expert group on the security and resilience of Communication networks and Information systems for Smart Grids	ALL, TNO, ABB
CIGRÉ (International Council on large electric systems) http://d2.cigre.org/ • CIGRÉ Working Group D2.31 Security architecture principles for digital systems in electric power utilities • CIGRÉ JWGB5/D2.46 Application and management of cyber security measures for Protection & Control systems • CIGRE D2; CIGRE WG C6.21; CIGRE JWG C6.25/B5/CIRED; CIGRE B5.48.	ALL KTH KTH ZIV
EU DG ENERGY TNCEIP	ALL
IEC TC57 WG10 PS IED Communications & Data Models	ABB
IEEE P1901.2 Narrowband Powerline Communications below 500 kHz for smart grids	ABB

IEEE C37.240 WG - PC37.240 Cyber Security Standard	ABB
NERC-CIP http://www.nerc.com/	ABB
Eurelectric http://www.eurelectric.org/	EDP
Prime Alliance http://www.prime-alliance.org	EDP, ZIV
ESNA http://www.esna.org /	ALL
ENTSO-E https://www.entsoe.eu/	ALL
LOGISTOP - Technology Platform in Logistics, Intermodality and Mobility www.**logistop**.org	IND
PESI - Spanish Technological Platform for Industrial Safety www.**pesi**-seguridadindustrial.org/	IND
Confederation of Netherlands Industry and Employers (VNO-NCW) – Cyber security committee	TNO
Electric Energy Systems - University Enterprise Training Partnership (EES - UETP) http://www.ees-uetp.com/	KTH
NEN NEC13 – Dutch Standardization Organization for Smart Meters	ALL
CPNI/NCSC Energy-ISAC	ALL
Spanish Association of Standardisation: AENOR SC94-95; AENOR SC57	ZIV
European Smart Metering Industry Group (ESMIG): Security and Privacy Group (SPG); Communications Technology Group (CTG).	ZIV
European Smart Grid Technology Platform	ZIV
Smart Grid Coordination group (SGCG): Smart Grid Information Security (SGIS), First Set of Standards (FSS)	ZIV
NIS Platform (https://resilience.enisa.europa.eu/nis-platform)	ENCS
NIST CPS-PWG (http://www.cpspwg.org/)	ENCS

Annex B: Initial exploitation ideas

In the table below, the initial ideas concerning exploitation of results per partner, as already included in the SEGRID proposal, are listed.

Table 7 Initial exploitation plans of partners

Partner	Planned use of project results	Timetable for (commercial) use	Expected market size
TNO	TNO aims to build a bridge between industry and the academic world, both in the Netherlands and on a European scale. We are therefore exceptionally well positioned to put the SEGRID scientific results into industry perspective. We are planning to apply the risk assessment methodology, developed in SEGRID, to our industrial and business customers. Also we expect to support the implementation of the newly developed security technology at our customers.	2-4 years after the project start	European smart grid stakeholders
SIC	SICS as a non-profit organisation, does only limited commercial exploitation of its research results. However, following its mission to support Swedish Industry, SICS helps their industrial partners to realise business opportunities on the basis of recent research results. Another more direct means of exploitation which SICS has used on several occasions in the past is to found and support spin-off companies based on commercially promising research results. Since 1997 thirteen such spin-off companies have been founded by members of SICS, of which two have been acquired by larger companies and eight are still in business.	2-4 years after the project start	Swedish smart grid stakeholders
KTH	KTH has two interests in exploitation of the results of SEGRID. Firstly, the enhanced CySeMoL framework targets industrial users. The end goal is that CySeMoL is used in end-user organisations for monitoring security and for aiding decision making about future development of smart grid solutions and architectures. Secondly, the smart grid lab, that will be further developed in SEGRID, is used as an integral part of education and research, but also commercial testing of smart grid solutions is planned for the future.	From project end.	European (in particular Swedish) utilities
IND	Increase the technical assistance to INCODE clients in the countries where have current presence	1-3 years after the project conclusion	INCODE maintains clients all over Spain, Portugal, Belgium and USA.

Partner	Planned use of project results	Timetable for (commercial) use	Expected market size
ENC	ENCS is established with the objective to increase the resilience of European critical infrastructures - such as the energy and water sector - against cyber-attacks. The project results will directly benefit to this objectives. The project results and the newly developed security technology will be used to further strengthen the ENCS security training program, and the ENCS end-to-end security test environment and to share the good practices with our customers in Europe. Further the project results will contribute to our ambition to develop a monitoring service for the smart grids and ICS/SCADA infrastructure for DSOs in Europe. ENCS is convinced – based on market research – that there will be a large market potential for this proposition.	1 to 3 years after project start	Grid companies , DSO's, TSO's in Europe
ALL	As a DSO end-user Liander is an important stakeholder to learn from the activities within the SEGRID project and to implement the results of this project. In 2013 Liander is preparing to introduce Cyber Resilience in the organization as a part of an IT/OT transition programme. Therefore Privacy & Cyber Security will be part of the Smart Grids design and the SEGRID results will be input for this design.	1-8 years after the project starts	3.6 million households in the Netherlands
ABB	ABB is a world leading vendor of communication products and solutions to the power industry. Among its offerings, solutions for wireless broadband IP communication is a future oriented area with substantial growth potential, especially with regard to the increasing importance of Smart Grids where secure wireless communication will be necessary. ABB is convinced that the results from SEGRID will be possible to use in the ABB products, mainly in the mesh routers family and the Gigabit products.	ABB expects that already in the second year of the SEGRID project intermediate results from SEGRID will be possible to integrate in our commercial products offerings. Further concrete results from SEGRID are expected in the following periods.	ABB is selling Smart Grid solutions on the world market and this is a part of the utility market part that will increase substantially. Secure communication solution and products is, and will be, a prerequisite for winning many of these contracts. The security requirement will grow in importance over the coming year.
FCU	FCUL has a tradition for exploitation of research results through technology transfer, and research groups have during the past few years performed collaborative projects with companies in several business segments. FCUL is mostly involved in research and teaching, therefore the core of its dissemination activities will be related to publications in high-impact, international venues, and participation in advanced courses and seminars. Moreover, the FCUL team is composed of professors currently involved in a Professional Master about security and dependability, which will be an important way of disseminating the project results among people that will become leaders in these areas in industry.	2-4 years after the project start	Portuguese industry

Partner	Planned use of project results	Timetable for (commercial) use	Expected market size
EDP	EDP Distribuição is building its electricity distribution smart grid which brings new cyber security risks when compared to the traditional grid. If the security of the grid is compromised it can have an impact in the integrity of the grid infrastructure, quality of service provided and safety of workers and clients. Therefore, EDP Distribuição is making a great effort to improve the cyber security and safety of its grid. SEGRID will enhance risk assessment methodologies and develop novel security measures to fill the gaps existing in current security technologies that EDP Distribuição can use to further improve its smart grid to an even higher level of security. Also, by participating in this project, EDP Distribuição's cyber security team will be able to share knowledge, experience and to improve its skills and competencies.	2 to 4 years after the start of the project, depending on the results	Portugal