FP7 Grant Agreement N° 607109

***S*ecurity for smart *E*lectricity *GRID*s**

Technical periodic report
Year 2

Due date of deliverable: 30/11/2016
Actual submission date: 07/12/2016
Number of pages: 48
Revision: Version 1.0
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	TNO Reinder Wolthuis
Contributor(s)	TNO Frank Fransen SIC Rolf Blom SIC Marco Tiloca KTH Mathias Ekstedt INC Antonio Silva Moriano ENC Maarten Hoeve ALL Sander Kruese ABB Gunnar Bjoerkman FCU Nuno Neves EDP Nuno Medeiros ZIV Exabier Bilbao Hernández

TABLE OF CONTENTS

1 Publishable summary

1.1 Summary description of project context and objectives

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 of the electricity grid. Not only does it add new routes through which cyber attackers can enter and attack the networks of grid operators, the automation also offers more possibilities to do damage to the electricity grid itself.

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. SEGRID has defined five use cases that clearly demonstrate this gradual evolving system concept. Moreover, these use cases have been selected to reflect important steps of the smart grid developments for the coming years, and theaddition of new functionality and components that inherently will introduce new vulnerabilities and widen cyber-attack surface.

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.

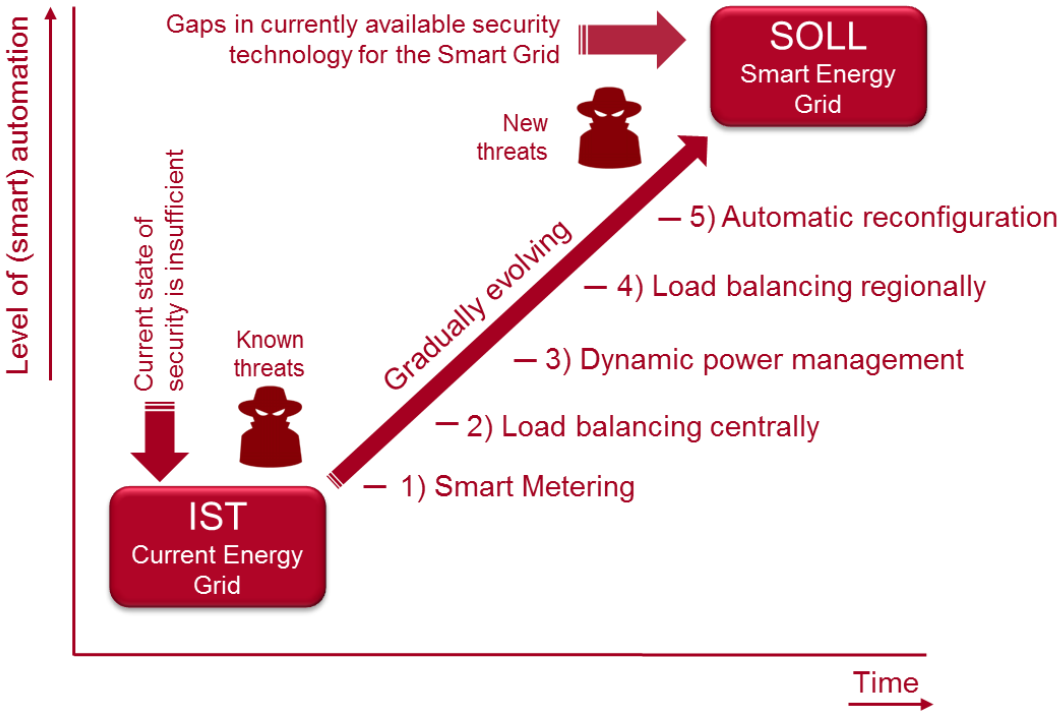

Figure 1: SEGRID storyline

SEGRID's main objective is to enhance the protection of smart grids against cyber-attacks. We are convinced that SEGRID will deliver a major contribution to the protection of future smart grids against cyber-attacks by:

- Identifying threats and potential future cyber-attack pathways, for the SEGRID use cases;
- Determining the gap between currently available security standards, methods and measures for smart grids in order to derive which additional security methods and measures are required for the SEGRID use cases;
- Developing the necessary new security methods and measures for privacy, communication and system security in smart grids, to mitigate the threats found in the SEGRID use cases, evaluate and test them;
- Building up a realistic test environment (Security Integration Test Environment, SITE) to test and verify new security methods and measures;
- Evaluating and improving current risk management methodologies in order to make them optimally suited to identify and address the key risk factors of smart grids of 2020;

- Feeding the established results from the SEGRID project into European and global standardisation bodies, industry groups and smart grid suppliers and make sure that the project results fit the needs of those communities and raise awareness among stakeholders.

1.2 Work performed and main results achieved so far

In chapter 2, the main results per work package are described.

1.3 Expected final results and potential impacts

Expected final results

Based on the SEGRID use cases, threats and risks of cyber-attacks on Smart Grids have been identified, and gapshave been identified between available and needed security techniques for smart grids to mitigate the identified threats and risks. Tools to analyse threat, risks and vulnerabilities in Smart Grids have been developed and made available. New security solutions have been developed and tested that are specifically targeted at the future smart grid and to fill some of the identified gaps.SEGRID results havebeen disseminated to appropriate industrial partners, standardisation groups, governmental bodies, research community and regulators.

Potential impacts

The SEGRID methods, tools and solutions willsupport building a secure, privacy preserving and resilient smart grid, which can be trusted by all stakeholders and interested parties, and which can support new business models, economic growth, and introduction of more sustainable and locally generated power.

SEGRID will have a focused dissemination effort to ensure that the results are fed to the appropriate industrial partners, standardisation groups, governmental bodies, research community and regulators.

Project public website address: http://www.segrid.eu

2 Core of the report for the period

2.1 Work progress and achievements during the period

This section describes the progress and achievements of SEGRID per Work package.

2.1.1 WP1

WP1 had three different contributions to be delivered during months 13 to 24: D1.2 (T1.1), D1.4 (T1.2) and D1.5 (T1.3).

- We have successfully delivered D1.2, where we provided an overview about the SEGRID project, by telling the story on how the different WP relate to each other, as well as the dependency and complementarity between the various deliverables.

- We have successfully delivered D1.4, where we defined the the *final set* of security & privacy goals for the SEGRID use cases, updating D1.3 based on the existing developments of the project and the current European security and privacy guidelines.
- We have successfully delivered D1.5, where we identified and analysed the most relevant existing standards and policies regarding Smart Grid Security and Privacy. This deliverable was initially planned for submission in month 15. However, since the SEGRID consortium was not satisfied with the overall quality of D1.5, a deadline extension to month 21 was requested and approved by the PO.
- D1.6 refers to recommendations of improvement for existing smart grid security policies and standards, and it was initially planned for submission on month 21. However, since it is dependent on the results from D1.5, its deadline has also been extended to December 31st 2016

Significant results

We successfully delivered D1.2, which intends to give an overview about the SEGRID project, by telling the story on how the different WP relate to each other, as well as the dependency and complementarity between the various deliverables.

We successfully delivered D1.4, which contains the final report on the security & privacy goals for the SEGRID Use Cases.

We successfully delivered D1.5, which provides a general overview of the most relevant existing standards and policies regarding Smart Grid Security and Privacy.

Deviations from the workplan, their impact and corrective actions

D1.5 had a deadline extension since the consortium was not satisfied with the results and the document overall quality. With the extra time, we were able to raise its quality and value, and have been able to deliver it on time for the new deadline, on month 21.

In a first stage D1.5 had a deadline extension due to our accepted proposal to broaden its scope. Besides our own analysis of existing standards and policies regarding smart grid security, we will also inquire other significant stakeholders about the topic in order to identify which are the most relevant standards and policies being adopted and the standing gaps that may lead to a new set of regulatory recommendations and policies.

There was a transfer budget from Incode to TNO of 3 PM. This is already in the list below.

The deadline of delivering D1.6 was extended to December 31st 2016 (planned for October 1st 2016).

Work package no.	**WP1**	Plan-Start:	**M01**	Plan-End:	**M36**
Lead Participant	**EDP**	Actual-Start:	**M01**	Actual-End:	
Work package title	**Use cases and security goals**				
Activity Type	**RTD**				

Resources allocated / Plan vs. Actual											
Participant	**Total**	**TNO**	**SICS**	**KTH**	**INC**	**ENCS**	**ALL**	**ABB**	**FCUL**	**EDP**	**ZIV**

Total PM planned for WP	**47**	11	2	2	4	5	5	2	5	8	3
Actual PM spent for WP in reporting period	**15,82**	4.37	1.2	0	2,3	0,5	0,9	0,2	0.3	5,8	0,25
Actual PM spent for WP in total	**31,77**	9.47	2.9	1,15	2	2,9	1,9	0,7	1.10	5,8	1,25
Remaining PM for WP in project	**15,23**	1.53	-0.9	0,85	-0,3	2,1	3,1	1,3	3.90	2,2	1.75

2.1.2 WP2

Summary of progress

WP2's objective is to

1) Perform a risk analysis on the SEGRID use cases to identify current and future threats and risks of cyber-attacks against smart grids;
2) Analyse the gap that there is between the risks that can be mitigated with existing security measures and risks that will require new security measures;
3) Evaluate, further develop and enhance risk management approaches specifically suited for the future smart grids that can be characterized by multiple administrative domains and high technical complexity.

WP2 has enhanced the step-based approach to risk assessment based on the HMG IA. Based on the recommendations from D2.1, we extended the 4 step approach to a full SEGRID Risk Management Methodology (SRMM) targeted to be used by organisations to assess risk in their Smart Grid developments. This methodology is described extensively in D2.2, including guidance for its use. We have improved the SRMM with notion of dependencies and responsibilities between systems and/or stakeholders in a system-of-systems environment. The risk estimation step has been enhanced to include the threat actor capability and motivation. The Impact Assessment includes an assessment of societal impact. To evaluate the methodology in practice we applied it to a selection of SEGRID use cases. Based on these experiences, we conclude that the SRMM provides the necessary enhanced guidance to manage risks in smart grids. It is distinct from other approaches by taking into account relevant aspects, such as society impact and stakeholder-interests in the smart grid area.

WP2 has performed a gap analysis of the current security technologies for smart grids. WP2 has identified several areas where further development of countermeasures (or security controls) are needed to improve the resilience and security of the smart grid. The analysis was performed by comparing existing solutions with ones that are predicted to be available in the near future, when the SEGRID use cases are made operational by the electrical Distribution System Operators (DSO) and other stakeholders that intervene in the power networks.

Within the SEGRID project, the results from the gap analysis are key to align the mitigation strategies and security mechanisms being designed and implemented in WP4, ensuring that they address a relevant subset of the gaps that were discovered. In addition, they help to frame the roadmap for smart grid security. The roadmap is aimed at DSOs and manufacturers and gives and overview of the technologies and methods that are needed to bring their smart grid technologies to the next level. The roadmap also informs policy makers and standardization bodies on how we think risk assessment methods will evolve in the future.

Significant results

WP2 has elaborated on the step-based approach to risk assessment based on the HMG IA and has gone further, extending the 4 step approach to a full SEGRID Risk Management Methodology (SRMM) targeted to be used by organisations to assess risk in their Smart Grid developments.

The risk estimation step has been enhanced to include the threat actor capability and motivation in the estimation of the likelihood of a threat being enacted. This enhancement has been submitted to the security standardization body ETSI TC Cyber as a CR to ETSI TS 102 165-2, the TVRA, and this CR has been accepted by TC Cyber, guaranteeing that this work of SEGRID will be used.

WP2 has enhanced the spreadsheet tools to support the stakeholder impact assessment, and the threat actor analysis.

WP2 has analysed the gap that there is between the risks that can be mitigated with existing security measures and risks that will require new security measures and based on this work has provided a roadmap for smart grid security.

Although there are no WP2 activities scheduled in Y3, we recommend publishing the SEGRID Risk Management methodology (but **not** the results of applying the SRMM to the SEGRID use cases) as a separate, publicly available methodology, including the accompanying toolset, such as empty templates of the impact and TVRA spreadsheets. Before publishing, we need to make some improvements, such as:

- Improving the methods for documenting the flows, the stakeholder processes and including the NRM.
- Improve the available tooling.
- Improve the layout of the diagrams from Step 1.

We propose to conduct this activity as part of the project, as this will improve the project impact. It can be conducted within the budget limits of the project.

Deviations from the work plan, their impact and corrective actions

The only deviation from the work plan was regarding the delivery of D.2.2, which was delayed by one month. The deliverable D2.2 was delivered to the EU on Monday, October 31st.

Work package no.	**WP2**	Plan-Start:	**M01**	Plan-End:	**M24**
Lead Participant	**ABB**	Actual-Start:	**M01**	Actual-End:	
Work package title	Application & enhancements of Risk Assessment				
Activity Type	**RTD**				

Resources allocated / Plan vs. Actual

Participant	Total	TNO	SICS	KTH	INC	ENCS	ALL	ABB	FCUL	EDP	ZIV
Total PM planned for WP	**28**	7	1	1	1	3	2	6	4	2	1
Actual PM spent for WP in reporting period	**19,13**	2.98	1	0	0,3	3,0	0,7	5,1	3.60	1,95	0,5
Actual PM spent for WP in total	**26,32**	5.08	1.4	0,44	0,6	3,0	1,7	7,4	4	1,95	0,75

Remaining PM for WP in project	**1,68**	1.92	-0.4	0,56	0,4	0,0	0,3	-1,4	0	0,05	0.25

2.1.3 WP3

Summary of progress

The objectives of WP3 are to identify and assess vulnerabilities in smart grids ICT components and architectures, and by doing this enabling future development of resilient ICT solutions. The work is divided into three tasks and where T3.1 and T3.2 focus on vulnerability assessment and T3.3 is devoted to vulnerability discovery. The work progress in WP3 is presented in D3.2.

T3.1 – Development of system-wide vulnerability assessment framework

In this task we have developed four reference architectures for key domains and components of smart grids. These reference architectures are SCADA systems, substation automation systems, automatic metering infrastructure, and (general purpose) operating systems. These reference architectures have been built in (two different) frameworks that enable automated vulnerability analysis. The majority of this work is finalized.

Furthermore, the work done in this task includes developing new vulnerability analysis capability serving the end goal of extending the vulnerability analysis frameworks as such. The capabilities addressed are: access control, privilege escalation, embedded systems, and protocol vulnerabilities. The main vehicle for this work is a new modelling language called pwnPr3d. The work with access control and privilege escalation is finalized whereas the latter two domains are work in progress.

T3.2 - Development of an active vulnerability assessment tool

The purpose of T3.2 is to develop method and a prototype for automated generation of vulnerability models in near real time, merging information from various existing system and network fingerprinting tools. In this task we have developed a general method for the import of the raw data. In essence the first step is to match the meta models (the model interchange format) of the raw data sources and the vulnerability model, secondly each raw data set needs an adapter, and thirdly merge the different potentially inconsistent data into a single consistent vulnerability model. This third step is the core of the research and here we are applying truth discovery algorithms and in particular Latent Credibility Analysis. Currently the theoretical model is in place and there is ongoing work to develop a fully working prototype. A first simple version of such prototype has been developed during year 2.

T3.3 – Vulnerability discovery and diagnosis tools

In this task we have made progress on the design and implementation of methodologies and tools for the discovery of vulnerabilities in software components used in smart grid infrastructures. We have focused in the following areas: (1) we have released the WAP tool for the discovery of vulnerabilities in applications programmed in the PHP language, namely web based interfaces; this tool is able to identify and correct automatically vulnerabilities; (2) we have made significant progresses on the development of a tool that can be employed to test and look for vulnerabilities in the devices connected to the control channel of a SDN network

(both switches and controller); (3) we have performed an assessment of some smart grid devices used by one of DSO partners, where we have identified some problems. These three lines of work will continue through the next year of the SEGRID project.

Significant results

- Reference architectures for SCADA, AMI, SAS (still some work remaining), and Operating Systems.
- A new vulnerability assessment framework, pwnPr3d, has been created.
- A theoretical methodology for automatic vulnerability model generation.
- A new version of the WAP tool has been released
- Results from the assessment of smart grid devices are being used by the DSO partner to improve the security of its infrastructure

Deviations from the workplan, their impact and corrective actions

There are no deviations, this work package still progresses according to the original work plan.

Work package no.	**WP3**	Plan-Start:	**M01**	Plan-End:	**M36**
Lead Participant	**KTH**	Actual-Start:	**M01**	Actual-End:	
Work package title	Enhancements of Vulnerability Assessment techniques				
Activity Type	**RTD**				

Resources allocated / Plan vs. Actual

Participant	Total	TNO	SICS	KTH	INC	ENCS	ALL	ABB	FCUL	EDP	ZIV
Total PM planned for WP	**56**	4	2	20	3	4	2	0	18	2	1
Actual PM spent for WP in reporting period	**21,99**	3.29	0.5	7	1	1,3	0,2	0	7.70	1	0
Actual PM spent for WP in total	**38,38**	3.54	0.7	14,24	2	1,6	0,2	0	15.10	1	0
Remaining PM for WP in project	**17,62**	0.46	1.3	5,76	1	2,4	1,8	0	2.90	1	1

2.1.4 WP4

Summary of progress

The objectives for WP4 are to develop novel secure, privacy-preserving and cyber-attack resistant ICT for the reference smart grid architecture(s) developed in WP1, the security gaps identified by WP2 and the cyber-attack paths identified in WP3.

During SEGRID Year 2, we have developed SPADE, an iterative design process to produce security and privacy architectures tailored to individual SEGRID use cases. Together with a

full description of SPADE, we have provided first examples of its application on SEGRID use cases 1-4.The other problem areas covered by WP4 are about how to: a) Provide secure virtualized platforms for secure execution of services with assurance of service integrity; b) Provide platform resilience, especially for SCADA systems, by means of machine replication protocols to tolerate arbitrary (or Byzantine) failures; c) Enhance network intrusion detection and prevention solutions for the protection of wireless mesh networks; d) Rely on the Software Defined Networking paradigm to assure a high level of communication resilience against faults and attacks in the network; e) Enhance robustness against Denial of Service attacks and scalability of key provisioning for TLS/DTLS; f) Enhance performance and scalability of group key management operations to support group software distribution based on secure broadcast communication; and, finally, g) Improve design and level of protection of personal information collected and processed in the smart grid. For area a), we have identified a list of security requirements to be fulfilled on platform-secure smart grid devices, and designed a preliminary model relying on virtualization techniques to be considered for the next development activity. For areas b)-f), we have provided initial specifications of related security and privacy solutions, with reference to the SEGRID use cases, and together with plans and schedules for testing and continuation during SEGRID Year 3. Finally, for area g), we have provided a description of privacy design patterns for smart grids.

A mapping of the above mentioned activities on the WP tasks is as follow:

T4.1 System & platform security:	SPADE process to design security and privacy architectures, problem areas a) and b)
T4.2 Communication protocols security:	Problem areas c) and f).
T4.3 Resilient communications infrastructure:	Problem areas d) and e).
T4.4 Privacy by design:	Problem area g)

Significant results

The main achievements of WP4 can be summarized as follows.

- WP4 has released its second deliverable D4.2 [D4.2] according to plans.
- WP4 has contributed to the definition of the final security and privacy goals presented in the deliverable D1.4 [D1.4], carried out by WP1.
- WP4 has contributed to the GAP analysis process carried out by WP2, towards the deliverable D2.3 [D2.3].
- WP4 has contributed to the deliverable D2.4 [D2.4] about the SEGRID cyber security framework and roadmap, by authoring a chapter about software security.
- WP4 has developed SPADE, an iterative process to design security and privacy architectures tailored to specific use cases. First examples of SPADE applied to SEGRID Use Cases 1-4 have been also provided. This has been a joint effort carried out especially with WP1 and WP2.
- WP4 has provided a first description of security and privacy solutions for the selected problem areas considered in SEGRID Year 1. The mapping between the scope of the preliminary solutions and the SEGRID use cases has also been enhanced.

- WP4 has scheduled specific test and evaluation sessions for the developed security and privacy solutions, in coordination with WP5 and starting from prototype software modules developed and/or integrated by WP4 partners. Therefore, the milestone MS6 due on M20 has been successfully achieved.
- WP4 has proposed a new research activity for SEGRID Year 3, covering the evaluation of impact of security attacks in SDN-based network environments, by means of network simulation tools.

Deviations from the work plan, their impact and corrective actions

This work package still progresses according to the original work plan.

But as can be seen from the resource allocation in the table below, the consumption of PM of SICS for WP4 is progressing faster than originally planned. This is mainly due to having a more junior researchers involved, but also doing more work than planned. SICS will certainly spend more than the remaining 6 man month over the next remaining year, but the expectation is that they will stay within the original budget.

Work package no.	**WP4**	Plan-Start:	**M03**	Plan-End:	**M36**
Lead Participant	**SICS**	Actual-Start:	**M03**	Actual-End:	
Work package title	Novel security solutions				
Activity Type	**RTD**				

Resources allocated / Plan vs. Actual

Participant	Total	TNO	SICS	KTH	INC	ENCS	ALL	ABB	FCUL	EDP	ZIV
Total PM planned for WP	**77**	9	21	0	2	4	1	5	25	2	8
Actual PM spent for WP in reporting period	**36,55**	4.27	12.7	0	0,7	0,4	0,1	1,7	11.78	0,9	4
Actual PM spent for WP in total	**73,55**	7.57	27.7	0	1,4	1,9	0,1	4,6	22.38	0,9	7
Remaining PM for WP in project	**3,45**	1.43	-6.7	0	0,6	2,1	0,9	0,4	2.62	1,1	1

2.1.5 WP5

Summary of progress

The goal of work package 5 is to develop the SITE test bed, and to use that test bed to evaluate the vulnerability assessment tools developed in work package 4, and the solutions developed in work package 4.

During the second year of the project, the establishment of the SITE test bed (task 5.2) was completed. Four test labs were established at the different project partners:

1. A joint lab by FCUL and EDPD with a focus on the networks and servers used in distribution automation SCADA systems.

2. A lab at ENCS with a focus on the embedded devices, such as RTUs, used in the substations for distribution automation.
3. A lab at KTH containing a full SCADA and distribution management system server system, and the wireless networking.
4. A lab at ZIV focused on testing smart meters and data concentrators, in particular those used in powerline communication networks.

Together these labs provide an almost complete coverage of the SEGRID use cases, as was planned in the original test bed design (deliverable 5.1). Procedures were established to connect the labs for future multi-site tests.

The second year also saw the start of the first test phase. In this phase, four solutions from work package 4 were integrated in the SITE test bed, and evaluated according to a pre-defined test plan. The solutions were:

1. *The group key management protocols developed by SICS*. These were integrated in the meters and data concentrators in the ZIV test bed. The initial tests have shown that the protocols do indeed lead to more efficient key management. Hence, they can be used for more efficient firmware distribution, one of the challenges in powerline communication networks, which have limited bandwidth.
2. *The resilient SCADA system solutions developed by FCUL*. The libraries for intrusion tolerant communication were integrated into the open-source Eclipse SCADA system in the FCUL labs. Tests have been performed showing the systems behave as expected.
3. *The resilient network solutions developed by FCUL*. These were integrated into the software-defined networking environment at FCUL, and evaluated on their performance.
4. *The DTLS improvements developed by SICS.* These were integrated into a simulated distribution automation environment at the ENCS test lab. In this environment, the IEC 104 protocol, commonly used in distribution automation SCADA systems, was run over the DTLS protocol to establish a secure communication channel. Then it was shown that the SICS improvements did indeed reduce the risk of certain denial-of-service attacks.

The tests are currently being completed. The results will be reported in deliverable 5.2, due in month 27. Demos were developed for the first, second, and fourth test activity above for the SEGRID workshop to be held in Barcelona on November 14.

Significant results

- Deliverable 5.2 was delivered according to plan.
- WP 5 continued the tight collaboration with work packages 3 and 4 to make sure the solutions developed there can be properly tested.
- Collaborations were established between different project partners for the tests: FCUL and EDPD collaborated on establishing the FCUL test environment, SICS and ZIV collaborated on the group key management protocols, and SICS and ENCS collaborated on the DTLS improvements.
- The group key management solutions were integrated by a manufacturer into actual smart meters and data concentrators, making a major step towards the actual deployment of the solutions in the field.
- Demonstrations were developed for the SEGRID workshop showing of three of the solutions from work package 4 integrated in the SITE test environment.

Deviations from the workplan, their impact and corrective actions

No deviations.

Work package no.	**WP5**	Plan-Start:	**M01**	Plan-End:	**M36**
Lead Participant	**ENCS**	Actual-Start:	**M01**	Actual-End:	
Work package title	Testing and evaluation				
Activity Type	**RTD**				

Resources allocated / Plan vs. Actual

Participant	Total	TNO	SICS	KTH	INC	ENCS	ALL	ABB	FCUL	EDP	ZIV
Total PM planned for WP	**63**	6	6	5	0	9	3	2	12	8	12
Actual PM spent for WP in reporting period	**23,56**	0	4.4	1,76	0	1,2	0,2	0	4.45	4,05	7,5
Actual PM spent for WP in total	**35,61**	0.2	5.3	3,36	0	5,1	0,2	0	8.90	4,05	8,5
Remaining PM for WP in project	**27,39**	5.8	0.7	1,64	0	3,9	2,8	2	3.10	3,95	3.5

2.1.6 WP6

Summary of progress

The main dissemination objectives of SEGRID are to inform the user community, to raise awareness among all relevant stakeholders of the risks of cyber-attacks on smart grids and how to addresses these risks, to develop the SEGRID smart grid security white paper, to organize and/or publish results in international event(s), to develop and implement an interactive and user friendly web site and to produce an exploitation plan. In Year1, important progress has been made on most of these objectives:

- SEGRID has presented on several conferences
- The SEGRID website has been maintained
- A SEGRID banner has been produced
- Some SEGRID gadgets were produced (cam cover and USB sync stop)

In the second year, the focus was on disseminating the results of SEGRID. Details can be found in the second dissemination report, D6.5. In the third year, the focus will be on exploitation of project results.

Figure 2 SEGRID website start page

Significant results

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. The accepted papers are published by IEEE, in the IEEE Conference Publication Program (CPP) and can be found on IEEE Explore.

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.

SEGRID presented a.o. 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.

A selection of papers that SEGRID submitted can be found in the table below.

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)

SEGRID has established a liaison with SPARKS, the other project that started under Topic SEC-2013.2.2-3. There has been coordination and cooperation on the following topics:

- Risk management
- Joint organization on workshop for CPS week 2016 (also with the SALVAGE project)

Deviations from the workplan, their impact and corrective actions

The SEGRID whitepaper was postponed from October 1st to December 31st, in order to include some of the results of deliverables that were due on October 1st.

Work package no.	**WP6**	Plan-Start:	**M01**	Plan-End:	**M36**
Lead Participant	**TNO**	Actual-Start:	**M01**	Actual-End:	
Work package title	**Dissemination & Exploitation**				
Activity Type	**OTHER**				

Resources allocated / Plan vs. Actual

Participant	Total	TNO	SICS	KTH	INC	ENCS	ALL	ABB	FCUL	EDP	ZIV
Total PM planned for WP	**32**	7	2	2	2	3	4	1	6	3	2
Actual PM spent for WP in reporting period	**8,04**	2.74	0.7	0	0,7	0,4	0,6	0	1.70	1,2	0.5
Actual PM spent for WP in total	**15,14**	4.84	0.9	0	0,7	1,1	0,6	0	4.10	1,2	1
Remaining PM for WP in project	**16,86**	2.16	1.1	2	0,6	1,9	3,4	1	1.90	1,8	1

2.2 Project management during the period

Meetings

The primary partner contacts of each partner meet in a progress conference call each month.

The progress meeting monitors the progress in the project and the alignment of the work in the WPs. So far all issues discussed in the progress meetings could be handled before an issue could turn into a risk.

Periodically (typically three times a year), general meetings are organized in which a general assembly is scheduled and (parallel) sessions for each work package are organized. In between these meetings, work package leaders have organized conference calls or physical

meetings when needed. See table below for an overview of the physical meetings in Year2. In the progress calls and general assembly meetings, no serious issues were raised. All partners are happy in the consortium and no partner has the intention to leave the consortium or substantially change their contribution to the project. None of the partners changed their legal status in Year2.

In Year2, one Segrid Advisory Board (SAB) meeting was organized, where the SAB provided feedback on the plans and approach of SEGRID.

Table 1 SEGRID meetings

SEGRID MEETING	DATE FROM	DATE TILL	LOCATION
Y1 Review meeting	11 Nov. 2015	12 Nov. 2015	The Hague
Consortium meeting	14 Dec. 2015	15 Dec. 2015	Amsterdam
Consortium meeting and SAB meeting	8 March 2016	9 March 2016	Lisbon
Consortium meeting	13 June 2016	14 June 2016	Oslo
Consortium meeting	5 Sep 2016	6 Sep 2016	The Hague

Quality

Although not a formal deliverable, SEGRID has made a project handbook which lays down the project internal quality procedures that are used in the project and the procedures that are necessary to handle classified information (EU restricted). In Year2, SEGRID will update this project handbook with relevant information.

Exchange of information and cooperation platform

To provide a cooperation platform, SEGRID uses a Sharepoint environment, provided by TNO, which is heavily used.

Because a number of the SEGRID deliverables are classified as ‘EU restricted’, SEGRID has acquired the encryption tool Filkrypto, manufactured by Tutus. This is a tool that is certified by the EU for the corresponding classification level. Tutus has given the SEGRID partners a short tutorial on the encryption tool and its use, during a general assembly meeting in Stockholm.

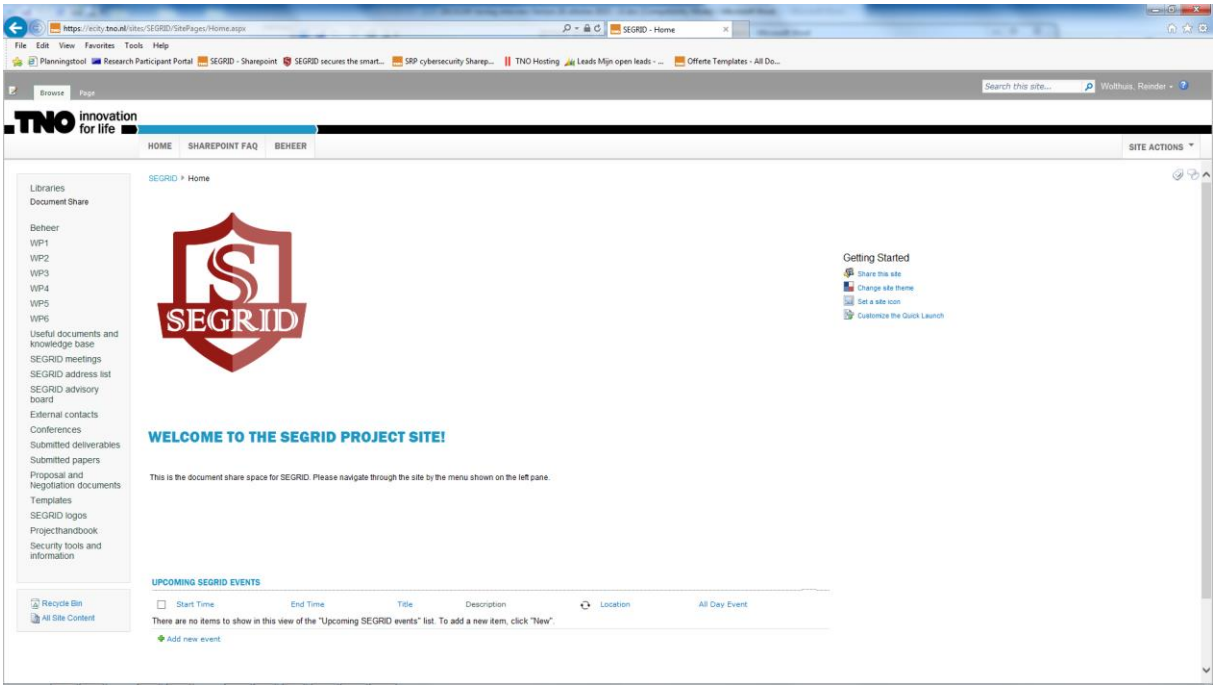

Figure 3 – SEGRID project internal cooperation platform

Project planning and status

To date, most project deliverables were submitted (very) close to the planned submission date, with only a few exceptions. See next paragraph for the deviations in deliverable submission.

Resource consumption is still according to plan (except for WP4, see explanation in 2.1.4)

Cooperation with other projects and project website

These topics are in the realm of WP6; see above in the WP6 progress section for details.

2.3 Deliverables and milestones tables

The table below shows the SEGRID deliverables of Year2

Deliverable number	Deliverable Title	WP no	Lead beneficiary number	Nature	Dissemination level	Delivery date from DoW	Actual Delivery date
D1.2	SEGRID smart grid security roadmap	1	9	R	PU	**18**	April 1st 2016
D1.4	Final report on security & privacy goals	1	1	R	PU	**24**	October 1st 2016
D1.5	Report on analysis of policies regarding smart grid security	1	4	R	PU	**12**	July 1st 2016
D1.6	Report with recommendations of improving smart grid security policies	1	4	R	PU	**21**	Delayed Dec. 31st 2016
D2.2	Enhanced methodology for risk assessment	2	1	R	Restreint EU	**24**	October 31 2016

Deli-verable number	Deliverable Title	WP no	Lead bene-ficiary number	Natu-re	Dissemi-nation level	Delivery date from DoW	Actual Delivery date
D2.3	SEGRID gap analysis	2	8	R	PU	**18**	April 1st 2016
D2.4	SEGRID Cyber Security Framework and Roadmap	2	5	R	PU	**24**	October 1st 2016
D3.2	Preliminary specification of smart grid vulnerability assessment techniques and tools	3	3	R	Restreint EU	**24**	October 1st 2016
D4.2	Preliminary specification of security solutions	4	2	R	Restreint EU	**24**	October 1st 2016
D5.2	Implemented SITE		5	O	Restreint EU	**18**	April 1st 2016
D6.4	SEGRID smart grid secu-rity white paper	6	1		PU	**24**	Delayed Dec. 31st 2016
D6.5	2nd report on dissemina-tion activities	6	1	R	PU	**24**	October 1st 2016

From the milestone table below one can derive that all milestones within the reporting period are met.

Milestone number	Milestone name	Lead bene-ficiary number	Delivery date from DoW	Actual deliv-ery date
MS1	Project start	1	1	October 1st, 2014
MS2	1st Annual Review	1	12	November 12th, 2015
MS3	2nd Annual Review	1	24	November 15th, 2015
MS4	Project end	1	36	-
MS5	Vulnerability assessment tool for integration in SITE	3	24	-
MS6	Novel security solutions of evalua-tion in SITE for 1st test phase	2	20	October 31st. 2016
MS7	Novel security solutions of evalua-tion in SITE for 2nd test phase	2	20	-

Deviations from the plan

There was some delay in the following deliverables:

- D1.5, due October 1st 2015, delivered July 1st 2016
- D2.2, due October 1st 2016, delivered October 31st 2016
- D1.6, due July 1st 2016, delayed until December 31st 2016
- D6.4, due October 1st 2016, delayed until December 31st 2016

The PO was pro-actively informed of these delays.

There was a budget transfer of 3 PM from Incode to TNO in WP1.

There were no other significant deviations from the plan in the reporting period. For the third year of the project we expect to meet all milestones and submission dates of deliverables.

2.4 Financial progress

The project will last 3 years. At the end of each year, all partners must report their financial data to the EU. Each partner must provide a form C, supplemented with the following tables:

For example:

- **PERSONNEL** entry should show reference to the:
  - Type of employment (part-time, full time)
  - Number of people involved
  - Person/months
  - hourly rate, standard productive hours …

- **TRAVEL** entry should show reference to the:
  - Number of participants (who)
  - Duration (when –exact dates)
  - Destination (where)
  - What kind of meeting, purpose of the meeting …

- **SUBCONTRACTING** entry should show reference to the:
  - Tasks performed by an external contractor
  - Description of the event/tasks

If the participant has no cost on one item, s/he should just delete that line from the table.

In the periodic report: The information is difficult to read and to be double-checked with the Forms C. Please adapt the table "Use of Resources" following the below **example**, and detail of information.

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 1 for the Period, TNO			
Work Package	Item Description	Amount in € with 2 decimals	Explanations
1,2,3,4,6,7	**Personnel direct costs**	*82,170.72*	*PM Junior Scientist: 3.73* *PM Scientist: 1.57* *PM Senior Advisor: 1.46* *PM Senior Scientist: 10.53* *PM Student: 2.39* *PM Technician 0.48* *PM Project assistant; 0.03*
	Subcontracting		
1,2,4,6,7	**Travel**	€ 571.73 € 1,630.68	TRAVELING: 4 persons, Den Haag (NL), 04 Sept 2016 until 06 Sept 2016, Meeting at ENCS TRAVELING: 4 persons, Lisbon (PT), 07 Mar 2016 until 09 Mar 2016, Project Meeting and Advisory Board

		€ 3,307.04	TRAVELING: 4 persons, Oslo (SE), 12 Jun 2016 until 15 Jun 2016, Project meeting
		€ 215.98	TRAVELING: 5 persons, Barcelona (SP), 13 Nov 2016 until 17 Nov 2016, Project meeting
		€ 160.44	1,2 TRAVELING: 2 persons, Amsterdam (NL), 13 Dec 2015 until 15 Dec 2015, Project meeting
		€ 111.02	1 TRAVELING: 1 person, Den Haag (NL), 10 Nov 2015, Project meeting
		€ 445.68	TRAVELING: 4 persons, Den Haag (NL), 04 Sept 2016 until 06 Sept 2016, Project meeting
		€ 823.73	7 TRAVELING: 4 persons, Lisbon (PT), 07 Mar 2016 until 09 Mar 2016, Project meeting and Advisory board
		€ 420.62	7 TRAVELING: 4 persons, Oslo (SE), 12 Jun 2016 until 15 Jun 2016, Project meeting
		€ 345.87	7 TRAVELING: 5 persons, Barcelona (SP), 13 Nov 2016 until 17 Nov 2016, Project review meeting
		€ 41.76	TRAVELING: 2 persons, Amsterdam (NL), 15 Dec 2015 until 16 Dec 2015, Project meeting
		€ 244.26	7 TRAVELING: 7 persons, Den Haag (NL), 1 Nov 2015, review meeting
		€ 1,276.15	TRAVELING: 4 persons, Lisbon (PT), 07 Mar 2016 until 09 Mar 2016, Project meeting
		€ 1,870.68	6 TRAVELING: 2 persons, Vienna (AT), 11 Apr 2016 until 14 Apr 2016, Workshop SPARK, SALVAGE
		€ 404.49	6 OTHER: Workshop SPARK, SALVAGE, Conference fee CPS 2016
		€ 172.94	6 TRAVELING: 5 persons, Barcelona (SP), 13 Nov 2016 until 17 Nov 2016, Project review meeting
		€ 404.60	6 TRAVELING: 1 person, Brussels (BE), 14 Oct 2015 until 15 Oct 2015, Presentation at EURELECTRIC
		€ 900.88	6 TRAVELING: 1 person, Sorrento (IT), 22 Sept 2016 until 23 Sept 2016, Project Presentation ETSI TC Cyber
	Consumables	€ 500.00	1 OTHER: Meeting Room in Barcelona Review
		€ 16.99	7 CONSUMABLES: Publication cost IEEE
		€ 125.00	6 OTHER: Hotel charged ETSI delegate package, Sorrento (IT), 22 Sept until 23 Sept 2016
			6 OTHER: Banner Segrid meeting,

		€ 181.50 € 162.50 € 495.00 € 1,013.51 € 39.00 € 1,375.00 € 1,950.00	Barcelona (SP), 13 Nov 2016 until 17 Nov 2016 6 OTHER: Website Segrid.eu 6 OTHER: Hosting website 2 years 6 CONSUMABLES: Hire meeting room, Barcelona (SP), 13 Nov 2016 until 17 Nov 2016 6 OTHER: Purchase of digital photos for dissemination Purpose 6 OTHER: Syncstop with Segrid Logo 6 OTHER: Webcamcover with Segrid logo
	Equipment		
1,2,3,4,5,6,7	**Indirect Costs**	*119,029.22*	
TOTAL COSTS [1]		*256,039.21*	

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 2 for the Period, SICS			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
WP1	**Personnel direct costs**	*8142*	*Rolf Blom, PhD (0,6 PM)* *Marco Tiloca,PhD((0,6 PM)*
WP2	**Personnel direct costs**	*6444*	*Rolf Blom, PhD (0,4 PM)* *Marco Tiloca, PhD (0,6 PM)*
WP3	**Personnel direct costs**	*3573*	*Rolf Blom, PhD (0,3 PM)* *Marco Tiloca, PhD (0,2 PM)*
WP4	**Personnel direct costs**	*61736*	*Rolf Blom, PhD (1,6 PM)* *Marco Tiloca, PhD (0,6 PM)* *RikardHöglund, BSc (3,1 PM)* *ArashVahidiMazinanu, PhD (0,6 PM)* *Jonas Haglund, Civ Ing (2,3 PM)* *Alexandra Stagkopoulou, BSc (2,7 PM)*
WP5	**Personnel direct costs**	*19152*	*Marco Tiloca, PhD (1,4 PM)*

			Rikard Höglund, BSc (3 PM)
WP6	**Personnel direct costs**	*4227*	*Rolf Blom, PhD (0,2 PM)* *Marco Tiloca, PhD (0,5 PM)*
WP7	**Personnel direct costs**	*4170*	*Rolf Blom, PhD (0,3 PM)* *Christian Gehrmann, PhD Prof ((0,15 PM)*
	Subcontracting		
WP7	**Travel**	*382,02*	*Rolf Blom, Project review* Amsterdam/Sloterdijk,Holland, Nov 11-13, 2015
WP4	**Travel**	*472,09*	*Marco Tiloca, Project meeting,* Amsterdam/Sloterdijk,Holland, Dec 13-16, 2015
WP4	**Travel**	*438,65*	*RikardHöglund, Project meeting,* Amsterdam/Sloterdijk,Holland, Dec 12-15, 2015
WP4	**Travel**	*444,46*	*Rolf Blom, Project meeting,* Amsterdam/Sloterdijk,Holland, Dec. 13-15, 2015
WP4	**Travel**	*444,23*	*Marco Tiloca, Project meeting,* Amsterdam/Sloterdijk,Holland, Jan 25-27, 2016
WP4	**Travel**	*562,51*	*Marco Tiloca, Project meeting,* Lisbon, Portugal, March 7-10, 2016
WP7	**Travel**	*553,84*	*Rolf Blom, Project meeting,* Lisbon, Portugal, March 7-11, 2016
WP4	**Travel**	*1009,58*	*Marco Tiloca, IEEE CPSR-SG2016 workshop and Segrid project meeting,*

			Vienna, Austria, April 10-14, 2016
WP4	**Travel**	*875,13*	*Rolf Blom, IEEE CPSR-SG2016 workshop and Segrid project meeting,* Vienna, Austria, April 11-13, 2016
WP4	**Travel**	*424,43*	*Marco Tiloca, Project meeting,* Oslo, Norway, June 12-14, 2016
WP4	**Travel**	*462,95*	*Rolf Blom, Project meeting, Oslo, Norway,* June 12-14, 2016
WP6	**Travel**	*1729,17*	*Marco Tiloca,* IEEE ISCC 2016 Conference, Messina, Italy, June 25 - July 1, 2016
WP4	**Travel**	*455,61*	*Marci Tiloca, Project meeting,* Den Haag, Holland, Sept 4-6, 2016
WP4	**Travel**	*463,88*	*Rolf Blom, Project meeting,* Den Haag, Holland, Sept 4-6, 2016
WP4	**Travel**	*568,00*	Alexandra Stagkoplulou, OMNET++ Community Summit 2016, Brno, Czech Republic, Sept 14-17, 2016
WP6	**Travel**	*626,38*	*Marco Tiloca,* OMNET++ Community Summit 2016, Brno, Czech Republic, Sept 14-17, 2016

WP4	**Consumables**	*157,99*	*Rolf Blom, Participate in NordSec, Oct 19-21, 2015*
WP7	**Equipment**	*106,02*	Folder cabinet 550x340x380
WP4	**Equipment**	*443,36*	Zigbee development kit
WP7	**Indirect Costs**	*1765*	
	Indirect Costs	*80105*	
TOTAL COSTS [2]		*118064,30*	*Does not include indirect costs*

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 3 for the Period KTH			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
1,2,3,5	**Personnel direct costs**	*62.236,46*	*Salary: Professor, 1,92 PM* *Salary: Professor, 3,24 PM* *Salary: Ph.D. student 3,60 PM*
	Subcontracting		
1,2,3,5,7	**Travel**	*662,23* *1.482,92* *1.440,55* *1.070,27* *1.297,67*	*Travel: 1 person: Haag, Review meeting Nov 11-12, 2015* *Travel: 2 person: Amsterdam, Project meeting, Dec 14-15, 2015* *Travel: 2 person: Lisbon. Project meeting, March 7-10, 2016* *Travel: 2 person: Oslo, Project meeting, June 12-14, 2016* *Travel: 2 person: Haag, project meeting, Sept 4-6, 2016*
	Consumables		
5	**Equipment**	*1.115,11*	*HP Proliant DL*
	Indirect Costs	*41.583,12*	
TOTAL COSTS [3]		*110.888,32*	

[2] Total costs have to be coherent with the costs claimed in Form C.

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 4 for the Period, INCODE			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
1,2,3,4,6,7	**Personnel direct costs**	*79.593,00*	*WP1:* • Marcial Valmorisco (aeronautical engineer expert in security area) • Antonio Silva (lawyer expert in privacy and ethical issues) The total p/m used in this period for this task was 2,3 p/m *WP2:* • Marcial Valmorisco (aeronautical engineer expert in security area) The total p/m used in this period for this task was 0,3 p/m *WP3:* • Marcial Valmorisco (aeronautical engineer expert in security area) The total p/m used in this period for this task was 1 p/m *WP4:* • Antonio Silva (lawyer expert in privacy and ethical issues) The total p/m used in this period for this task was 0,7 p/m *WP6:* In these cities technical meetings were prepared with presentation objective. Uses cases, smartgrid risk

			in each city This cost corresponding to an effort of 0,7 p/m WP7: The p/m of this figure is 0,7
	Subcontracting		
	Travel	*3.137*	*ANTONIO SILVA 12-15/06/2016 OSLO* *MARCIAL VALMORISCO 12-15/06/2016 OSLO* *ANTONIO SILVA 07-097/03/2016 LISBON* *MARCIAL VALMORISCO 07-09//03/2016 LISBON* *ANTONIO SILVA 14-15/12/2015 LA HAYA* *MARCIAL VALMORISCO 14-15/12/2015LA HAYA*
	Consumables		
	Equipment		
	Indirect Costs	*16.546,14*	
TOTAL COSTS [4]			

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 5 for the Period, ENCS			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
1,2,3,4,5	**Personnel direct costs**	39,967.53	WP 1: 0,5 PM WP 2: 3,0 PM WP 3: 1,3 PM WP 4: 0,4 PM WP 5: 1,2 PM Person months per function: Security tester: 1,9 PM Researcher: 2,9 PM Manager: 1,7 PM
	Subcontracting	*0*	
	Travel	*553,98*	*Bilbao plenary meeting; 6-9 Sept 2015; 1 person*

Total costs have to be coherent with the costs claimed in Form C.

		44,78 *504,76* *892,5* *341,71* *1735,46*	*Disseminiation workshop Elaad 13 May 2016; 1 person* *Lisbon plenary meeting; 8-9 March; 1 person* *Oslo plenary meeting; 13-15 June 2016; 2 persons* *Stockholm plenary meeting; 7-9 June 2015; 1 person* *The Hague plenary meeting; 5-6 September 2016; 3 persons*
	Consumables	*35,55*	*Paper risk assessment*
	Equipment	*4071,52* *619,10*	*Depreciation of DA Test Bed* *Depreciation of network equipment for lab connections*
	Indirect Costs		
TOTAL COSTS [5]			

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 6 for the Period, ALLIANDER			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
	Personnel direct costs	*€ 22.099,52*	*Rob Epskamp* *Bart Luijkx* *Johan Rambi* *Rick van Dijk* *Sander Kruese*
	Subcontracting	*€ -*	

[5] Total costs have to be coherent with the costs claimed in Form C.

	Travel	*€*	*2.480,38*	*Lissabon meeting (Rob Epskamp, Johan Rambi, Arno Tuinman)* *OSLO meeting (Rob Epskamp, Johan Rambi, Arno Tuinman, Sander Kruese)*
	Consumables	*€*	*1.659,89*	
	Equipment	*€*	-	
	Indirect Costs			

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 2 for the Period, ABB			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
WP1, 2 ,4	**RTD, Personnel direct costs**	*79.251,30 €*	*Gunnar Björkman, Senior advisor, part time, consultant. Primary contact for ABB.* *1,84 PM* *Judith Rossebo, Senior scientist, part time. WP2 leader.* *3,98 PM* *Batool Tahla, scientist, part time, employment ended 1/1 2016.* *1,27 PM*
WP7	**Management, Personnel direct costs**	*6.549,20,00 €*	*Gunnar Björkman, Senior advisor, part time, consultant. Primary contact for ABB.* *0,56 PM* *Financial support from ABB Norway.* *0,03 PM*
	Subcontracting	*0 €*	
WP1, 2, 4	**RTD, Travel**	*511,44 €*	*Judith Rossebo, 10/11-12/11 2015, Project Review Meeting in Den Haag, Holland*

		361,56 € *393,80 €* *634,59 €* *516,79 €* *787,82 €* *39,38 €* *1.023,87 €* *678,93 €* *598,82 €*	*Gunnar Björkman, 13/12-14/12 2015. SEGRID working group meeting at Alliander in Sloterdijk, Holland* *Batool Tahla, 13/12-14/12 2015. SEGRID working group meeting at Alliander in Sloterdijk, Holland* *Gunnar Björkman, 25/1-26/1 2016. SEGRID working group meeting at Alliander in Sloterdijk, Holland* *Judith Rossebo, 25/1-26/1 2016. SEGRID working group meeting at Alliander in Sloterdijk, Holland* *Judith Rossebo, 7/3-10/3 2016. SEGRID project meeting at FFCUL Lisbon, Portugal* *Judith Rossebo, 5/4 2016, SPARKs Workshop Brussels (cancelled - only cancel fee)* *Judith Rossebo, 11/4-12/4 2016, SEGRID Joint Workshop CPSR-SG2016 Vienna, Austria* *Judith Rossebo, 25/8-27/8 2016, SPARKs Workshop at Queen's University in Belfast (rescheduled)* *Judith Rossebo 4/9-6/9 2016, SEGRID working group meeting at ENCS in den Haag Holland*
WP7	**Management, Travel**	*614,36 €* *601,35 €*	*Gunnar Björkman, 7/3-10/3 2016. SEGRID project meeting at FFCUL Lisbon, Portugal.* *Reported as Management Cost* *Gunnar Björkman, 13/6-15/6 2016. SEGRID project meeting at ABB AS, Oslo Norway.*

			Reported as Management Cost
	Consumables	*2.985,10 €*	*Cost for Project Meeting in Oslo 13-15 June, 2016*
	Equipment	*15.896,00 €*	*Purchase of Tropos routers for SEGRID test system*
	Indirect Costs	*59.438,09 €*	
TOTAL COSTS [6]		*170.832,45 €*	

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 8 for the Period, FFCul			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
1,2,3,4,5,6,7	**Personnel direct costs**	*97020.32*	*Salary costs of FFCUL (Young researchers – 20.32 PMs): Ricardo Jorge Pato Fonseca; André Ricardo Lopes Nogueira; Eric Emmanuel Pascal Vial; Pedro Alexandre Pacheco Pinto Maia; Diogo Miguel Henriques Duarte; Luís Ferrolho; Frederico Brito; Bruno Valala* *Salary costs of FCUL (Senior researchers – 9.55PMs): Nuno Neves; António Casimiro; Alysson Bessani; Fernando Ramos; Pedro Ferreira*
	Subcontracting	*0.00*	
1,2,3,4,5,6,7	**Travel**	*17366.13*	***TRAVEL – RTD**:* *- Nuno Neves & Fernando Ramos; SEGRID Meeting; Amsterdam, Netherlands; 14-15 December 2015;* *- Nuno Neves; SEGRID Meeting; Amsterdam, Netherlands; 26 January 2016;* *- Nuno Neves & Fernando Ramos; SEGRID Meeting; Oslo, Norway; 13-15 June 2016;*

Total costs have to be coherent with the costs claimed in Form C.

			- Fernando Ramos; SEGRID Meeting + 2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids (CPSR-SG2016); Vienna, Austria; 12-14 April 2016; *- Nuno Neves; SEGRID Meeting; The Hague, Netherlands; 5-6 September 2016.* ***TRAVEL – MNG**:* *- Nuno Neves; SEGRID Review Meeting; Amsterdam, Netherlands; 11-12 November 2015;* *- Nuno Neves & André Nogueira; Workshop & Review Meeting SEGRID; Barcelona, Spain; 12-15 November 2016.* ***TRAVEL – OTHER**:* *- Bruno Vavala; SRDS 2015; Montreal, Canada; 28 September-01 October 2015 (Subsistence allowance);* *- Fernando Ramos; IFIP Networking 2016; Vienna, Austria; 17-19 May 2016;* *- Miguel Henriques; EuroSys 2016; London, UK; 17-21 April 2016;* *- Ibéria Medeiros; Conference DSN 2016; Toulouse, France; 28 June-1 July 2016;* *- Alysson Bessani; Conference DSN 2016; Toulouse, France; 28 June-1 July 2016;* *- Nuno Neves; IFIO WG 10,4 Meeting + Conference DSN 2016; Sorèze + Toulouse, France; 24-27 June 2016 + 28 June-1 July 2016.*
	Others	*1435.38*	*Rack material to buid FFCUL-EDP join testbed; Organisational costs -*

			SEGRID Meeting, 8-9 March 2016, Lisbon; Conference poster - EuroSys 2016
	Equipment	*3877.03*	*Depreciation costs of 2 servers, 1 switch and associated components*
1,2	**Indirect Costs**	*71819.32*	
TOTAL COSTS [7]		*191518.18*	*(including indirect costs)*

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 8 for the Period (2nd year), EDP			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
WP1	**Personnel direct costs**	**13.858,91 €**	*Coordination, several contributions and review of D1.1; Kick off on draft D1.2 (T1.1); First draft D1.2 (T1.1); Contribution for D1.5; Finish and review draft D1.2 (T1.1); Contribution on Privacy for D1.4; Final Review for D1.4; Final review on D1.5. 511 senior hours (Aurélio Blanquet, Francisco Melo, Nuno Emanuel Pereira; Nuno Medeiros and Pedro Gama).*
WP2	**Personnel direct costs**	**7.705,56 €**	*T2.2: Reviewing link between assets and business processes in D2.2; Review D2.2; T2.3: Contribution Gap Analysis D2.3; Review D2.3; Contribution for D2.4 and Final Review D2.4. 252 senior hours (Aurélio Blanquet, Francisco Melo, Nuno Emanuel Pereira; Nuno Medeiros and Pedro Gama).*
WP3	**Personnel direct costs**	**4.602,77 €**	*T3.2: Contribution for D3.2 and Final Review for D3.2. 140 senior hours (José Isabelino Coelho, Nuno Emanuel Pereira, Nuno Medeiros and Pedro Gama).*
WP4	**Personnel direct costs**	**1.740,55 €**	*T4.2: Final Review for D4.2. 70 senior hours (Nuno Emanuel Pereira).*

[7] Total costs have to be coherent with the costs claimed in Form C.

WP5	**Personnel direct costs**	**10.786,10 €**	*T5.2: Implementation of FCUL/EDPD SEGRID Test beds; Contribution for D5.2; Final review D 5.2; Preparation for implementation of FCUL/EDPD SEGRID Test beds. 420 senior hours (Diogo Alves Lopes, Nuno Emanuel Pereira and Nuno Medeiros).*
WP6	**Personnel direct costs**	**6.327,09 €**	*Preparation and participation in "Segrid General Meeting in Oslo"; Preparation and participation in "Segrid General Meeting in Den Hague" 168 senior hours (Amélia Mota; Francisco Melo, Nuno Medeiros and Susete Albuquerque).*
-	**Subcontracting**	-	-
WP5	**Travel**	**2.296,97 €**	*WP5: SEGRID Amesterdam Workshop, 14th December 2015: Nuno Medeiros (1,167.94 euros) and Francisco Melo (1,129.03 euros).*
WP6	**Travel**	**4.069,57 €**	*WP6: SEGRID Genereal Meeting and Workshop in Oslo, 13th June 2016: Nuno Medeiros (1,351.39 euros) and Francisco Melo (1,303.90 euros) and SEGRID General Meeting and Workshop in Den Hague, 5th September 2016: Nuno Medeiros (620.43 euros) and Francisco Melo (793.85 euros).*
-	**Consumables**	-	-
-	**Equipment**	-	-
-	**Indirect Costs**	-	-
TOTAL COSTS [8]		**51.387,52 €**	-

Table 3.1 Personnel, Subcontracting and Other Major Cost Items for Beneficiary 10 for the Period, ZiV			
Work Package	**Item Description**	**Amount in € with 2 decimals**	**Explanations**
1, 2, 4, 5, 6	**Personnel direct costs**	*€ 72.436,16*	*Salary of:*

[8] Total costs have to be coherent with the costs claimed in Form C.

			1 Miguel Angel Alvarez, Project coordinator for ZIV. (1,87 PM) WP 4, WP5. *2. Exabier Bilbao, Researcher. (4,26 PM)* *WP1, WP2, WP4, WP5, WP 6.* *3. Cristina Martínez: Researcher and technical contributor (1,29PM) WP4.* *4. Rubén Castillo, Researcher. (2,58 PM)* *WP 4, WP5.* *5. Jesús Pico Macho, Researcher. (2,75 PM) WP4, WP5.*
	Subcontracting	*€ 0*	
4,5	**Travel**	*€ 1164,71*	*Traveling: Exabier Bilbao: Oslo Consortium meeting. 13 and 14 June 2016*
	Consumables	*0*	
	Equipment	*0*	
1,2,4,5,6	**Indirect Costs**	*€ 14.720,17*	
TOTAL COSTS [9]		***€ 88.321,04***	

3 Recommendations 2nd year review

The reviewers and PO provided the following recommendations as a result of the review meeting for Y2.

R1	Make sure that the various parts of SEGRID are more integrated. This includes formal consistency (like naming conventions, see the attack tree vs attack graph) but especially work integration among partners and WPs, that allows WPs to reinforce each other and provide consistent SEGRID outcomes and image. Especially during the presentation of results (dissemination activities, including the white paper), select one use case to show the results of all WP's in an integrated manner. But also in the upcoming WP5 deliverable, where the WP

[9] Total costs have to be coherent with the costs claimed in Form C.

	would link the solutions together and test them.
R2	D2.2 will be rejected. There are three improvements to be made for the improved version: • Split D2.2 in a public part (the methodology) and an EU restricted part (the results of applying the methodology), according to the proposal of the SEGRID consortium. Make a plan for this, discuss this with the Security Advisory Group and propose the plan to the PO. The PO will discuss internally in the EU and provide a decision from the Commission (which is the "originator" for what regards classified information. The methodology will be published as a separate document. • Include in the RA methodology an assessment of the existing controls. This is also in ISO/IEC 27005 and else we cannot claim that the SEGRID RMM is in line with ISO/IEC 27005. • Improve the impact assessment section. In particular, o Clarify what we did with National Risk Assessment for the Societal Impact. Why is impact on 3 Dutch NRB black out scenario's different? o Why only assess black-out for societal impact and not privacy breach or other impacts? • Clarify the EBITDA in the example Impact table from SGIS. Check how IRAM2 does this.
R3	Be more Smart Grid specific, especially for WP3 and WP4. Provide clear context for all the work on how it relates to Smart Grids and in particularly smart grid specific security challenges. While the explanation that some tools are not smart-grid specific is convincing in most cases, in these cases the smart grid specificity should be enhanced acting on, for example, their applications and making the smart grid use cases as detailed and applied as possible to the tools and methods
R4	Make sure that the individual chapters of WP4 are more integrated. Now it seems that they address different things and they seem a bit disconnected. Explain why the subjects covered in the chapters are the most relevant ones for smart grid security.
R5	The first SEGRID workshop was good, but it was a lot of sending information and very little interaction. Make sure a follow-up SEGRID workshop is organized in such a way that interaction is stimulated. E.g. setup demo's such that

	audience can play with them interactively.
R6	In dissemination, try to cooperate with e.g. ISF, LSeC, Eurolectric. Focus on what the audience can get out of the project results and how this benefits them. The audience(s) should be better characterized, recognizing that different audiences may need tailored messages. Regarding exploitation, each partner has to think to what they would do with SEGRID results, and individually and as consortium think to how to manage and exploit IP. The discussion should start early so there is the time to already implement dissemination events according to the strategy as well as plan possible future exploitation. The Roadmap could be a good basis for the strategy; it is suggested to increase targeting to power systems/grid events besides computer/engineering ones.
R7	Try to replace the SEGRID Advisory Board members that did not attend any SAB meetings until now
R8	Make a plan in the consortium how to efficiently use the remaining budget of Y3 and discuss with the PO.
R9	When working on the exploitations plans (D6.6) take into account: • What was planned at the start of the project; what is the current plan. • Address IPR & EU restricted issues
R10	D1.1 version 1.0 (delivered in Y1) will be rejected on request of the consortium, to provide an updated version.

4 Recommendations 1st year review

The following describes the results of the recommendations provided by the project officer and reviewers at the end of the first year review. They have been included in the *"Technical periodic report - Year 1"*.

4.1 General

R1	**Include a list of acronyms in the future deliverables and in the year 1 periodic report.**
Actions	One common list is organized and maintained by TNO. This is used as a basis for the acronyms list in all our deliverables.
Results	All deliverables after 1st year review contain Acronym list.

R2	**Be pro-active towards standardization bodies and initiatives. In particularly, on recommendation towards smart grid specific security standardization and privacy by design.**
Actions	Initiate actions towards standardization bodies, and become pro-active.
Results	• CEN-CENELEC JWG 8: *TNO submitted a document describing the work on Privacy-by-design within SEGRID* • ETSI TC Cyber: *TNO & ABB submitted a CR for TS 102 165 Part 1 (TVRA) based on WP2 work.* ***CR accepted****.* • Cigré working group D2.40: *KTH contributed* • IEC 62351 series and ISA99/IEC 62443: *ABB actively participates and uses SEGRID results* • Expert Group 2: *ALL is working on presenting SEGRID* • PLC Prime: *EDP/ZIV is working on presenting SEGRID*

R3	**Intensify cooperation between work packages. There already is some cooperation, but this can be improved. In particularly, harmonize asset naming conventions between the different work packages (i.e. WP1, WP2, and WP3).**
Actions	Ensure SEGRID use cases is used as basis for collaboration in all WPs. Ensure coherence between WPs, including harmonization on asset naming.
Results	D1.2 - SEGRID Smart Grid Security Roadmap More active collaboration between WPs has taken place: • WP1 and WP3 on naming (addressed in D3.2) • WP1 and WP2 & WP4 on Security & Privacy Goals • WP2 and WP3 on relation Risk Assessment & CySeMol • WP4 and WP1 & WP2 on design of SPADE • WP5 and WP4 on testing

4.2 WP1

R4	**Provide recommendations for standardization bodies how they can improve the standards towards smart gird security. Get in contact with Technical Committees of relevant standardization bodies.**
Actions	The focus of the analysis of D1.5 and D1.6 SEGRID is not security standards but existing policies and their existing gaps and space for improvement. However, one of our recommendations, where needed, shall be the adoption of existing standards. Additionally, and according to R2, the consortium is trying to become more active in standardization committees and influence standardization work on security & privacy.
Results	• IETF DICE group: *SICS submitted DTLS work* • CEN-CENELEC JWG 8: *TNO submitted a document describing the work on Privacy-by-design within SEGRID* • ETSI TC Cyber: *TNO & ABB submitted a CR for TS 102 165 Part 1 (TVRA) based on WP2 work.* ***CR accepted****.* • Cigré working group D2.40: *KTH contributed* • IEC 62351 series and ISA99/IEC 62443: *ABB actively participates and uses SEGRID results* • Expert Group 2: *ALL is working on presenting SEGRID* • PLC Prime: *EDP/ZIV is working on presenting SEGRID* • Reference on Eureletric Smart Grid Cybersecurity Position Paper (to be published until the end of the year)

4.3 WP2

R5	**In step 3 of the SEGRID practical approach to RA it is recommended to refer to *'Threat & Vulnerability analysis'* instead of *'Threat analysis'*.**
Actions	Change the terminology
Results	Done in D2.2, we now use 'Threat & vulnerability analysis', see Clause 4.1.2.2.1

R6	**Provide guidance on how to balance impact levels between the stakeholders and categories in the impact tables.**
Actions and result	Done, see par. 4.1.2.2.1 in D2.2

R7	**Provide more explanation for the impact tables. In particularly, explain why the impact table is asymmetric. The structure of the impact table is a business decision (where to put the focus). The**

	table may be symmetric or asymmetric. The table's structure and the choice made in this structure should be explained.
Actions	Explain the impact table in D2.2
Results	This has been addressed in D2.2 in Clause 5.1.1.2.1

4.4 WP3

R8	**The work is very interesting but a bit too academic. Clarify the link of CySeMol to the rest of the project and explain how application of CySeMol will improve smart grid security.**
Actions	CySeMoL (SecuriCAD) is a generic vulnerability assessment language/tool. We have developed detailed models within the tool of smart grid specific systems that also are in focus in the SEGRID project use cases. (The smart grid is also increasingly dependent on general purpose technology and OT and IT are increasingly interconnected, so capturing both sides is key to smart grid security. Also, of course, OT is also nothing but software and hardware so the underlying fundamental security mechanisms are the same on both sides.)
Results	Reference architectures for SCADA, SAS, and AMI described in D3.2

R9	**Explain how WP3 activities are linked to WP2.**
Actions	WP3 complements the work in WP2 with a more detailed analysis. First and foremost the scope is different WP2 deals with all aspects of security risk assessment, including impact assessment and attacker capabilities. WP3 deals only with vulnerability assessment. The WP3 work goes into deeper details relating to the identification of threats and vulnerabilities and also provides a more fine-grained assessment of the likelihood that are different types of attacks are successful both in various parts of the analysed ICT infrastructure.
Results	We have explained this in par. 1.3 in D3.2

4.5 WP4

R10	**Become proactive on privacy-by-design standardization activities that are currently ongoing under the mandate M/530. In particular, TNO could become active through NEN, and other partners via their national standardization bodies.**
Actions	Be pro-active towards M/530.
Results	TNO have kept in contact with M/530 and other standardization bodies. • We did draft and submitted a contribution on the work in Task 4.4 to CEN JWG8 "Privacy management in products and services". It was presented by TNO colleague, Gabriela Bodea, at

	the CEN JWG8 meeting in Paris (2016-01-27/28). • We spotted that ISO JTC1 SC27 WG5 started working on Privacy Engineering (now known as AWI 27550). Jaap-Henk Hoepman contacted the editor of that work item and pointed to the approach we also work on in Task 4.4 with privacy design strategies and privacy patterns. This has been included in their initial document (ISO/IEC JTC 1/SC 27/WG 5 N391 - text for NP letter ballot).

4.6 WP5

No recommendation.

4.7 WP6

R11	**Work more towards 'joint' publications. Between SEGRID partners, and also with partners outside SEGRID (e.g. FP7 project SPARKS).** .
Actions	• Plan for more joint papers • Seek cooperation with partners outside SEGRID
Results	• We have published the paper by TNO and ABB: 'Including Threat Actor Capability and Motivation in Risk Assessment for Smart Grids' for the CPSR SG2016 workshop. • We were invited to provide a paper for a special IEEE magazine issue on RA. We are working on that with ABB, EDP and TNO • We have co-organized the CPSR SG2016 with SPARKS and SALVAGE • We have proposed the CPSR SG2017 workshop, co-organized the CPSR SG2016 with SPARKS and SALVAGE

R12	**Increase the number of smart grid conferences and papers. The list of publications in majority contains publications in non-smart grid (more towards general reliability & dependability) conferences and papers.**
Actions	Strive for more smart grid oriented papers and conferences
Results	• We have shown improvement, considering the list of presentations and papers (see D6.5).

R13	**Clearly define beforehand the target audience for the white paper: for which smart grid stakeholders do you write the white paper.**
Actions	Define the target audience for the white paper
Results	The current target audience is defined as smart grid policy makers and higher management of stakeholders, further refined (after the review meeting to higher management and security officers of DSOs

R14	**Include some text in the next half year report (only technical, not financial) on the results and added value of the cooperation with SPARKS.**
Actions	Include text on the added value of this cooperation
Results	Done, see the Y2H1 report of SEGRID: SEGRID has cooperated with SPARKS in a number of area's and SEGRID organized a workshop with SPARKS and SALVAGE in April 12th 2016. This experience has proved that there are several benefits from cooperating with other EU projects: • The projects and the organizations and people participating in the projects get to know each other, which results in efficient cooperation between the projects and helps to avoid overlap in the activities. The people involved will learn from each other • The exchange of knowledge and experience (e.g. in the area of Risk assessment methodologies and regulations) will improve the individual project results • The cooperation with other projects in the organization of dissemination activities results in reaching a wider audience which ensures higher impact and visibility than individual projects could reach • Jointly organising dissemination events ensures that the workload is shared and is therefore more efficient • Because the people and organizations from the different projects get to know each other and learn their strengths and weaknesses, cooperation for future calls will be more efficient and easy. • One of the partners (KTH) is participating in SEGRID, SPARKS and SALVAGE. For them, joint project activities will mean high efficiency .

5 Glossary

Acronym	Description
ABAC	Attribute-Based Access Control
AMI	Advanced Metering Infrastructure
API	Application programming interface
APT	Advance Persistent Threat
ASLR	Address Space Layout Randomization
BLP	Bell-LaPadula
BYOD	Bring Your Own Device
CAPEC	Common Attack Pattern Enumeration and Classification
CC	Common Criteria
CDF	Cumulative Distribution Function
CEM	Common Methodology for Information Technology Security Evaluation
CEN	European Committee for Standardization.
CENELEC	European Committee for Electrotechnical Standardization.
CERT	Computer Emergency Response Team
CIS	Customer information system
CORAS	Risk Analysis of Security Critical Systems
CPS	Cyber-Physical System
CSO	Charge Spot Operator.
CVE	Common Vulnerabilities and Exposures
CySeMoL	Cyber Security Modeling language
DAC	Discretionary Access Control
DAN	Distribution automation node
DC	Data Concentrator.
DEP	Data Execution Prevention
DER	Distributed Energy Resources
DMS	Distribution management system
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial of Service
DoW	Description of Work
DPIA	Data Protection Impact Assessment
DRAACS	Demand-response analysis and control system
DSO	Distribution System Operator.
Dx.y	Deliverable x.y
EA	Enterprise Architecture
EAM	Enterprise asset repository
EC	European Commission
ECI	European Critical Infrastructure
EDSA	Embedded Device Security Assurance
EMS	Energy management system
EMSP	E-Mobility Service Provider.
ERP	Enterprise resource planning
ETSI	European Telecommunications Standards Institute.
EU	European Union
EV	Electric Vehicle.
FE	Front end
FHS	Filesystem Hierarchy Standard
FS	Forecasting system

FTP	File transfer protocol
G3	Alliance for PLC technology.
GIS	Geographical Information System.
GDPR	General Data Protection Regulation
GMS	Generation management system
GOOSE	Generic Object Oriented Substation Event
GPRS	General Packet Radio Service.
GPS	Global Positioning System
GSSE	Generic Substation State Events
GUI	Graphical User Interface.
HAN	Home area network
HE	Head End
HES	Head-End System.
HMI	Human Machine Interface.
HTTPS	Hypertext transfer protocol secure
HSE	Health, Safety and Environment
HV	High Voltage.
IACS	Industrial Automation and Control Systems
ICC	Inter Control Center
ICCP	Inter Control center Communications Protocol
ICS	Industrial Control System
ICS-CERT	Industrial control systems computer emergency response team
ICT	Information and Communication Technology
IDS	Intrusion detection system
IEC	International Electro technical Commission (ISO)
IED	Intelligent Field Device
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol (IPvx = IP version x)
IPS	Intrusion prevention system
IPSec	IP Security
ISO	International Organization for Standardization.
IT	Information Technology
KV	Kilo Volt
LAN	Local area network
LCA	Latent Credibility Analysis
LDAP	Lightweight Directory Access Protocol
LN	Local Network.
LV	Low Voltage.
MAC (1)	Media Access Control
MAC (2)	Mandatory Access Control
MDMS	Meter Data Management System.
MMS	Meter management system
MOF	Meta object facility
MS	Member State
MU	Merging unit
micro-CHP	Micro combined heat and power.
MV	Medium (level) Voltage.
NAN	Neighborhood area network
NMS	Network management system
NN	Neighbouring Network.
NRM	Network Risk Management
NTP	Network Time Protocol
NVD	National Vulnerability Database
OMS	Outage Management System

OS	Operating System
OSCP	Open Smart Charging Protocol
OSGP	Open Smart Grid Protocol
OSI	Open Systems Interconnection
OT	Operational technology
OTP	One-Time Password
PCT	Programmable communicating thermostat
PHP	PHP: Hypertext Preprocessor (a recursive acronym
PLC	Power Line Communication.
PQ	Power Quality
PV	Photovoltaic
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RF	Radio frequency
RFC	Request for Comments
RTU	Remote Terminal Unit.
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition.
SCS	Substation control system
SDLA	Security Development Lifecycle Assurance
SE	Secure Element.
SEGRID	*S*ecurity for smart *E*lectricity *GRID*s.
SFTP	SSH File Transfer Protocol
SGAM	Smart Grid Architecture Model.
SG-CG	Smart Grids Coordination Group (ETSI).
SIC	Social Impact Cost
SIM	Social Impact Magnitude
SMITP	Smart metering Information and Telecommunication Protocol.
SNTP	Simple Network Time Protocol
SSH	Secure Shell
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege
SUC	System under Consideration, or Subject under Consideration
TCP/IP	Transmission Control Protocol / Internet Protocol
TEE	Trusted Execution Environment
TEPT	Trained Execution Path Tree
TOE	Target Of Evaluation
TSO	Transmission System Operator.
TTC	Time To Compromise
TVRA	Threat, Vulnerability and Risk Analysis
Tx.y	Task w.y
UC	Use Case
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
VPN	Virtual private network
WAMS	Wide Area Monitoring System
WAN	Wide area network
WAP	Wireless Application Protocol
WMS	Workforce management system
WPx.y	Work Package x.y
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations

3G / 4 G	Third/ Forth generation mobile communication.