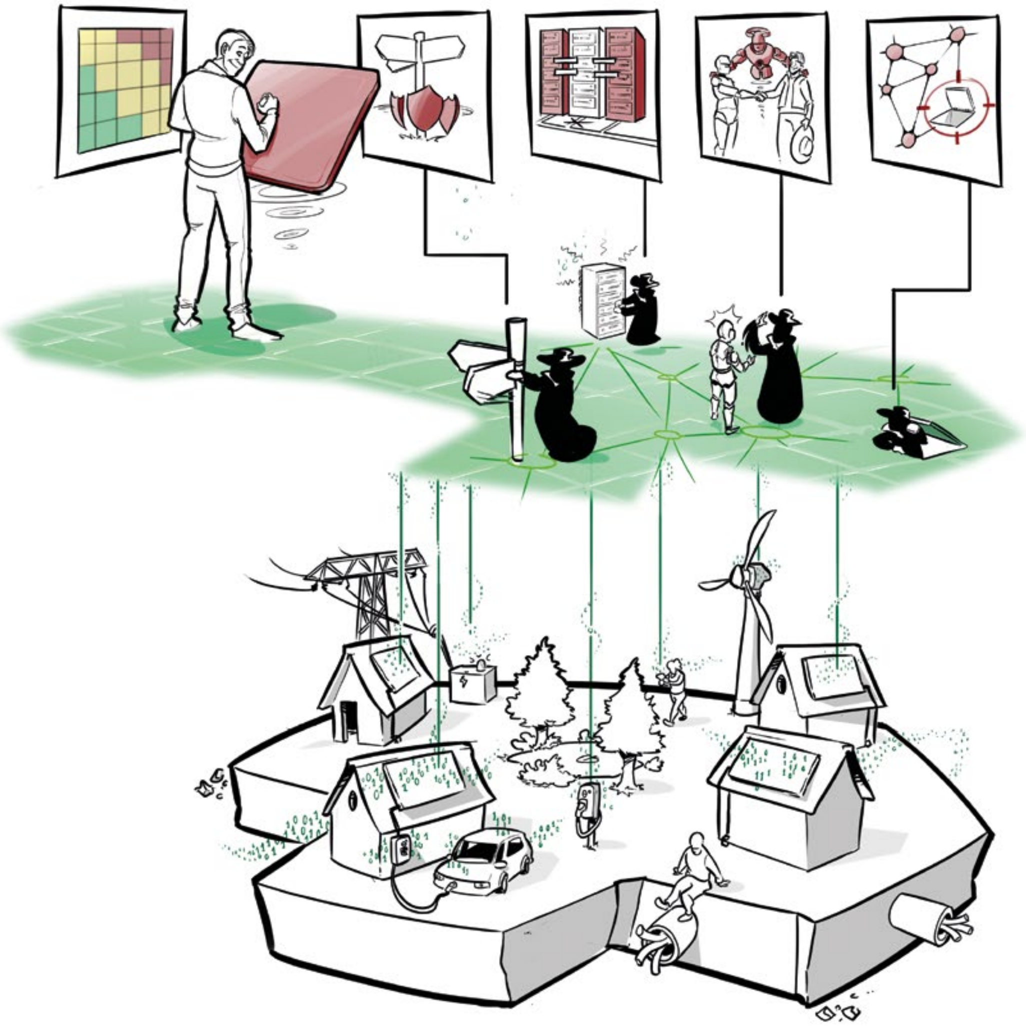
SEGRID

Security for smart Electricity GRIDs

How to address the security challenges in Smart Grids



This white paper discusses challenges and innovative solutions for cyber security and privacy in Smart Grids resulting from the work of the Security in Smart GRIDs (SEGRID) project.
This white paper specifically targets management and security specialists of Distribution System Operators (DSO) but can also be beneficial to other Smart Grid stakeholders.

List of Contributors

Exabier Bilbao Hernández (ZIV)
Gunnar Björkman (ABB)
Aurélio Blanquet (EDP)
Mathias Ekstedt (KTH)
Frank Fransen (TNO)
Maarten Hoeve (ENCS)
Sander Kruese (Alliander)
Eric Luiijf (TNO)
Nuno Medeiros (EDP)
Nuno Neves (FFCUL)
Johan Rambi (Alliander)
Judith Rossebø (ABB)
Marco Tiloca (RISE SICS)
Marcial Valmorisco (Incode)
Reinder Wolthuis (TNO)
Lenny Zilverberg (TNO)

Editors:

Frank Fransen & Reinder Wolthuis

Foreword

The energy sector is undergoing a digital revolution, and utilities are becoming increasingly dependent on the complex and highly interconnected digital environment. A number of disruptive elements are leading the digital transformation, such as distributed energy resources (DER), microgeneration, electrical vehicle (EV), and customer engagement. The sector is responding to these changes by increasing the level of intelligence of the power grid, through sensing, monitoring, control, automation and communications, i.e. the so called Smart Grid.

The data generated by the Grid Digital Transformation leverages the real-time capabilities necessary to encompass the increasingly dynamic pattern of consumption and generation at the Low Voltage (LV) levels, the intermittence of renewable generation, and support for customer interaction with the grid. These conditions reflect the new paradigm that the sector is heading to, and we as DSOs, must adjust our capabilities and business processes to ensure that the grid security, reliability, resilience and quality of service remain fundamental goals in order to face the ongoing challenges.

Although the digitalisation process is clearly part of the solution, we recognize that the introduction of increasingly complex, innovative and interconnected digital assets adds new vulnerabilities and greater exposure to cyber threats and poses new cyber security challenges. Hence, this transformation of the traditional threat landscape requires an appropriate response to ensure the protection of assets, both physical and informational, as part of their business digital transformation.

One should also recognize that any disturbance of the power supply has a very significant impact both on society and on the economy, making it an appealing and attractive critical infrastructure to target. Moreover, beyond any scenarios, we have already witnessed the impact of the successful cyber-attack on the Ukrainian Power Grid, which was unprecedented and a real awakening trigger for utilities around the globe.

For all these reasons, we feel the sense of urgency to develop and mature a cyber security culture within our organisation, emerging as a new priority risk on the Board agenda. By establishing common values and behaviours, improving security awareness, and developing strong preventive and reactive capabilities against cyber threats, DSOs can reduce the risks of the fast pace of digitalisation.

Considering the typical limited resources and financing for cyber security, to ensure an efficient and effective implementation of controls we should ground our strategy and project portfolio in risk assessment and management. Risks need to be managed throughout, including the various levels of the grid, and ensuring the right focus on the most relevant and critical risks for the organisation.

Additionally, since the technological ecosystem is evolving fast, both in complexity and interdependency, all utilities must recognize that they cannot and should not be dealing with these challenges by themselves. Rather, they should develop open and strong collaboration initiatives with other organisations (e.g, European projects, EE-ISAC, TNCEIP, DSOs partnerships, etc.) in order to jointly innovate and develop a more protected and resilient power grid. This is EDP Distribuição's commitment since we are all facing the same cyber security challenges and are struggling equally to protect our grids; therefore we should be sharing experiences, and knowledge about threats and vulnerabilities, and helping each other to leverage efforts.

The SEGRID project is one of these initiatives where utilities, manufacturers, research institutes and academia have been working in close cooperation to address the complex cybersecurity and privacy challenges of Smart Grids, to improve the security and resilience of the European Digital Grid.

Aurélio Blanquet
Director of the Grid's Digital Platform Division,
EDP Distribuição

Contents

Executive Summary

To manage all changes that occur in the electricity grid, it will be equipped with intelligent devices for sensing, monitoring, control, automation and communications - the electricity grid evolves to a Smart Grid. The introduction of the Smart Grid in combination with the entrance of many new and inexperienced stakeholders will dramatically increase the threat surface for malicious attacks on the electricity supply. The cyber-attack on the Ukrainian distribution grid in December 2015 is a prominent example of what could happen and a real-life illustration of the resulting impact. Additionally, the Smart Grid will collect and process large amounts of information, which in many instances will be related to the privacy of customers and must be protected against misuse. The SEGRID project, sponsored by the European Framework 7 research and development program, addresses the challenges that arise with the introduction of the Smart Grid. Because the SEGRID consortium includes scientific partners, applied research organisations, manufacturers and DSO's, the results are scientifically sound but also applicable in practice in the near future.

SEGRID has achieved the following results:

- *Security and Privacy Architecture DEsign (SPADE)* – The SPADE iterative process produces as final outcome a security and privacy architecture, ready to be deployed to fulfil the identified security and privacy requirements, employing Security-by-Design and Privacy-by-Design approaches.

- *Vulnerability threat modelling* – A vulnerability threat modelling tool models a network architecture and all of its components and simulates how probable it is for cyber-attacks to be successful. SEGRID has enhanced an existing vulnerability modeling tool called securiCAD, to make it more suitable for use in Smart Grids and for use in operational environments, so that changes in a network architecture can be fed into the model and analysed in real time.

- *SEGRID Risk Management Methodology* – SEGRID developed the SEGRID Risk Management Methodology (SRMM) that builds on state of the art risk assessment methodologies while providing guidance and enhancements for use in Smart Grids. The SRMM is supported by a tool and by practical guidance for each step of the method. The SRMM applies a stakeholder oriented approach which takes into account the dependency between Smart Grid stakeholders.

- *Resilient SCADA system* – One of the major threats of SCADA systems is an attacker that gains access to it, which can result in a catastrophic scenario. In SEGRID, we have developed a concept for a SCADA system that is able to operate correctly even under intrusions. The key idea is to replicate the SCADA system, allowing replicas to deterministically execute the same sequence of requests (e.g., operator commands) in such a way that, despite the failure of a fraction of the replicas, the remaining ones have the same state and ensure correctness of the offered services.

- *Resilient communication infrastructure* – In SEGRID, we have designed and implemented a new Software Defined Network (SDN) based solution to improve the resilience of the network that connects the primary substations to the control center(s) of a DSO.

- *Improved resource management for (D)TLS* – In Smart Grid systems, the TLS and DTLS protocols are widely used. However, these protocols suffer from a severe security vulnerability, which makes (D)TLS servers highly exposed to a Denial of Service (DoS) attack. SEGRID has proposed a solution that neutralizes the DoS attack described above. The proposed solution does not break current standards, and has been successfully tested on real RTUs communicating over a secure DTLS channel.

The cyber security field is rapidly evolving, which means that the SEGRID project also looked into the future. SEGRID has laid out a roadmap for future security developments, in which we note the following major trends:

- *Operational security organisation* – Up to now much Smart Grid security work has focused on the design of new systems or re-design of existing ones. When these Smart Grid systems become operational, new vulnerabilities and incidents will pop up more and more frequently, which introduces the need for DSOs to closely monitor the infrastructure and ICT equipment with respect to security. For this, intrusion detection systems (IDS) are needed but also an operational team, usually called Security Operations Center (SOC), to manage the events and alerts that are generated by these IDS-es. Many DSOs are therefore now considering to purchase intrusion detection systems to monitor their critical infrastructure and ICT equipment. Once these systems are operational, a need arises for a team to analyse and respond to the alerts. It can be expected that the role of these SOCs will expand in the future (to e.g. incident response, vulnerability scanning, forensics, managing firewalls), as it has done in other industries such as telecommunication and banking.

- *Security is extending from the network to the endpoints* – The security measures DSOs have taken in the past years were mostly implemented on network level, which was necessary due to the presence of many, highly vulnerable, legacy devices. Now that most DSOs have network level security measures in place, they are focusing more on defense-in-depth to make it harder for attackers to reach critical systems. The logical next step would be to focus more on strong security on all the endpoints, and draw defensive perimeters around each component. We expect that this model will be increasingly used in the design of Smart Grids. The advantage of this kind of model is that it reduces complexity, but it also requires new technical solutions and better security testing.

1. Introduction

Growing penetration of renewables across Europe's distribution grid over the past few decades has led to increasing challenges in maintaining the stability and reliability of the grid. Looking ahead, the European Commission (EC) has set a goal to meet at least 40 percent of the continent's demand for electrical power with renewables by 2030. To achieve this ambitious target, Distribution System Operators (DSO) will need to make major changes to the way they run their networks. It will force the introduction of Smart Meters, renewable generation and local storage on medium and low voltage levels. DSOs must learn to operate their grids in new ways. Power flows that traditionally have flown from higher voltage levels down to consumers on lower levels will now be able to flow in both directions.

However, these changes will not happen overnight. The DSOs have enormous investments in the grid that cannot be substituted quickly. These changes will happen gradually but they must be introduced immediately to be able to meet the ambitious European targets.

These paradigm changes, which are summarized in the concept of Smart Grids, bring with them an increased and extensive use of digital solutions and communication. The new, smart Information and Communication Technology (ICT) infrastructure will be much more connected than today to allow new types of information flows between new sets of stakeholders. The Smart Grid concept will introduce a growing number of organisations and individuals (the 'Smart Grid stakeholders') that are involved in the demand – production (supply) – transmission – distribution chains, making the new Smart Grid considerably more complex than the grid currently is.

The introduction of these new technologies will substantially increase the attack surface for cyber-attacks on the energy infrastructure. There are already real examples of sophisticated cyber-attacks on control systems engineered by highly motivated threat actors and carried out by skilled attackers. A prominent example is the cyber-attack on the Ukraine operated distribution network (see text box below). The disruption of energy supply coming from cyber-attacks can heavily impact the distribution grid and other society sectors which are depending on reliable supply of electricity.

Privacy is another important issue to consider because of the growing amount of privacy sensitive data that is processed and stored in the Smart Grid. The Smart Grid stakeholders already have a moral obligation to consumers to carefully handle privacy sensitive data, but the recently introduced EU privacy regulation also puts legal requirements on stakeholders who handle privacy sensitive data.

Consequently, cyber security has become an important challenge for Europe's economic development. It is, therefore, very important to evaluate cyber-security risks; to understand and reduce the number of vulnerabilities in the corresponding ICT systems and the potential impact that a disruption of the electrical supply might have.

SEGRID (Security of smart Electricity GRIDs) is a European funded FP7 project and is addressing these issues. This white paper describes some of the results of the SEGRID project. Please see the website[1] and appendix for more details on the SEGRID project. In the next section, the Smart Grid security challenges are described. Then we will elaborate on how the SEGRID results may help to better equip grid owners and other stakeholders against cyber-attacks. In the last section, we present the future developments of Smart Grid security.

Ukrainian Cyber Attack 2015

The primary cause of the Ukrainian blackout was that an attacker (or group of attackers) managed to infiltrate the corporate Information Technology (IT) networks of the targeted DSOs through phishing techniques. Once inside the corporate networks the attacker could open existing Virtual Private Network from the IT network to the Supervisory Control and Data Acquisition (SCADA) workstations in the Operations Technology (OT) network. After the attacker gained access to these workstations, he could view and operate SCADA displays and use normal operator dialogues to open circuit breakers in thirty substations (seven 110KV and twenty-three 35KV substations) thereby interrupting the electrical supply to approximately 225,000 customers. The attacker subsequently attacked serial-to-internet devices in the substations by downloading false firmware to make them inoperable. He also flooded the trouble call centers with numerous calls (a Denial of Service attack) and made the Uninterruptable Power Supply in the control centers inoperable. These follow-up attacks had the aim to delay restoration efforts. The distribution grid had to be manually restored by sending personnel to the impacted substations which is a time-consuming undertaking and ultimately the blackout duration was between one and six hours. A detailed description of the careful preparations, the actual attacks paths, the synchronization and follow-up attacks can be found in [SANS].

[1] *https://www.segrid.eu*

2 Smart Grid Security & Privacy Challenges

A DSO will face several different challenges, both technical and administrative, in connection to the introduction of Smart Grids

Long life-cycle of existing solutions

SCADA and Substation Automation systems, (such as RTUs), typically have a very long life time. It is not uncommon that different parts of a system belong to different technology generations and are coming from different vendors. These dissimilar parts form a very complex "system-of-systems". These different devices communicate with each other using a mixture of proprietary and standard protocols which in many cases lack support for security mechanisms such as proper encryption. This situation poses a substantial challenge when introducing a stringent cyber security strategy.

Rapid evolution of cyber threats

In contrast to the long-life time of legacy and modern components of the control systems, cyber threats emerge and disappear continually. New types of cyber threats coming from many different types of threat actors appear almost on daily basis. Global threat actors come into play, sometimes even nation state actors with large resources. Cyber conflict is currently a frequently used term in political discussions.

Smart Meter Deployment

Smart Grid requires frequent collection of detailed measurement data on consumption and generation throughout the grid. This was one of the motivations for the ongoing extensive installation of Smart Meters to replace old technology meters. The immense and complex task of deploying millions of new Smart Meters is a threat in itself. The deployment means that millions of Internet Protocol enabled devices will be installed in the grid. The installation is very often outsourced and not under the full control of the DSOs. In addition to the administration challenges, the introduction of Smart Meters also introduce many new security and privacy challenges.

IT/OT integration

Due to the increased application of Information and Communication Technology (ICT) in the operational domain of the distribution network and an increased and deeper integration between the IT and Operations Technology (OT) environments, new vulnerabilities are introduced and the attack surface is increased. The new ICT technology introduces standardized and widely used technology and protocols. Vulnerabilities in this technology are frequently found and the knowledge of these vulnerabilities is spread rapidly. Examples of new ICT technologies are the new Smart Meters and Metering systems, advanced RTUs with Intelligent Electronic Devices (IEDs) for protection. In addition, an increased integration between existing IT and OT environment is occurring. The IT environment is increasingly connected to and dependent on data from the OT environment, e.g. for grid extension planning, and vice versa is the OT environment connected to and using data from IT, e.g. weather data for load forecasting or generation schedules. This means a much deeper interconnection between the two DSO environments with many different types of users and complex data flows for which security is difficult to manage.

Dependence of external system

Many of the external systems and devices which are required in the extended OT and in the IT/OT integration are outside of the DSO's direct control and ownership. One example of the latter is the introduction of RTUs at distributed energy resources which are owned by independent energy suppliers. The DSO must be able to control these RTUs (i.e. setting new set-points) to reduce or increase production to meet energy balance requirements. The DSO thus depends on the cooperation of independent energy suppliers for energy balancing, and must interact with these external systems. These dependence and interaction with external system introduce new challenges for security.

Increased number of stakeholders

The number of stakeholders (outsourced and internal) interacting with the OT environment will substantially increase with the introduction of Smart Grids. This increase will introduce greater interdependencies, including more IT interconnections, and more complex processes for managing the energy supply chain. These new interdependencies will expose grid systems to new types of vulnerabilities which might endanger the security of the electrical supply. In addition, it will also have an impact on the privacy of the consumer as more personal data is potentially shared with a larger set of stakeholders.

Need of security expertise

Traditional DSO employees are not very ICT oriented and have limited knowledge and expertise in ICT and cyber security. This has not been a problem in the past, as the Operational Technology (OT) domain used to be isolated from the IT environment. Due to the increased IT/OT integration this situation has changed. DSOs will increasingly need cyber security personnel in the OT oriented domain to encompass the fast-changing threat landscape and the energy sector's digital transformation.

Qualified experts with Smart Grid domain knowledge and knowledge of risk management, security architectures, testing, incident detection and response are scarce.

Cost Benefit for Cyber Security

Balancing cost benefits while implementing security controls in Smart Grid components will be delicate. Ten euro cents extra cost for security in a Smart Meter will result in an extra € 600.000 in a roll-out of 6.000.000 meters. Motivating such security investments is often difficult. Particularly, in organisations with low cyber security maturity. Another example is frequent reconfiguration of the medium voltage network, e.g. due to loss minimisation, which will cause the maximum number of allowed switchings for each load breaker to be passed within a very short time period. Replacement of load breakers in the medium voltage network requires a considerable investment which cannot be motivated by decreased losses or lower average interruption times. Although this is not specifically a Cyber Security cost benefit issue, it demonstrates the difficulty of cost benefit analysis in the Smart Grid domain.

Cyber Security and Data Protection regulations

With the increasing digitization of society, new law and regulations are being introduced for cyber security and privacy. Examples are the directive on security of Network and Information Systems (NIS Directive) [NIS] and General Data Protection Regulation (GDPR) [GDPR]. These regulations are also applicable to DSOs, which means that the DSOs are faced with the challenge to implement and comply with the cyber security and privacy related directives and regulations.

How to better equip yourself against these challenges

Coherent approach

Information security is typically defined as the preservation of confidentiality, integrity and availability of information. These information security properties are also applicable and important for the information assets in the Smart Grid. However, in the Smard Grid domain cyber security involves a much wider range of security properties and issues that need to be addressed, ranging from physical and logical security of a component to resilience and robustness of the system as a whole.

Addressing cyber security needs to be done in a coherent way, including people, processes, and technology, and requires a continuous process to identify the necessary protections to mitigate risks, improve these protections, remove vulnerabilities and adapt to the changing threat landscape. There are multiple standards and methods to support organisations with establishing such a continuous process. The most well-known security standard is ISO/IEC 27001[27001], which provides requirements to implement an Information Security Management System.
An essential element in this is Risk Management. Risk Management is the systematic application of procedures and practices to identify, analyse, evaluate, treat, monitor and review cyber security related risks.

The continuous transformation of the power grid towards the Smart Grid introduces new interconnected ICT systems. These new ICT systems introduce new vulnerabilities and enable new cyber-attacks. Risk assessment is the process within risk management to identify these threats, vulnerabilities, and risks. Selecting security controls to mitigate the risks should be an integral part of the evolution towards the Smart Grid. The SEGRID project studied and developed risk assessment and risk management for the Smart Grid system. This is addressed in more detail in the section describing risk management. For identification and mitigation of privacy related risks a Data Protection Impact Assessment (DPIA) should be performed.
The EU Expert Group for Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment has developed a DPIA template specifically for Smart Grid and Smart Metering systems [DPIA].

Specific security controls need to be selected to mitigate the cyber security risks in new ICT systems of the Smart Grid. The code of practice for information security ISO/IEC 27002 [27002] provides a set of best practice information security controls that accompany ISO/IEC 27001.

Additional guidance for application of ISO/IEC 27002 within the energy utility is described in ISO/IEC 27019 [27019]. These standards provide a good framework for establishing information security at an organisational level. At the technical level, more guidance is among others provided by the ISA/IEC 62443 set of standards. Cyber security control may provide different types of protection, such as prevent a cyber-attack from being successful, or reduce the impact of an attack by means of incident detection, response and recovery. Although cyber security and privacy controls depend on people and procedures, many security and privacy controls are technological in nature. These security and privacy-preserving technologies should be an integral part of a system. The strength and effectiveness provided by the security and privacy technology should be assessed during the whole life-cycle of a component or system (e.g. specification, design, implementation, test, operation, and end-of-life). Most importantly during the development phase by means of Security-by-Design and Privacy-by-Design approaches. To support the selection of security and privacy controls during the development phase and design a security and privacy architecture, the SEGRID project designed a specific process called SPADE (see box below). In the SEGRID project, focus has been put on innovation in security technologies for Smart Grid systems. This is addressed in more detail in the section describing Security Controls, Mechanisms and Technologies.

SEGRID contribution

Security and Privacy Architecture DEsign

The SEGRID Security and Privacy Architecture DEsign (SPADE) iterative process has been conceived to design, validate and evaluate security and privacy architectures for Smart Grid systems. The SPADE process considers a Smart Grid use case as its main reference input, and produces as final outcome a security and privacy architecture which is specific for that use case, ready to be deployed to fulfil the identified security and privacy requirements, and displaying sustainable and satisfactory performance.

From a high-level perspective, SPADE considers three different phases, namely Design, Check and Evaluation, which are iteratively performed until a satisfying security and privacy architecture has been produced for the considered use case.

In principle, the first Design phase takes as input the specific use case to consider, related cost and performance requirements, related security and privacy goals, as well as a prioritized list of risks assessed previously during a threat and vulnerability risk analysis. Then, it produces a complete but temporary security and privacy architecture for the considered Smart Grid use case. The temporary architecture is provided as input to the Check phase, which has the goal to verify that the security and privacy requirements as well as other design criteria are satisfactorily fulfilled. If such validations fail, the process falls back to the Design phase to (re)design an improved version of the security and privacy architecture. Otherwise, the SPADE process can proceed to the Evaluation phase, when extensive practical tests are performed and a performance analysis is carried out. Such an analysis may suggest to perform minor fixes and tunings to achieve a better, final, security and privacy architecture ready to be deployed, or instead force to move back to the Design phase, in case major flaws and issues are identified.

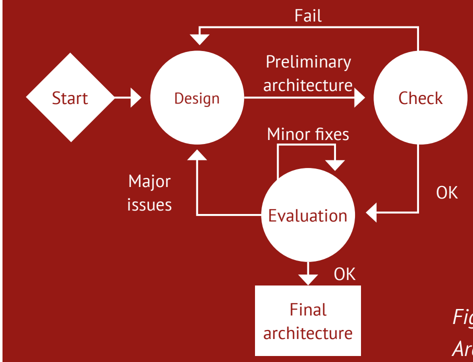
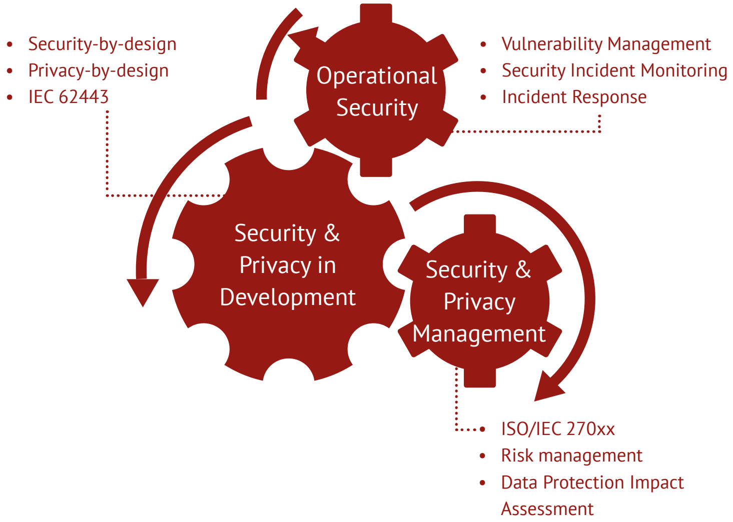


Figure 1. Security and Privacy Architecture DEsign (SPADE)

Finally, maintaining the security during the operational life-cycle of the system is becoming more important. The threat landscape is evolving rapidly with new more advanced cyber-attack methods continuously being developed and new vulnerabilities are being discovered in components and systems. Organisations should therefore continuously monitor their system for potential attacks, identify and resolve vulnerabilities in components and systems and develop and maintain a capability to quickly and efficiently respond to cyber-attacks. As these operational security capabilities for the OT domain of the power grids are a (near) future development, it will be discussed in more detail in chapter 4.



- Security-by-design
- Privacy-by-design
- IEC 62443
Operational Security
- Vulnerability Management
- Security Incident Monitoring
- Incident Response
Security & Privacy in Development
Security & Privacy Management
- ISO/IEC 270xx
- Risk management
- Data Protection Impact Assessment

Figure 2. Coherent approach to security & privacy

Risk Management

Risk assessment and risk management is necessary to ensure that effective controls are implemented in an efficient and effective way, limiting the exposure to cyber threats and incidents. Application of risk assessment and risk management is a must during the transition towards the Smart Grid. There are many risk management frameworks available, with various differences among them, making the selection of the most appropriate one a challenging task. Although these can indeed be applied in the Smart Grid domain, some specific characteristics make risk assessment to Smart Grids systems less straightforward.

As the Smart Grid is a system of systems involving multiple stakeholders, the risk assessment method should be suitable for performing (technical) security threat and risk assessment across multiple stakeholders/organisations. Traditional risk assessment methodologies typically consider only one stakeholder. Furthermore, impact scales and categories need to be made suitable to Smart Grid scenarios and can vary per stakeholder.

Another important aspect to consider is that society is increasingly dependent on the proper functioning of the electric power grid, which in turn supports most other critical infrastructures (e.g. water systems, telecommunications, finance, air traffic control, railroads), the risk assessment should consider societal impact due to the cascading effect of a power outage. The power grid should consider different types of threat actors, ranging from script kiddies to state sponsored attackers. The motivation and capabilities of these different threat actors may also differ significantly.

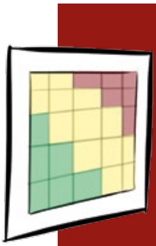
The SEGRID project investigated current risk assessment methodologies and the need for enhancements for application to Smart Grids. The project then developed the SEGRID Risk Management Methodology (SRMM) that builds on state of the art risk assessment methodologies while providing guidance and enhancements for use in Smart Grids. The SRMM is supported by a tool and by practical guidance for each step of the method.

Based on the results of application of the SRMM within the SEGRID project, it is believed that the new methodology can positively position itself as the most appropriate and enhanced risk management approach for Smart Grid environments, allowing DSOs to understand the potential threats, the business and societal impacts for the various stakeholders if a threat is successful, and the likelihood of occurring. This stakeholder oriented approach enables the selection of the most relevant security and data protection controls, which can be traceable to the effect they have on the various stakeholder's business processes risks. See the text box for more information on SRMM.

SEGRID also engage in more detailed threat modelling where vulnerabilities of Smart Grid ICT infrastructure is the focus area. This part does not consider different threat actor profiles nor the consequences of successful attacks, it simply attempts to answer the following question; if a professional penetration tester attempts to attack a system architecture at a given point, how difficult would it be (in terms of how much time would it take) to compromise all other components of the architecture? To answer this question SEGRID makes use of the threat modelling tool called securiCAD[2] (which is based on the research framework Cyber Security Modelling Language). For more details on this SEGRID contribution, see the section on Future Development.

The securiCAD tool requires a detailed description of the Smart Grid ICT infrastructure, which is typically not yet available at the beginning of the design stage. SRMM can be applied to an abstract description of the Smart Grid ICT infrastructure, but can also integrate the results of securiCAD at a later stage of system design to further improve the estimation of the level of vulnerability of an ICT infrastructure. SecuriCAD can also be integrated with SPADE to support the assessment of the effectiveness of security controls.

[2] *https://www.foreseeti.com/products*



SEGRID contribution

SEGRID Risk Management Methodology

The SEGRID Risk Management Methodology (SRMM) is focused on application for Smart Grids [SRMM]. The methodologies that formed the basis for the SRMM are:

1. *HMG IA Standard No. 1(IS1)*
   The HMG IA Standard No. 1 (IS1), was developed as the UK government's technical risk assessment (RA) methodology [IS1]. The Dutch association of Energy Network Operators, Netbeheer NL[3], adopted the IS1 methodology for application on Smart Metering and other Smart Grid use cases, simplifying the methodology and extending the approach for application in multi-stakeholder environments.

2. *ISO/IEC 27005*
   The ISO/IEC 27005 standard [27005] provides a framework for information security risk management.

3. *Network Risk Management (NRM)*
   NRM [NRM] was specifically designed to provide insight in dependency, the responsibility and the propagation of risks through value chains. An advantage is that it makes it possible to relate the cyber security risk analysis to risks that affect real business interests.

4. *ETSI Threat & Vulnerability Risk Assessment (TVRA)*
   The TVRA method was developed by ETSI for use in the ICT standards domain to identify the rationale for specification of security solutions, and published as ETSI TS 102 165-1 [TVRA]. SEGRID enhanced the TVRA a.o. to include an assessment of the motivation and capability of the attacker in the risk estimation step.

The SEGRID Risk Management Methodology (SRMM) consists of seven steps depicted in the figure below. For the first 5 steps SEGRID provides specific methodologies.

1. Context establishment
   a. Define criteria necessary for performing the risk assessment and managing the risks.

[3] http://www.netbeheernederland.nl/

   b. Identify the scope, boundaries and context of the RA, including stakeholders, processes, assets, and existing security controls. The assets need to be linked with stakeholder processes.
   c. Identify the NRM scopes and sub scopes. These are demarcations based on organisational responsibilities. Each NRM (sub)scope has an identifiable responsible person.
   d. Define NRM obligations and expectations and verify if they match between scopes.
   e. If personal data is included in the RA scope, conduct a Data Protection Impact Assessment (DPIA) and ensure that the DPIA and SRMM are aligned.
2. Impact assessment - assess asset risk impact for each stakeholder impact category, societal impact, and on obligations in each scope.
3. Threat and vulnerability assessment - identify threat sources, threat actors, vulnerabilities and threat scenarios.
4. Risk estimation and prioritization- estimate the risks in terms of likelihood and impact and prioritize the risks against the risk evaluation criteria.
5. Risk treatment - identify the risks that need to be treated and specify a risk treatment plan in terms of required security controls.
6. Risk acceptance – based on the risk treatment plan and the residual risk assessment a risk acceptance decision is made, using the ownership of the NRM scope as reference.
7. Document and communicate results, and monitor and review risks (reiterating the assessment when needed).

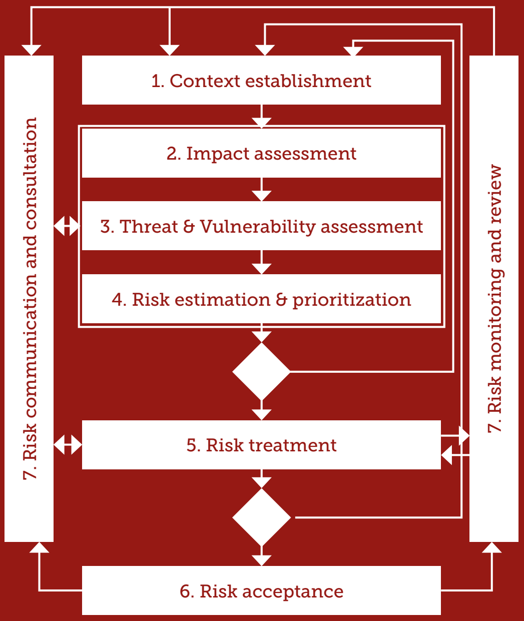
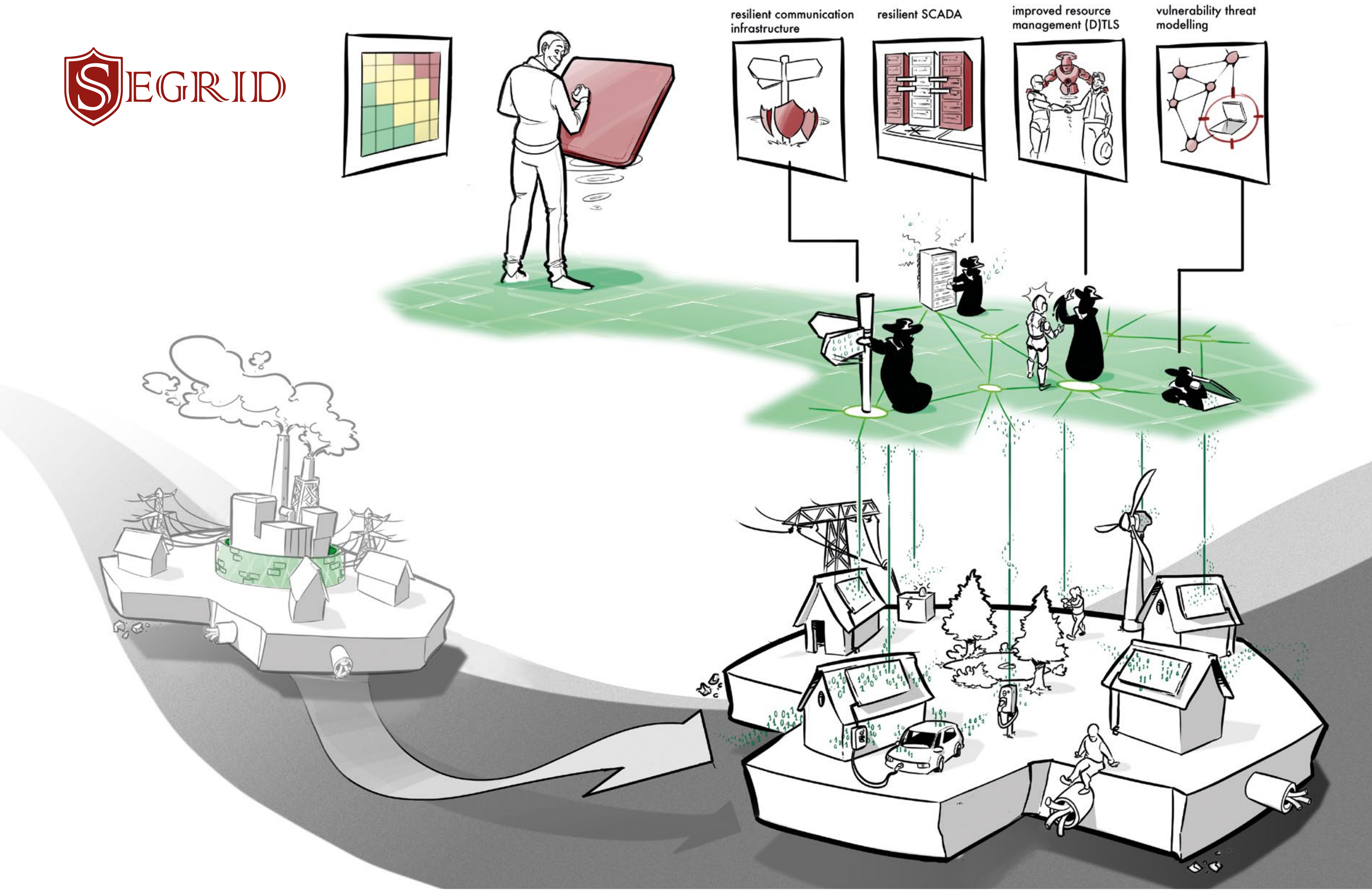

1. Context establishment
2. Impact assessment
3. Threat & Vulnerability assessment
4. Risk estimation & prioritization
5. Risk treatment
6. Risk acceptance
7. Risk communication and consultation
7. Risk monitoring and review

Figure 3 SEGRID Risk Management Methodology

SEGRID


resilient communication infrastructure
resilient SCADA
improved resource management (D)TLS
vulnerability threat modelling

A DSO perspective on enhancing the security of the Smart Grid

Security Controls, Mechanisms and Technologies

To mitigate the risks identified in the risk management process, DSOs need to select and implement security controls. As mentioned above, SEGRID developed an approach, called SPADE, to support the selection of security controls and design a security and privacy architecture for Smart Grid systems. This section introduces and briefly describes a set of security controls, which are recommended to be considered for adoption for the Smart Grid. In addition, three specific areas are described in more detail for which SEGRID has developed new controls or improved existing controls.

Monitoring and intrusion detection.

This includes logical and/or physical mechanisms and technologies for monitoring the Smart Grid system, and detecting and reporting anomalies, misbehaviour and intrusions. To this aim, it is helpful to rely on event and activity logging, i.e. to produce, record and maintain information related to the evolution of the values and attributes in the Smart Grid system over time.

Resilience assurance.

This mainly includes mechanisms for ensuring and maintaining resilience in Smart Grid systems, in particular:

- Approaches enabling logical and/or physical redundancy of Smart Grid entities and functionalities, e.g. by replicating physical entities or logical/software components. Among other things, this makes it possible to achieve: i) backup of information, services, and physical entities; ii) local consensus among different cooperating entities; iii) easier detection of unreliable and/or malevolent information flows and compromised entities; iv) practical avoidance of single points of failure.
- Technologies and mechanisms to quickly and effectively preserve service availability as well as system and communication performance, in the presence of accidental malfunctioning and/or security attacks. This comprises the ability to establish on demand new routes for network control and data traffic, and to isolate suspected sources of malevolent network traffic in the Smart Grid.

Secure management and control.

This includes i) workstations and terminal points enabling administrative or technical authorized personnel to monitor, control, maintain and administer the Smart Grid system as a whole and/or from a single component perspective; as well as ii) interfaces between the Smart Grid system and the final user/consumer, in order to assure privacy, transparency and control of personal information assets distributed, stored and processed in the Smart Grid system.

Secure platforms.

This includes technologies and mechanisms that can be employed to fulfil platform security requirements on (embedded) devices in the Smart Grid system. Typical expectations from secure platforms include: i) trust bootstrapping of operating systems; ii) hardware platform verification; iii) separation, non-interference and safe execution of software processes.

Secure communication.

This mainly includes mechanisms for establishing and maintaining over time secure message exchange among different entities deployed in the Smart Grid system, in particular:

- Protocols to protect communication at different layers of the network stack, in order to fulfil, among other things, confidentiality, message integrity and authentication, and replay protection. These secure communication protocols fundamentally rely on the establishment of secure sessions and the use of cryptographic key material. Besides, they commonly rely on additional supporting entities, including trusted third parties and key managers.
- Key management protocols adopted for managing, generating, providing, revoking and (re)distributing cryptographic key material, possibly used in group communication contexts. The execution of key management protocols is typically enforced by key manager entities, which in turn may need to tightly cooperate with dedicated supportive entities, such as intrusion detection systems as well as trusted third parties.
- Trusted Third Parties (TTPs) as entities aimed at enabling or easing secure interactions between two entities in the Smart Grid system. Relevant examples of TTPs include certification authorities, trust anchors, group membership managers, and access control and/or authorization enforcers. As a particular case, TTPs play a main role as components of Public Key Infrastructures (PKIs).
- Mechanisms and protocols for secure resource discovery that allow entities in the Smart Grid system to specify the assumed known identity of a third entity, and then securely retrieve authentic information about how to (securely) contact it.

Smart Grid introduces new constraints and challenges on the implementation of these security controls. Often, novel security mechanisms and technologies have to be developed to ensure that the security control can be applied in a Smart Grid environment. The SEGRID project provides several novel security solutions that can be used to fulfil Smart Grid security requirements. To facilitate the use of these solutions, this section links some of the SEGRID solutions to the requirements in the IEC 62443-3-3 standard [62443-3-3]. IEC 62443 is a series of security standards for industrial automation and control systems (IACS) that is widely used by DSOs and manufacturers. IEC 62443-3-3 was not written to look at requirements in isolation, but is intended to be used to build a defence in depth approach to protecting the control system and describes the system requirements that must be met for a secure industrial control system. The basis of these system requirements comes from the definition of a set of seven foundational requirements (FRs). The SEGRID solutions can be mapped towards IEC 62443-3-3 security requirements.

Improved system integrity and availability through intrusion tolerant server replication

By replicating critical servers in an intrusion intolerant manner, SEGRID provides a completely new solution to achieve the intention of two of the foundational requirements of the IEC 62443-3-3. These are FR 3 System Integrity and FR 7 Resource availability.

The purpose of FR 3 is described as follows [62443-3-3]:

> *Ensure the integrity of the IACS to prevent unauthorized manipulation.*

The purpose of FR 7 is described as follows [62443-3-3]:

> *Ensure the availability of the control system against the degradation or denial of essential services.*

The concept of replication components for safety is well-known. Generally, replication does only help against casual or coincidental manipulation, that is on IEC 62443 security level 1. By using special technology, it is however possible to use replication to ensure system availability and mitigate integrity threats, even when performed by skilled attackers (IEC 62443 security level 3 and 4). The SEGRID project has demonstrated that this type of replication is possible for SCADA servers.

SEGRID contribution

Resilient SCADA System

Supervisory Control and Data Acquisition (SCADA) systems form the backbone of critical infrastructures. However, with the integration of field and corporate networks, SCADA systems became more exposed to the plethora of attacks plaguing the Internet, which may lead to operational failures. To address this issue, companies depend on firewalls and intrusion detection solutions to secure their infrastructures. However, often these technologies are incapable of defending against novel or tailored attack vectors that enable the implementation of malicious actions.

One of the major threats to the SCADA systems is that an attacker gains access to the main computer – the SCADA Master. This computer manages all operations under the SCADA supervision, and therefore an intrusion can result in a catastrophic scenario. Ideally, the SCADA Master should operate correctly even in presence of malicious compromises. Although it is not possible to achieve this by using intrusion detection and prevention technologies, it could be accomplished by employing intrusion tolerant techniques, based on replication.

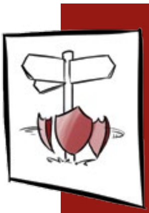
In the SEGRID project, we have developed a SCADA system that can operate correctly even under intrusions. The solution is built using Byzantine-Fault Tolerant State Machine Replication. The key idea is to replicate the SCADA Master, allowing replicas to deterministically execute the same sequence of requests (e.g., operator commands) in such a way that, despite the failure of a fraction of the replicas, the remaining ones have the same state and ensure correctness of the offered services. This solution addresses transparently both accidental failures, as commonly done by commercial SCADAs, but in addition enhances security by addressing the malicious compromise of Master replicas.

Improved denial-of-service protection in software-defined networks

As part of the resource availability foundational requirements, IEC 62443-3-3 contains the following requirement [62443-3-3]:

> *SR 7.1 RE 1: Manage communication loads: The control system shall provide the capability to manage communication loads (such as rate limiting) to mitigate effects of information flooding types of DoS events*

Software-defined networks (SDNs) provide a good way to manage communication loads. Although they are currently adopted in ISP and datacenter networks, it is expected that they will become an important part of Smart Grids in the future. However, SDNs themselves are vulnerable to specific types of denial-of-service attacks. The SEGRID project provides solutions to detect and prevent such attacks.



SEGRID contribution

Resilient Communication Infrastructure

Smart grids bring modern communication technology to the electrical infrastructures, in order to support a set of new capabilities which enable a more efficient use of resources while ensuring a high quality of electrical power delivery to end users. Smart grid applications are typically run in equipment inside the (primary) substation and are connected to an edge switch to enable the exchange of data with the other parts of the grid (namely the head end systems). In SEGRID, we have focused on improving the resilience of the communications outside of the substation, as these are spread over large geographical areas, and consequently are more prone to failures.

We have investigated how the Software Defined Network (SDN) paradigm could be applied to Smart Grids. In particular, we designed and implemented a new SDN based solution to manage the core (or WAN) network, which connects together the primary substations and the control center(s) of a DSO. We want to leverage the SDN principles to be able to enforce across the infrastructure network policies that promote the resilience of the communications as well as taking into consideration the requirements imposed by the Smart Grid applications.

Overall, the aim is to ensure that applications running in the Smart Grid can exchange data with the required levels of reliability and quality of service. This should occur even if the infrastructure experiences failures, namely localized congestion, link disruption, or some form of attack (e.g., Denial of Service). Of course, this sort of objective can only be achieved if the network is adequately provisioned with physical redundancy, which allows traffic to be rapidly rerouted from the parts of the infrastructure that are being affected by the problems. Moreover, different wide-area communication providers may be employed to ensure that a diversity of paths is available, so that, when a part of network is underperforming, the remaining part can still effectively deliver packets.

Improved resource management for (D)TLS

As part of the resource availability foundational requirement, IEC 62443-3-3 contains the following resource management requirement [62443-3-3]:

> *SR 7.2 Resource management: The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.*

The SEGRID project has shown that the TLS and DTLS protocols are vulnerable to resource exhaustion attacks [SICS_DTLS]. The TLS protocol is one of the cornerstones of Smart Grid security. It provides communication security in diverse systems from Smart Metering to electric vehicles and distribution automation. DTLS is based upon the TLS protocol, but provides communication security for datagram protocols such as UDP. DTLS is expected to play a large role in Internet-of-things systems, which will also become part of the Smart Grid ecosystem. Hence, new security solutions are needed to fulfil the SR 7.2 requirement. The SEGRID project has proposed a solution to improve resource management for (D)TLS.

SEGRID contribution

Improved resource management for (D)TLS

In Smart Grid systems, a number of communication segments are secured through standardized dedicated security protocols. Among them, the TLS and DTLS protocols especially emerge as the defacto solutions for secure communication at the transport level of the typical stack, in case connection-oriented or datagram-oriented communication is adopted, respectively. Relevant Smart Grid entities adopting secure communication based on (D)TLS are, for instance, SCADA units and RTUs in secondary substations.

Two entities that want to communicate over (D)TLS, i.e. client and server, need to first establish a secure channel through a message exchange known as handshake. In particular, the client unit takes the initiative by sending a ClientHello message to start the handshake with the server unit. When the handshake process is completed, the two parties agree on shared cryptographic material and can securely communicate, while practically preventing message forgery, replication and unauthorized overhearing.

However, the handshake process itself suffers from a severe security vulnerability, which makes (D)TLS servers highly exposed to a Denial of Service (DoS) attack. In particular, an adversary can repeatedly send ClientHello messages to a server unit, e.g. a RTU, and relentlessly force it to perform a considerable number of invalid, resource-demanding, handshake processes. It follows that the server establishes 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 requests from legitimate client units, and hence endangering the expectedly correct and safe operations in the Smart Grid system. Although some techniques have been considered in the past, they are not effective against well determined adversaries exploiting valid and/or spoofed source IP addresses.

The SEGRID project has considered this security vulnerability and proposed a solution that allows servers to identify invalid ClientHello messages and promptly abort the handshake execution at its very first step [SICS_DTLS]. This effectively neutralizes the DoS attack described above, by substantially limiting its impact and so preserving service availability in the system. The proposed solution does not break current standards, and has been successfully tested on real RTUs communicating over a secure DTLS channel.

Future Development

In the coming years, we expect two major trends in Smart Grid security. First, the creation of operational security organisations at DSOs tasked with actively responding to vulnerabilities and incidents. Second, the transfer of the responsibility for security from the network to the endpoints.

Operational security organization

Up to now Smart Grid security work has focused on the design of systems. Major new infrastructures are being developed for Smart Metering, distribution automation, electric vehicles, and demand response. These infrastructures require a security architecture, and the selection of security controls. At the same time, existing (legacy) infrastructures also need to be redesigned to improve their security. The security staff of DSOs has therefore worked on long term risk management cycles: what will be the risks of each system over its lifetime, and what technical solutions need to be used to mitigate these risks.

As these systems become operational, the security organisation at the DSOs also needs to encompass operational security. A much shorter cycle is needed to deal with incidents and vulnerabilities that will start popping up.

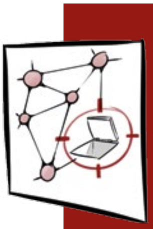
The first sign of this trend towards operational security is the current interest in security monitoring. Many DSOs are now considering purchasing intrusion detection systems for their critical SCADA systems. Once these systems are in place, a need arises for a team to analyze and respond to the alerts. Hence, DSOs are working on creating security operations centers (SOCs) for their Smart Grid systems.

It can be expected that the role of these SOCs will expand in the future, as it has done in other industries such as telecommunication and banking. They will take on tasks such as vulnerability monitoring, real-time security incident monitoring, incident response, forensics, and penetration testing.

The operational teams will create a demand for better security tools. Starting with Stuxnet, a lot of research effort was put into intrusion detection tools. This has resulted in several interesting network-based intrusion detection tools for SCADA systems that are on the market now. These tools are also adding vulnerability discovery capabilities. Other tools will likely be developed to meet future needs.

One of the main benefits of these tools is a greatly increased situational awareness about security. DSOs get better insight into which assets are in their networks, how these fit together, and where they are vulnerable. This allows DSOs to improve their security much faster than before, when they only had information from a small number of penetration tests and audits performed each year.

The end goal for situational awareness would be to have a real-time view of the security risks. To obtain this view, developments are needed in two directions. First, an improvement in the modelling of systems to allow for quantitative, probabilistic risk assessments. SEGRID is contributing to this with the work on vulnerability assessments.
Second, an integration of all relevant data in the security operations center. Once good models are available, they will need to be fed with information about vulnerabilities, threat intelligence, and business impact (from long term risk assessments). Once such a real-time risk view is available, DSOs can use it to prioritize both which preventive measures they take, and to decide which alerts and incidents they respond to.



SEGRID contribution

Vulnerability threat modeling

To identify vulnerabilities in a Smart Grid ICT infrastructure, SEGRID makes use of the threat modelling tool called securiCAD. This tool is based on the research framework Cyber Security Modelling Language. The tool generates probabilistic attack graphs given a model of an ICT infrastructure architecture. In short, this means that the tool user makes a model describing things such as which networks, computer hosts, services, data flows, and user accounts constitute the ICT infrastructure. In addition, the components' properties are described such as how well the various software components are patched, what data flows are encrypted, how well firewalls are managed, and what kind of authentication and access control mechanisms that are employed. From this model, the tool automatically generates (a myriad of) potential attack vectors through the architecture and simulates how difficult it is to succeed with them. Thus, the tool can be seen as a virtual penetration test (on a model, not the real technology) attempting not only a single or a few cyber-attacks, but all possible attack vectors. In SEGRID, we have added Smart Grid specific components to the tool and modelled the Smart Grid ICT infrastructure architectures necessary for implementing the SEGRID use cases.

In SEGRID, we have also worked on automatically generating a model of an existing Smart Grid ICT infrastructure in near real time, merging information from various data sources, such as network scanners, vulnerability scanners, and configuration management systems. Ultimately this will enable a DSO to more easily assess its existing Smart Grid ICT infrastructure for vulnerabilities, and automatically re-assess it when changes in this infrastructure are detected.

Security is extending from the network to the endpoints

The security measures DSOs have taken in the past years were mostly implemented on network level. This was a choice by necessity. Many legacy devices present in most grids have vulnerabilities that cannot be solved due to end of maintenance or unavailability of updates or patches. They need to be protected by the network architecture, and by applying external security devices, such as firewalls, routers with VPN, and proxies.

Now that most DSOs have these measures in place, they are focusing more on defence-in-depth. They are adding more defensive lines to make it harder for attackers to reach critical systems. The logical next step would be to add strong security on all the endpoints, and draw defensive perimeters around each component.

This is already the model for IT systems. Each laptop or smart phone is expected to protect itself in a hostile environment (the internet). It is also a model used in newer Smart Grid systems. Even though they are some of the cheapest Smart Grid components, Smart Meters are expected to be resilient against cyber and physical attacks up to some level. We expect that this model will be extended to more classically designed systems, such as distribution automation SCADA systems.

The advantage of a model with security on the endpoints is not just adding an extra layer of defence. It also reduces complexity. Currently to assure secure Smart Grid operations you need to understand how the entire system works. This is highly challenging because large systems are continuously changing and have many dependencies, also on third parties. One backdoor can compromise the entire system. With more security in the endpoints, the scope of assurance can be significantly reduced. For instance, if end-to-end encryption and authentication is used, the integrity and confidentiality of data only depends on the communication endpoints. Attacks carried out on a telecommunications network, which may be a public network owned by a telecom operator, will not compromise these properties.

Moving security to the endpoints requires new technical solutions. It requires the use of end-to-end secure protocols. It requires better protocols and tools to manage keys and access rights on large number of components. And it requires methods to ensure the integrity of software on the component, such as firmware signing, and the use of secure boot processes. Intrusion detection will shift from monitoring the network to monitoring the endpoint logs.

Besides these new solutions, the model also requires improved security test methodologies. The traditional approach of performing penetration tests and code reviews when new components are delivered is insufficient. There are too many new components, and too few skilled penetration testers. Moreover, there is a trend towards agile development methods with a much larger number of software releases than in previous generations of systems. Security testing will need to be largely automated if it is to keep pace with these trends.

References

[27001] ISO/IEC 27001:2013; “Information technology —Security techniques — Requirements”; Second edition; 2013-10-01.

[27002] ISO/IEC 27002:2013; “Information technology —Security techniques — Code of practice for information security management”; Second edition; 2013-10-01

[27005] ISO/IEC 27005:2011; “International Organisation for Standardization: ISO Information technology — Security techniques — Information security risk Management”; 2011

[27019] ISO/IEC TR 27019:2013; “Information technology – Security techniques – Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry”; 07-05-2013

[62443-3-3] IEC 62443-3-3:2013; “Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels”; 2013

[DPIA] “DPIA Template for Smart Grid and Smart Metering Systems”; Smart Grid Task Force 2012-14; Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment; 18-03-2014

[GDPR] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union; 27-04-2016,

[IS1] HMG IA Standard Numbers 1 & 2 – Supplement; “Technical Risk Assessment and Risk Treatment”; CESG; Issue No: 1.0; April 2012

[NIS] 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; L 194/1; 19-07-2016.

[NRM] R. Wolthuis and R. Joosten; “El Metodo - Managing Risks in Value Chains”; Proceedings of the ISSE 2011 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe 2011 Conference; November 2011

[SANS] SANS/E-ISAC White Paper; “Analysis of the Cyber Attack on the Ukrainian Power Grid”; 18-03-2016

[SGAM] CEN-CENELEC-ETSI Smart Grid Coordination Group; “Smart Grid Reference Architecture”; 2012

[SICS_DTLS] Marco Tiloca, Christian Gehrmann and Ludwig Seitz; “On Improving Resistance to Denial of Service and Key Provisioning Scalability of the DTLS Handshake”; International Journal of Information Security; Volume 16; Issue 2; pp 173–193; April 2017

[SRMM] Judith E.Y. Rossebo, Reinder Wolthuis, Frank Fransen, Gunnar Bjorkman, and Nuno Medeiros; “An Enhanced Risk-Assessment Methodology for Smart Grids”; IEEE Computer vol. 50 no. 4; p. 62-71; 2017

[TVRA] ETSI TS 102 165-1; “TISPAN; Methods and Protocols; Part 1: Method and Proforma for Threat, Vulnerability, Risk Analysis”; 03-2011

Appendix, SEGRID Project

SEGRID (Security for smart Electricity GRIDs) is a collaborative research project funded within the 7th framework program by the European Union. The partners of SEGRID are presented in the table below.

Type	Partners
DSOs	Alliander and EDP
Manufacturers	ABB and ZIV
Research and knowledge institutes	ENCS, RISE SICS, and TNO
Universities	KTH and FFCUL

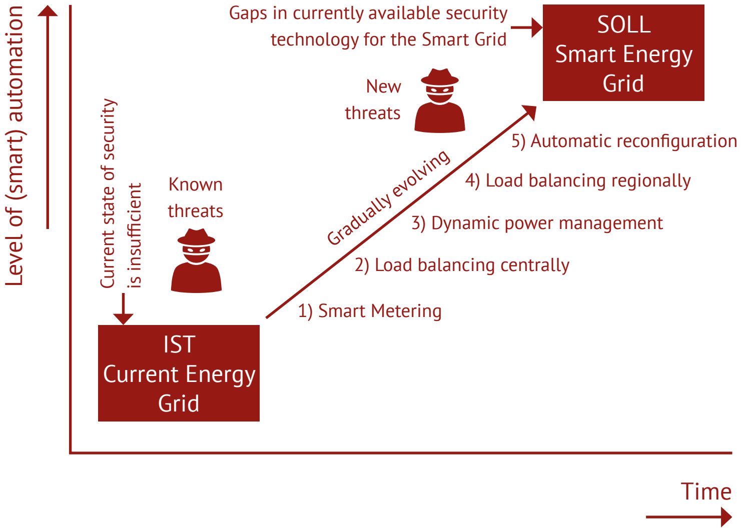
SEGRID's main objective is to enhance the protection of Smart Grids against cyber-attacks.

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 DSOs increased control to influence that flow. But the increased automation also has major consequences for the cyber security of the electricity grid. Not only does it add new routes through which cyber attackers can enter and attack the networks of DSOs, the automation also offers more possibilities to do damage to the electricity grid itself.

The Smart Grid will not come into existence overnight; it will be composed of a mix of old, even legacy, and new components. The Smart Grid can be seen 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. Within the SEGRID project the work has been focused around five concrete use cases:

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); and
5. Automatic reconfiguration of the power grid.

These five use cases reflect important steps in the developments of the Smart Grid, and will cover the most relevant security and privacy issues that will arise. The use cases are of increasing complexity and automation. This is depicted in Figure 4.



Level of (smart) automation
Gaps in currently available security technology for the Smart Grid
SOLL Smart Energy Grid
New threats
5) Automatic reconfiguration
4) Load balancing regionally
Gradually evolving
3) Dynamic power management
2) Load balancing centrally
1) Smart Metering
Current state of security is insufficient
Known threats
IST Current Energy Grid
Time

Figure 4 SEGRID storyline

SEGRID has evaluated risk assessment methodologies and developed a practical approach for assessing risk in Smart Grid developments. This RA method has been applied to the SEGRID use cases to evaluate the method and identify new threats and risks due to the introduction of these use cases. The risk assessment was used as a basis to develop the SEGRID Risk Management Methodology (SRMM) which was based on IOS/IEC 27005 with specific enhancements to make the methodology more suited for application within Smart Grids (e.g. addresses multi-stakeholder, interdependencies between stakeholders and systems, and societal impact). Based on the risk assessment a GAP analysis was performed to identify security & privacy technologies that are insufficient, or even non-existing, to address the current and future cyber-security risks. Based on the risk and GAP analysis a cyber security roadmap has been developed to guide DSOs and security research policy in required developments. SEGRID has also performed an analysis of Smart Grid security related policies and provided guidance to policy makers on improvements.

Within SEGRID work has been done on the developments of tools to support the secure design of Smart Grid architectures and software, and on technology for:

- secure and resilient systems & platforms
- secure communication protocols
- resilient communication infrastructure;
- privacy by design.

Some examples of the SEGRID developments are described in this white paper. These developments have been tested in the SEGRID Integrated Test Environment (SITE). In the last year, a cost-benefit analysis will be undertaken to provide guidance for the adoption and exploitation of the developed security solutions.

A publication of the SEGRID Project

www.segrid.eu
info@segrid.eu

P.O. Box 1416
9701 BK Groningen
The Netherlands

Acknowledgment & disclaimer

This work was funded by The European Commission in the EU FP7 SEGRID project under Framework 7 agreement 607109. The views expressed are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.