FP7 Grant Agreement N° 607109

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

D1.7 Cyber Security Cost Assessment

Due date of deliverable: 30/11/2017
Actual submission date: 28/11/2017
Workpackage 1: Requirements and use cases
Number of pages: 51
Revision: Version 1
Classification level: Public

Project type:	Collaborative project – small or medium scale focused research project
Thematic Priority:	FP7-SEC-2013-1
Start date of project:	October 1st, 2014
Duration:	39 months

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

Management summary

This report reflects the work performed in SEGRID Task 1.4, in which the expected costs of developing, implementing and operating four selected smart grid security solutions (Resilient SCADA Systems, SecuriCAD Based Active Vulnerability Assessment Tool, Robust Scalable (D)TLS and Key Management for Group Software Distribution) are determined and weighed against their expected level of risk reduction in a particular use case scenario (uc2sc2) of SEGRID.

The report describes the cost assessment and risk reduction methodologies and the outcomes of the assessment. Assessing the costs of a security solution provides insight into those factors and elements that together determine the costs to the investor. In this study a mid-sized Distributed System Operator (DSO) with 4 - 6 million consumers was assumed as the investor for smart grid security solutions. The investor can then weigh the costs against the expected benefits, in this case, the expected reduction of risk.

The cost assessment methodology is based on a life-cycle approach in which the costs of development, implementation, use and maintenance are taken into consideration. The methodology proved to be useful for performing security solution cost assessments. Not surprisingly, the cost assessment shows that the bandwidth of some cost estimates is substantial. This reflects the difficulties and uncertainties that are involved when estimating costs of new, innovative solutions that have not yet been fielded and/or commercialised. It also reflects the variety in assumptions that can be made in cases where it is not yet clear what exactly is needed for a security solution to work. Therefore, having done the assessment, it can be concluded that this is where the assessment's primary value lies: in fully thinking through the security solution: its elements, how it should be implemented and what is needed for it to work and to keep working. The cost assessment also shows that business models - who is willing to pay how much for what - are in some cases not yet clear. These business models need to be considered whilst further developing the security solutions. This deliverable can be used to provide input for business model development.

The non-monetary benefits of applying the security solution in a smart grid setting have been translated into the level of risk reduction that is reached. In SEGRID Work Package 2 (WP2), the first four steps of the SEGRID Risk Management Methodology (SRMM) were applied to SEGRID use case 2, scenario 2 (uc2sc2) 'Load balancing renewable energy centrally'. This resulted in a list of risks, which was the input for the risk treatment/risk reduction step. For all the identified risks it was assessed whether one of the selected security measures would reduce the risk.

Authors	Eldine Verweij (TNO)
Contributors	Exabier Bilbao Hernandez (ZIV) Gunnar Björkman (ABB) Corine Bonte (TNO) Rick van Dijk (Alliander) Maarten Hoeve (ENCS) Mathias Ekstedt (KTH) Judith Rossebø (ABB) Marco Tiloca (SICS) Reinder Wolthuis (TNO)

Security Assessment	See deliverables table for security assessment requirements
Approval Date	17/11/2017
Remarks	Some of the information is removed from the main document and put in a separate annex that is classified as 'EU Restricted'

TABLE OF CONTENTS

MANAGEMENT SUMMARY 2
1 INTRODUCTION – RATIONALE OF THIS DOCUMENT 6
1.1 The SEGRID Project 6
1.2 The objective of Deliverable D1.7 7
2 METHODOLOGY 9
2.1 Introduction 9
2.2 Cost Assessment 9
2.2.1 Cost assessment methodology overview 9
2.2.2 Planning 9
2.2.3 Definition 11
2.2.4 Analysis preparation 12
2.2.5 Analysis 16
2.2.6 Reporting 17
2.2.7 Overview 18
2.3 Risk reduction 18
2.3.1 Risk reduction methodology overview 18
2.3.2 Risk reduction 19
2.3.3 Embedding the risk reduction in the SRMM 22
3 SELECTED SECURITY SOLUTIONS FOR COST ASSESSMENT 24
3.1 Introduction 24
3.2 Selection process / rationale for selection 24
3.3 Selected security solutions 24
3.3.1 Resilient SCADA systems 25
3.3.2 Active vulnerability assessment tool 25
3.3.3 Robust scalable (D)TLS 25
3.3.4 Key Management for Group Software Distribution 26
4 COST ASSESSMENT 28
4.1 Introduction 28
4.2 Cost assessment scope and goal 28
4.3 Resilient SCADA systems 29
4.3.1 Solution description 29
4.3.2 Cost assessment 29
4.3.3 Observations 30
4.4 SecuriCAD based active vulnerability assessment tool 32
4.4.1 Solution description 32
4.4.2 Cost assessment 32
4.4.3 Observations 33
4.5 Robust scalable (D)TLS 33
4.5.1 Solution description 33
4.5.2 Cost assessment 34
4.5.3 Observations 35
4.6 Key Management for Group Software Distribution 35
4.6.1 Solution description 35
4.6.2 Cost assessment 36

4.6.3 Observations ... 37
4.7 Cost assessment summary ... 37
4.7.1 Approach ... 37
4.7.2 Results ... 38
5 RISK REDUCTION/IMPACT ASSESSMENT ... 40
5.1 Introduction ... 40
5.2 Resilient SCADA systems ... 40
5.3 SecuriCAD based active vulnerability assessment tool ... 41
5.4 Robust scalable (D)TLS ... 41
5.5 Key Management for Group Software Distribution ... 42
5.6 Risk reduction ... 42
6 CONCLUSION ... 43
7 REFERENCES ... 45
A1 EXCEL TEMPLATE COST ASSESSMENT ... 46
A2 COST ASSESSMENT RESULTS ... 50
A3 RESTREINT UE/EU RESTRICTED ANNEX ON RISK REDUCTION RESULTS ... 51

1 Introduction – Rationale of this document

1.1 The SEGRID Project

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

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

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

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

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

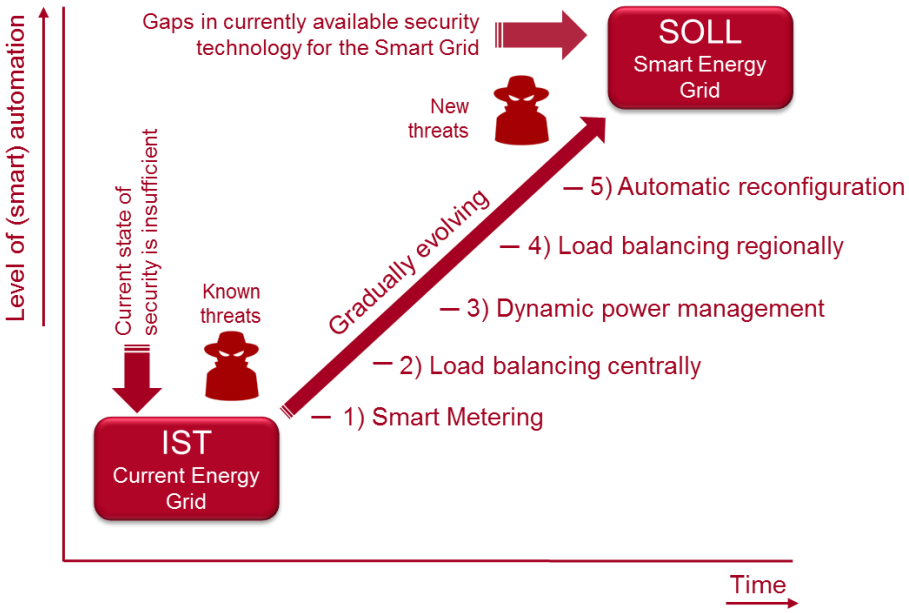


Figure 1: SEGRID storyline

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

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

1.2 The objective of Deliverable D1.7

This deliverable (D1.7) reflects the work done in SEGRID Task 1.4, in which the expected costs of applying security solutions are determined and weighed against the expected (non-monetary) benefits.

This deliverable consists of two major parts. First, it describes the cost assessment that was performed of the security technology solutions described and developed within WP3 and WP4 respectively. For this purpose, a selection of security solutions was made based on data availability and maturity of the security solution. A major element of the cost assessment is the methodology that was used. The methodology is based on a life-cycle approach [1] in which the costs of development, implementation, use and maintenance are taken into consideration. The methodology includes setting boundaries on security mechanisms, identifying relevant cost items and underlying parameters and estimation of costs. In this study non-monetary benefits of applying the security solution in a smart energy setting have been translated into the level of risk reduction that is reached. Therefore, and secondly, this deliverable describes a Proof of Concept in which the amount of risk that is reduced by applying the security solutions is assessed. The SEGRID Risk Management Methodology (SRMM) [3] is used to describe the risk

reduction methodology and to illustrate its use. Both the methodology and the outcomes are addressed. This deliverable includes a ‘RESTREINT UE/EU RESTRICTED’ Annex with sensitive information (containing the detailed results of the risk reduction step). That Annex is not necessary to read, understand and use this report but is provided as background information for designated officials of the EU and its member states. The ‘RESTREINT UE/EU RESTRICTED’ Annex is only available to SEGRID project partners and designated EU officials.

2 Methodology

2.1 Introduction

This chapter describes the methodologies that were used for the cost assessment (2.2) and the risk reduction assessment (2.3).

2.2 Cost Assessment

This paragraph describes the cost assessment methodology. The methodology is mainly based upon a method that has been developed by and used within TNO to perform life cycle cost assessments [1]. This methodology has proved its worth during numerous life cycle cost studies that were performed for underpinning investment decisions. It offers a generic - i.e. suitable for all domains - and logical step-by-step approach and is as such a hands-on methodology that covers the theoretical backgrounds of life cycle cost analysis. Also, advancements in cost assessment developed in the FP7 study ValueSec that was performed in 2011 [2] were used.

2.2.1 Cost assessment methodology overview

The Life Cycle Costs of a security solution cover all the costs that are made by a party that plans to invest in a security solution ('the investor') to acquire, install, use, maintain and decommission the security solution during its life cycle. Analysing the life cycle costs provides insight into those factors and elements that together determine the costs to the investor. The investor can then weight the costs against the expected benefits of the security solution, in this case, the expected reduction of risk.

The methodology that was used for SEGRID consists of various steps (Figure 2). These steps are subsequently described in the paragraphs that follow. By following these steps, a systematic and replicable cost assessment can be performed.

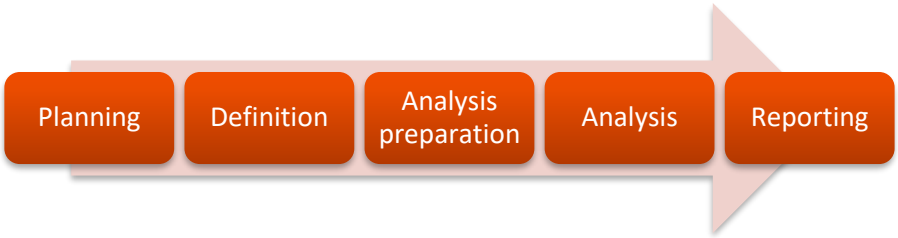


Figure 2: Steps in SEGRID Cost Assessment

2.2.2 Planning

The aim of the planning phase is to consider the cost assessment's scope and goal, who is going to do the assessment, determine which preconditions and constraints apply, consider data availability and to make a planning. This phase is the first, but

very important step towards executing a cost assessment. The planning phase determines the level of detail, based on the cost assessment's purpose. Effectively, the planning phase serves as a preparation and reference to the costs assessment's execution.

Cost assessment scope and goal

A cost assessment can address various goals, often depending on the specific stakeholder scope. The scope is about identifying the stakeholder for whom the cost assessment is performed. In the case of SEGRID, this could be the Distributed System Operator (DSO) or the security solution developer. The goal is about answering the question which decision is to be supported by performing the cost assessment.

Cost assessments can basically be sub-divided into two categories of goals:

1. To determine the costs of one security solution and outweigh these costs against the expected benefits, and compare this with the option to 'do nothing', i.e. not implement the security solution.
2. To determine the costs of more than one security solution and outweigh these costs against the expected benefits, and compare the security solutions with each other.

Examples of cost assessment goals are:

- Comparing various security solutions with each other from a cost perspective to justify investments in one or more security solutions. This is typically a question from the scope of the DSO with limited means for investments and recurring costs and balancing that with a wish to limit the risk of unforeseen costs.
- Cost optimisation or calculating costs of new products. The scope is that of vendors who would like to know if there is a business case for the products that they have developed or want to develop.

Preconditions and constraints

In the planning phase preconditions and constraints that apply to the security solution cost assessment should be identified, e.g.:

- The available budget for performing the security solution cost assessment;
- The lead time: when does the study have to be finished?
- Capacity: are the right people available for the cost assessment?

Project team

The team that is performing the cost assessment needs to have certain knowledge:

- Technical knowledge of the security solution, its development, implementation and use.
- Financial knowledge: people who know how to do cost assessments and have knowledge of financial modelling.
- Project management: people with experience and knowledge in security projects who know how much time several parts of developing, implementing, using and maintaining a security solution will take and what kind of expertise is needed.

Data availability

In order to make a detailed planning (see next) for the cost assessment, it is useful to have an overall insight into the availability of required data (e.g. quantities, prices, manhours, wage costs). Potential data sources are: experts, literature, databases, accounting systems etc. Data availability is often depending on the level of maturity and hence the level of details of the security solution and whether there are comparable or previously implemented solutions of which the costs are known.

Detailed planning

Finally, a detailed planning for the security solution cost assessment should be made, that addresses available budget and time frame.

2.2.3 Definition

The purpose of the definition phase is to define the security solution(s) and its boundaries (see paragraph below). It also involves thinking about the solution's intended operational use and maintenance. This phase is not about identifying cost elements, cost parameters or assigning costs. It is about defining the security solution: what is it about, what does it comprise, what is part of the solution and what is not, how will it be used and maintained. The exact definition of what the security solutions(s) comprises (and what not) and its intended use needs to be clear before any costs can be assigned. If the goal of the cost assessment is to compare various alternative security solutions, this phase must be done clearly and unambiguously for each of the security solutions.

Security solution definition

The security solution that is assessed should be described in terms of what is included and therefore part of the solution, and what is excluded and therefore not part of the cost assessment. The elements need to be described in such a way that costs can be attributed, e.g. what hardware and/or software are needed for the solution. Excluding elements from the cost assessment can be based on the fact that such elements are/have been procured as part of another budget, or that these elements are already in use by the organisation, therefore no extra investments are needed, e.g. current data servers that can be used for the security solutions at no extra cost. Other aspects that need to be considered during this step are:

- What is the setting in which the security solution will be used?
- What is needed for security solution implementation?
- What is the technical or economical life time of the security solution? When will the solution or components of it, be replaced or need upgrading?
- Which parts of the organisation play a role in implementing, using and maintaining the security solution?

Use of the security solution

Key question in this step is: 'How will the security solution be used once it has been developed and implemented?' The costs of a security solution will vary depending on the choices made in terms of usage and operational efforts. Therefore, it is important to document and describe these

aspects before the analysis starts. An example would be following-up on a security alert. This type of usage can be outsourced or can be done in-house. These choices involve different costs.

Maintenance of the security solution

Key question in this step is: 'How will the security solution be maintained during its life time?' Once the security solution is in place, it needs to be updated, patched etc. Also, hardware needs to be replaced regularly. This can be part of a contract with suppliers or software vendors. These choices concerning the security solution's maintenance need to be clearly documented in order to calculate costs in a later stage.

2.2.4 Analysis preparation

This step involves the preparatory activities that are needed to perform the cost assessment and can be described as the core of the cost assessment. There are four major elements that together form the analysis preparation (Figure 3):

- Identifying relevant cost items
- Choosing estimation methods for each cost item
- Collecting data
- Modelling.

Figure 3: Elements of the analysis preparation phase

Cost item identification

This part is about constructing a so called 'cost tree': a list of cost items and sub cost items applicable to the particular security solution. Usually a generic cost items list is used. The applicable cost items are selected based on the security solution's definition and its intended use and maintenance concept. Naturally, this can only be done when the previous step of the cost assessment has been successfully executed. Cost items that are not applicable to the security solution and/or its setting can be ignored or marked as 'not applicable'. It is important to state the assumptions that are used when identifying the relevant cost items, e.g. there is no need for extra data storage because the currently available data storage is sufficient for the security solution's life-time. This means that no extra costs have to be incurred. Another example is that current communication networks can be used for the security solution at hand, resulting in no extra costs for communication networks.

At a high level, costs can be sub-divided into:

- Procurement and installation / investment costs (CAPEX)
- In-service / operational costs (OPEX)
    - Use;
    - Maintenance.
- Long term cost items, e.g. costs of disposal.

This can be regarded as a high level 'cost tree'. However, to make a more accurate cost estimate, the cost tree should be extended. Table 1 shows a relatively generic example of a list of cost items that can be used for cost assessments of IT-based security solutions. The cost items list that was used for the actual SEGRID cost assessment (Annex A1) is based on this generic list but adapted in such a way that it can be used more intuitively and is fit for purpose, e.g. some items have been combined or left out because they are not of applicable for this analysis.

Table 1 Generic list of cost items for IT security solutions cost assessment

Investment cost items (CAPEX)	Purchasing:
	Network hardware and software
	Server hardware and software
	Workstation hardware and software
	Additional infrastructure
	Installation and integration of hardware and software, testing
	Initial technology training
	Warranties and licenses
	License tracking - compliance
	Migration expenses / organisational adaptation to new technology
	Risk: susceptibility to vulnerabilities, availability of upgrades, patches and future licensing policies, etc.
Operational cost items (OPEX)	Licenses for software and hardware
	(External) Support for software and hardware
	IT and Operational Technology (OT) management, maintenance

	Infrastructure (e.g. floor space)
	Electricity
	Downtime, outage and failure expenses
	Diminished performance
	Security
	Technology training
	Audit (internal and external)
	Insurance
	IT and Operational Technology (OT) department(s)/overhead
Long term expenses OPEX/CAPEX	Replacement
	Future upgrade or scalability expenses
	Decommissioning

Cost estimation methods

The next step is to identify the method that will be used to estimate the various selected cost items. Choosing the appropriate estimation method depends on data availability and/or the degree in which a security solution is comparable to existing solutions and their costs. Several cost estimation methods can be distinguished. In practice a combination of methods is often used.

- Analogy. Estimate the costs by comparing a (part of the) security solution with existing similar security solutions (Figure 4). The level of similarity between the security solution's (sub) item and the analogous security solution is a decisive factor in determining the usability of the cost data.

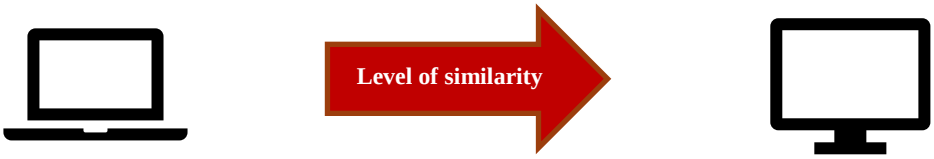


Figure 4: Cost estimating method: analogy

- Parametric. The parametric method uses Cost Estimating Relationships (CERs). These relationships are mathematical functions of the cost item and several system characteristics, e.g. storage space per server. The CER is determined statistically using regression analysis and assumes that the outcome can be used as an estimate of the costs for the new system. The use of so called Function Points is an example parametrically estimating the costs of software development.

Figure 5: Cost estimation method: parametric

- Analytical. Like the parametric method, the analytical method uses mathematic equations to estimate costs. However, the elements of the security solution and their associated costs are estimated in much more detail. This method needs detailed data and information from industry and users.

Costs for initial technology training = number of people * average hourly wage * hours needed for training

Figure 6: Cost estimation method: analytical

- Expert opinion. This method consists of asking one or more experts for information, based on their experience and professionalism. Reliability will generally increase when more experts are asked to give their opinion. This method is often used in the case of completely new, innovative security solutions and when other cost estimation methods cannot be used.

Figure 7: Cost estimation method: expert opinion

Data collection

Once the cost items have been identified, it is time to gather the cost and other required data, using the appropriate data collection method(s). This is usually the most time-consuming part of the cost assessment and involves constructing questionnaires/templates that need to be filled in by both industry (or the entity that developed the security solution) and end users. As part of the SEGRID project, the cost assessment template in Annex A1 was developed. For those instances in which a single point estimate is not possible or hard to give, the template includes the possibility to give bandwidths for data items.

Table 2: Generic data sources for cost assessment of security solutions

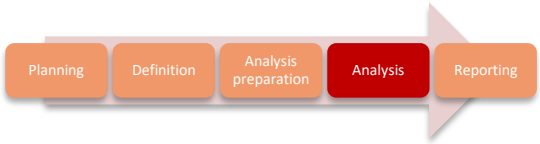
Data	Industry / developing entity	(Future) end user user*
Security solution	✓	
Use		✓
Maintenance organisation		✓
Maintenance	✓	
Organisational setting		✓

*The end user for SEGRID is the DSO

Modelling

The data and their interrelations are usually modelled in a calculation tool or spreadsheet – for example Microsoft Excel - in order to make cost calculations.

2.2.5 Analysis



The first step (step 1) of the cost assessment methodology was about determining the goal and scope of the cost assessment and the preconditions and constraints that apply. In the definition phase (step 2), the security solution's boundaries were defined, including how the solution will be used and maintained. In the analysis preparation (step 3), the cost items that are relevant for performing the analysis were identified and data was collected. Now, after a lot of work has been done in the previous steps, this step (step 4) is about actually calculating the costs and interpreting the outcomes. There are three major elements that should be considered in this step:

- Cost calculation;
- Sensitivity analysis;
- Identifying cost drivers.

Cost calculation

After the data has been collected and modelled in the calculation tool, it is time to have a look at the outcomes. It is important to look at the outcomes with intelligence to be able to understand the outcomes. The basic question is: why are the outcomes what they are? E.g. are they based on the assumptions that were used regarding the system definition, or regarding how the security solutions will be used? To convincingly communicate outcomes to management, it is key to understand the background of the cost calculations and keep in mind the decisions that were made in the previous steps of the cost assessment, including data validity.

An important aspect when comparing alternative security solutions is the possible difference in life cycle. The economic and technical life cycles of (a) security solution(s) and its sub-components can differ. Comparing alternatives is then permitted by either one of the following options[1]:

[1] Since the SEGRID cost assessment is not about comparing alternatives, this aspect has not been considered.

- Calculating the costs of the *lowest common denominator of life cycles*, e.g. if security solution A has a technical life cycle of five years and security solution B has a technical life cycle of ten years, the costs are to be calculated for a ten-year life cycle.
- Calculating the *equivalent costs per year*, where - following the example above - the costs of solution A are calculated for five years and the costs of solution B for ten years. By dividing the total costs by the life cycle, the average costs per year are calculated.
- Looking at the *planning horizon*. In some cases, an investor does not want to look further than a certain time period because the future is insecure. In the case of security solutions, this is a likely approach because future threats are hard to predict. Therefore, it is also difficult to predict if current security measures will offer a viable solution to these threats in the future. In such cases, the costs of the security solutions will be determined for the established planning horizon. However, often the life cycle of the security solution will be longer than the planning horizon making it necessary to estimate a disposal value for the solution. A disadvantage of this method is that - because of the arbitrarily chosen time period - possibly high costs that arise outside the time period - are not considered.

Sensitivity analysis

Performing a sensitivity analysis is about identifying the consequences of changing the value of one of more variables. By changing the value of a variable, costs can change to a more or lesser extent. Variables should be included in the sensitivity analysis if they are:

- Highly uncertain;
- Main cost drivers (see next);
- Distinctive to alternative security solutions.

It is a good idea to give uncertainty bandwidths during data collection, as this will make it easier to perform the sensitivity analysis.

Cost drivers

A cost driver is a variable that has a strong influence on the costs. By changing the value of a cost driver, the costs will change significantly. It is important to identify cost drivers because these are the parameters that can change the costs considerably and are therefore potential enablers for cost reduction. An example is the Resilient SCADA security measure: the level of accepted risk is a major cost driver because it determines the number of servers, which in turn determines part of the costs. A design characteristic can also be a cost driver. In that case, costs can possibly be reduced by changing the design.

2.2.6 Reporting

During the previous phase, the costs have been calculated. The final step in the cost assessment is to present the outcomes. What is presented and how it is presented is of vital importance. A proper report (or presentation) allows for a correct interpretation of the results by the 'decision maker', e.g. the person or company

entity that is making the decision to invest in the security solution or not. Such reporting can be done by writing a report and/or by giving presentations.

Besides presenting the end results, it is important to show which elements underlie the actual cost assessment. It needs to be made clear which costs are included and which are not. In short, the report (or presentation) that concludes the cost assessment needs to represent a complete overview of the activities, decisions, assumptions and sensitivity to outcomes to clarify the validity of the cost assessment's outcome to the decision maker. Clear reporting also allows for reproducing the outcomes. Needless to say, using graphical techniques strengthens the purport of outcomes and should be part of any report or presentation.

2.2.7 Overview

Figure 8 presents a graphical overview of the cost assessment methodology as described in the previous subsections and the activities underlying each step.

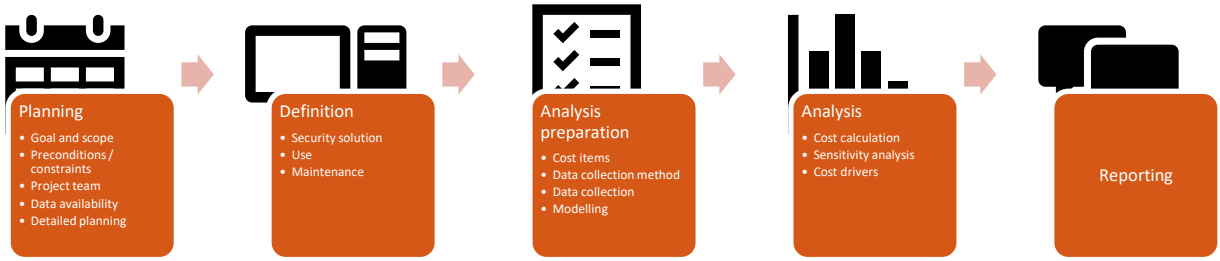


Figure 8: Cost assessment methodology steps 1 through 5

2.3 Risk reduction

This paragraph describes the methodology that is applied to calculate the reduction of risk when a security measure is implemented. We link to the SEGRID Risk Management Methodology (SRMM) that was developed by the SEGRID project. The white paper [3] describes the methodology and shows how it is used. However, the principles of the risk reduction methodology can also be used in combination with other risk management methodologies.

2.3.1 Risk reduction methodology overview

In the picture below the SEGRID Risk Management Methodology (SRMM) is shown.

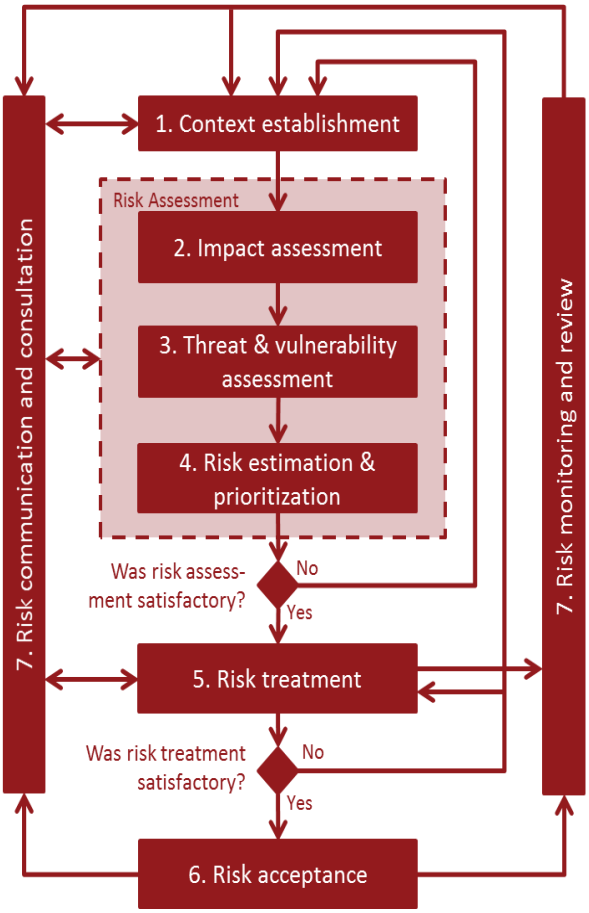


Figure 9: SEGRID Risk Management Methodology

The risk reduction and the cost assessment will typically take place during the 'Risk treatment' and 'Risk acceptance' step of the SRMM. The input for risk treatment is a list of risks prioritised according to the risk evaluation criteria. In the risk treatment step, security controls are selected to reduce, retain, avoid or share the risk. These are recorded in the risk treatment plan. A cost assessment is conducted on security controls that are planned for implementation. In the risk acceptance step, the risk treatment plan is evaluated and the residual risk is evaluated against the pre-defined risk acceptance criteria and the cost of implementation of selected controls. Either the decision is taken to implement the selected controls and the residual risk is accepted, or the risk treatment step must be revisited, and the risk treatment plan must be revised.

2.3.2 Risk reduction

In the SRMM, a Threat & Vulnerability Analysis (TVRA) is conducted to establish the risks for relevant assets in a SEGRID use case. See the figure below.

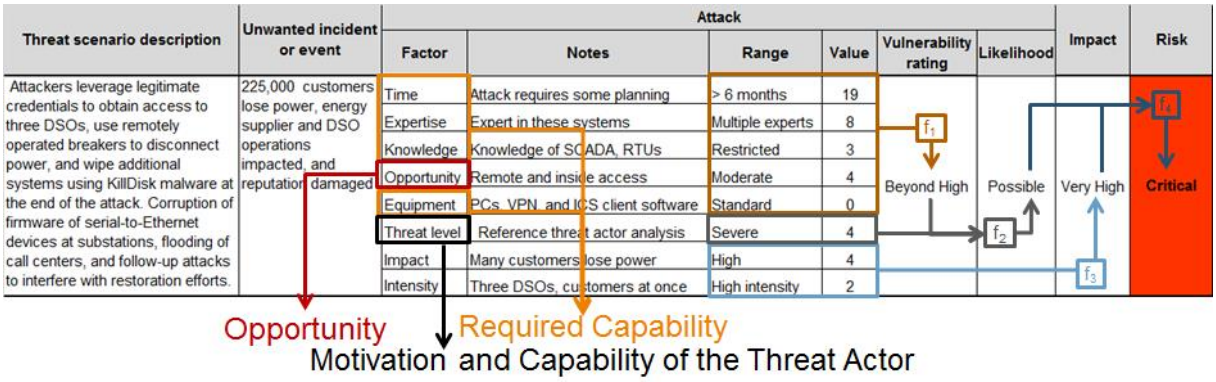


Figure 10: Likelihood and impact estimation using the TVRA tool

An asset is always linked to an obligation that must be fulfilled by a stakeholder (e.g. a DSO) in the use case. Risk is defined as (see Figure 10):

Risk = Impact of a threat x Likelihood of a threat

Where:

- *Impact* is the obligation impact of the threat; if the threat becomes reality, it is the maximum impact on the stakeholder's obligations to which the asset is linked. This is combined with the intensity of an attack to obtain the final impact.
- *Likelihood* is the likelihood that the threat becomes reality. As can be seen from Figure 11, this involves several aspects. First, the attack potential is estimated. The difficulty for the attacker of mounting an attack is rated based on five factors: time, experience, knowledge, opportunity, and equipment (tools). These aspects are mapped onto the vulnerability rating. The vulnerability rating is an indication of the efforts required to perform the attack. The vulnerability rating is then combined with the threat level to arrive at the likelihood of attack.

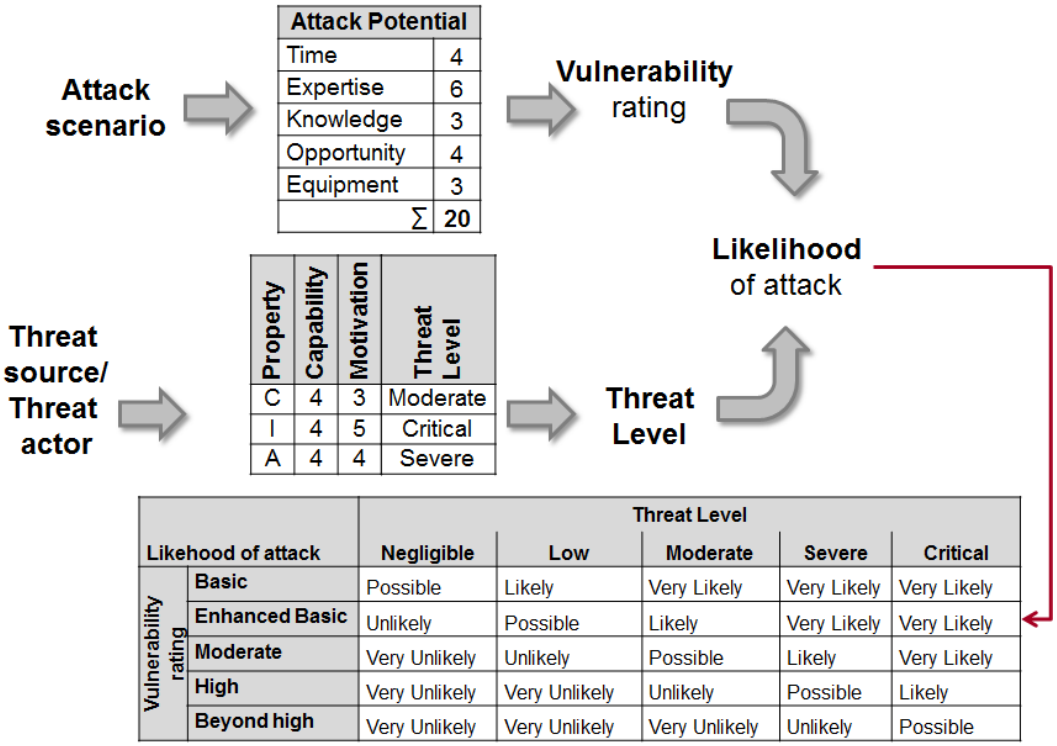


Figure 11: Estimation of the likelihood of an attack scenario

A security control can be selected to reduce the risk. A security control must be implemented by selecting a specific security measure. We want to establish how the security measure, once implemented, reduces the risk. We will therefore examine whether the security measure influences one of the elements that collectively lead to the risk level. These elements are:

Impact

- Impact - verify if the security measure reduces the impact. If this is the case, reduce the impact score accordingly. Reduction of impact can e.g. be realised by segmentation or containerisation.
- Intensity of impact - verify if the security measure reduces the intensity of the impact. If this is the case, reduce the impact intensity score accordingly.

Likelihood

- Time (time needed to prepare the attack) - verify if the security measure increases the time needed to mount an attack. If this is the case, increase the time level.
- Expertise (expertise needed to mount the attack) - verify if the security measure increases the needed expertise level to mount an attack. If this is the case, increase the expertise level.
- Knowledge (knowledge needed to mount the attack) - verify if the security measure increases the level of required knowledge to mount an attack. If this is the case, increase the knowledge level.

- Opportunity (window of opportunity to perform an attack (e.g., minutes/weeks/days/ years) - verify if the security measure reduces the window of opportunity. If this is the case, increase the opportunity level.
- Equipment (Complexity of equipment and or tools needed to mount an attack) - verify if the security measure increases the complexity of the equipment and or tools needed to mount the attack. If this is the case, increase the equipment complexity level.
- Threat level - this parameter cannot be influenced by implementing a technical security measure.

These steps must be taken for each threat. The exact change in levels that the security measure will introduce is a matter of expert opinion.

After this verification step, the new risk levels can be established by running a new workshop using the TVRA spreadsheet that contained the original threats and risk as a basis. As a result of this activity, a new document with adjusted factors for each of the threats listed in the spreadsheet is produced. Combined with the cost assessment of the security measure, this document provides the input that is needed to decide whether to implement the selected security measure(s) or not.

2.3.3 Embedding the risk reduction in the SRMM

The risk reduction methodology needs to be embedded in the Risk management method that is used by the investor and or end-user organisation. In this document we use the SRMM. The following paragraphs describe the SRMM steps that relate to risk reduction.

2.3.3.1 Risk treatment step

In this step of the SRMM, the list of prioritised risk elements is analysed, considering the risk evaluation criteria. For each risk element, an assessment must be made to either:

- Reduce the risk - appropriate security controls will have to be selected that reduce the risk. A residual risk might still be present, even with the selected security controls implemented, but it will be lower than the original risk.
- Accept the risk - the risk as-is being accepted entirely.
- Transfer the risk - Transferring risk can be done by, e.g., insurance against the consequences of a risk, or by sub-contracting a partner that will take over part of the responsibility.
- Avoid the risk - the risk can be avoided by, e.g., changing the intended use of functionality or context of the original planned activities.

In the risk reduction methodology, we will focus on the first bullet above: reduce the risk by implementing security controls. When risk is transferred or avoided, there will also be a risk reduction and resulting residual risk. Risk transfer or risk avoidance may incur costs; these are out of scope of this activity.

As part of the risk reduction activity, a gap analysis will be performed on security controls and technical measures to determine which controls and technical measures are needed to reduce

risk but are missing or not available today. For these missing controls, a cost assessment must be conducted, and the risk reduction must be calculated. These steps are all recorded in the risk treatment plan.

2.3.3.2 Risk acceptance step

In this step, residual risks are evaluated and accepted.

The costs of security measures are linked with the reduction of risk and the residual risks are evaluated against the pre-defined risk acceptance criteria. The acceptability and costs of the risk treatment plan are evaluated, and a decision is made whether the residual risks that do not meet the pre-defined risk acceptance criteria are justified.

If the costs are too high, or the residual risk remains too high, the previous step (risk treatment) must be revisited, providing clear guidance to adapt the risk treatment plan (e.g. lower costs for security measures or increased reduction of the residual risk).

3 Selected Security Solutions for Cost Assessment

3.1 Introduction

The methods that are described in the previous chapter have been used to assess various security solutions that have been developed within SEGRID. This chapter describes the selection process (3.2) and provides a short generic description of each selected security solution (3.3).

3.2 Selection process / rationale for selection

Within SEGRID's WP4 "Novel security solutions", several security solutions have been developed. However, not all security solutions are equally suitable for cost assessments. Some solutions are still in a very conceptual stage, making it hard to clearly define these solutions to an extent were a reasonable cost assessment is even possible.

The following developed SEGRID security solutions were considered:

1. Security and Privacy Architecture DEsign
2. Privacy by Design
3. Trusted Platform
4. Resilient Supervisory Control and Data Acquisition (SCADA) systems ("Resilient SCADA")
5. Resilient communication infrastructure
6. Key management for group software distribution
7. Robust and scalable (D)TLS-based communication
8. Intrusion Detection System (IDS) and authentication in mesh networks
9. Development of an active vulnerability assessment tool
10. Vulnerability discovery and diagnosis tool.

It should be noted that the first two items on this list are strategic measures and not security controls as such. These measures should be in place (which requires skilled staff and a suitable culture), and if not, implementation of other security controls will be far costlier.

The following items were considered suitable for a cost assessment, based on (a) the level of concreteness of the security solution, and (b) the expected data availability. Below, in brackets the 'owners' within the SEGRID consortium are pinpointed that were believed to have access to cost-related knowledge about the security solution developed by SEGRID:

1. Resilient SCADA systems (FFCUL, ABB, EDP, Alliander).
2. Development of an active vulnerability assessment tool (KTH, ENCS, TNO, Alliander).
3. Robust and scalable (D)TLS-based communication (SICS, ENCS, ABB).
4. Key management for group software distribution (SICS, ZIV, Alliander).

3.3 Selected security solutions

3.3.1 Resilient SCADA systems

SCADA systems form the backbone of critical infrastructures (e.g. the power grid and drinking water supply systems). To enhance the control of critical infrastructures, modern information and communication technologies are integrated with Operational Technologies such as SCADA systems and field devices. However, the integration of field networks with corporate and enterprise networks make SCADA systems more exposed to the plethora of cyber-attacks plaguing Internet-based systems [Bak11], which may lead to operational failures.

An intrusion-tolerant SCADA system, where the SCADA Master is replicated, can be a solution to enhance the protection capabilities against malicious cyber-attacks.

3.3.2 Active vulnerability assessment tool

The active vulnerability assessment tool consists of two main parts: 1) the vulnerability assessment tool, and 2) the active modeller. The work in SEGRID (related to this task) has been focused on developing the active modeller and to use an already existing vulnerability assessment tool[2]. Thus, in the following description the assumption is that the active modeller needs to be developed while the vulnerability assessment tool is bought/used off-the-shelf. The idea is to use existing tools for system and security management, and merge the results from the active modeller into a consistent model (that can be used for vulnerability assessment). Examples are network scanners, vulnerability scanners, SIEMs, IDSs, etc. These security tools are primarily software based, but some need their own hardware components. Some are passive in nature (just observing) whereas others actively log in or require agents out in the studied ICT/OT-infrastructure. In principle the idea is to reuse existing security tools as the source of information, but one can also imagine enterprises buying such tools for the sole purpose of the application. The active vulnerability assessment tool considered is scaled by numbers of users and nodes in the network.

3.3.3 Robust scalable (D)TLS

The White paper on the Security and Privacy Architecture DEsign (SPADE) methodology [4] represents the Datagram Transport Layer Security (DTLS) protocols as a relevant option to provide secure end-to-end communication between nodes in a Smart Grid system. In particular, this concerns smart grid communication channels where Data Hubs, DSOs, Meter Data Concentrators and OMSs take part.

As has been anticipated by SEGRID D4.1, the DTLS protocol displays two relevant security and performance issues. First of all, DTLS is highly vulnerable to a specific form of Denial of Service (DoS) attacks aimed at establishing a high number of invalid, half-open, secure sessions. Secondly, even when the efficient pre-shared key provisioning mode is considered, the key storage on the DTLS server-side scales poorly with the number of DTLS clients. SICS Swedish ICT has designed a security architecture that efficiently addresses both issues without breaking the current standard.

[2] The assessment tool used here is called securiCAD developed by a start-up company called Foreseeti, which is a refinement of a previous research product called CySeMoL.

The TLS and DTLS protocols are the de-facto solution for securing communications at the transport layer. In smart grid infrastructures, relevant entities adopting (D)TLS are, for instance, SCADA units and RTUs in secondary substations. Two entities that intend to communicate over (D)TLS, namely a client and a server, first perform a specific message exchange - known as handshake - to establish a secure channel. The client typically takes the initiative by sending a ClientHello message to the server.

The handshake itself is vulnerable to a security threat, which makes (D)TLS servers highly exposed to a DoS-attack. In fact, an adversary can repeatedly send ClientHello messages to a server and force that server to continuously perform invalid, resource-demanding, handshake processes. The server is then induced to establish a consistent number of invalid, half-open, (D)TLS sessions. This can exhaust memory and network resources on the server, making it less responsive or even unavailable to process ClientHello requests from legitimate clients, and hence endangering the expectedly correct and safe operations in the system.

The solution developed in SEGRID allows (D)TLS servers to identify invalid ClientHello messages and promptly abort the handshake execution at its very first step. This relies on a Message Authentication Code (MAC) over the ClientHello message, computed by the client through key material obtained from a Trust Anchor entity, and included in the ClientHello message as an extension. The server registered at the Trust Anchor derives the same key material and checks the MAC to determine whether continuing or aborting the handshake. This effectively neutralises the Denial of Service attack, substantially limits its impact and preserves service availability in the system. The proposed solution does not break current standards, and can additionally support a seamless and highly-scalable derivation of key material in case the (D)TLS handshake is based on the Pre-Shared Key (PSK) mode.

3.3.4 Key Management for Group Software Distribution

With particular reference to the SEGRID use case 1[5], one Data Concentrator device and a number of associated Smart Meter devices can be intended and configured as members of a same *group*. Among other tasks such as collecting measurements from and issuing commands to the Smart Meters in the group, the Data Concentrator is responsible for distributing software updates (e.g. new firmware versions) to the Smart Meters. This operation can be efficiently performed via multicast communication within the group. In this way, a reduced amount of information has to be transmitted and the update process can be completed in a shorter time.

Nonetheless, it is necessary to secure the software update process by encrypting communication within the group. This is vital in order to prevent an external adversary from collecting the distributed software updates, analysing and/or reverse-engineering them, and possibly finding vulnerabilities that can be exploited to mount cyber-attacks against Smart Meter devices.

In order to provide secure communication within the group, the software distribution process must rely on some cryptographic key material. However, this results in the additional task to properly and securely manage the key material itself, i.e. revoking and re-distributing it in a

secure and effective way upon the occurrence of specific events. In addition, this key management process is required to be efficient and scalable with the number of devices in the group, as well as to display a limited and affordable impact on network and system performance. SEGRID developed a solution for ‘Key management for group software distribution’, applying a novel group key management protocol. It is highly scalable and has efficient collusion recovery procedures.

4 Cost Assessment

4.1 Introduction

The cost assessment methodology description in paragraph 2.2 offers a complete overview of cost assessment elements. After defining the scope and goal of the cost assessment, this chapter provides a description of the actual cost assessment that was performed for the four selected security solutions (see 3.3). The following aspects of each security solution's cost assessment are highlighted:

- description of the security solution aimed at performing a cost assessment,
- the cost assessment's identification of main cost items,
- the actual numerical outcome, and
- observations following from the cost assessment.

Annex A2 includes the detailed excel spreadsheet that is underlying the figure used in this chapter.

It should be noted that not all previously described elements of the cost assessment methodology are covered in the actual SEGRID cost assessment, e.g. since the assessment is not about comparing security solutions, possible differences in life cycle between solutions have not been considered. Also, some of the advanced analysis options, e.g. extensive cost driver identification and sensitivity analysis, have not been performed at this stage because it was out of the scope of the project.

4.2 Cost assessment scope and goal

When performing a cost and benefit assessment, it is of major importance to determine the scope for which the assessment is made (see also paragraph 2.2.2). The scope is usually that of the stakeholder that is about to invest in the security solution and is facing the decision to invest or not. A good insight into the costs that are associated with the security solution - both non-recurring and recurring - is key to underpinning that decision. Alike, good insight into the risk that is reduced by the security solution is needed. Another focus could be that of the developer of security solutions, who wants to know how much investment is needed in research and development and the production of the security solution. Knowing the costs, will there be a market for the security solution?

For this study, the stakeholder scope is that of a mid-sized DSO (4-6 million consumers) that has to decide whether to invest in the implementation of a security solution or not. It should be noted that the main goal of the cost assessments in the next chapter is to test the methodology and to identify lessons learned for conducting cost assessments of smart grid cybersecurity solutions.

4.3 Resilient SCADA systems

4.3.1 Solution description

Replicating the SCADA Master can increase the protection of the SCADA system against cyber-attacks. Because changes in the SCADA system can be both cost and time consuming, it is important to set clear boundaries for this particular solution as a first step in the cost assessment. The cost assessment is performed from the viewpoint of a mid-sized DSO with 4-6 million consumers. Some assumptions are made about the current combined IT and OT landscape of such a DSO. Both assumptions and boundaries are described below and replicated in the actual cost assessment spread sheet.

The resilient SCADA system is characterised by:

- The system is resilient against the compromise of one copy of the SCADA servers. Four copies of the server are required to make the system this resilient.The servers should use a Smart Meter Requirements (SMR) protocol in their interactions;
- Diversity controls that are kept to a minimum*;
- Distribution of the four servers over two geographically separated locations, to protect against accidental disruptions (such as fires or floods) of one location. Assuming a mid-size DSO has already 2 data centres (DCs), these would be the places;
- Co-located servers at these DCs which use separated hardware but are connected to the same communications network.

* The minimum is to have no diversity, but then the security measure is not strong. The amount of diversification is one are in which operational costs at the DSO need to be balanced against risk reduction. Diversity can be found in:

- Application layer software from same SCADA vendor
- Operating system
- Team maintaining the servers
- Log in through central authentication system (LDAP, AD, …)
- Possibility to log in with local (emergency) admin credentials, used if the central authentication system is used.

In the solution that we have considered, the first bullet point is not diversified (we consider a solution wehre all SCADA applications come from the same SCADA vendor), the other bullet points are implementation decisions of the DSO.

The Resilient SCADA will have impact on the following system components; central SCADA servers, Front-End servers, Application Servers, Historian, HMI workstations. The number of servers, workstation and Front-Ends must be flexible. The same software must be used for all configurations either automatically or through configuration files. Software development must be done in the inner core of the SCADA system, e.g. in the real-time database management, in the HMI, in the Front Ends. Some elements are not considered part of the solution (and thereby cost assessment): RTUs, Wide Area Network and connection to office networks.

4.3.2 Cost assessment

4.3.2.1 Main identified cost items

Although both the solution procurement and installation as well as the solution use and maintenance costs are calculated, most of the costs are associated with the procurement and installation of the resilient SCADA solution within the current SCADA system of a DSO.

More specifically, the highest cost items for this solution are software development, installation, testing and migration expenses. These expenses will be explained in more depth below:

Software development: Software development must be done in the inner core of the SCADA system, e.g. in the real-time database management, in the HMI, in the Front Ends. The estimate for this development is a couple of man-years, i.e. about 80 man-weeks. At an internal cost of about 100 € per man-hour this represents a cost of 320 k€. However, the testing, will be considerably more expensive because testing such applications should be done thoroughly and is therefore time-consumiing. Ten man-years seem a reasonable estimate which represents about 1,6 million € as a lower boundary estimate. Upper boundary is at least plus 50%.

Installation costs: This is the extra costs if you install the system on site (site test). It is € 50.000-100.000 from the vendor's point of view. Adding another € 500.000 - 1.000.000 for internal testing by the DSO**.**

Testing and migration expenses: This is a total system upgrade to a new release, not only resilient SCADA. To implement resilient SCADA on an end user system will require a total release upgrade. DSO requires engineers to go to every site. Such costs may keep DSOs back on quickly migrating to new systems.

Some other costs are taken into account, but these are less substantial and therefore not explained in more depth. Examples are costs for extra servers, additional training for system operators and some ongoing technology training.

4.3.2.2 Cost assessment results

Solution procurement and installation	€ 6.825.000 – € 10.050.000
Solution use and maintenance	€ 275.000 – € 480.000 /year

The costs for developing the solution from a manufacturers point of view are included in the total amount of procurement and installation costs. The use and maintenance costs include the licencing costs for the SCADA system, because this particular solution will not be sold as a separate service, but will be included in the current system structure.

4.3.3 Observations

During the different phases of the cost assessment for the resilient SCADA systems security measure, there were several difficulties to overcome. By describing these difficulties, others can learn from them.

Planning

Involve the right people; although technical people that are involved with the SCADA system within a DSO can tell all about the current technological system, they are not

always able to translate the features necessary for the security solution into concrete costs. So, project managers (sometimes not experienced with the extension or purchase of SCADA systems in specific) or team managers were needed the estimate all the costs.

Definition

Vendor assumptions; some parts of the solution will be bought from an external supplier. For the SCADA system, there may already be a partnership with the current supplier. Therefore, the assumption was that that supplier would implement the given solution. Assuming that a DSO would have to switch suppliers just for implementing this solution would increase the total costs significantly. Also, it was important to discuss the boundaries of the system definition in the beginning with all the different parties together. Because all partners involved in the cost assessment had a different background, it was valued to take time to discuss different angels to the assessment.

Analysis preparation

Defining all the costs; not all costs were easy to define. Some costs were straightforward, but others were interrelated with different assumptions and other costs aspects. It took some time to gather all the required data from within the participating DSOs and SCADA suppliers. Even when this was completed, the assessment mostly relied on the cost estimate by an internal expert of SCADA. Only for a few cost items historical data (for example costs of servers) was available.

Analysis

Different people estimate different costs. Due to both the first two observations, it became clear the cost assessment spreadsheet was filled in by people each of them using different reasoning, knowledge and insight. Therefore, the validity of the total cost assessment was at stake. In order to gain a wider spread in understanding of the costs amongst all partners (both DSOs and vendors/suppliers), a call was organised which helped in mutually filling in the cost assessment.

General observations

Make assumptions explicit: many assumptions made by the people that were involved in the cost assessment were implicit. They all are experts in a particular field and often forget to mention the assumptions on a topic which is very familiar to them. They consider these assumptions as given, although they may impact the cost assessment. Making assumptions explicit as much as possible is important in order to use the same assumptions for all the cost items.

Defining all necessary changes: during the cost assessment, it proved not feasible to asses all costs because an analysis of the current situation was needed. The current SCADA system had to be mapped including service agreements and other aspects, in order to determine if the solution would bear costs on these aspects or not. This made the cost assessment a time-consuming exercise. Also, because different architectures and technologies are in use at the participating DSOs, discussion was needed to see what would be a right base for the general (hypothetical example) mid-sized DSO.

4.4 SecuriCAD based active vulnerability assessment tool

4.4.1 Solution description

The Active Vulnerability Assessment Tool (AVAT) is built up from two main parts: a) a system vulnerability assessment tool, and b) a tool for active autonomous scanning and modelling of an existing ICT-system infrastructure. The main focus of the research and development made in the SEGRID project has been part b). However, in this cost assessment we also consider part a) since it is needed to make a useful tool in the end. For part a) we have been using the tool securiCAD[3]. Some of the cost assessments are based on discussions around the current business model for securiCAD, but this is of course subject to change over time. Also, with another vulnerability assessment tool, the cost assessments could be different. For part b), no close to commercial products exist. Thus, the costs assessment on this part is based on assumptions and best guesses of how such a tool could be priced once it exists. The cost assessment made here is made from the end user point of view.

In general, both parts (a and b) are software products. Thus, the end user would buy two (or possibly one bundled set of) software components from a vendor of the AVAT. In order to execute the software, hardware is needed. In the end, the amount of hardware needed will vary extensively with the ambition of the use of the AVAT. With smaller ICT-infrastructures and a low frequency of assessments quite little hardware is needed, maybe just a few standard PCs possibly and potentially cloud based. In our assessment we have assumed costs of a moderate ambition equalling some limited part of the overall enterprise ICT-infrastructure (say 500 to 1.000 machines distributed over a number of networks) in a nominal case. Some variance to those assessments is also provided.

In addition to the software and hardware of the AVAT, the solution also assumes that there exists a number of operational ICT (security) management tools in place at the end user premises to be used as sources for “raw data” input. Such tools include network vulnerability scanners, network traffic analysers, security information and event management (SIEM) systems and many more. Many such tools are normally in place at end user organisations, but rarely all types. The AVAT does not put an explicit requirement on any such specific tool and the general approach of the AVAT is on the contrary to make the most of existing data, not to collect more (even though this could come as a consequence for end users of AVAT that would like to improve their cyber security capability even further). For this reason, the cost assessment excludes these costs.

4.4.2 Cost assessment

4.4.2.1 Main identified cost items

The main identified cost items are:

- License costs of software (annual costs).

[3] securiCAD is produced by the start-up foreseeti (www.foreseeti.com). securiCAD is based on previous research results from KTH described in the Cyber Security Modelling Language (CySeMoL).

- Hardware for executing the software tool (either as annual cost or investment plus depreciation).

Costs for installation and technical maintenance have been considered minor.

4.4.2.2 Cost assessment results

Solution procurement and installation	€ 10.000 – € 500.000
Solution use and maintenance	€ 0 – € 4.000 / year

4.4.3 Observations

The cost estimate is showing a very large bandwidth for procurement and installation costs. In general, the main challenges for this cost assessment are the uncertainties related to how the AVAT would be commercialised and the amount of hardware needed. The AVAT would require much development and many business model related decisions must be taken. Very little hard data was available.

Planning

No particular challenges.

Definition

The cost will vary greatly with the usage of AVAT. Deciding on a good reference case has been the source of much discussion.

Analysis preparation

Very little "hard data" has been available so many 'guesstimates' had to be made.

Analysis

No particular challenges.

General observations

None.

4.5 Robust scalable (D)TLS

4.5.1 Solution description

The Robust (D)TLS solution addresses the issue of secure communication in a SCADA system between the SCADA Front-Ends and the RTUs in the electrical substations. This communication is the core of any SCADA system in the electrical energy sector. Without such communications, there is no value at all of the SCADA system since DSOs will not have contact with the electrical power grid. For the DSO as stakeholder, the SCADA asset is the most critical in

order to fulfil its obligation to deliver power to its customers and to the society. The RTU communication will always be the core part of any SCADA system and therefore its relevance will always exist.

The widely adopted DTLS communication protocol is affected by two different issues. First, it is possible to perform a DoS-attack against server hosts during the initial handshake process and inducing the establishment of several invalid, half-open, sessions. The current standard countermeasure based on Cookie exchange is not effective against such a cyber-attack. Second, even efficient handshake modes require server hosts to store one pre-shared cryptographic key per possible client host. This scales poorly with the number of clients and complicates key provisioning in dynamic scenarios. SEGRID has designed a single approach that overcomes both issues. In particular, the DoS-attack is efficiently neutralised and preserves the robustness and service availability of server hosts. Besides, the number of keys stored on each server host is reduced to a single one, so assuring high scalability of the solution. The proposed approach does not require additional communication between clients and servers, does not break the current standard, and is immediately adoptable as part of the TLS protocol.

Some SCADA systems use OpenSSL for the implementation of TLS and DTLS communications. OpenSSL is freeware. It is preferable not to easy to add one's own extension to OpenSSL, therefore Robust (D)TLS has to be implemented by OpenSSL. Such a request has been made by SICS.

The improvements to (D)TLS have the most value for DTLS. That is why the costs are assessed for implementing in to Phasor Measurement Units (PMUs) that use DTLS. The solution also prevents denial-of-service attacks on TLS. TLS is the standard method to protect IEC 60870-5-104 (according to the IEC 62351 standard), and is also widely used to protect web interfaces and maintenance connections.

Also observe that the Robust (D)TLS protocol must also be implemented in the RTUs to work. A normal SCADA system has a mixture of RTUs from different vendors and ages which will make it difficult to have a complete implementation of Robust (D)TLS.

The following cost assessment assumes that OpenSSL will adapted the Robust (D)TLS solution.

4.5.2 Cost assessment

4.5.2.1 Main identified cost items

The main identified cost items are:

1. Testing of the updated OpenSSL library and verifying that no bugs are introduced.
2. Development of key storage in the SCADA server and handling of keys for the DTLS communication.
3. Testing of Robust (D)TLS in individual customer projects and setting of relevant keys.

Additional training will be very limited since this is an embedded function in the DTLS protocols and will not be seen by the end users. The additional training cost is negligible.

4.5.2.2 Cost assessment results

Solution procurement and installation	€ 8.000 - € 32.000
Solution use and maintenance	€ 4.000 - € 8.000 / year

4.5.3 Observations

Robust (D)TLS is a relatively simple function to implement in an existing SCADA system. As stated above, it is assumed that OpenSSL will implement the actual solution so what is left for the SCADA vendor is to integrate Robust (D)TLS in the existing SCADA Front-Ends and to implement a key management functionality in the SCADA server.

The cost assessment for the SCADA system has not provided any special difficulties, because it is only an update of existing libraries. Of course, the cost assessment should be done by a SCADA expert on RTU communication, but such an expert has been available in the SEGRID project. However, it should be observed that this solution will make no sense if it is not implemented on the RTUs. In an existing SCADA system, there will be mixture of RTUs from different vendors and of different technology generations. A cost assessment for all these RTU types of different generations and different vendors is not possible to give.

4.6 Key Management for Group Software Distribution

4.6.1 Solution description

The mainly considered key management setting in smart grids consists of:

i) the multicast group composed of the Smart Data Concentrator and the associated Smart Meters, and
ii) the Key Manager functionality running as an additional service on the same Smart Data Concentrator.

More in general:

i) the Key Manager functionality can run on a different machine/host than the Smart Data Concentrator, and
ii) the key management solution as such can be used also in alternative secure group communication contexts than group software distribution.

It is assumed that:

- The system is already relying on a secure group software distribution functionality.
- There is already a(n alternative) group key management service up and running and eligible to be replaced by something better.
- The available group key management service is already supported by satellite related services such as a Group Membership System and an Intrusion Detection System with which it cooperates.

4.6.2 Cost assessment

4.6.2.1 Main identified cost items

The solution involves costs of:

- Theoretical design and analysis of the group key management protocol.
- Implementation and testing of a prototype for general purpose hosts.
- Solution's first design, development and testing.

The costs of acquiring the solution is expected to be nil, since the available prototype implementation is an open software library and is based on (relies on) open software modules (libraries). There are no fees for licensing the solution. The owner of the rights permits even commercial use of the solution with no other condition than stating that he/she is the creator of the solution.

The costs of incorporating/installing the solution takes into account the assumptions and boundaries mentioned in Section 4.6.1. The costs really depend on the particular system composition/configuration where the solution is going to be deployed and used, essentially as a software library.

In a general case, this requires a software port to (re-)implement and test the whole key management library, while on the other hand the overall functional behaviour of the group key management solution remains unchanged. The fact that it is not necessary to redesign the solution as such compensates the expected effort required to produce and test the porting of the implementation to possibly different hardware platforms, operating systems and network communication stacks.

Having said that, it is reasonable to estimate such porting/incorporation/installation/re-testing costs for a general case to an amount that is comparable to the cost estimation for the first implementation and testing of the prototype for general purpose hosts, since a complete re-testing in envisaged for security and reliability issues.

The cost estimate excludes the purchase costs of smart meters and data concentrators.

The costs for use and maintenance is expected to be (close to) zero, since it is a service provided by a software library operating automatically with no need per se for particular ordinary intervention.

4.6.2.2 Cost assessment results

Solution procurement and installation	€ 523.000 – € 704.000
Solution use and maintenance	€ 0 / year

There is a large difference between best and worst cases. Best case assumes that about half the smart meters currently under operation in a target geographical area can host the new solution and all the data concentrators can also operate it with no other condition than performing a FW update on concerned devices. The worst case assumes that all devices must be substituted by brand new ones (or there is the need to deploy a new complete AMI infrastructure from scratch).

4.6.3 Observations

During the different phases of the cost assessment, there were several difficulties to overcome while doing the cost assessment for Key Management for Group Software Distribution.

Planning

At the time of planning the works related to the development of the security solution, there have not been issues. The description of the solution was fully available and understandable from the very beginning, and enough resources were allocated from the very first time.

Definition

There were some concerns regarding the scope of the solution in terms of maximum number of devices to be administrated through a unique data concentrator. This concern was solved by arguing that the current data concentrator can host not only the solution itself but also the worst estimation of memory storage needs for operational data.

No other issues were found in this phase. Upgrades were said to be performed in just the same way as commonly actioned, and this statement solved eventual issues regarding maintenance, along with the automatic operation of the security solution and the underlying communications infrastructure.

Analysis preparation

No particular challenges.

Analysis

No particular challenges.

General observations

None.

4.7 Cost assessment summary

4.7.1 Approach

This chapter describes the cost assessment that is performed for the four selected security solutions by following the steps that are described in the Methodology section of this report. It can be concluded that each security solution's cost assessment has its own specific dynamics and

difficulties, however some observations turn out to be more common and in most cases independent of the specific security solution:

- Overall it was not easy to estimate the costs. Solutions are often at a stage in which they are not yet commercially available, and many business model related decisions are not yet clear, making it hard to estimate certain costs. E.g. the costs of software licenses depend not only on the development costs but also on the number of expected future customers of the software.
- It turned out that defining the security solution is often not straightforward. The solution will often become part of an existing configuration, making it challenging to identify those elements that are specific for the security solution and those that are already in place and will therefore not invoke any extra costs. The existing situation may also differ between DSOs, making it important to reach agreement between DSOs about the current baseline situation and clarifying the underlying assumptions.
- In most cases people that have been active within SEGRID have a technical background, making it hard to say anything about costs. Some explanation was needed regarding the methodology, what each cost item was about, etc.
- Historical cost data is hard to come by because of the innovative nature of most solutions. Therefore, many 'guesstimates' needed to be made, resulting in large bandwidths for most cost estimates.
- Many assumptions had to be made to provide cost estimates. Often, different people make different assumptions and often these assumptions are made implicitly. It proved of vital importance to make assumptions explicit in order to gain mutual understanding between experts as well as between the participating DSOs.

4.7.2 Results

The overall outcomes of the cost assessment (table below) vary widely over the four assessed security solutions, mainly caused by the great variance in software and hardware requirements for each security solution. The costs of maintaining and using the solution after its implementation are usually considered to be quite limited, usually because little maintenance is needed or can easily be included in the day-to-day activities and procedures that are already in place at no or little extra cost.

The bandwidth of the cost estimates is quite considerable, showing the difficulties and uncertainty that comes with estimating the costs of new, innovative solutions that have not yet been fielded and commercialised. Also, the difference between low and high cost estimates reflect the variety in assumptions that can be made when it is not yet clear what exactly is needed for a security solution to work and what is already in place within a midsized DSO. For future analyses it is recommended to include a sensitivity analysis in the cost assessment.

Table 3: Outcome cost assessment for the four security solutions

x € 1.000	Procurement & Installation		Use & Maintenance / year	
	Low	High	Low	High
Resilient SCADA system	6.825	10.050	275	480

Active vulnerability assessment tool	10	500	0	4
Robust scalable (D)TLS	8	32	4	8
Key Management	523	704	0	0

5 Risk Reduction/Impact Assessment

5.1 Introduction

This chapter describes the actual Proof of Concept of risk reduction that is conducted in SEGRID. We have used the Risk assessment results of WP2, where the first four steps of the SEGRID Risk Management Methodology (SRMM) were applied to SEGRID use case 2, scenario 2 (uc2sc2)) 'Load balancing renewable energy centrally'. In step 5 (risk treatment) of a normal SRMM process, we would select all risks that exceed the risk appetite. We would try to find appropriate security measures that can help to reduce the risk to a level below the risk appetite.

SEGRID has chosen four security measures to be subjected to the cost assessment activity (see paragraph 3.3). The risk treatment step will therefore use these four selected security measures and verify if they actually will reduce the risks identified by the risk assessment of uc2sc2. The first four paragraphs of this chapter will describe in which way the four selected security measures (on which a cost assessment was done) can reduce the cyber security risk.

Paragraph 5.6 describes the high-level results of and experience with the risk reduction step with these four measures. The detailed results can be found in an annex to this document that, due to the sensitivity of the results, is classified as 'RESTREINT UE/EU RESTRICTED' Annex and will be handled accordingly. This information is only available to the project partners and designated officials of the EU and its member states.

5.2 Resilient SCADA systems

The Resilient SCADA concept developed within the SEGRID project is built on the principle that more servers work in parallel on all tasks of the SCADA systems. These tasks include both handling of incoming data from the supervised processes which must be stored in the SCADA server and treated in many ways, as well as outgoing data from the SCADA operators working at SCADA control workstations to the actuators driven by the RTUs, e.g. to change the grid configuration, send setpoints to generation units, or change transformer tap settings. The Resilient SCADA concept will compare data and results from all involved servers, and, if the result from some of the servers deviate from the others, introduce a voting system where the majority of servers can exclude a misbehaving server. A deviation in any of the servers could come either from a cyber-attack, or, simply, an error in that server. This means that the Resilient SCADA concept could be used both to improve availability of SCADA systems above the normal dual redundancy concept, and to discover cyber-attacks on a single server.

It must be understood that the availability and security of SCADA systems together with the performance are the most critical aspects of such systems. This means that a concept like Resilient SCADA cannot be introduced in an existing SCADA environment without a very extensive testing to be sure that the critical aspects mentioned above are not endangered. A SCADA controlled environment is not a deterministic system, it is a real-time system where process events might occur at any time and may interrupt any ongoing action. This makes the number

of test situations almost unlimited and makes the verification of a new availability and security concept very time consuming and expensive.

5.3 SecuriCAD based active vulnerability assessment tool

The Active Vulnerability Assessment Tool (AVAT) is mainly a management tool (strategic and operational) to support more effective cyber security decisions. This means that the tool is only indirectly improving the cyber security posture as such (as opposed to security mechanisms such as intrusion detection systems or anti-malware solutions). We would however argue that a (good) AVAT is extremely important to be able to achieve actual resilience. The reason for this is that ICT-infrastructures for smart grids are extremely complex integrated systems-of-systems. It is very difficult to get a good understanding of the security of the infrastructure as a whole. Without it, the security can easily become poor. With just a single vulnerability (say, an unpatched software) in one part of the infrastructure, all other well working and advanced protection mechanisms (say, two-factor authentication and IDSs) in another part of the infrastructure can be bypassed. Cyber security is an optimisation challenge to maintain enough security in all parts of the infrastructure, an infrastructure that is constantly changing and is thus inherently challenging to keep track of.

Even though difficult to prove, it is believed that with a good decision support for cyber security management, the cyber security can be improved manifold. Or inversely, obtaining the same level of cyber security could be done at a much lower cost depending on the end user preferences.

5.4 Robust scalable (D)TLS

Modern SCADA systems use TCP/IP based protocols like IEC 60870-5-104 to communicate with their connected RTUs. According to the IEC 62351 standard, these protocols should be protected by TLS. The (D)TLS improvement will protect such communication against denial-of-service attacks. TLS is moreover also widely used on maintainance channels on RTUs, for instance to protect web interfaces or vendors specific configuration protocols.

The solution will however probably be of even bigger value on Phasor Measurement Units (PMUs). PMUs will most probably be introduced on a bigger scale in future SCADA systems but first PMUs must be installed in the substations. The PMU communication will, most probably, be based on DTLS but, as stated, is very little used today. Also observe that the Robust (D)TLS must also be implemented in the RTUs to work. A normal SCADA system communicates with a mixture of RTUs from different vendors and ages which will make it difficult to have a complete implementation of Robust (D)TLS.

Therefore, the risk reduction in existing energy grids of DSOs will be small. In the future, when PMUs are introduced in power grid supervision on a more general scale, the development of Robust (D)TLS will be more valuable to avoid DoS-attacks on PMU communications. It is easy to imagine a DoS-attack on PMU communications which will make the SCADA operators take the wrong decisions in the control room due to lack of relevant data from the PMU process. An

actual risk reduction is very difficult to estimate since this improvement only protects against one type of possible attacks on DTLS and TLS communication.

5.5 Key Management for Group Software Distribution

In order to achieve high scalability and performance, a single Smart Data Concentrator can send software updates to multiple associated Smart Meters at once, by means of multicast group communication. Such communications are secured by using a commonly shared group key.

Upon a number of events, the group key must be revoked and renewed. Until this operation is successfully completed, secure group communication between the Smart Data Concentrator and the associated Smart Meters must be suspended.

The proposed solution developed in SEGRID is extremely efficient and highly scalable with the number of Smart Meters considered in the same group. Therefore, unlike with alternative approaches, it is possible to fully restore secure communication within the group in a shorter amount of time, and more efficiently for Smart Meters from a performance point of view. The gain in time to process the change of a former broadcast key to a new one, and the fact that the amount of exchanged messages is less than for other former approaches, make the chance for an attacker to take advantage of the compromised nodes, whilst there is a change in broadcast key, to diminish dramatically.

Then, by reducing the amount of time required to fully restore security in the group, the SEGRID security solution reduces the risk that:

i) stale and/or compromised group keys can be exploited by an adversary to break secure communication in the group, so enabling, e.g., reverse engineering of software updates;
ii) the set of Smart Meters is involved in key management operations for an amount of time which is too long to endure, and can degrade/interfere with operations in the smart grid.

Finally, it is worth noting that this security solution applied to smart meter networks (regardless the underlying communications technology used, but conveniently adapted to work along with this solution) can be used not only for performing FW updates on a large number of meters, but also for setting common sets of parameters to smart meters which are of the same type or, at least, are going to have the same behaviour (with consistent settings table, but not necessarily of the same model or type).

5.6 Risk reduction

We have evaluated whether the four security measures would reduce the risks that were assessed on use case 2, scenario 2. This information is only available to SEGRID project partners and designated EU officials and is laid down in annex 3 of this document, which is classified as ‘EU Restricted’.

6 Conclusion

The cost assessment shows that the bandwidth of the cost estimates is substantial. This reflects the difficulties and uncertainties that are involved when estimating costs of new, innovative solutions that have not yet been fielded and commercialised. It also reflects the variety in assumptions that can be made in cases where it is not yet clear what exactly is needed for a security solution to work, and what part of the solution is already in place and therefore incurring no extra costs to the organisation.

The cost assessment also shows that business models are in some cases not yet clear, making it hard to estimate some of the costs. Business models - who is willing to pay how much for what - should be considered whilst further developing the security solutions.. Otherwise, the result will be a nice technical solution that nobody is willing to pay for. This especially applies to the Active Vulnerability Assessment Tool. The cost and risk reduction assessment can be used to provide input for business model development.

It can be concluded that the cost assessment is a good first attempt to estimate the costs. However, the value of the assessment does not lie in the numerical outcome. The real value is in fully thinking through the security solution: its elements - what is included and what is not - how should the solution be implemented, and what - and who - is needed for it to work and keep working. The exercise clarifies what the unknown or uncertain factors are. These uncertain factors become clear in the form of assumptions. Unknown factors and uncertainties need to be clarified and resolved as much as possible, otherwise the decision to invest may not be justified. Therefore, the cost exercise should be updated whilst developing the security solution and a sensitivity analysis should be performed. The step-by-step approach that is presented in this report can serve as a guideline.

In a regular risk assessment, risk treatment would have been done by taking the following steps: review the list of assessed risks, select which risks need to be reduced, select security controls to reduce the risk, select appropriate candidate security measures, assess them on cost and then decide which measures need to be implemented (balancing cost versus risk reduction). But we could not follow these steps, because we had to start with an existing list of risks which resulted from a risk assessment done by WP2 on SEGRID use case 2 scenario 2. Moreover, we had to assess only four security measures developed by SEGRID that were selected for cost assessment because they were suitable, based on (a) the level of concreteness of the security solution, and (b) the expected data availability. We nonetheless have verified our cost assessment methodology with a small Proof of Concept, using this available information. The results are only available to designated officials of the EU and its member states.

The trade-of between cost and risk reduction cannot be reflected in a single number. It is the investing organisation that needs to decide what a certain degree of risk reduction is worth. By following the steps that have been laid down in this report, an investing organisation (in this example case the DSO) is able to calculate the expected costs of the security solution and start the dialogue about it internally. Together with the risk reduction assessment, the organisation can then decide whether a security solution is worth implementing or not.

7 References

[1] Ir. B. Bhola en Ir. J.A.M. van Wees, "FEL-SALDO, een Stappenplan voor het Analyseren van Levenscycluskosten binnen de Defensie-Organisatie", FEL-93-A337, 1993 (in Dutch).

[2] VALUESEC, WP2. T2.3 & T2.5 / D2.2; Data model and decision model – basis descriptions.

[3] SEGRID Risk Management Methodology (SRMM), White paper and worksheets. SEGRID Consortium, 2017.

[4] Security and Privacy Architecture Design (SPADE) for Smart Electricity Grids, White paper, SEGRID consortium, 2017

[5] SEGRID D1.1 ‘Architecture and design for use cases’, SEGRID consortium, April 1st 2015

A1 Excel Template Cost Assessment

Instruction:
This is a generic cost assessment template designed for describing a security solution and its associated life cycle costs.
1. Please fill in the grey coloured fields below. PLEASE BEAR IN MIND THAT YOU SHOULD FILL IN THE ITEMS BELOW FROM A DSO PERSPECTIVE.
2. Definitions of the various items 1 through 6 can be found in tabpage "Definitions".
3. If cost items are not applicable to the solution fill in N/A.
4. If cost items are missing, please insert a new row.
5. If necessary, remarks can be added in column I.
6. For each cost item the lower and upper boundary is requested in column F and G. In case there is no uncertainty please fill in the same

	Resilient SCADA systems	Description of the security solution		
		Specification	Assumptions	Remarks
1	Stakeholder focus			
2	Security solution setting			
	Number of clients served and/or geographical area and/or size etc.			
3	Time horizon			
	Total life cylce of product/service (time till replacement)			
4	Solution definition			
	System definition: what are the elements that make up the security solution:			
	Hardware (e.g. network, server, workstation)			
	Software (e.g. related to network, server, workstation)			
	Solution boundaries: what is specifically not part of the security solution			

Solution procurement and installation costs (€)	Specification	Assumptions	Lower boundary of **total** costs	Upper boundary of **total** costs	Cost source (pick from dropdown list)	Remarks
Elements that can be bought off the shelf						
> Hardware (e.g. number of servers, workstations, networks)						
> Software (e.g. related to number of servers, workstations, networks)						
Elements that require development						
> Hardware (e.g. number of servers, workstations, networks)						
> Software (e.g. related to number of servers, workstations, networks)						
Installation and integration of hardware and software, testing (manhours)						
Migration expenses (manhours, user data migration, testing)						
Decommissioning costs						
Initial technology training (manhours)						
Other project costs (e.g. investigating susceptibility to vulnerabilities, availability of upgrades, patches and future licensing policies, possible costs other stakeholders need to make in order to implement the solution etc.)						
TOTAL			€ -	€ -		

Solution use and maintenance costs (€)	Specification	Assumptions	Lower boundary of **total** costs per year	Upper boundary of **total** costs per year	Cost source (pick from dropdown list)	Remarks
Licenses for software and hardware						
(External) Support for software and hardware (manhours or included in license)						
Internal IT Management and maintenance (FTEs)						
Implement minor changes: upgrades, patches, licenses						
Incident & problem management						
Backup and recovery process						
Data storage						
(Extra) bandwidth						
Infrastructure (floor space)						
Electricity (for related equipment, cooling, backup power)						
Ongoing technology training						
Replacement of hardware (depreciation per year)						
Management of IT department(s) / overhead						
Other recurring costs						
TOTAL			€ -	€ -		

Item	Definition
Description of the security solution	A general description of the security solution. What is it? What does it do in terms of risk reduction?
Assumptions	The assumptions that are underlying the specifications.
Stakeholder focus	The stakeholder focus defines the viewpoint from which the cost assessment is performed.
Security solution setting	The security solution setting describes the context in which the security solution is implemented. The context dictates boundaries to the solution definition and the associated cost estimates. Context can relate to e.g. number of clients served.
Time horizon	The time horizon sets the time boundary for the cost assessment. It is of specific importance for calculating the costs of use and maintenance of a security solution. For SEGRID, the time horizon is the time until replacement of the security solution, either by replacing it with a similar solution or by implementing a new technology.
Solution definition	The solution definition is a description of the elements that make up the security solution from the focus of the stakeholder defined under Stakeholder Focus. Usually, the solution is defined in terms of needed hard- and software. The solution definition also sets the solution boundaries: what is specifically NOT included in the security solution and therefore not included in the cost estimate.
Solution procurement and installation costs (€)	In this section the costs items should be listed that are related to the procurement and installation of the security solution as described under 'Solution definition' and from the focus of the stakeholder as defined under 'Stakeholder focus'. Generally, these are all non-recurring (one-time) costs that are incurred by the stakeholder in order to buy, develop, install, test, and integrate the security solution in a sustainable manner.
Lower boundary of total costs	Define the lower boundary of the total costs if applicable. Do not include extremes and outliers.
Upper boundary of total costs	Define the upper boundary of the total costs if applicable. Do not include extremes and outliers.
Cost source	Specify the source of the cost specification, choose from dropdown list.
Solution use and maintenance costs (€)	In this section all cost items should be listed that are related to use and maintenance of the security solution as described under 'Solution definition' and from the focus of the stakeholder as defined under 'Stakeholder focus'. These are recurring costs that are incurred by the stakeholder in order to use and sustain the security solution over the lifetime of the security solution.

Item	Definition
Lower boundary of total costs per year	Define the lower boundary of the total costs per year. Do not include extremes and outliers.
Upper boundary of total costs per year	Define the upper boundary of the total costs per year. Do not include extremes and outliers.

A2 Cost Assessment Results

20171106
Integrated file.xlsx

A3 RESTREINT UE/EU RESTRICTED Annex on Risk Reduction Results

This information is only available to SEGRID project partners and designated officals of the EU and its member states.