FP7 Grant Agreement N° 607109

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

D2.4 SEGRID Cyber Security Framework and Roadmap

Due date of deliverable: 01/10/2016
Actual submission date: 30/09/2016
Workpackage: WP 2 Application & Enhancements of Risk Assessment
Number of pages: 35
Revision: Version 1.0
Classification level: Public

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

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

Author(s)	Mathias Ekstedt (KTH) Frank Fransen (TNO) Jaap-Henk Hoepman (TNO) Maarten Hoeve (ENCS) Pei-Hui Lin (ENCS) Judith Rossebo (ABB) Marco Tiloca (SICS)
Contributor(s)	Sander Kruese (Alliander) Francisco Melo (EDP)

Security Assessment	**See deliverables table for security assessment requirements**
Approval Date	30/09/2016
Remarks	None

TABLE OF CONTENTS

1 INTRODUCTION 5
1.1 The SEGRID Project 5
1.2 The objective of Deliverable D2.4 6
2 SMART GRID THREAT LANDSCAPE 8
2.1 Current Situation 8
2.2 Near Future (2020) 9
2.3 Long Term (2025) 9
3 RISK ASSESSMENT 10
3.1 Current Situation 10
3.2 Near Future (2020) 10
3.3 Long Term (2025) 11
4 VULNERABILITY ASSESSMENT 12
4.1 Current Situation 12
4.2 Near Future (2020) 13
4.3 Long Term (2025) 13
5 SECURITY ARCHITECTURE 15
5.1 Current Situation 15
5.2 Near Future (2020) 16
5.3 Long Term (2025) 16
6 SOFTWARE SECURITY 17
6.1 Current Situation 17
6.2 Near Future (2020) 19
6.3 Long Term (2025) 20
7 SECURITY MONITORING 22
7.1 Current Situation 22
7.2 Near Future (2020) 22
7.3 Long Term (2025) 23
8 PRIVACY 25
9 GLOSSARY 28

Classification level: Public

10 REFERENCES 32

1 Introduction

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.

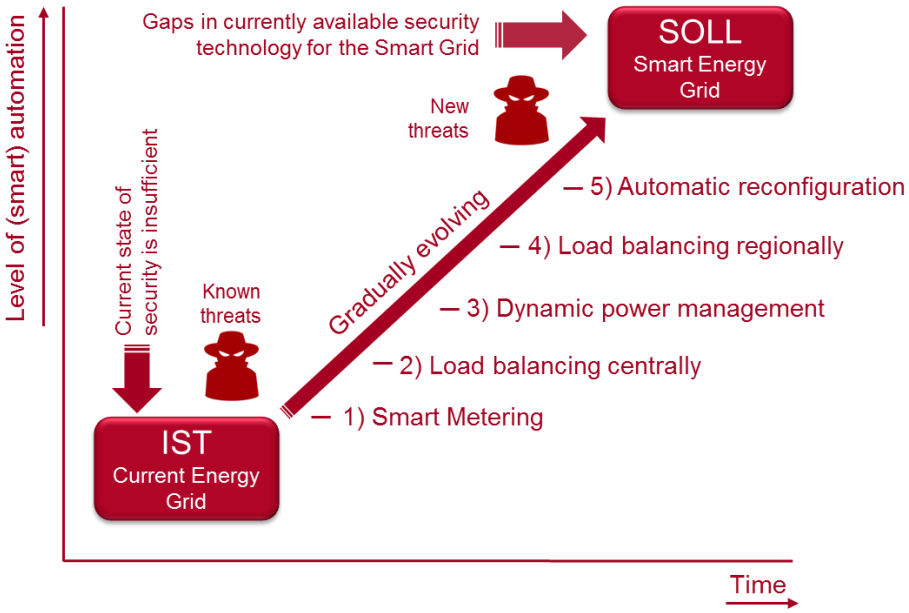


Figure 1: SEGRID storyline

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.

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

1.2 The objective of Deliverable D2.4

This document presents a roadmap for Smart Grid security from the perspective of the SEGRID partners project. The document is aimed at different groups.

First, it is aimed at DSOs and manufacturers. This roadmap is meant to give them an overview of which technologies and methods they can use to bring their technologies to the next level. For the short term this includes currently available technologies and methods coming from other fields such as IT and telecommunications. In the long term it includes technologies and methods coming out of research.

Second, it is aimed at researchers and policy makers in the research field. The roadmap aims to give them some insight into the specific challenges DSOs have in securing the Smart Grid. Hopefully this will lead researchers to find new application areas for their innovations, and will help to steer the research agenda for Smart Grid security in the right direction.

Finally, it is aimed at policy makers and standardization bodies especially in the area of Smart Grid security risk assessments. With the extensive work that has been done within SEGRID on risk assessments, we thought it important to inform these groups of how we think risk assessment methods will evolve in the future.

The SEGRID project has a focus on risk and vulnerability assessments on the one hand, and technical security solutions on the other hand. This roadmap has the same focus. It has been organized into six themes that are important for Smart Grid security:

1. Risk assessments
2. Vulnerability Assessments
3. Security Architecture
4. Software Security
5. Security Monitoring
6. Privacy

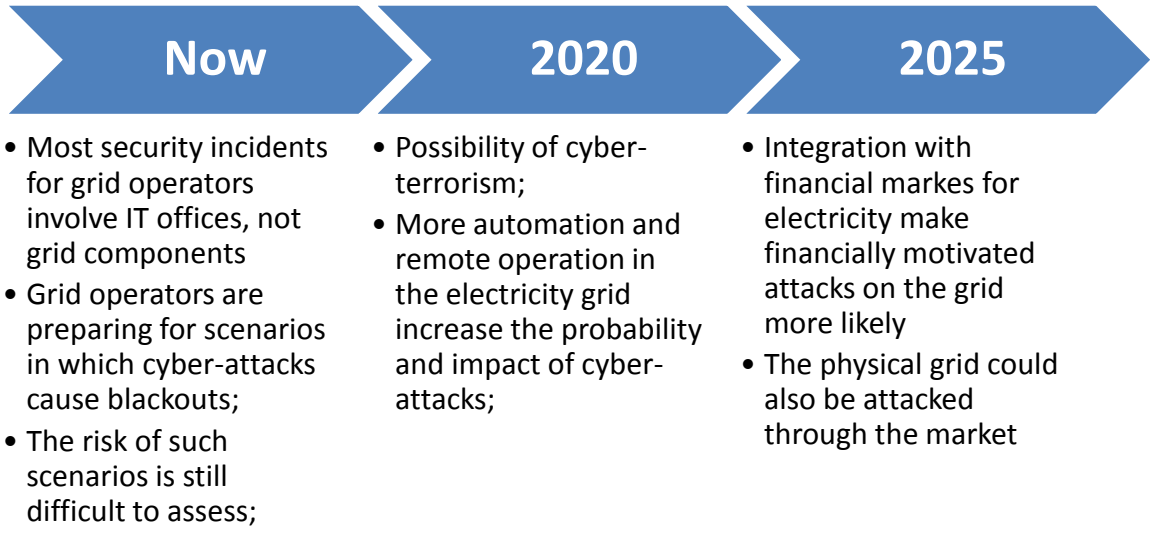
To motivate the developments in these areas, the document starts with an overview of the evolving threat landscape for Smart Grids.

We realize that the focus on these themes means that certain important areas are not treated in the detail they deserve. In particular, security policy at all levels, from the EU as a whole to individual organizations, is not addressed in this roadmap. It will be treated in more detail in the "Report with recommendations of improving Smart Grid security policies" (deliverable 1.6 of the SEGRID project).

The roadmap aims to inform different stakeholders of developments at different timescales. To stress these different timescales, we look for each theme at how it will evolve both in the near future (roughly to 2020), and in the longer term (2025). These dates are only rough markers to set to provide some milestones on the road to a secure Smart Grid. Different DSOs may reach these milestones at different times.

2 Smart Grid Threat Landscape

To motivate the developments in the next Chapters, this chapter presents an overview of the evolving threat landscape for electricity grid operators.



2.1 Current Situation

Among the security people at grid operators there is an uneasy feeling about cyber security threats. The day-to-day security problems are mostly in the office IT, viruses or ransomware on laptops, or attacks on the website. Maybe there are some metering fraud cases for variation. The new EU regulations on security, and especially privacy require a lot of attention (see Chapter 8). But overall, they however seem in control of cyber security. In the back of their mind however is a fear for a cyber-attack causing a major blackout.

Scenarios in which cyber-attacks cause blackouts are not hard to imagine. The systems that control the grid, such as SCADA systems, contain a lot of legacy components. So they are widely known to be vulnerable to cyber-attacks. Stuxnet (2010) has shown in 2010 that it is possible that a cyber-attack causes physical damage. Similar attack scenarios on the electricity grid have been worked out in sector documents [1], and even in books for the general public [2] [3].

Most measures in this document are devised to meet these blackout attack scenarios. Because many legacy components in the grid are vulnerable, they need external protection. To prevent attacks, there is a need for a good security architecture (Chapter 5). To detect and respond to attacks, there is a need for security monitoring (Chapter 7). And improvements in software security (Chapter 0) are needed to ensure that the next generation of equipment is more secure on its own.

This raises the question if these advanced security measures are really necessary: what it the real risk of the blackout cyber-attack scenarios? We know that nation states have been building up what they call offensive cyber capabilities. There are signs that some of these capabilities are aimed at the electricity grid. The US ICS-Cert yearly report for instance shows that there are many incidents in the

energy sector. Spear-phishing is commonly used, showing that the attacks are really targeted. Most are probably reconnaissance activities [4]. There is only one data point of a recent incident fulfilling the blackout scenario: a recent blackout in Ukraine [5]. The incident showed on the one hand that the attack scenarios were realistic. As the scenarios had predicted, the SCADA system was attacked through IT systems. On the other hand, the impact was however far from apocalyptic. There was major blackout with about a quarter million people without power. But power was restored soon despite DoS attempts, by going manual. These two sides of the incident leave it open for interpretation. In the end we can only answer this question with better risk assessment methods (Chapter 3).

2.2 Near Future (2020)

In the near future, there are three factors that could change the threat landscape. One would be if Europe gets involved in a conflict with a nation state with cyber-warfare potential. At the moment this does not seem far-fetched. If the reason there have been no major incidents is indeed that nations states have restricted themselves to reconnaissance up to now, this factor could increase the risks a lot.

The second is terrorists discovering cyber-attacks. Europe is a target for terrorists, but up to now they have resorted to low-tech solutions. If they would discover cyber-attacks, this could drastically change the threat landscape for grid operators. Criminal hacker groups are getting very professional. Terrorists could probably buy the knowledge and support they need for an attack from them. And unlike nation states, terrorists will not wait until there is a conflict situation.

The third is an internal change at grid operators: the increasing automation of the grid. The reason that the Ukraine incident had limited impact was that they could switch to manual mode. This will become harder when the grid becomes more automated. At most DSOs, the number of staff trained and licensed to work on substations is reduced. They can no longer operate manually for a sustained period. So the impact of a possible incident is increasing.

2.3 Long Term (2025)

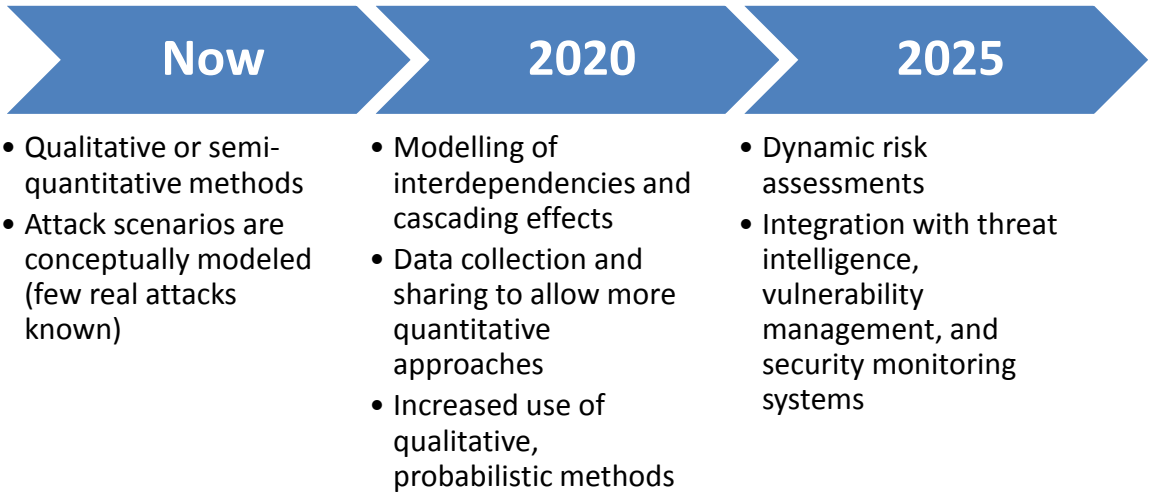
In the long term the Smart Grid threat landscape will fundamentally change because of the increasing integration with the electricity markets. To be able to cope with increased use of solar and wind power sources, whose output cannot be controlled, the demand for electricity will need to actively follow the supply. In many cases this will likely be done with (near) real-time market mechanisms. Control of the grid becomes intertwined with the systems that run these markets.

On the one hand, this will create an incentive for financially motivated attacks. There will be money to be made with attacking the Smart Grid. Confidentiality of data may become an issue, because early access to grid measurements could lead to insider trading.

On the other hand, attackers could attack the physical grid through the market. Markets are not known for their stability, even without malicious actors on them. But they can probably also be manipulated by attackers in creative ways. False rumours for instance have led to flash crashes. What happens if a market crashes, and the market has real-time control of the electricity grid?

3 Risk Assessment

Security risk assessment methodologies provide advice on how to carry out the whole risk analysis process: establishing the context (scope), risk identification, risk analysis, risk evaluation, and risk treatment [6].



3.1 Current Situation

Currently most DSOs use qualitative or semi-quantitative risk assessment to evaluate their security risk. Not only is do qualitative risk assessments normally take less time, there is also usually not enough data available on security incidents to perform quantitative assessments. Estimating Smart Grid security incidents is especially difficult, because they involve risks with low probabilities, but catastrophic consequences. Current methods cannot frequency-based statistical methods estimate such risks with any accuracy [7] [8].

DSOs are used to apply quantitative methods to non-security risks, such as the risks of accidents or equipment failure. Risk owners in the DSO's asset management department need to have quantitative assessments to be able to compare security risks to risks in other domains, so that they can correctly allocate budgets. Many people involved in assessing security risks feel that the qualitative methods currently used, are not sufficient for this purpose. The main problem is that they use relative scales that only compare security risks with each other, not with risks from other domains.

DSO roadmap for vulnerability assessments:

- Increase information sharing about security incidents
- Gradually implement quantitative risk assessments

3.2 Near Future (2020)

As the Smart Grid gets more interconnected, new risk management models are needed that can account for interdependencies. Existing risk assessment methodologies often do not address cascading effects. More research is needed to develop methods that improve the accuracy of impact calculation in complex systems. We expect to see more model-based approaches in cyber security. Although such models exist, work is still to be done to validate them on real world systems [9].

To move to quantitative risk assessments, there is a need for more data. Most quantitative models are probabilistic. They typically use statistical data to estimate probabilities of for instance vulnerabilities and attacks. A probabilistic risk model of a large system, such as a SCADA system, requires estimates of hundreds or thousands of probabilities. However, statistical data on cyber incidents in SCADA systems is notoriously scarce [10].

Several ways have been proposed to collect more statistical data [9], such as collecting data from experiments in test platforms, and creating databases with security incidents. Most experts agree however that the most important way is to improve information sharing within the industry. With more DSOs using security monitoring, we expect that more DSOs will start sharing threat information. More information on incidents may also become available because of the NIS Directive [11].

Once more statistical data is available, it will undoubtedly stimulate the validation of quantitative risk assessment methods. We expect that will lead to an improvement of the methods, and a more trust in their results.

Research roadmap for vulnerability assessments:

- Develop models that can estimate impacts in complex cyber physical systems
- Develop quantitative models that can estimate probabilities for Smart Grid security
- Research how risk assessments can be integrated with vulnerability assessments and security monitoring

3.3 Long Term (2025)

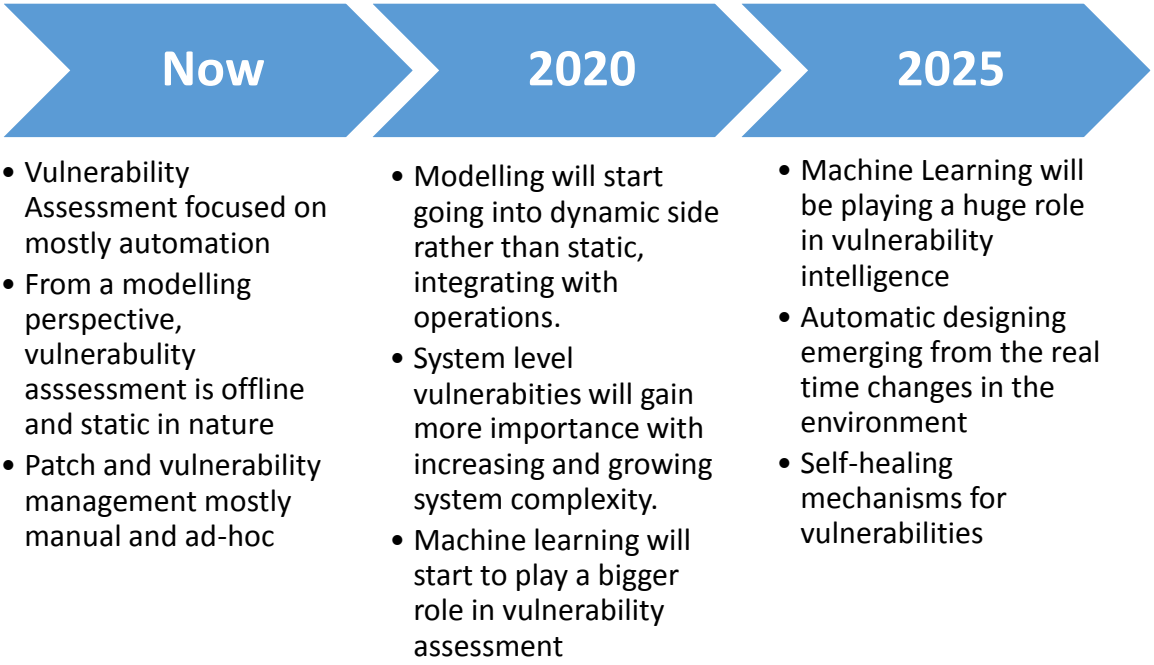
On the long term we expect a need for more dynamic risk assessments that can include new threat and vulnerability information in (close to) real-time. By continuously updating the risk assessment with information from threat intelligence, vulnerability management, and intrusion detection systems security managers will have a better view on their current security risks. At the same time, it will allow people working in security monitoring to better prioritize events.

SEGRID contributions:

- Models to work with security risks in chains (deliverables 2.2)
- Systematic risk assessment approach that fits into the methods used by DSO's asset management departments (deliverable 2.1 and 2.2)

4 Vulnerability Assessment

Vulnerability assessment has become a common practice in most organizations as it provides a first line of defense against cyber-attacks. It has also become an integral part of most well-known compliance and regulatory frameworks, making it essential for almost all medium to large scale organizations to implement it as such. This in turn gives it more priority in both R&D in academia and in industry.



4.1 Current Situation

In IT systems vulnerability assessments is today largely semi-automatic. Vulnerability scanners are regularly used to collect statistics on vulnerabilities in enterprises' ICT infrastructures. Even though they reveal much, they miss potential vulnerabilities such as zero day vulnerabilities and many configuration errors. Thus scanning is commonly complemented with other techniques, such as penetration testing and bug bounty programs. The current research direction focuses on the further automation of vulnerability assessment [12] [13] [14] [15] [16] [17] [18], to be able to cope with ever-growing networks and systems. Efforts are largely aimed at defining standardized formats for vulnerability information, to make it easier to exchange data or store it in one database. Examples are the Security Content Automation Protocol (SCAP) [19] [20], which encompasses various interrelated vulnerability standards like CVE [21], CWE [22], CPE [23], CVSS [24] [25], and is used by the National Vulnerability Database (NVD) [26]. Other examples are the Open Vulnerability and Assessment Language (OVAL) and Extensible Configuration Checklist Description Format (XCCDF) [27].

For many operational technology (OT) environments, such as SCADA systems, active vulnerability scanning is difficult. The systems are both fragile and critical. Commonly used vulnerability scanners can cause crashes or other incidents with disastrous consequences. Hence, these OT environments are usually excluded from scans, and assessed manually through penetration tests and audits.

4.2 Near Future (2020)

DSO roadmap for vulnerability assessments:

- Implement automated vulnerability scanning on OT networks, for instance using passive scanners or IDSs
- Integrate vulnerability management with other operational security activities in a security operations center

To fill the gap in automated vulnerability scanning for OT systems, we expect that DSOs will start deploying passive vulnerability scanners. Many network-based IDS systems aimed at SCADA systems, especially those with deep-packet inspection, already provide vulnerability discovery. Pilot projects with such systems at DSOs found that finding misconfigurations and other security weaknesses was one of the main strengths of these systems.

There also exist several analytical tools and approaches that turn raw data on individual vulnerabilities into an overall picture of the vulnerability of the system. One could see this as a move from vulnerability assessments to vulnerability intelligence. One group of such approaches uses attack graphs for these assessments [28]. Often they employ some form of analytical reasoning to make the assessment. In SEGRID we use CySeMoL (Cyber Security Modeling Language) [29], securiCAD [30] and pwnPr3d [31] that all belong to this group. Other similar tools include for instance MulVAL [32], NetSPA [33] (and its successors GARNET [34] and NAVIGATOR [35]), TVA-tool [36] (made available commercially as Cauldron [37]), RedSeal [38], and Skybox [39].

In the near future, we expect a further integration of operational security tools, such as vulnerability scanners and intrusion detection systems, into these analytical tools. It would be reasonable to expect integrated security tools for security operation centers that also can cover the OT systems within the Smart Grid.

4.3 Long Term (2025)

On the long term, the challenge for vulnerability assessments will be to handle very large, complex, and dynamic environments. Machine learning techniques will probably play a key role in vulnerability assessments, for instance in dynamic gathering of threat intelligence, for continuous updating of the severity of individual vulnerabilities as well as their role in different attack vectors in different contexts, for continuously identifying and updating models of the ICT infrastructure, and for identifying best practice solutions in different domains.

Research roadmap for vulnerability assessments:

- Develop methods to feed analytical vulnerability intelligence tools with data from vulnerability scanners or IDSs
- Validate the analytical tools on Smart Grid systems
- Develop vulnerability intelligence tools that can deal with large, complex, and dynamic networks (for instance using machine learning)

We also expect that the vulnerability intelligence tools will provide more and more support in choosing the right tactical actions in security operations: which vulnerabilities need to be dealt with first, and what do we do to stop or contain an attack. Much like you would run optimal power flow analysis within the SCADA system before actual reconfiguring the power network, the security intelligence tools would estimate the result of tactical actions for the security operations teams. The tools may even be applied to implement self-healing capabilities.

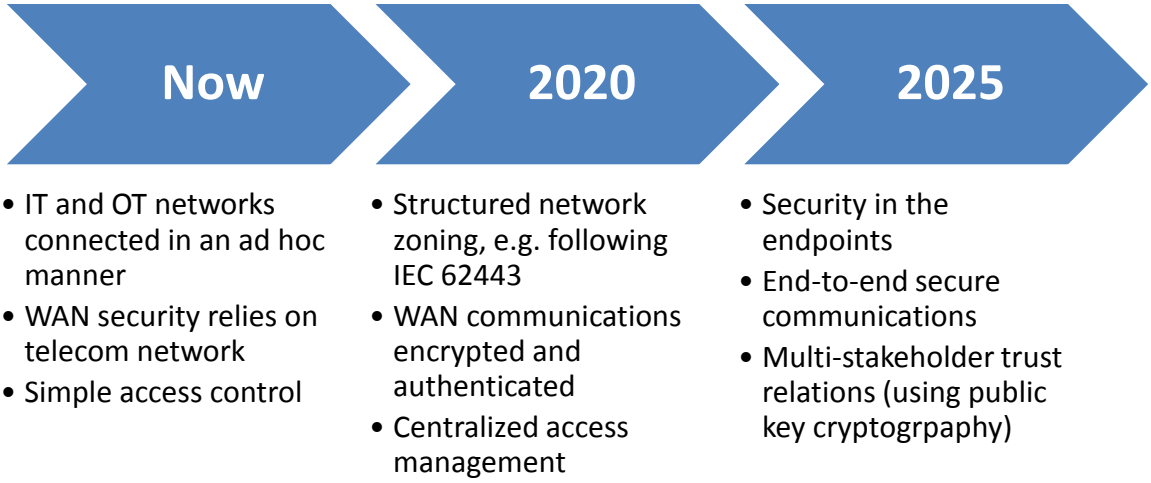
On the strategic level we expect an integration of the vulnerability intelligence tools with risk assessment tools (see also the risk assessment chapter). In this way long term decisions on security measures are always aligned with the latest security state of the network.

SEGRID contributions:

- Modelling of SCADA and Smart Metering systems in CySeMoL to determine if the analytical modelling approach works for Smart Grid systems (deliverables 3.1, 3.2, and 3.3)
- Development of an active vulnerability assessment tool to feed the analytical tools with real-time network data (deliverables 3.1, 3.2, and 3.3)

5 Security Architecture

As the Smart Grid grows more complex and interconnected in the coming years, it is crucial that it is designed to be secure. A good security architecture is crucial. We see three important topics. First, how the operational technology (OT) systems, such as SCADA systems, smart metering systems and legacy systems, are connected first to the IT systems of DSOs, and then (indirectly) to the rest of the world. Second, how the WAN communications with the many devices spread over substations, homes, businesses, and other places are secured. And third, how access to the different components and systems is controlled.



5.1 Current Situation

Most DSOs are coming from a situation where there is no conscious security architecture. IT and OT networks have been connected to fulfil the business needs. But the impact this has on security has not been fully thought through. Many DSO are now working hard to fix this.

For the wide-area network (WAN) communication to components in the fields, such as RTUs in substations, DSOs often have taken no security measures. The security of these communications relies on the telecom network provider. Sometimes this is good, when a dedicated lines or modern cellular networks are used, but often the security is lacking.

Access control to OT components is arranged in a simple way. Often there is just one local account that gives full administrative access to the device. It is protected by a password that is shared by the engineers working on the system.

DSO roadmap for security architectures:

- Implement a zoned network architecture that protects the interface between IT and OT systems
- Secure the WAN communication in the next generation of systems
- Define and implement centralized access control

5.2 Near Future (2020)

Most DSOs are now in the process of defining their security architecture, often starting with the network zoning. The IEC 62443 standard seems to be the preferred approach to this zoning. Often the zoning project will take several years to fully implement over all critical systems, including legacy systems. Especially challenging it to securely set up remote access for vendors that needs to reach their systems for maintenance. Usually these are required to log onto a local system (jump server or stepping stone), often in virtualized instances.

For the WAN security there is a trend towards using internet-derived technologies. Usually either IPSec or TLS is used. (The exception is smart metering, where application layer technologies are used.) This provides a good way to quickly build secure communication channels into the systems. Often existing (open-source) software libraries such as OpenSSL or StrongSwan are be used, reducing the chance of implementation errors.

Access control is getting more centralized. Either this is done by concentrating the access control in the central systems (SCADA servers, head-ends) that control the field components, or by setting up a separate authentication server (using e.g. RADIUS or Kerberos). This allows for the use of individual user accounts, leading also to better logging.

5.3 Long Term (2025)

In the long term the responsibility for security will probably shift from the network and system level to the individual components. Components will be more and more expected to be able to function in a hostile environment. This is already happening for smart meters, which can (if implemented correctly) work securely even if an attacker has full network access to them. RTUs and other devices in substations will also become more resilient, allowing for more defense in-depth. Having more resilient environment is also a prerequisite for having more peer-to-peer communications in networks, as then they become difficult to monitor centrally.

Research roadmap for security architecture:

- Develop access control and authentication schemes that will work in the future multi-stakeholder Smart Grid.

In the long term, more stakeholders will also get involved in the Smart Grid. Consumers and companies will become more active customers implementing demand response, and electric vehicle charging will also introduce new players. DSOs will interface with all of these stakeholders. Certainly in the beginning this will mostly be through IT platforms accessible from the internet. Later on, there may however be also direct interactions with some devices in the OT domain. This requires that other stakeholders can access OT assets owned by DSOs.

SEGRID contributions:

- Group key management for PLC networks (deliverable 4.2 and 4.3)
- Resilient SCADA servers that allow replication (deliverable 4.2 and 4.3)
- Resilient networking for software-defined networks (deliverable 4.2 and 4.3)

6 Software Security

Software security generally concerns the ability to assure that software components are developed, maintained and running in such a way that security requirements are fulfilled, and the expected security level is promptly and effectively restored in case of failure or security attacks exploiting software vulnerabilities. Although software security can comprise several specific domains, this chapter considers three areas of particular interest, namely: A) *software testing*; B) *software upgrading*; and C) *process separation*. More and more DSOs are becoming aware that it is particularly important to assure that these processes are improved in the mid-long term, especially as to their affordability, ease of deployment and usage, effectiveness, efficiency and scalability. Currently, DSOs are investing and putting effort in order to improve available software security solutions, mechanisms and technologies for Smart Grids.

- Lack of tools for patching and vulnerability management; point-to-point inefficient distribution of software upgrades
- Lack of tools for patching and vulnerability management; point-to-point inefficient distribution of software upgrades.
- Very limited process separation based on traditional multi-process kernels

- Testing procedures embedded in components' life-cycle management; support from open/standardized tools; testing based on agreed best practices
- Adoption of COTS tools; efficient multicast distribution of software upgrades; automatic cooperative collection of misbehavior from smart grid components
- First gross-grain support for secure separation of different services

- Automated penetration tests on single units and whole systems; support for large-scale smart grids security testing and assessment
- Highly automated software upgrade; improved support and performance on large-scale smart grids
- Advanced fine-grain support for secure separation of different services; arbitrary complex separation of virtual devices

6.1 Current Situation

Software testing general targets consist in discovering bugs and retrieving information about the software quality of a product with respect to correct functioning, handling of errors and security attacks. Software testing should be performed during product development on module, system and product levels. DSO's should perform acceptance tests on software security when new products and solutions are introduced. Acceptance tests should include penetration testing, functional and error tests, as well as review of the manufacturers' software development process and quality assurance procedures.

Today, DSOs perform irregular and unstructured penetration testing of purchased equipment. Moreover, there is a lack of a general testing practice and framework covering the specific aspects of Smart Grids. That is, DSOs tend to develop their own procedures and standards, which makes it difficult to share and reuse testing results between different customers and stakeholders. Manufacturers' software quality assurance procedures are normally proprietary, and thus reviewing them often requires a big, even infeasible, effort and good insights into software development lifecycle procedures.

Software upgrading. DSOs can be required to update software modules running of Smart Grid components because of different reasons. On top of them, it is fundamental to distribute software upgrades as patches to suspected or detected security vulnerabilities that can be exploited to mount security attacks against the Smart Grid system. Software upgrades can concern, to different extents, high-level applications, operating system modules, and even low-level firmware. In order to preserve/restore security in the Smart Grid system, it is required that: i) patches to software vulnerabilities are easily designed, managed, and possibly improved; and ii) possible software upgrades are performed promptly and efficiently in order to fully restore secure operative conditions in the Smart Grid as soon as possible.

However, there is currently a significant lack of tools for easy and effective management of software vulnerabilities in the Smart Grid and the following enforcement of "patches" based on software update distribution. Moreover, the actual distribution of software updates is often performed in a point-to-point fashion, i.e. affected Smart Grid components are separately provided with new software releases or specific patches one by one. Although this is obviously the easiest possible approach, it results to be extremely inefficient and scales poorly with the number of components deployed in the Smart Grid, hence resulting in software update operations of non-negligible duration, during which the Smart Grid remains in a vulnerable state.

Process separation. Process separation consists in partitioning the processes running on a system in such a way that they cannot interfere with each other's memory areas or those reserved to the operating system. In practice, this can be achieved by using virtualization techniques that monitor the execution of running processes to ensure that they comply to a set of rules for interacting with each other and the hardware platform. Another commonly used approach relies on hypervisors, namely monitoring software- or hardware-based systems responsible for the creation and trusted execution of virtual machines. The benefits that a DSO can gain by employing process separation are several. Firstly, the financial expenses in terms of hardware can be considerably reduced, as different sensitive components can share the same hardware while being virtually separated, so avoiding physical separation. Secondly, this results in a number of security benefits. In particular, process isolation prevents attacks mounted against a part of the system from spreading to other components.

Currently, DSOs adopt process separation very rarely. This holds for any part of Smart Grid systems, ranging from the back end to the devices in the customer's premises. Even in the case where process separation is partially adopted, many processes tend to unsecurely share the same system resources, and separation is entrusted to the operating system kernel. This only provides limited protection for processes influencing each other's memory areas. For back end systems running on general-purpose computers, there are available solutions for virtualization. However, when it comes to embedded devices like smart meters, there are fewer options for achieving process separation. This is mainly due to the special difficulty to implement such approaches in embedded, often resource-constrained, platforms. Currently, many DSOs simply deploy the software to be run on smart meters as a single process where all services, including logging and command processing, share the same memory space.

6.2 Near Future (2020)

Software testing. DSOs have access to agreed best practices with respect to penetration testing of components and systems for all security lifecycle management phases. In particular, the testing procedures are expected to be open and standardized. Also, efficient tools that are easy to set-up and display good test coverage are expected to be available. New tools for system wide software security assessment start to appear and be used, but best practices and agreed standards are still missing.

Manufacturers have implemented high quality software assurance procedures which are still mostly proprietary. Testing is automated in the software development lifecycle and is integrated into a "continuous software delivery" process. During the process, modules, components and systems are always tested before they are released for integration in the next level product. There are automatic systems for tracing software component releases in products to help decide what for and where it is necessary to perform software updates. Regression testing is more or less automatic.

Formal methods appear in research activities aiming to prove software correctness and absence of vulnerabilities

Software upgrading. In order to improve current software upgrade procedures, two fundamental steps are clearly of great importance.

First of all, the design, management and possible improvement of vulnerability patches should rely on the adoption of available Components-Off-The-Shelf (COTS) tools. Their adoption would be particularly convenient, as they represent reliable, pre-tested, mechanisms and technologies that would also considerably limit or even reduce costs due to their deployment and maintenance.

DSO roadmap for software security:

- Enhanced life-cycle management of Smart Grid components, including software testing procedures.
- Adoption of open/standardized tools and best practices for software testing.
- Adoption of reliable and affordable COTS tools to perform software upgrade.
- Efficient software upgrade procedures based on multicast communication.
- Available support for secure separation of services on single physical units.

Secondly, it is necessary to rely on efficient, highly-scalable, alternative techniques for the actual distribution of software updates. A particularly promising technical mean consists in multicast network communication. This makes it possible to considerably achieve better performance and complete the distribution of software updates earlier than by adopting current point-to-point techniques. As a result, it is possible to quicker improve/restore secure operations in the Smart Grid. In order to assure that a multicast distribution of software is in turn properly secured, it is necessary to also adopt efficient and highly-scalable schemes to manage, revoke and distribute cryptographic key material used to implement secure multicast communication.

Process separation. In order to enhance the support for process separation in DSO systems, a number of improvements are required in the short term.

First, existing virtualization solutions for general-purpose computers should be considered for adoption, since many of them are available and deployable on different operating systems. Secondly, support for process separation on embedded systems need to be especially improved. A few approaches are currently available, but they are strictly bounded to specific hardware platforms, and typically more difficult to employ compared to those for general-purpose computers. The actual development of

software for embedded systems also need to take this into account, and design applications into consistent separate components that can then interact with each other through a hypervisor, rather than sharing the same memory areas or accessing sensitive services and resources in an unmonitored way.

As to smart meter devices, this can mean separating the logging services from the command processing. More generally, it makes it possible to combine multiple functionalities that are currently provided by physically different devices into one hardware platform. Other components like data concentrators and back end systems can also achieve security by employing this method.

In the near future, the support for process separation will rely on multiple processes running within the same virtual machine. Although this is a first necessary step to take, this approach is yet not able to provide fine-grained individual process isolation.

6.3 Long Term (2025)

Software testing. For the future, we envision the development of automated penetration tests for single components and whole Smart Grid systems. These new developments will aim for modelling the Smart Grid in such a way that testing results from components and parts of the grid will be composable. Furthermore, efficient tools for predicting vulnerabilities in Smart Grids and for improving the possibility to assess the effects of cyber attacks in large-scale Smart Grid systems will be developed.

Software development will start to be based on model driven designs in which formal methods can more easily be applied to prove software correctness and absence of vulnerabilities. Thus the importance of practical penetration testing will decrease.

Software upgrading. In the long term, we expect research activities to focus on two main aspects. First of all, it is highly desirable to rely on highly automated techniques and procedures that, with no particular human intervention, can autonomously develop patches to detected or suspected software vulnerabilities, and distribute them to different components in the Smart Grid.

Research roadmap for software security:

- Develop automated penetration tests for single components and whole Smart Grid systems.
- Improve the support for testing in large-scale Smart Grid systems.
- Achieve automated development and distribution of patches against software vulnerabilities
- Improve performance and support of software upgrade procedures for large-scale Smart Grid systems.
- Enable support for advanced fine-grained separation of services on single physical units.
- Enable support for advanced secure separation of services on single physical units.

Secondly, it is fundamental to considerably improve the overall performance of the actual procedures for software update distribution, and to make them highly scalable with the number of Smart Grid components involved in the update process. We believe that such research developments can have a massive positive impact in improving the readiness and accuracy of software update procedures, as well as the overall security and reliability of Smart Grid systems.

Process separation. Long term research and improvements in this area will need to focus especially on enabling more fine-grained process separation techniques.

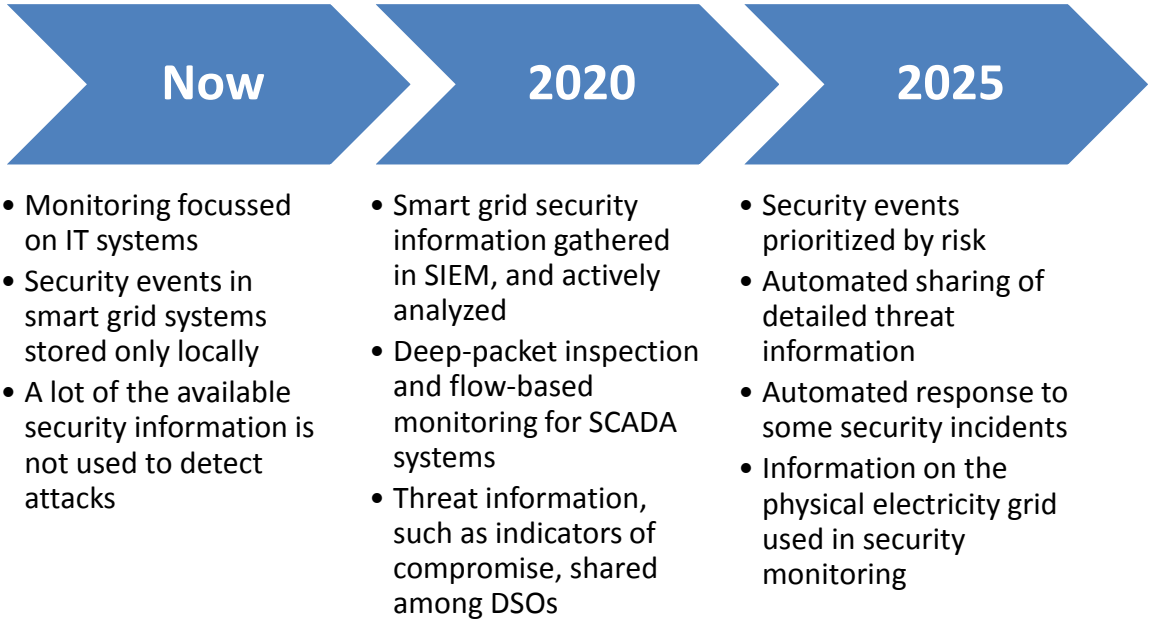
Current methods and even some currently under development are coarse and allow many processes to share a same virtual machine. This has the main benefit that an attack against a process in one virtual machine is to some extent confined, i.e. it cannot spread to other virtual machines. However, an attack against one process can still be able to affect other processes in the same virtual machine. In this sense, such a separation approach does not allow for fine grained control of process separation. A promising future direction of research is investigating how to enable a more secure separation of individual processes, in such a way that they cannot influence any other process unless explicitly permitted to do so. Furthermore, it is important to improve the enforcement of current process interaction patterns relying on hypervisors as well as of the interactions between virtual machines.

SEGRID contributions:

- Group key management to support efficient and highly scalable group software distribution in large-scale systems (deliverables 4.2 and 4.3)
- Research into trusted platform modules and hypervisors for smart meters and data concentrators (deliverables 4.2 and 4.3)

7 Security Monitoring

Security monitoring concerns the detection of vulnerabilities and security incidents. More and more DSOs are becoming aware that not all cyber-attacks can be prevented. They are investing in security monitoring to be able to respond to attacks.



7.1 Current Situation

Although most DSOs now realize that security monitoring is important, they are still in the beginning of setting up security monitoring for Smart Grids. If systems are being monitored, they are usually the IT environment, such as the public facing websites and laptops used by employees.

A lot of information is available that could be used to detect security incidents. Firewalls, workstations, and servers all generate useful logs. More and more embedded devices, such as smart meters and RTUs, also log security events. The information is currently however not being collected or analyzed.

DSO roadmap for security monitoring:

- Set up a SIEM system and start to collect information
- Set up teams to analyze and respond to security events
- Deploy SCADA network-intrusion detection systems with deep-packet inspection and flow-monitoring
- Start sharing information on threats with other DSOs

7.2 Near Future (2020)

The first step most DSOs are taking is to set up a Security Information and Event Management (SIEM) system to collect all the events, and teams to analyze and respond to them. This strategy allows them to gradually roll-out monitoring by adding more and more data sources to be monitored.

To monitor the critical SCADA systems controlling the grid, many DSOs are looking into specialized network-intrusion detection systems for SCADA. A lot of research

was done in this area in the past years, and it has resulted in a number of viable commercial products. These products offer deep-packet inspection of SCADA protocols, and detecting strange network flows. They often use machine learning techniques, not normally seen in IT systems.

We also expect to see an increased sharing of threat information of threat information between DSOs. Sharing information, such as indicators of compromise is common for banks and large companies. Initiatives are being taken to increase information and knowledge sharing between DSOs. Currently these initiatives work mostly at policy level. Once more DSOs have operational teams analyzing and responding to incidents, such teams can also use these platforms to share threat information.

Research roadmap for security monitoring:

- Integrate intrusion detection with risk models to be able to prioritize events on risk
- Develop platforms that allow for trusted sharing of information on vulnerabilities and incidents
- Develop automatic counter measures for cyber-attacks that do not disrupt the electricity grid
- Use information on the physical state of the electricity grid to detect cyber attacks

7.3 Long Term (2025)

On the long term we expect that the security monitoring systems and teams will have to deal with larger and larger volumes of events. On the one hand, the roll-out of the SIEM and intrusion detection systems will lead to data being gathered from more and more systems within the Smart Grid. On the other hand, the Smart Grid systems will become more complex, and generate more and more traffic and other data. Increased automation is needed to deal with this increase in data.

One part to automate is the prioritization of security events. The prioritization should be risk-based. More advanced risk assessment models are expected to become available in the near future. To make sure that the scarce people available to analyze incidents work on the right things, these risks models should be used to guide their work. A lot of research is still needed to connect the models developed for risk assessments with the information from intrusion detection systems.

Another part to automate is the sharing of threat information, such as indicators of compromise. A challenge here is the information sharing infrastructure. This infrastructure should be secure enough to be trusted by all parties involved. More and more stakeholders are getting involved in the Smart Grid. They need to find a trusted way to share information about vulnerabilities and incidents. Most organizations prefer not to make such information public. A possible solution may be to allow anonymous sharing of some information.

Finally, some of the response may also have to be automated. Especially with the millions of devices placed in-home or in the field, it is not possible to have an analyst go to the device to analyze and fix it. It will be a challenge to find automated counter-measures that do not create a risk of disturbing the Smart Grid.

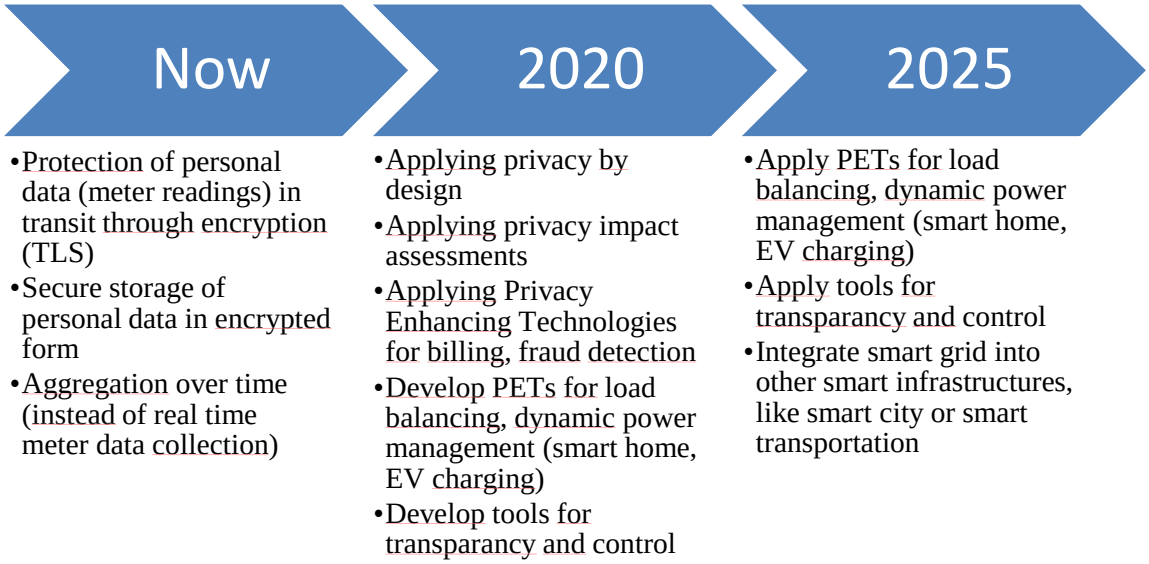
Besides the increase automation, we also see an opportunity to use more of information on the physical state of the grid, as collected by the SCADA system, for security monitoring. The most dangerous attacks are those that physically affect the grid. Detecting such attacks by their effect on the grid is already an active area of research.

SEGRID contributions:

- Intrusion detection methods for wireless mesh networks (deliverables 4.2 and 4.3)

8 Privacy

Privacy concerns the protection of personal identifiable information (aka personal data). DSOs (and other parties involved in the Smart Grid) are aware of the fact that they are collecting data related with energy as well as personal data. With the adoption of the General Data Protection Regulation [40] in April 2016, a strong push towards stronger privacy protection is expected in the coming years, especially when, in May 2018, the GDPR must have been enacted into national law by EU member states.



8.1 Current situation

After a false start where initial designs and actual implementations of smart meters were sorely lacking privacy protection controls we now see that a few baseline countermeasures have been implemented.

The communication of data (both measurement data and switch data) is now protected through the use of adequate, standardized, cryptographic schemes that protect the confidentiality, integrity and authenticity of the data exchanged.

Instead of offering DSOs real time access to measure data generated by the meter, measurement data is aggregated over time. Access to this data is typically restricted depending on the purpose. For example, the most fine grained access (in the Netherlands at least) of 15 minute interval usage data is only allowed for network management purposes. For billing, only access to quarterly usage statistics are allowed.

Finally, personal data is not only secured in transit but also when stored at servers of the DSO, either using secure databases or using secure (read encrypted) cloud storage.

8.2 Near future (2020)

The General Data Protection Regulation [40] was adopted on 27 April 2016. It enters into force 25 May 2018. It mandates (among many other things) that data controllers perform a privacy impact assessment [41] and that they apply privacy by design [42] and by default when developing new systems. We therefore expect, in the Smart Grid case, DSOs to establish a basic framework to perform such privacy impact assessments and to implement privacy by design and default. We also expect larger DSOs to appoint a Data Protection Officer to oversee these processes (if only because this also required by the GDPR).

DSO roadmap for **privacy**

- Appoint a Data Protection Officer
- Perform Privacy Impact Assessments.
- Set up a privacy by design process and apply it.
- Apply Privacy Enhancing technologies for billing and fraud prevention

Methodologies to perform a privacy impact assessments are available [43]. Implementing privacy by design is a different matter [44]. An initial framework for expressing legal requirements in to design goals that are easier for engineers to understand build around eight privacy design strategies [45] has recently be augmented [46]. This requires more work to turn into a proper methodology, which is integrated into existing development processes. In particular, privacy design patterns are underdeveloped [47] (especially those that are applicable to the Smart Grid), although some work to extend and unify existing scattered approaches is underway[1].

Complementing this top down approach, we expect DSOs to simultaneously continue to work on a bottom up approach to make the Smart Grid more privacy friendly. In particular we expect them to apply existing Privacy Enhancing Technologies (PETs) specifically designed for billing and fraud detection in the Smart Grid [48] [49] (some of which have even been submitted for standardization [50]).

In terms of research directions for the short term this requires strengthening the privacy by design methodology and process, and finding ways to integrate this into existing system development processes. Moreover, in the area of privacy enhancing technologies, protocols for privacy friendly load balancing and dynamic power management (smart home, EV charging) need further investigation before they can be applied in practice. Similarly more research to develop tools for transparency and control is needed to bridge the gaps identified [51].

Research roadmap for privacy:

- Strengthen the privacy by design methodology and process
- Develop tools and technologies to improve transparency and control
- Develop technologies and standards to do load balancing and dynamic power management in a privacy friendly fashion.

8.3 Long term (2025)

For the longer term, further development of PETs for load balancing, dynamic power management and other aspects of Smart Grids is required, and we expect them to be applied in future generation Smart Grid infrastructures. This is also true for tools and technologies for

transparency and control. An effort to bring the result of these efforts to standardisation is also foreseen.

A much more challenging perspective is offered when we consider parallel developments in smart cities [Kom09] and intelligent transportation systems and smart logistics [OST15]. At some point the systems set up for these smart infrastructures will start to intersect with the Smart Grid infrastructure. It is important to start thinking about how best to facilitate this integration while at the same time respecting user privacy.

SEGRID contributions:

- Privacy design tactics and design patterns for the Smart Grid (deliverable 4.2)

9 Glossary

This glossary serves as inventory of abbreviations used in the document.

This is a standard glossary, used for all technical SEGRID deliverables

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

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

NMS	Network management system
NN	Neighbouring Network.
NTP	Network Time Protocol
NVD	National Vulnerability Database
OMS	Outage Management System
OS	Operating System
OSCP	Open Smart Charging Protocol
OSGP	Open Smart Grid Protocol
OSI	Open Systems Interconnection
OT	Operational technology
OTP	One-Time Password
PCT	Programmable communicating thermostat
PHP	PHP: Hypertext Preprocessor (a recursive acronym
PLC	Power Line Communication.
PQ	Power Quality
PV	Photovoltaic
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RF	Radio frequency
RFC	Request for Comments
RTU	Remote Terminal Unit.
SAL	Security Assurance Level
SCADA	Supervisory Control and Data Acquisition.
SCS	Substation control system
SDLA	Security Development Lifecycle Assurance
SE	Secure Element.
SEGRID	*S*ecurity for smart *E*lectricity *GRID*s.
SFTP	SSH File Transfer Protocol
SGAM	Smart Grid Architecture Model.
SG-CG	Smart Grids Coordination Group (ETSI).
SMITP	Smart metering Information and Telecommunication Protocol.
SNTP	Simple Network Time Protocol
SSH	Secure Shell
SUC	System under Consideration, or Subject under Consideration
TCP/IP	Transmission Control Protocol / Internet Protocol
TEE	Trusted Execution Environment
TEPT	Trained Execution Path Tree
TOE	Target Of Evaluation
TSO	Transmission System Operator.
TTC	Time To Compromise
Tx.y	Task w.y
UC	Use Case
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VLAN	Virtual LAN
VPN	Virtual private network
WAMS	Wide Area Monitoring System
WAN	Wide area network
WAP	Wireless Application Protocol

WMS	Workforce management system
WPx.y	Work Package x.y
XACML	Extensible Access Control Markup Language
XML	Extensible Markup Language
XSLT	Extensible Stylesheet Language Transformations
3G / 4 G	Third/ Forth generation mobile communication.

10 References

[1] National Electricity Sector Cybersecurity Organization Resource (NESCOR), Technical Working Group 1, "Electricity Secture Faulure Scenarios and Impact Analyses, Version 1.0," 2013.

[2] M. Elsberg, "Blackout," Blanvalet Verlag, 2012.

[3] T. Koppel, "Lights Out: A Cyberattack, A Nation Unprepared, Surviving the Aftermath," Crown, 2015.

[4] NCCIC/ICS-CERt, "Year in REview, FY2015," 2015.

[5] Sans ICS, E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid: Defense Use Case," 2016.

[6] ISO, "ISO 31000:2009: Risk Management - Principles and guidelines," 2009.

[7] H. Morgan, "Cyber security risk management in the SCADA critical infrastructure environment," *Engineering Management Journal,* vol. 25, no. 2, pp. 38-45, 2013.

[8] Y. Haimes and C. Chittester, "A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems," *Journal of Homeland Security and Emergency Management,* vol. 2, no. 2, p. 121, 2005.

[9] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, "A review of cyber security risk assessment methods for SCADA systems," *Journal of Computers and security,* vol. 56, pp. 1-27, 2016.

[10] E. Byres, D. Leversage and N. Kube, "Security incidents and trends in SCADA and process industries," in *The industrial Ethernet book,* 2007, pp. 12-20.

[11] European Commission, "Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union," *Official Journal of the European Union,* 2016.

[12] W. Huang, W. Wen and D. Yu, "Automated Vulnerability Assessment and Intrusion for Server Vulnerabilities," in *Proceedings of the Sixth International Conference on Intelligent Systems and Knowledge Engineering (ISKE2011),* Shanghai, China, Dec 2011.

[13] M. Barrere, R. Badonnel and O. Festor, "Vulnerability Assessment in Automatic Networks and Services: A Survey," *IEEE Communications Surveys & Tutorials,* vol. 16, no. 2, pp. 988-1004, Second Quarter 2014.

[14] Z. Anwar, R. Shankesi and R. Campbell, "Automatic security assessment of critical cyber-infrastructures," in *2008 IEEE International Conference on Dedendable Systems and Networks With FTCS and DCC (DSN),* Anchorage, AK, 2008.

[15] A. Nakamura, "Towards Unified Vulnerability Assessment with Open Data," in *2013*, Japan, IEEE 37th Annual Computer Software and Applications Conference Workshops (COMPSACW).

[16] L. Wehenkel, M. Glavic, P. Geurts and D. Ernst, "Automatic learning of sequential decision strategies for dynamic security assessment and control," in *IEEE Power Engineering Society General Meeting*, Montreal, Quebec, 2006.

[17] O. Ximming, S. Govindavajhala and A. W. Appel, "MulVAL: A Logic-Based Network Security Analyzer," *USENIX Security*, 2005.

[18] M. L. Artz, Netspa: A network security planning architecture (Phd diss.), Massachusetss Institute of Technology, 2011.

[19] NIST, Security Content Automation Protocol, 2012.

[20] C. Hlyne, P. Zavarsky and S. Butakov, "SCAP Benchmark for Cisco router security configuration compliance," in *10th International Conference for Internet Technology and Secured Transactions (ICITST)*, London, 2015.

[21] MITRE, "Common Vulnerabilities and Exposures," 2012. [Online]. Available: http://cve.mitre.org/.

[22] MITRE, "Common Weakness Enumeration," 2012. [Online]. Available: http://cwe.mitre.org/.

[23] MITRE, "Common Platform Enumeration," 2012. [Online]. Available: http://cpe.mitre.org/.

[24] FIRST, "Common Vulnerability Scoring System," 2012. [Online]. Available: http://www.first.org/cvss/.

[25] P. Kamongi, S. Kotikela, K. Kavi, M. Gomathisankaran and A. Singhal, "Vulcan: Vulnerabilitiy assessment framework for cloud computing," in *2013*, IEEE 7th International Conference on Sofware Security and Reliability (SERE).

[26] NIST, "National Vulnerability Database," 2012. [Online]. Available: http://nvd.nist.gov/.

[27] A. Hahn and M. Govindarasu, "An evaulation of cybersecurity assessment tools on a SCADA environment," in *IEEE Power and Energy Society General Meeting*, San Diego, CA, 2011.

[28] A. Singhal and O. Xinming, "Security risk analysis of enterprise networks using probabilistic attack graphs," US Department of Commerce, National Institute of Standards and Technology (NIST), 2011.

[29] H. Hannes, K. Shahzad, M. Buschle and M. Ekstedt, "P CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 626-639, 2015.

[30] E. Matthias, P. Johnson, R. Laerström, D. Gorton, J. Nydrén and K. Shahzad, "Securi CAD by Foreseeti: A CAD Tool for Enterprise Cyber Security Management," in *IEEE 19th International Enterprise Distributed Object Computing Workshop*, 2015.

[31] P. Johnson, A. Vernotte, M. Ekstedt and M. Lagerström, "pwnPr3d: an Attack Graph Driven Probabilistic Threat Modeling Approach," in *Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES)*, 2016.

[32] J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, R. Rajagopalan and A. Singhal, "Aggregating vulnerability metrics in enterprise networks using attack graphs," *Journal of Computer Security*, vol. 21, no. 4, pp. 561-597, 2013.

[33] K. Ingols, M. Chu, R. Lippmann, S. Webster and S. Boyer, "Modeling modern network attacks and countermeasures using attack graphs," in *Annual Computer Security Applications Conference 2009 (ACSAC '09)*, 2009.

[34] L. Williams, R. Lippmann and K. Ingols, "GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool," in *Visualization for Computer Security*, Berlin Heidelberg, Springer, 2008, pp. 44-59.

[35] M. Chu, K. Ingols, R. Lippmann, S. Webster and S. Boyer, "Visualizing attack graphs, reachability, and trust relationships with navigator," in *Proceedings of the 7th International Symposium on Visualization for Cyber Security*, 2010.

[36] S. Jajodia, S. Noel and B. OBerry, "Topological analysis of network attack vulnerability," in *Managing Cyber Threats*, New York, Springer, 2005, pp. 247-266.

[37] S. Jajodia, S. Noel, P. Kalapa, M. Albanese and J. Williams, "Cauldron: Mission-centric cyber situational awareness with defense in depth," in *Proceedings of the IEEE Military Communications Conference*, 2011.

[38] "RedSeal," [Online]. Available: https://redseal.co/.

[39] "Skybox security," [Online]. Available: https://www.skyboxsecurity.com/.

[40] European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of per-sonal data and on the free movement of such data, and repealing Directive 95/46/EC," [Online]. Available: http://data.europa.eu/eli/reg/2016/679/oj.

[41] D. Wright and P. d. Hert, Privacy Impact Assessment, Springer, 2012.

[42] A. Cavoukian, "Privacy by design - the 7 foundational priniciples," Tehcnical report, Information and Privacy Commissioner of Ontario, January 2011.

[43] Smart Grid Task Force (SGTF) Expert Group 2 (EG2), "Data protection impact assessment template for Smart Grid and smart metering systems," 2014.

[44] S. Gürses, C. Troncoso and C. Díaz, "Engineering privacy by design," in *Computers, Privacy & Data Protection Conference*, January 2011.

[45] J.-H. Hoepman, "Privacy design strategies," in *IFIP International Conference on Information Security*, 2014.

[46] M. Colesky, J.-H. Hoepman and C. Hillen, "A critical analysis of privacy design strategies," in *2016 International Workshop on Privacy Engineering (IWPE '16)*, San Jose, CA, 2016.

[47] G. Danezis, J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Metayer, R. Tirtea and S. Schiffner, "Privacy and data protection by design - From policy to engineering," ENISA, 2014.

[48] M. Jawurek, M. Johns and F. Kerschbaum, "Plug-in privacy for smart metering billing," in *Privacy Enhancing Technologies Symposium*, 2011.

[49] G. Barthe, G. Danezis, B. Grégoire, B. Kunz and S. Béguelin, "Verified computational differential privacy with applications to smart metering," in *IEEE Computer Security Foundations Symposium*, 2013.

[50] B. Defend and K. Kursawe, "Implementation of privacy-friendly aggregation for the smart rid," in *ACM Workshop on Smart Energy rid Security*, 2013.

[51] SEGRID Project, "Deliverable 2.3: Gap Analysis," 2016.