FP7 Grant Agreement N° 607109

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

D1.2 SEGRID Smart Grid Security Roadmap

Due date of deliverable: 31/03/2016
Actual submission date: 01/04/2016
Work package: WP1 Use Cases and Security Goals
Number of pages: 25
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

Management summary

The SEGRID project has defined five use cases that are exemplary for the gradually evolving system concept of Smart Grids in Europe. The use cases will be used to identify new cyber-threats and vulnerabilities as well as the gap between available and needed cyber security solutions for Smart Grids. The SEGRID use cases have been selected considering:

1. The relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power.
2. Addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

In this deliverable D1.2 the project roadmap is presented. It contains a detailed planning of the SEGRID project, together with the short term and long-term goals and milestones of the project applied to the SEGRID use cases, including the responsibilities and deadlines.

This deliverable also describes the "story" of the SEGRID project, by unfolding the existing connections between the different deliverables. Some of the deliverables require important inputs from others, and in some cases, there are deliverables that represent improved versions from previous, due to the learning that emerge throughout the project, and the work and research being done.

Author	Nuno Medeiros (EDP Distribuição)
Contributors	Judith Rossebø (ABB AS) Mathias Ekstedt (KTH) Marco Tiloca (SICS) Maarten Hoeve (ENCS)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	30/03/2016
Remarks	None

TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 5
1.1 The SEGRID project 5
1.2 Work Package 1 – Use Cases and Security Goals 5
1.3 Deliverable D1.2 – SEGRID Smart Grid Security Roadmap 5
2 SEGRID SMART GRID SECURITY ROADMAP 6
2.1 Introduction and context 6
2.2 SEGRID Storyline 7
2.3 SEGRID approach 10
2.4 SEGRID Work Packages and workflow dependencies 12
2.4.1 Work Package 1: Use cases and security goals 12
2.4.2 Work Package 2: Application & enhancements of Risk Assessment 14
2.4.3 Work Package 3: Enhancements of Vulnerability Assessment techniques 16
2.4.4 Work Package 4: Novel Security Solutions 18
2.4.5 Work Package 5: Testing and evaluation 20
3 GLOSSARY 23
4 REFERENCES 25

Classification level: Public

1 Introduction – Rationale of this document

1.1 The SEGRID project

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. The SEGRID project and its goals and approach are described extensively in chapter two.

1.2 Work Package 1 – Use Cases and Security Goals

Work Package 1 is a key building block for the SEGRID project, setting the basis for all activities within SEGRID.

The Work Package 1 main objectives are:

- Elaborate on the SEGRID reference architecture and describe the five use cases.
- Establish the security & privacy goals for each of the SEGRID use cases.
- Identify points of improvement with respect to Smart Grid security and privacy in policies and regulations related to the identified SEGRID use cases.
- Assess the cost of implementing security and privacy protection technologies that are developed in WP4 for each of the Smart Grids use cases.

1.3 Deliverable D1.2 – SEGRID Smart Grid Security Roadmap

SEGRID task T1.1 aims to establish the basis for the overall SEGRID project and its activities. On one hand, deliverable D1.1 [4] provides the detailed specification of the SEGRID Smart Grid architecture and the specific requirements for the different use cases, which are key to facilitate a thorough analysis of their potential cybersecurity and privacy vulnerabilities and to investigate and develop mitigation strategies.

On the other, this deliverable D1.2 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. Through the description and narrative around the SEGRID deliverables, the responsibilities and deadlines are indicated.

The deliverable is structured in only one main section. Chapter 2 is divided in two complementary parts. First, there is an overview of the SEGRID project, where the various objectives are presented and the several work packages briefly described. The complete outline of the interrelation between the SEGRID deliverables is also presented. On the second part, there is a fine grained description of the various deliverables, with the indication of the responsible entities and the deadlines for delivery. Additionally, the established dependencies and pairing between the various deliverables is explained.

2 SEGRID Smart Grid Security Roadmap

2.1 Introduction and context

The electrical distribution grid is considered one of the most critical infrastructures in industrially developed societies. Hence, there is an increasing awareness and concern regarding its security and protection against cyber threats.

Until now grid operators have lived security-wise in a relatively protected stand-alone environment. Specialized Industrial Control Systems built with dedicated hardware/firmware allow grid operators to monitor and control the gas and electricity networks and they are largely isolated from corporate networks, the Internet, vendors, customers and 3rd party service providers.

However, there is a now a clear paradigm change related to the utilities technological environment. To be able to deal with the new challenges presented by the integration of renewable energies, distributed generation, electrical vehicles, and the 2020 targets: 20% of energy from renewable sources and 20% increase in energy efficiency; utilities are currently going through a digital transformation to make their grids "smarter".

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.

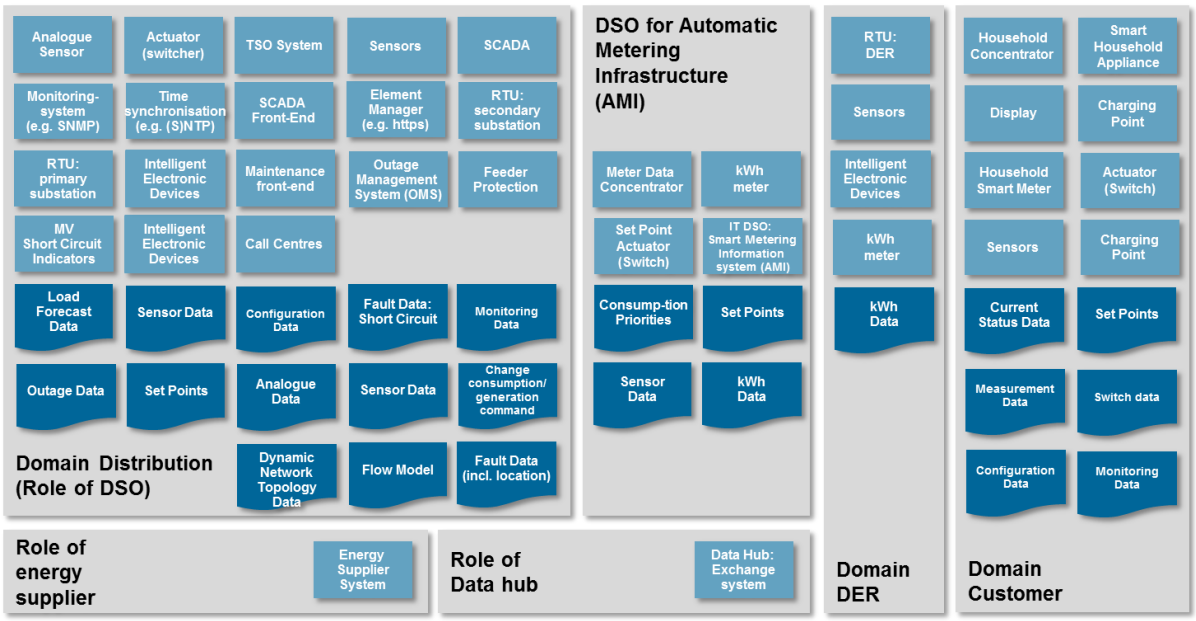

Figure 1 – SEGRID Smart Grid - Information and system assets by domain

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. And of course that, considering the added potential impact, brings additional incentives for malicious activities.

Given this context, security and safety of the power grid infrastructure become important requirements. Systems and communications are required to display high availability, strong integrity protection, and confidentiality protection for, among others, privacy sensitive information. Moreover, the Smart Grid should keep operating correctly, with minimum possible impact in performance, during a degraded state of operation caused by any adverse event; therefore, resilience of SCADA systems and communications is required.

Additional requirements are privacy and confidentiality, which must be specifically considered when looking at the Smart Metering (SM) functionalities which are also provided by the Smart Grid. SM capabilities can be used for three basic purposes: 1) providing detailed information to the client in order to foster the improvement of his consumption habits, 2) providing new services to the client (e.g., flexible tariffs) and 3) collecting LV power grid data related with energy usage, consumption and micro generation, which can be used to feed advanced Smart Grid functionalities. Depending on what and how information is collected, transmitted, processed and stored, privacy issues may come into place as a relevant concern; therefore, for SM purposes, the Smart Grid needs to provide strong confidentiality protection for privacy sensitive information, together with the integrity and availability requirements that were already referred to.

In order to comply with the identified requirements, both for current and advanced functionalities, the Smart Grid's privacy, security and reliability assuring mechanisms must be improved. The SEGRID project is addressing the technological aspect of this necessity by proposing a set of new technological solutions that address different aspects of these requirements in the remit of the five defined SEGRID Use Cases. Resilient communications and resilient SCADA will enable compliance with integrity and availability requirements. Intrusion detection and prevention will address confidentiality and integrity requirements. Privacy by-design will be more focused on confidentiality and privacy concerns.

2.2 SEGRID Storyline

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 organisations, such as public telecom networks and third party-delivered (outsourced) application services. There will potentially be many new channels of 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.

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 new functionalities are added to accommodate new use cases with the challenge to maintain the security (and privacy) of the Smart Grid as a whole.

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 [1] and M/490 [2] as well as based on the work and competence of the project partners.

The rationale for the five SEGRID use cases is based on:

- Relevance for new business, economic growth, and supporting the introduction of more sustainable and locally generated power.
- Addition of new functionality and components that inherently will introduce new vulnerabilities and a wider cyber-attack surface.

The five SEGRID use cases are:

1. Smart meter used for on-line reading of consumption and technical data;

   This use case refers to the smart meter capability of reading both the energy consumption and the energy generation of a customer. It is one of the most relevant Smart Grid capabilities since it replaces the costly manual readings. However, the smart meter has several other capabilities and services it can provide.

2. Load balancing renewable energy centrally;

   By central load balancing of renewable energy the DSO is able to balance the renewable energy supply to the demand, in such a way that regional congestion is avoided. The decision making is all done centrally, by the DSO SCADA system. The system is constantly acquiring data from the loads and generation units, and, if required, issues controls to the MV RTUs at the DER.

3. Dynamic power management for smart homes, smart offices, and electric vehicles;

   Dynamic Power Management is based on the use of flexibility in demand and supply. The device agent, controlling the customer loads, offers services such as “increase demand” or “decrease demand” to the central management system, which monitors the state of the grid at the supply side and might decide to use those services automatically or it might propose the usage of those services to the Grid Operators. This use case defines when and how these services can be used.

4. Load balancing renewable energy regionally (substation automation);

   Load balancing renewable energy regionally is a way of control imposed by DSOs, to locally balance the renewable energy supply to the demand, to avoid congestion and/or local power quality problems like unacceptable voltage rise. The difference with Load balancing renewable energy centrally is that the control is shifted to automated subsystems. These automated systems could be on the scale of a primary MV substation or even on an underlying secondary MV/LV substation.

5. Automatic reconfiguration of the power grid.

   Automatic reconfiguration and self-healing in Smart Grids is a subject that is studied in European projects like Grid4EU and fits in near future grids, however DSOs today are testing pilots of self-healing distribution grid, namely in MV grids with radial or ring typologies. The goal is to locate and isolate the fault through a network (re)configuration minimizing the number of affected customers and power parameters. This kind of systems uses an ICT layer with peer-to-peer communication between the involved substations.

We believe that the SEGRID use cases reflect important steps in the European Smart Grid developments until 2020 and beyond (SEGRID storyline, see Figure 2). Moreover, the SEGRID use cases will cover the most relevant security and privacy issues that will arise from the increasing complexity of the evolving Smart Grids.

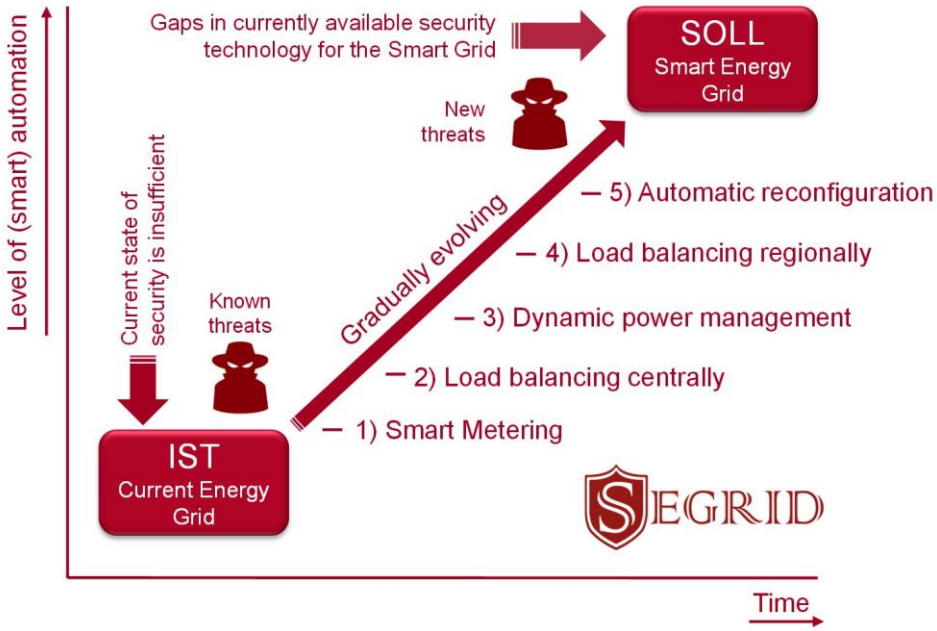

Figure 2: SEGRID storyline

2.3 SEGRID approach

SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks. This is achieved by applying a risk management analysis approach (WP2) to the selected five SEGRID Smart Grid use cases (WP1), to identify the threats and potential future cyber-attack pathway (WP2). Then, the existing gaps between currently available security techniques and measures will be determined (WP2), in order to derive which additional security techniques and measures are required for the SEGRID use cases (WP4). The novel security solutions for privacy, communication and system security in Smart Grids, to mitigate the threats and risks identified in the SEGRID use cases, are then implemented, evaluated and tested in the SEGRID test environment – the SITE (Security Integration Test Environment), a realistic test environment (WP5).

Furthermore, the identified gaps and the analysis itself will give input to the enhancement of risk assessment methodologies (WP2), in order to make them optimally suited to identify and address the key risk factors of Smart Grids of 2020.

Another effort for the risk mitigation strategy for the SEGRID Smart Grid reference architecture and use cases is a vulnerability assessment framework developed in Cyber Security Modelling Language (CySeMoL) (WP3). This framework, based on active vulnerability assessment tools and vulnerability discovery and diagnosis tools, shall support the planning and design phase of future Smart Grid solutions. These tools are to be tested on SITE (WP5).

The following table enumerates the project RTD work packages, and includes the SEGRID partner responsible for the overall success of all the WP deliverables, and the conforming activity periods.

Table 1 SEGRID work packages and responsible partners

WP	WP Title	WP Leader	Start month	End month
WP1	Use cases and security goals	EDPD	1	36
WP2	Application & Enhancements of Risk Assessment	ABB	1	24
WP3	Enhancements of Vulnerability Assessment techniques	KTH	1	36
WP4	Novel Security Solutions	SICS	1	36
WP5	Testing and evaluation	ENCS	1	36

The next table presents the indicative efforts per WP per partner.

Table 2 SEGRID indicative effort per WP per partner

RTD Activities	TNO	SICS	KTH	INC	ENCS	ALL	ABB	FFCUL	EDPD	ZIV	Total
WP1	8	2	2	7	5	5	2	5	8	3	47
WP2	7	1	1	1	3	2	6	4	2	1	28
WP3	4	2	20	3	4	2	0	18	2	1	56
WP4	9	21	0	2	4	1	5	25	2	8	77
WP5	6	6	5	0	9	3	2	12	8	12	63
Total Research	34	32	28	13	25	13	15	64	22	25	271

Taking into account the above description made of the project objectives, and specifically of the work involved in each WP, the figure below depicts the relationships and interdependencies between the various WP and corresponding deliverables.

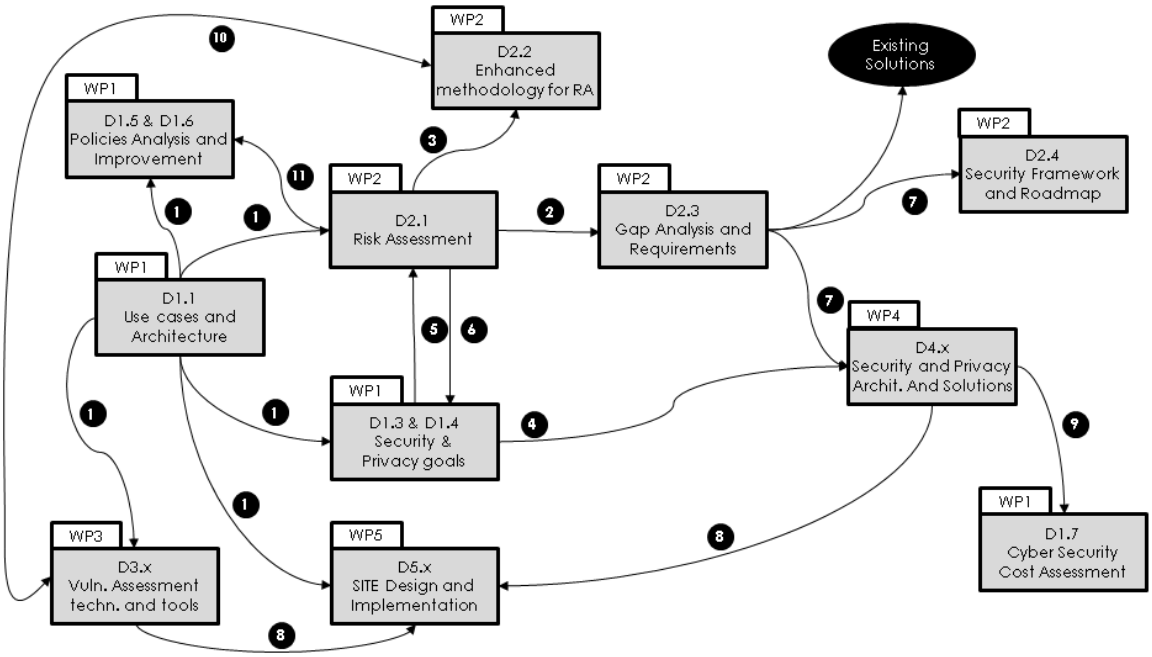

Figure 3: SEGRID work package interdependencies

2.4 SEGRID Work Packages and workflow dependencies

2.4.1 Work Package 1: Use cases and security goals

WP1 is a key building block for the SEGRID project, setting the basis for all activities within SEGRID.

The specific objectives for WP1, as stated in the Description of Work, are to:

- Elaborate on the SEGRID use cases and provide an architecture design for each use case;
- Establish security & privacy goals for the SEGRID use cases;
- Identify points of improvement with respect to Smart Grid security and privacy in policies and regulations related to the SEGRID use cases;
- Asses the cost of implementing security technology that is developed in WP4 in Smart Grids use cases.

The table below shows the deliverables related to WP1.

Table 3 SEGRID work package 1 deliverables

Deliverable	Deliverable title	Leader	Delivery date
D1.1	Architecture and design for use cases	EDPD	6
D1.2	SEGRID Smart Grid security roadmap	EDPD	18
D1.3	First report on the security & privacy goals	TNO	6
D1.4	Final report on the security & privacy goals	TNO	24
D1.5	Report on analysis of policies regarding Smart Grid security	TNO	12
D1.6	Report with recommendations of improving Smart Grid security policies	ENCS	21
D1.7	Cyber Security Cost Assessment	TNO	36

The next figure depicts the interdependencies between WP1 deliverables and the other SEGRID deliverables.

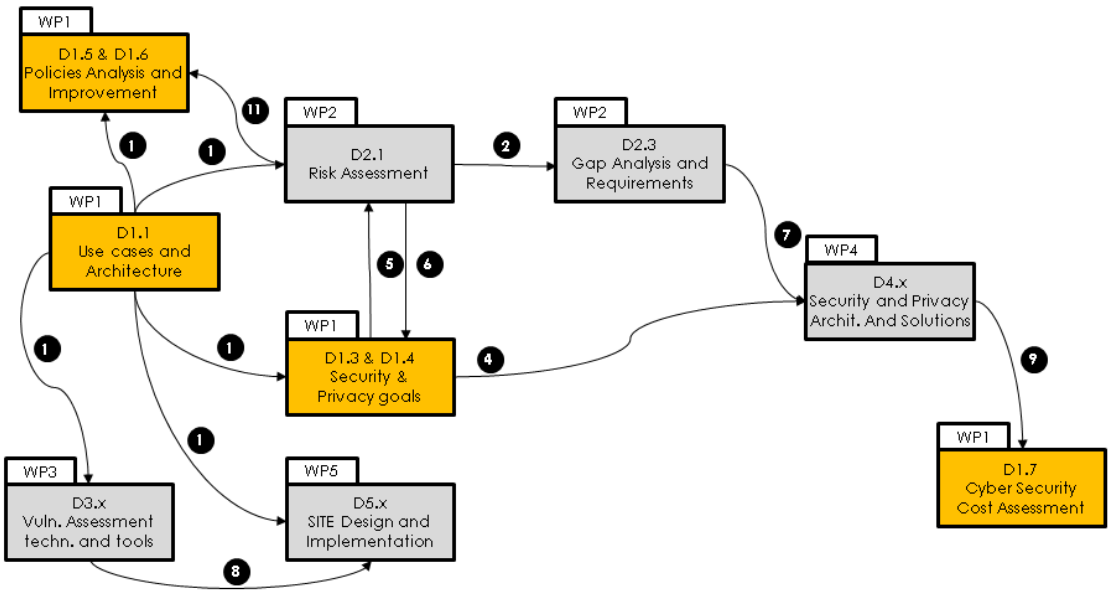

Figure 4: SEGRID WP1 Interdependencies

Deliverable D1.1 provides a report containing a detailed specification of the SEGRID Smart Grid reference architecture and the specific requirements for the different use cases to be analysed during the course of the project.

(1) The D1.1 provides a very important input to all the other work packages. By defining and detailing the SEGRID architecture and its use cases, it assures a common baseline for the different objectives within the project, and the right alignment for its storyline.

The D1.3 defines the initial security & privacy goals for these SEGRID use cases and provides an overview of the state of the art in Smart Grid security and privacy controls, while D1.4 represents an improvement on the previous, based on the lessons learnt and discoveries coming from WP2.

(5) The security & privacy goals will be used in D2.1 to assist and guide the risk and threat assessments.

(4) The outcome from D1.4 will drive, as well as the results from WP2, the scope and objectives of WP2.

(6) The results from the risk and threat assessment will provide valuable input for D1.4, where the scope will be extended to security goals on properties, such as system security and security life cycle management.

Deliverable D1.5 provides an analysis of policies regarding Smart Grid security and their applicability for different stakeholders.

(1) and **(11)** Based on the analysis in deliverable D1.5, the results of D1.1 and the findings in other SEGRID work packages, recommendations to improve Smart Grid security policies will be formulated in D1.6. These recommendations shall support European standardisation bodies and regulators in their development of Smart Grid-related policies and regulations.

D1.7 is one of the last deliverables of the SEGRID project. It will report the costs related to the novel security solutions developed for the SEGRID use cases.

(9) The novel security solutions selected under WP4 scope will provide the required input for the cost assessment expected in D1.7.

2.4.2 Work Package 2: Application & enhancements of Risk Assessment

The specific objectives for WP2, as stated in the Description of Work, are to:

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

The WP2 deliverables are listed in the table below.

Table 4 SEGRID work package 2 deliverables

Deliverable	Deliverable title	Leader	Delivery date
D2.1	Threat vulnerability and risk assessment applied to SEGRID UC	ABB	12
D2.2	Enhanced methodology for risk assessment	TNO	24
D2.3	SEGRID gap analysis	FFCUL	18
D2.4	SEGRID Cyber Security Framework and Roadmap	ENCS	24

The next figure depicts the interdependencies between WP2 deliverables and the other SEGRID deliverables.

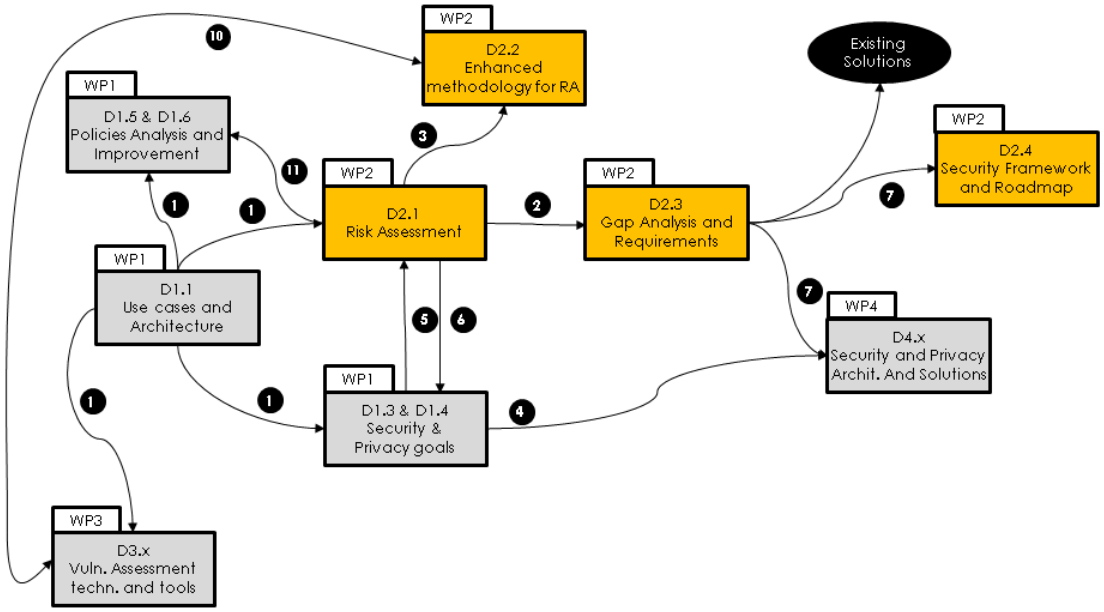

Figure 5: SEGRID WP2 Interdependencies

WP2 depends on WP1 to provide the SEGRID use case descriptions and provides the result of the gap analysis to WP4.

(1) Input to D2.1 are the SEGRID use cases and scenarios and the process for documenting use cases (described in chapter 3 of D1.1 and the actual use cases documented in chapter 5 of D1.1). The process is used during step 1 of the risk assessment: the scope is described. The stakeholders are identified and the stakeholder assets are documented. Assets and components are represented according to the Smart Grid Architecture Model (SGAM) interoperability layers [3].

(2) Input to D2.3 are the results of the threat, vulnerability and risk assessments. The list of critical threats identified need to be mapped in D2.3 to security controls as a basis for the gap analysis.

(3) Input to D2.2 from D2.1 is the list of recommendations for enhancements for improvements of the SEGRID risk assessment methodology. These recommendations will be used to guide the enhancement of security risk assessment processes for Smart Grid in SEGRID.

(5) and **(6)** D2.1 receives the security and privacy goals as input to the practical applications of the SEGRID risk assessment methodology. At the same time, during the drafting phase of the deliverable, threat assessment workshops on specific use cases provided input to identifying the security and privacy goals.

(7) The results of the gap analysis D2.3 are an identification of which existing security measures address the needs identified, and the identified gaps that need to be addressed by novel security measures. Input to D4.x are the identified gaps which identify which novel

solutions are required, in order to specify these and propose solutions. Input to D2.4 are the identified gaps and required solutions as a basis for specifying a security framework and roadmap.

(10) The results from the vulnerability assessments of the SEGRID use cases are compared to the risk assessment results from WP2, and both D2.2 and D3.3 will describe how these methodologies differ and how they can best be used to strengthen the overall outcome.

2.4.3 Work Package 3: Enhancements of Vulnerability Assessment techniques

SEGRID WP3 is focused on cyber vulnerability assessment. The goal is to develop new mechanisms for vulnerability analysis and discovery both on a component level (Task 3.3) and on a system-wide level (Task 3.1 and 3.2).

The specific objectives for WP3, as stated in the Description of Work, are to:

- Aid the development of attack resilient ICT infrastructures for Smart Grids;
- Identify and assess vulnerabilities and address both the individual components of Smart Grids as well as Smart Grids ICT infrastructure as a whole.

The table below lists the WP3 deliverables.

Table 5 SEGRID work package 3 deliverables

Deliverable	Deliverable title	Leader	Delivery date
D3.1	Preliminary specification of the system-wide vulnerability assessment framework	KTH	12
D3.2	Preliminary specification of Smart Grid vulnerability assessment techniques and tools	KTH	24
D3.3	Final specification of Smart Grid vulnerability assessment framework and tools	KTH	36

The next figure depicts the interdependencies between WP3 deliverables and the other SEGRID deliverables.

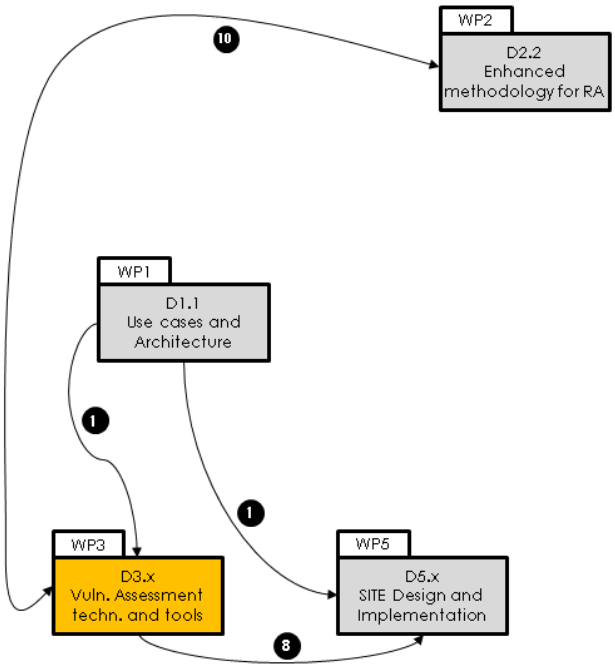

Figure 6: SEGRID WP3 Interdependencies

The deliverables in WP3 are reporting on the results from all tasks in WP3 rather than on individual topics. Thus in order to outline the dependencies to and from WP3 is better done by considering the WP3 tasks.

The purpose of T3.1 is to build a framework for assessing vulnerabilities in system architectures. For the sole purpose of the development of the framework, there is no dependencies on other WPs. However, the framework will be applied to the SEGRID use cases developed in WP1, reported in D1.1

(1) Task 3.1 will make a mapping of the SEGRID reference architecture components to different components in CySeMol, in order to describe the various use cases in CySeMol. The purpose of task T3.2 is to develop a prototype for automatically make vulnerability assessments as developed in T3.1. To realize this the output of external tools will be used, such as vulnerability scanners and network analysers and build logic for automatically merge this data and convert it into models that are analysable by the vulnerability assessment framework. This task has a strong dependency to WP5.

(8) It has an inbound dependency insofar that the data miner tools considered should be possible to apply on the planned test bed environment. The outbound dependency lies in the fact that the theoretical setup should be practically developed as a proof-of-concept in WP5, and also applied to the test bed.

The purpose of task T3.3 is to develop tools and methods for discovering zero day vulnerabilities. The task is largely independent of other work in the project, nevertheless, since the analysis subject will be Smart Grid ICT components, it still depends on D1.1 as guidance on choosing which components to work with. In addition, there is a dependency to

T3.2 in so far that the results of T3.3 will be examined as a potential source of automatic modelling.

The vulnerability assessments of the SEGRID use cases will also be compared to the risk assessment results from WP2. The goal is to identify how these methods can complement each other.

(10) In D2.2 and D3.3, there will be a description on how both methodologies differ and how they can best be used to strengthen the overall outcome.

2.4.4 Work Package 4: Novel Security Solutions

SEGRID WP4 objective is 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.

The table below lists the WP$ deliverables.

Table 6 SEGRID work package 4 deliverables

Deliverable	Deliverable title	Leader	Delivery date
D4.1	Preliminary security and privacy architecture	SICS	12
D4.2	Preliminary specification of security and privacy solutions	SICS	24
D4.3	Final specification of security and privacy architecture and solutions	SICS	36

The next figure depicts the interdependencies between WP4 deliverables and the other SEGRID deliverables.

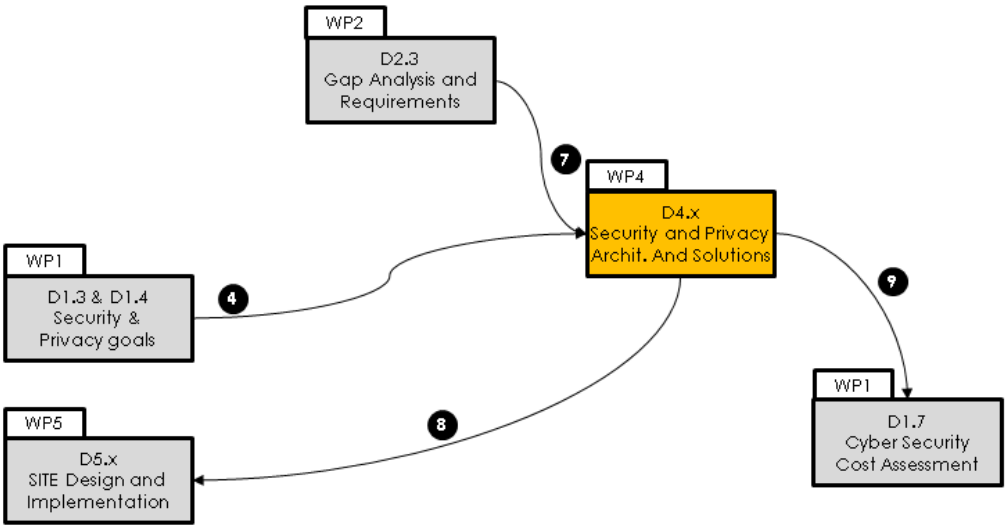

Figure 7: SEGRID WP4 Interdependencies

Deliverable D4.1 includes i) a preliminary iterative model to instantiate use case specific security and privacy architectures; and ii) design principles according to which security and privacy solutions will be developed throughout the rest of the project, with reference to the SEGRID use cases and tentative test plans. In particular, security and privacy solutions comprise: mechanisms for platform security; resilient SCADA systems; intrusion detection and authentication in wireless networks; resilient communication; enhancements to the TLS and DTLS protocols; efficient management of cryptographic group key material; privacy patterns.

(4) Deliverable D4.1 takes into account the preliminary security and privacy goals described in D1.3 (M6). That is, D4.1 proposes a preliminary security and privacy architecture as well as a set of security and privacy solutions designed to support the satisfactory fulfilment of the security and privacy goals.

(8) Deliverable D4.1 provides preliminary information as to the security and privacy solutions to be tested in the integrated test bed SITE described in D5.2 (M18).

Deliverable D4.2 will include: i) a preliminary specification of the security and privacy architecture, as an iterative process, which is use case based and life-cycle oriented; and ii) preliminary specifications of the security and privacy solutions proposed in deliverable D4.1.

(4) Deliverable D4.2 will take into account the preliminary security and privacy goals described in D1.3 (M6). That is, D4.2 will propose: i) a preliminary specification of the iterative model to instantiate use case specific security and privacy architectures, such that the suitability of use case specific architectures can be checked according to the preliminary security and privacy goals from D1.3; ii) security and privacy solutions designed to support the satisfactory fulfilment of the security and privacy goals from D1.3.

(7) Deliverable D4.2 will consider the outcome from the GAP analysis reported in D2.3 (M18) as a priority guideline for designing and configuring the preliminary security and privacy architecture as well as the preliminary security and privacy solutions.

(9) Deliverable D4.2 will provide preliminary information necessary as input to the cost assessment of the designed security and privacy solutions, to be included in D1.7 (M36).

(8) Deliverable D4.2 will provide preliminary specifications of the security and privacy solutions, considered for experimental tests in the integrated testbed SITE and whose results will be included as a preliminary test report in D5.3 (M27).

Deliverable D4.3 will include: i) a final specification of the security and privacy architecture, as an iterative process which is use case based and life-cycle oriented; and ii) a final specification of the security and privacy solutions elaborated in deliverable D4.2.

(4) Deliverable D4.3 will take into account the final security and privacy goals, described in D1.4 (M24). That is, D4.3 will propose: i) a final specification of the iterative model to instantiate use case specific security and privacy architectures, such that they conform with the final security and privacy goals from D1.4; ii) final specifications of security and privacy solutions.

(7) Deliverable D4.3 will consider the outcome from the GAP analysis reported in D2.3 (M18) as a priority guideline for designing and configuring the final security and privacy architecture, as well as the final security and privacy solutions.

(9) Deliverable D4.3 will include final information necessary as input to the cost assessment of the designed security and privacy solutions, to be included in D1.7 (M36).

(8) Deliverable D4.3 will include final specification of the security and privacy solutions considered for experimental tests in the integrated test bed SITE and whose results will be included as a final test report in D5.5 (M36).

2.4.5 Work Package 5: Testing and evaluation

The goal of work package 5 is to facilitate, through the implementation of an integrated test site, the testing and assessment of the solutions developed in some of the other work packages.

The specific objectives for WP5, as stated in the Description of Work, are to:

- Establish an environment (Security Integration Test Environment (SITE)) to evaluate and test new security technology for Smart Grids;
- Evaluate and test integration of the SEGRID security approaches using SITE;
    - Feasibility of integrating new security solutions;
    - Test security concepts and design.

The table below lists the work package 5 deliverables.

Table 7 SEGRID work package 5 deliverables

Deliverable	Deliverable title	Leader	Delivery date
D5.1	Design of SITE	ENCS	9
D5.2	Implemented SITE	ENCS	18
D5.3	Intermediate summary of test report	ENCS	27
D5.4	Active security assessments tool prototype	ENCS	36
D5.5	Final summary of test report	ENCS	36

The next figure depicts the interdependencies between WP5 deliverables and the other SEGRID deliverables.

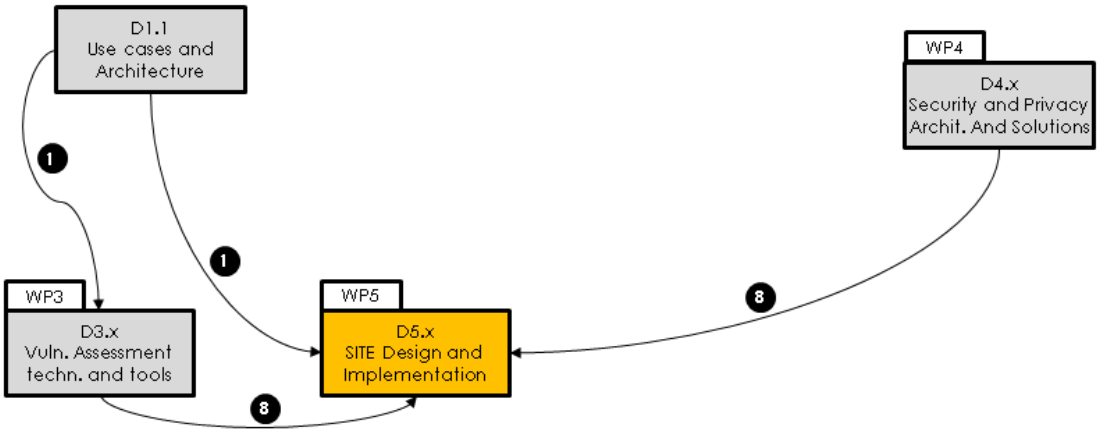

Figure 8: SEGRID WP5 Interdependencies

Requirements for what is needed for this goal have been gathered in the first phase of the project. Based on this a design for the SITE test bed has been made (D5.1) and implemented (D5.2).

In the second phase of the project the solutions developed in SEGRID will be integrated into the SITE, and then tested. The solutions to be tested are the automated vulnerability assessment tools from work package 3 (D3.x), and the novel security solutions developed in work package 4 (D4.x). The novel solutions will be tested in two structured test phases. The vulnerability assessment tools will only be tested in the second of these phases. In between the testing phases there is room for spontaneous testing. Two summaries of the test reports will be delivered (D5.3 and D5.4), one for each test phase.

(1) The use cases and architecture description from work package 1 (D1.1) have been used as one of the input of the design of the SITE (D5.1). The test bed was designed to implement the use cases as far as was possible, according to the proposed architecture.

(8) Some of the solutions developed in work package 4 (D4.x) will be tested in the SITE test bed. They will be integrated into the test bed architecture. Together with the researchers working in work package 4, a test plan will be developed, and then executed. The automated security assessment tools developed in work package 3 (D3.x) will be tested in the same way.

3 Glossary

This glossary serves as inventory of technical terms and abbreviations used in the document. For detailed background information on cryptographic primitives or testing procedures we refer to the referenced literature.

CEN	European Committee for Standardization.
CENELEC	European Committee for Electrotechnical Standardization.
CSO	Charge Spot Operator.
DC	Data Concentrator.
DER	Distributed Energy Resources
DMS	Distribution Management System.
DSO	Distribution System Operator.
Dx.y	Deliverable x.y
EMS	Energy Management System.
EMSP	E-Mobility Service Provider.
ETSI	European Telecommunications Standards Institute.
EV	Electric Vehicle.
G3	Alliance for PLC technology.
GIS	Geographical Information System.
GPRS	General Packet Radio Service.
GUI	Graphical User Interface.
HAN	Home Area Network.
HES	Head-End System.
HMI	Human Machine Interface.
HV	High Voltage.
IEC	International Electrotechnical Commission (ISO).
IED	Intelligent Field Device.
ISO	International Organization for Standardization.
LAN	Local Area Network.
LN	Local Network.
LV	Low Voltage.
MDMS	Meter Data Management System.
Meter	The term "meter" refers unless stated otherwise to the electricity meter. When necessary the document distinguishes between electricity meter and utility meter.
MV	Medium (level) Voltage.
micro-CHP	Micro combined heat and power.
NN	Neighbouring Network.
OMS	Outage Management System
OSCP	Open Smart Charging Protocol
OSGP	Open Smart Grid Protocol
OSI model	ISO Basic Reference Model for Open Systems Interconnect.
PLC	Power Line Communication.
PQ	Power Quality
PV	Photovoltaic
RTU	Remote Terminal Unit.

SCADA	Supervisory Control and Data Acquisition.
SE	Secure Element.
SEGRID	*S*ecurity for smart *E*lectricity *GRID*s.
SGAM	Smart Grid Architecture Model.
SG-CG	Smart Grids Coordination Group (ETSI).
SMITP	Smart metering Information and Telecomm Protocol.
TSO	Transmission System Operator.
Tx.y	Task w.y
UMTS	Universal Mobile Telecommunications System
Utility meter	Meter for, e.g., power, gas, water, and heat consumption.
WAN	Wide Area Network.
WPx.y	Work Package x.y
3G / 4 G	Third/ Forth generation mobile communication.

4 References

[1] M/441 EN; "*Standardisation mandate to CEN, CENELEC and ETSI in the field of measuring instruments for the development of an open architecture for utility meters involving communication protocols enabling interoperability*"; European Commission Directorate-General For Energy; Brussels; 12th March 2009.

[2] M/490 EN; "*Smart Grid Mandate Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment*"; European Commission Directorate-General For Energy; Brussels; 1st March 2011.

[3] CEN-CENELEC-ETSI Smart Grid Coordination Group - Smart Grid Reference Architecture.

[4] SEGRID D1.1 - Architecture and design for use cases – April 1st 2015 – Public - http://www.segrid.eu/d1-1-architecture-and-design-for-use-cases/