**FP7 Grant Agreement N° 607109**

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

# D6.8 SEGRID results elaborated on a use case scenario

Due date of deliverable: 30/11/2017
Actual submission date: 01/12/2017
Work package: WP6 Dissemination
Number of pages: 14
Revision: Version 1
Classification level: Public

| | |
|---|---|
| Project type: | Collaborative project – small or medium scale focused research project |
| Thematic Priority: | FP7-SEC-2013-1 |
| Start date of project: | October 1st, 2014 |
| Duration: | 36 months |

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

| | |
|---|---|
| Author(s) | Frank Fransen (TNO) |
| Contributor(s) | Nuno Medeiros (EDP Distribuição)<br>Marco Tiloca (RISE SICS)<br>Mathias Ekstedt (KTH)<br>Maarten Hoeve (ENCS)<br>Judith Rossebo (ABB)<br>Gunnar Björkman (ABB)<br>Nuno Neves (FCIENCIAS.ID)<br>Reinder Wolthuis (TNO) |

# TABLE OF CONTENTS

1 INTRODUCTION – RATIONALE OF THIS DOCUMENT ..... 4
1.1 The SEGRID Project ..... 4
1.2 Deliverable D6.8: SEGRID results elaborated on a use case scenario ..... 5
2 NEW SEGRID DISSEMINATION STORYLINE ..... 6
3 APPLICATION OF SEGRID RESULT TO UC2.2 ..... 9
3.1 Brief overview of UC2.2 ..... 9
3.2 Application SEGRID results to UC2.2 ..... 9

# 1 Introduction – Rationale of this document

## 1.1 The SEGRID Project

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

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

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

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

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

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

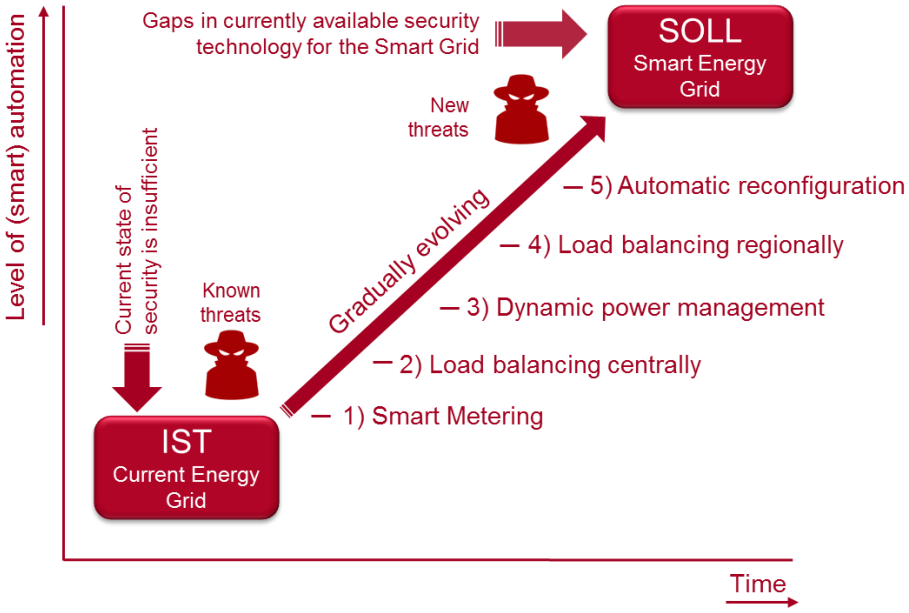



**Figure 1: SEGRID storyline**

## 1.2 Deliverable D6.8: SEGRID results elaborated on a use case scenario

The SEGRID project used this SEGRID storyline, described in section 1.1 and depicted in Figure 1, to guide the research and developments. Although this approach worked good to collaboratively identify and work on important cyber security and privacy challenges, when presenting the SEGRID results the storyline did not provide a framework for presenting all results in a coherent manner. In order to present the SEGRID results better, we decided to:

1) create a new storyline for presenting the SEGRID results that clearly shows how the results fit together to protect Smart Grids against cyber-attacks, and
2) present the SEGRID results in context of a single use case, in particularly use case 2 scenario 2 (UC2.2) - balancing MV renewable energy centrally.

This deliverable describes the new storyline to present the SEGRID results and a brief overview of the SEGRID results in context of UC2.2 as they have been presented at the SEGRID Summit.

# 2 New SEGRID dissemination storyline

The goal of the SEGRID dissemination storyline was to present the different SEGRID innovations in a coherent manner. The SEGRID innovations were developed in different Work Packages and address different aspects of information security management. In the table below the main SEGRID innovations that we want to show-case are listed.

| WP1 | WP2 | WP3 | WP4 |
|---|---|---|---|
| • Cost Assessment<br>• Operational Security Capability Model | • SEGRID Risk Management Methodology (SRMM) | • SecuriCAD & UC2.2 model<br>• Automated model generation<br>• Vulnerability Detection and Correction with Web Application Protection (WAP)<br>• Prevention of Injection Attacks in DBMS | • Security and Privacy Architecture DEsign (SPADE)<br>• Trusted Platform<br>• Resilient SCADA systems<br>• IDS and authentication in mesh networks<br>• Robustness and scalable (D)TLS<br>• Resilient communication infrastructure<br>• Key management for group software distribution<br>• Privacy by design |

Using the information security risk management in both operations and development phase it was possible to present a story in which most of the SEGRID innovations can be introduced and the interrelationship can be explained. In Figure 2 this new view is depicted. The story how it is presented in four steps is described below.

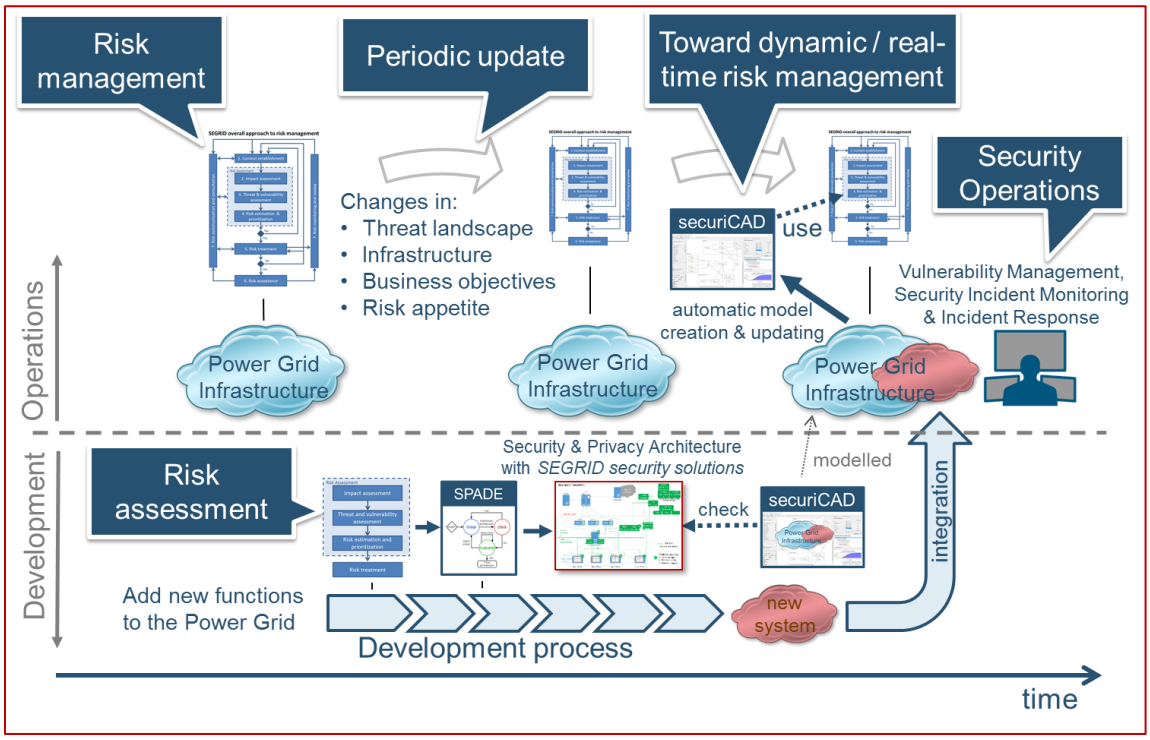
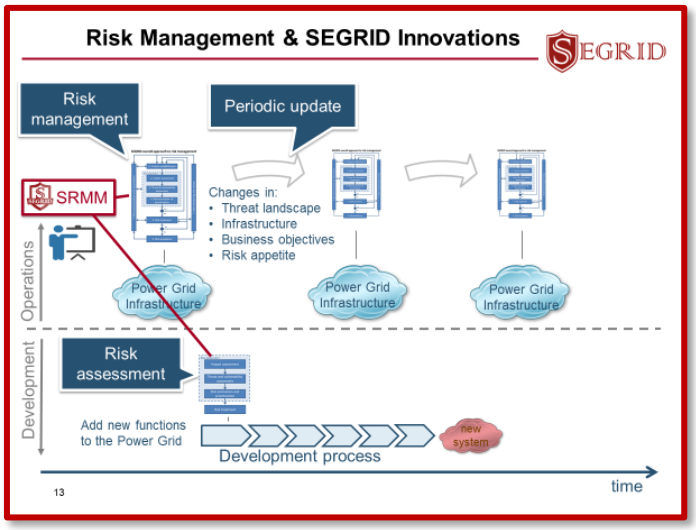



**Figure 2: View on how SEGRID innovations fit together[1]**

[1] Not all SEGRID innovations are depicted in the figure.

### *Step 1) Risk Management & Risk Assessment*

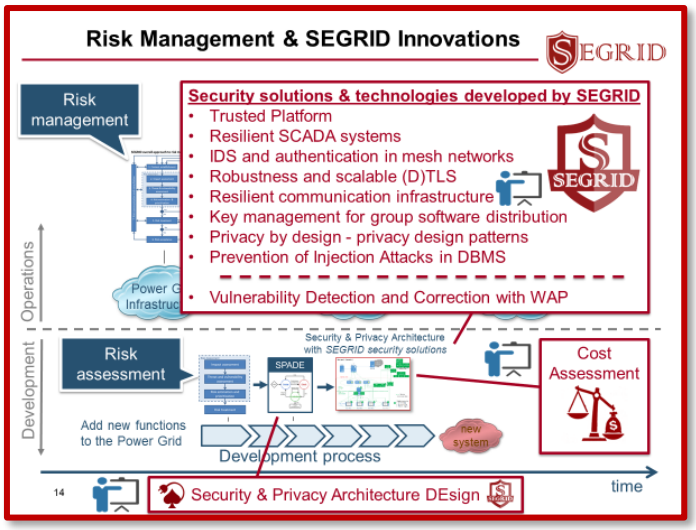
We introduce Risk Management and state that it should be applied to the power grid infrastructure. Risk Management needs to be periodically updated because of, for instance changes in: a) the threat landscape, business objectives, risk appetite. Next we state that when a new system is to be developed to introduce new functionality in the power grid, such as one of the SEGRID use cases, a development process is typically executed. Part of this development process is the execution of a risk assessment. Then we introduce SEGRID Risk Management Methodology (SRMM) as a solution for the Risk Management in the operations and the risk assessment part of the SRMM can be applied in the development process.




### *Step 2) Security & Privacy Design Architecture Engineering, novel security solutions & cost assessment*

The risk assessment on the initial design produces a prioritised list of risks and a risk treatment plan. This is used to develop security & privacy architecture for the new system. The SEGRID project eveloped SPADE to facilitate this design process. It is a cyclic approach to develop the security & privacy architecture, with three phases: *design*, *check* and *evaluation*. In SPADE's design phase security and privacy solutions will be selected to mitigate risks. SEGRID has developed several innovative security solutions and technologies, that can be considered for mitigating risks.

As part of SPADE check phase a cost assessment can be performed. SEGRID developed a cost assessment approach that can be used for this purpose.



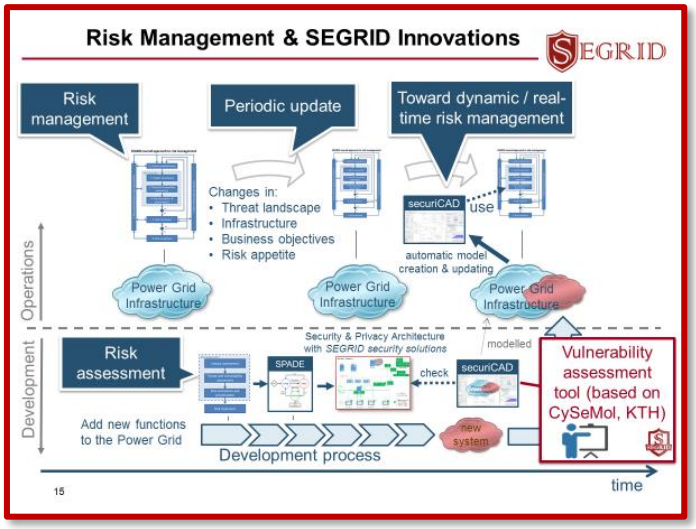



**Classification level: Public**

### *Step 3) Vulnerability Assessment tool securiCAD*

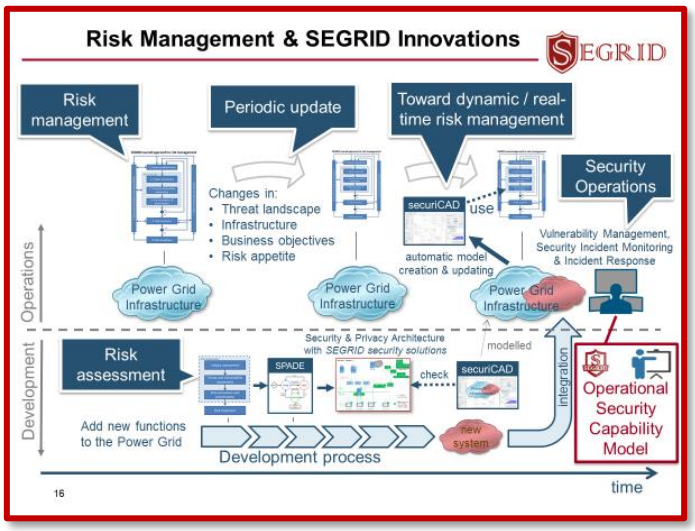
As part of the SPADE check phase the designed security & privacy architecture should be evaluated. This can be done with e.g. the vulnerability assessment tool securiCAD. The new system can be modelled in context of the existing infrastructure to determine if all infrastructure vulnerabilities are sufficiently dealt with.

In addition, when the existing infrastructure is modelled, securiCAD can also be used within risk management for more detailed threat assessment. SEGRID also worked on automatic model generation using scan, configuration management and monitoring data. When it is possible to automatically detect changes in the infrastructure and update the model, we envision that securiCAD enables a more dynamic / real-time risk management.




### *Step 4) Security Operations*

As the new system becomes operational, the security organisation at the DSO needs to include these systems within the security operations. These new smart grid systems typically have much shorter cycle to deal with incidents and vulnerabilities that will start popping up. We expect that DSOs in the coming years will have to focus more on vulnerability management, security incident monitoring and incident response. To enable this, they will typically establish a so called security operations centres for the OT domain. To support DSOs with this development, SEGRID developed an Operational Security Capability Model.

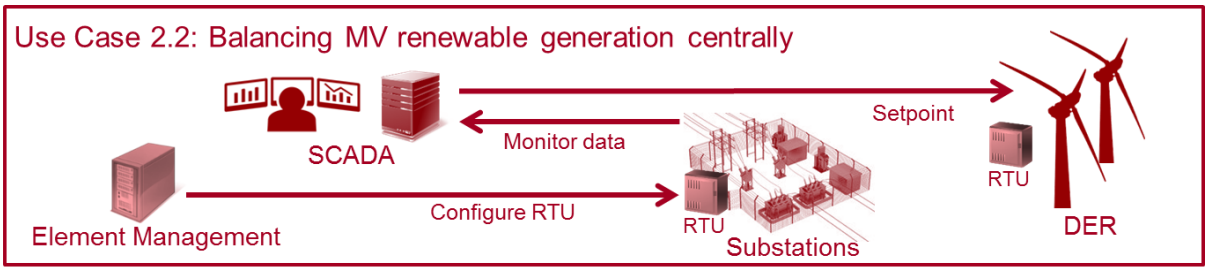


# 3 Application of SEGRID result to UC2.2

As described in chapter 1, we decided to select one use case to demonstrate what the SEGRID innovations can provide. Use case 2 scenario 2 (UC2.2) on balancing MV renewable energy centrally was selected for this purpose. The SEGRID results were developed in the context of five available use cases, but not all SEGRID results are relevant in the context of the single use case UC2.2. For instance, as there is no personal data involved in this use case, the work on privacy-by-design and privacy enhancing technologies (PETs) cannot be presented in the context of this UC. Furthermore, some of the SEGRID novel security solutions are less relevant for application within this use case.

In this section we give a brief overview of UC2.2 and list the SEGRID results that have been applied to UC2.2 and presented at the SEGRID summit.

## 3.1 Brief overview of UC2.2




In this use case, the DSO balances the renewable energy supply to the demand, in such a way that regional congestion is avoided. The decision-making is all done centrally by the DSO SCADA system. The system is continuously acquiring process data from the Remote Terminal Units (RTUs) at the primary and secondary substation to determine load and generation, and comparing it with the forecast ('Load Forecast Data'). If required, the SCADA system can send new Set Points to the RTUs at the Distributed Electrical Resource (DER) to reduce or increase generation.

The DSO AMI system for industrial customers collects the kWh Data from the kWh Meter at the DER station and makes that available for Energy Supplier.

The use case also includes remote management of the RTUs at the primary and secondary substations. The Element Manager of the DSO can upload new Configuration Data to the RTUs at the primary and secondary substations. The Element Manager from the energy supplier can do the same for the RTU at the DER station.

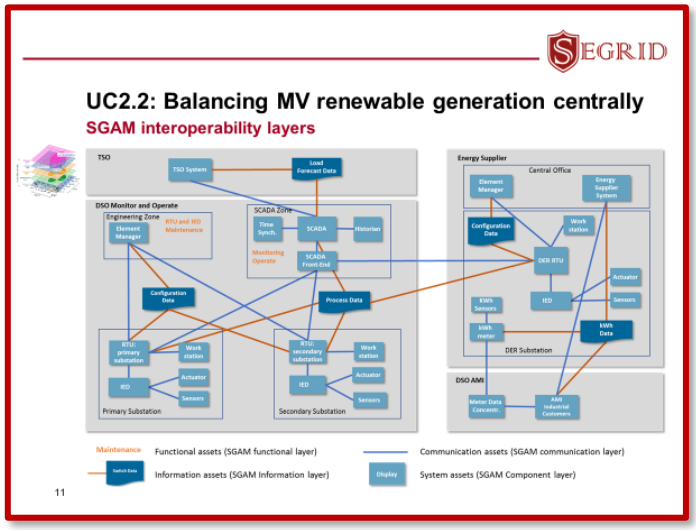
## 3.2 Application SEGRID results to UC2.2

At the SEGRID Summit, that was held on October 2nd 2017, several SEGRID results were presented in the context of use case 2.2. Below some of the slides that were used to present the SEGRID results are depicted to give an overview of the application of SERGID results to UC2.2. The presentations of the SEGRID summit are available on the SEGRID website[2].

[2] www.segrid.eu

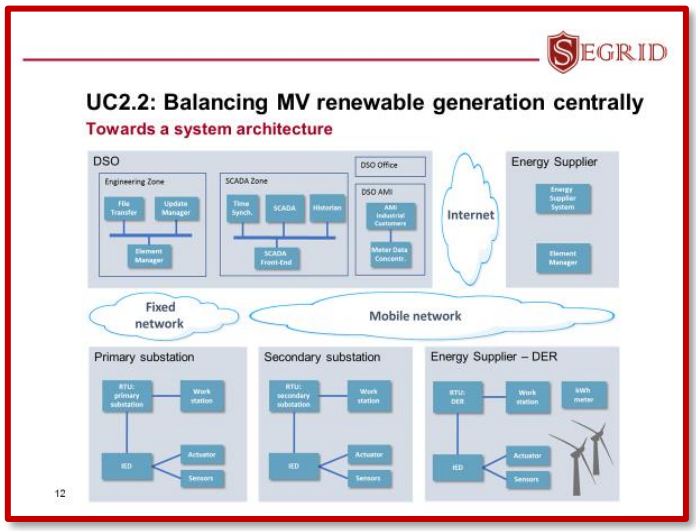
### *SGAM model of UC2.2*

Depicted on the right are the Smart Grid Reference Architecture Model (SGAM) interoperability layers for UC2.2.



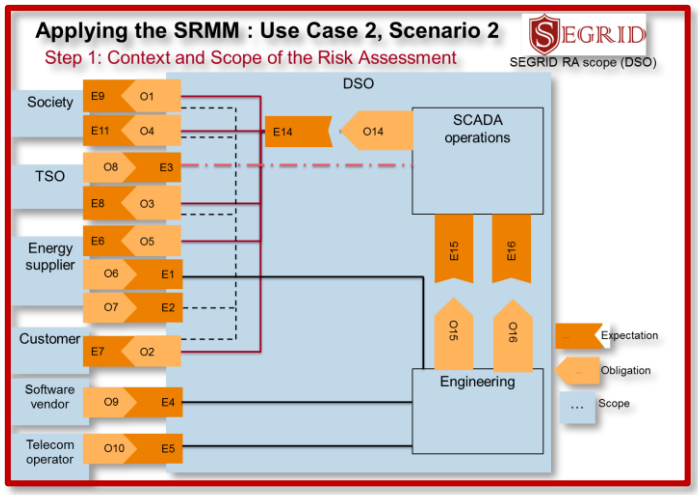

### *High level system architecture of UC2.2*

As the SGAM interoperability layers figure was a rather abstract, a more high level system architecture figure was drafted. That figure was used for the risk assessment using SRMM.




### *Application of SRMM to UC2.2*

The SRMM approach has been applied to UC2.2. At the SEGRID summit the SRMM was presented by showing the application of the SRMM steps to UC2.2. On the right, step 1 (Context and scope of the Risk assessment) is depicted. The picture shows scopes and sub scopes, obligations and expectations and their interrelation. The picture is based on the SGAM interoperability layers figure above. It is important to notice that SRMM scoping is scoping of responsibilities rather than functional or technical scoping.



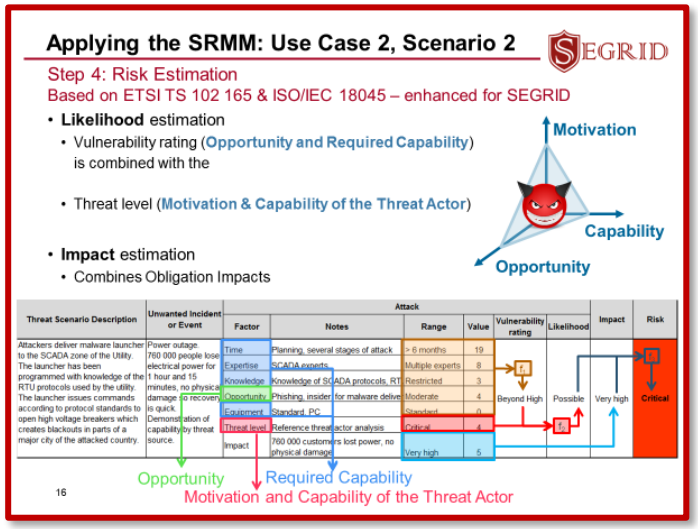



**Classification level: Public**

### *Application of SRMM to UC2.2*

Step 4 of the SRMM is the risk estimation step, this is shown in the picture on the right. It is based on the ETSI Threat, Vulnerability, Risk Analysis (TVRA).

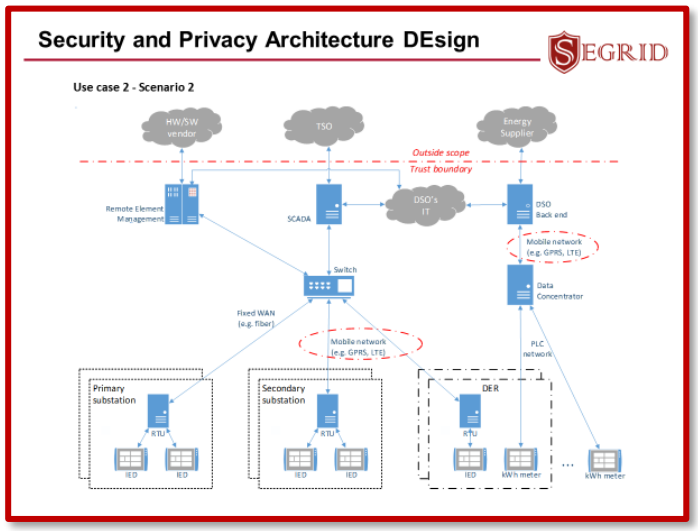
*Based on this work, SEGRID submitted a Change Request for ETSI TS 102 165 Part 1: "Method and proforma for TVRA", this was accepted in 2016 and will be included in the next version of the standard.*




### *Application of SPADE to UC2.2*

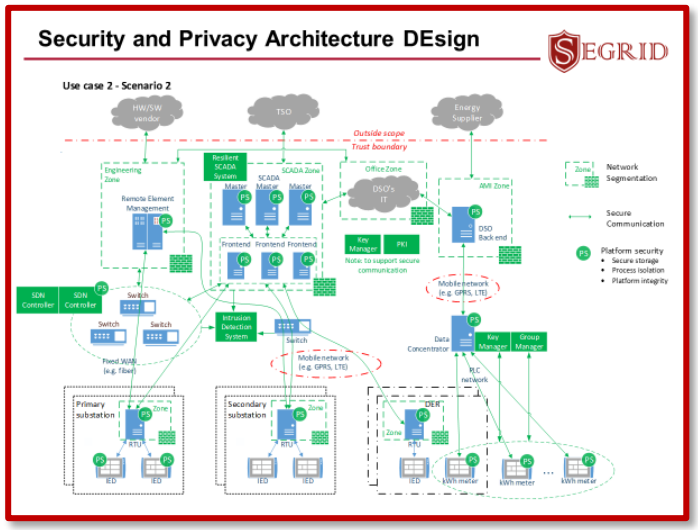
The Security & Privacy Design Architecture Engineering (SPADE) method has also been applied to UC2.2.

As the a first step, the SGAM interoperability layers figure of UC2.2 (see first picture above) has been modelled in an architecture figure depicted on the right.




### *Application of SPADE to UC2.2*

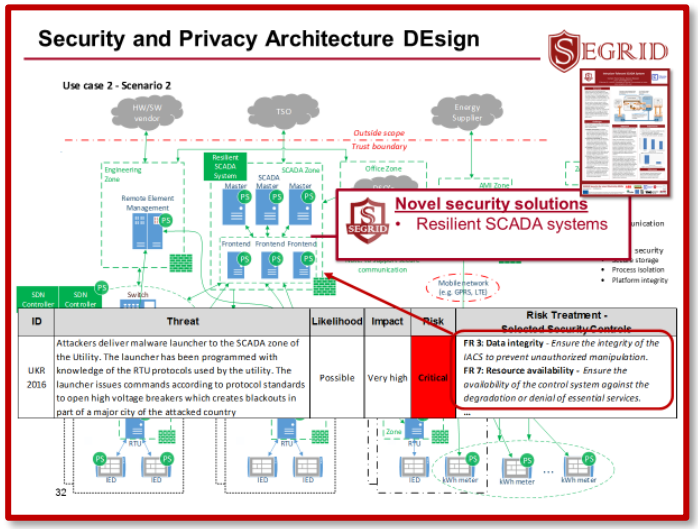
By applying SPADE the following security design architecture was created. Note that as there is no personal data being processed in UC2.2, no privacy enhancing techniques have been depicted.



### *Application of SPADE to UC2.2*

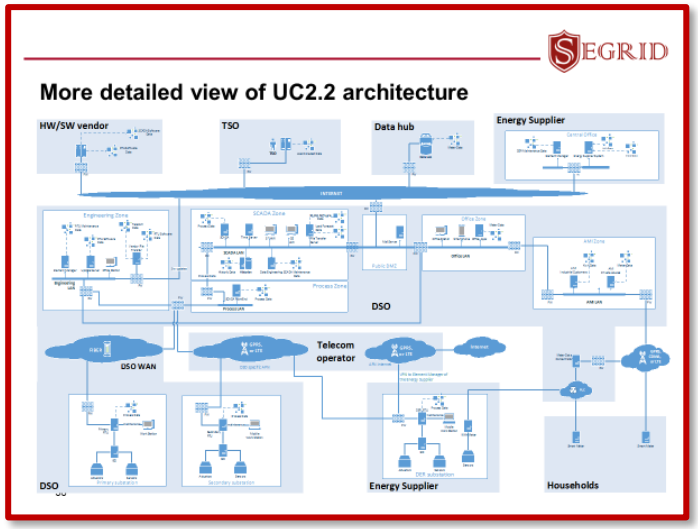
The slide on the right depicts an example of the selection of one of SEGRID's novel security solutions – resilient SCADA system – to mitigate a risk that was identified using SRMM.

At the SEGRID workshop in Barcelona in 2016 this SEGRID result was presented and demonstrated. At the SEGRID summit the resilient SCADA was presented using a poster.



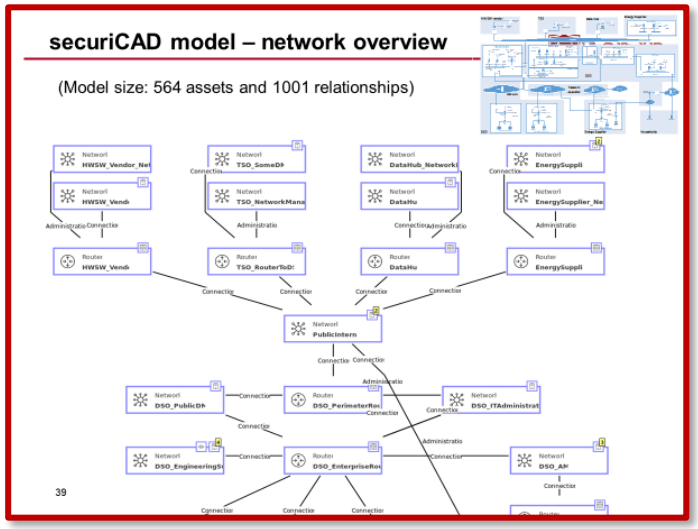

### *Application of securiCAD to UC2.2*

Also securiCAD was applied to UC2.2. In order to create a securiCAD model of UC2.2 the use case had to be worked out in much more detail. As a first step this more detailed architecture was drafted.



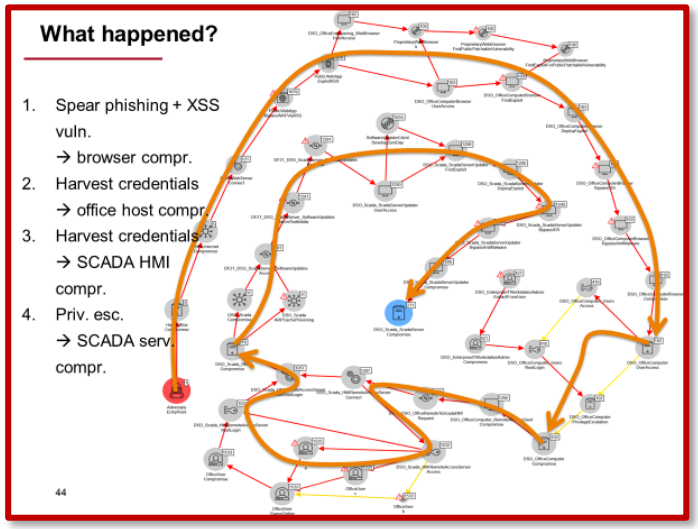

### *Application of securiCAD to UC2.2*

Depicted on the right is a part of the securiCAD model that consists of 564 assets and 1001 relationships. We had to define about 50 data flows and define many security configuration parameters.



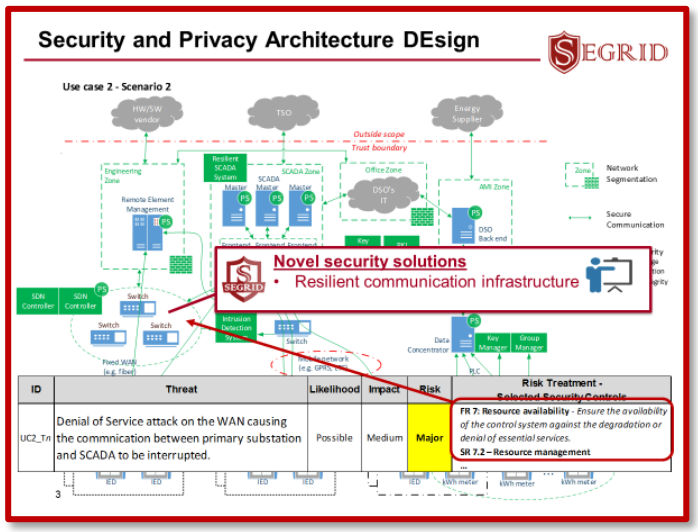
### *Application of securiCAD to UC2.2*

Several threat scenarios have been analysed with securiCAD on the model of UC2.2. On the right an attack graph is depicted that was generated.




### *Resilient communication for UC2.2*

The resilient communication infrastructure solution that was developed in SEGRID has been identified by SPADE as a solution to mitigate a Denial of Service attack on the WAN.





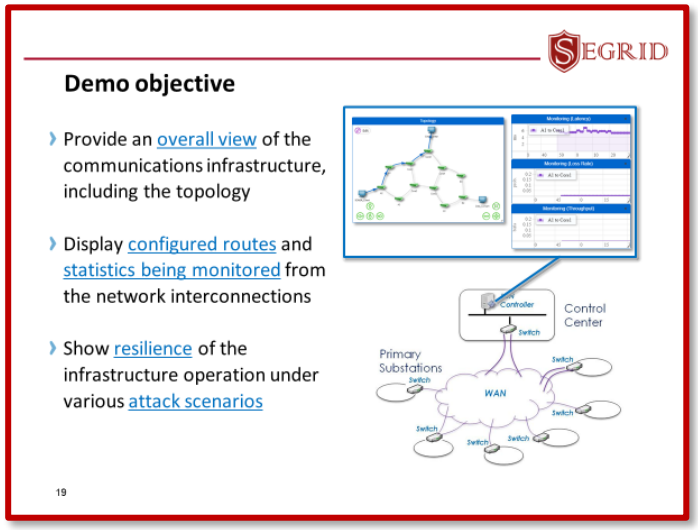

**Classification level: Public**

### *Resilient communication for UC2.2*

The resilient communication solutions is a Software Defined Network (SDN) based solution and consists of two components:

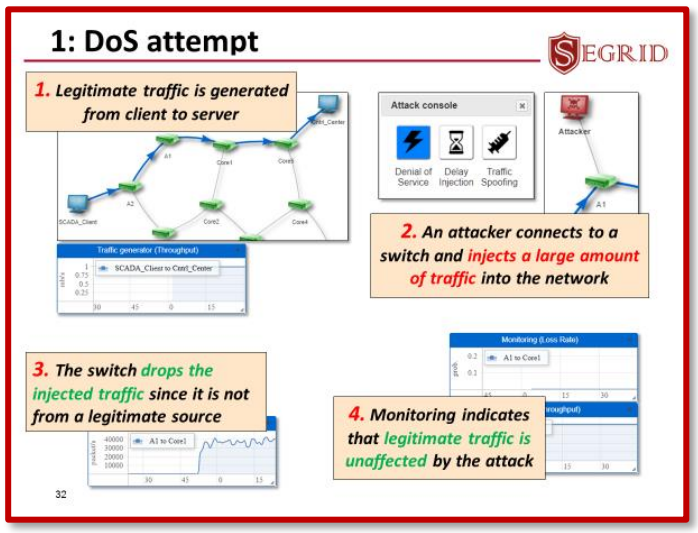
- A SDN controller running specialized monitoring, routing and traffic engineering applications, typically operating at the control centre;
- An auxiliary traffic collector application located at multiple sites near substations (i.e., the edge communication switch)

The SDN controller can adjust routes according to monitored metrics by re-installing forwarding rules in the switches.




### *Resilient communication for UC2.2*

At the SEGRID summit the resilient communication solution was demonstrated, a.o. how the solution can mitigate a DoS attack.






**Classification level: Public**