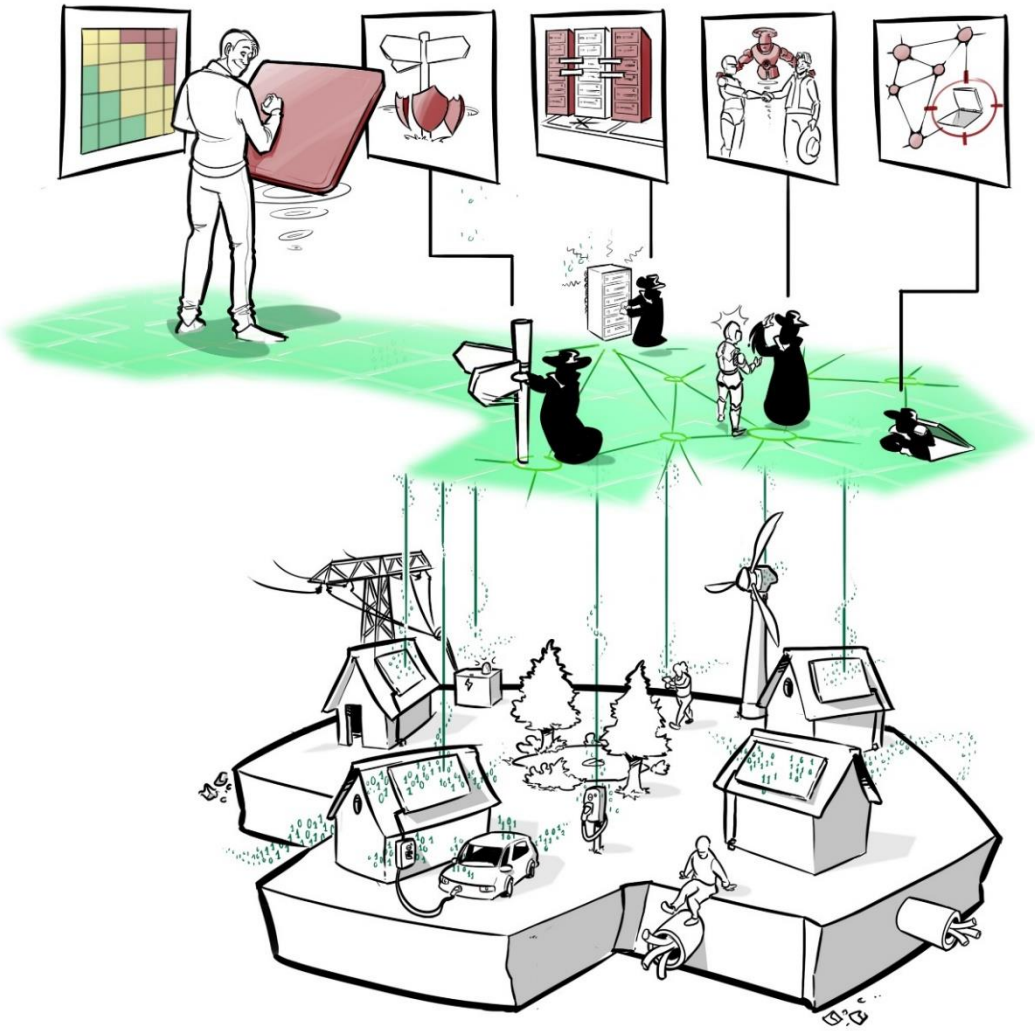
SEGRID

Security and Privacy Architecture Design (SPADE) for Smart Electricity Grids



This white paper presents SPADE, the Security and Privacy Architecture DEsign process developed during the Security for smart Electricity GRIDs (SEGRID) project. SPADE is an iterative process conceived to design, validate and evaluate use-case-specific security and privacy architectures for smart Grid systems.

List of Contributors

Marco Tiloca (RISE SICS)
Rikard Höglund (RISE SICS)
Rolf Blom (RISE SICS)
Frank Fransen (TNO)
Eric Luiijf (TNO)
Mathias Ekstedt (KTH)
Maarten Hoeve (ENCS)

Editors: Marco Tiloca (RISE SICS)

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.

Contents

List of Contributors 2
Acknowledgment & disclaimer 2
Introduction 4
Overview of the SPADE process 5
Detailed description of the SPADE process 6
SPADE Phase 1: Design 7
Walk-through of the SPADE Design phase 8
Security and privacy controls, mechanisms and technologies 10
SPADE Phase 2: Check 11
SPADE Phase 3: Evaluation 13
References 14
Appendix, SEGRID Project 15

Introduction

This document describes SPADE, the Security and Privacy Architecture DEsign process developed during the Security for smart Electricity GRIDs (SEGRID) project. SEGRID has been an EU Framework 7 security project with the objective of enhancing the protection of Smart Grids against cyber-attacks. SPADE is an iterative process conceived to design, validate and evaluate use-case-specific security and privacy architectures for smart Grid systems.

From a high-level perspective, SPADE considers three different phases, namely Design, Check and Evaluation. As shown by the high-level design flow in Figure 1, the three phases are performed in a repeated sequence while refining the temporary design, until a satisfying security and privacy architecture has been produced for the considered smart grid implementation scenario, hereafter referred as "use case".

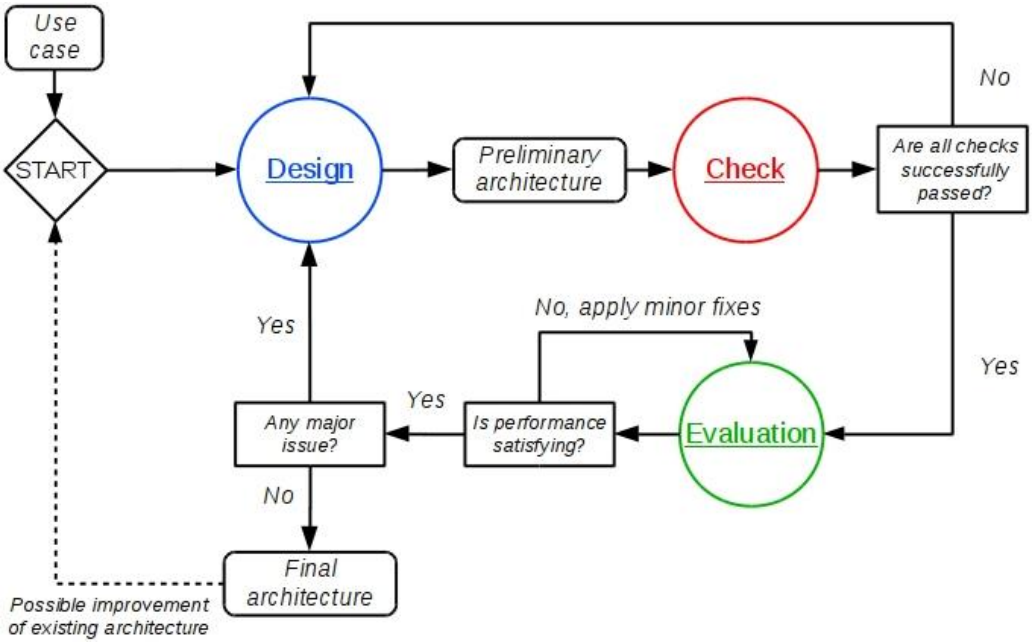


Figure 1: High-level overview of the SPADE process.

In particular, the SPADE process considers a smart grid use case as its main reference input. Then, SPADE 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. The iterative nature of SPADE makes it possible to incrementally improve an already existing security and privacy architecture, which can be provided as an overall aggregated input to the initial Design phase.

Finally, the SPADE process is essentially an instance of a more generic approach, and hence can be easily re-shaped and re-adapted to design, validate and evaluate security and privacy architectures for Information Technology(IT) systems other than smart electricity grids. Therefore, we are confident that SPADE can significantly help designers of IT systems to better ensure that security and privacy requirements are properly and conveniently achieved, from the early specification and design stages. At the same time, we believe that SPADE has been defined and adequately specialised to produce security and privacy architectures for smart grid systems.

The remainder of this document is organised as follows. Section 2 provides a high-level overview of the SPADE process, while Section 3 describes SPADE in more details, separately for the three different phases Design, Check and Evaluation. Finally, Section 4 includes references.

Overview of the SPADE process

This section provides a high-level overview of the SEGRID Security and Privacy Architecture DEsign (SPADE) process.

Intuitively, SPADE considers as main input a specific use case, its requirements as well as a list of prioritised risk factors and the security controls selected to mitigate the risk. That is, SPADE assumes that the risk assessment process over the use case has been previously completed.

Then, SPADE iterates through three distinct phases (namely Design, Check, and Evaluation) until it has produced an adequate security and privacy architecture for that use case. We refer to security and privacy architecture as to a modular composition of interconnected, possibly depending and cooperating, security and privacy controls mechanisms and technologies.

Finally, by adopting and deploying such security and privacy architecture, the use case successfully fulfils its security and privacy goals and satisfactorily addresses and mitigates the identified security threats and risk factors. In addition, despite the presence of additional security services and resulting overhead, the use case displays overall acceptable performance.

With reference to Figure 1, the three different phases Design, Check, and Evaluation are iteratively performed, until a satisfying security and privacy architecture has been produced for the considered use case.

In particular, the SPADE process starts with the Design phase, whose main goal is to produce a complete but yet temporary security and privacy architecture for the referred use case. Once it is ready, the temporary architecture is provided as input to the Check phase, whose goal is to verify that the current architecture satisfactorily fulfils the security and privacy requirements, as well as other design criteria. If such validation fails, the process moves back in order to (re)design an improved version of the security and privacy architecture. Otherwise, SPADE proceeds to the Evaluation phase, when extensive practical tests are performed and a performance analysis is carried out. This analysis may suggest performing minor fixes and tunings to achieve a better, final, security and privacy architecture ready to be deployed, or instead force the process to move back to the Design phase in case major flaws and issues have been identified.

The following Section 3 describes the SPADE process in detail and provides a thorough walk-through of the Design phase (Section 3.1), aimed at building a first preliminary security and privacy architecture. The latter is going to be validated and evaluated in the following SPADE phases Check (Section 3.2) and Evaluation (Section 3.3).The aim is to produce a final security and privacy architecture ready to be deployed.

When describing the Design phase, we also provide: i) an overview of each input considered by the SPADE process; ii) a step-by-step procedure followed during the architecture design (Section 3.1.1); and, finally, iii) a description of available security and privacy controls, mechanisms and technologies (Section 3.1.2).

Detailed description of the SPADE process

This section provides a more detailed description of the SPADE process and the three phases Design, Check and Evaluation. In particular, we refer to the diagram depicted in Figure 2. Dashed lines highlight the steps that are required to be completed before SPADE can start.

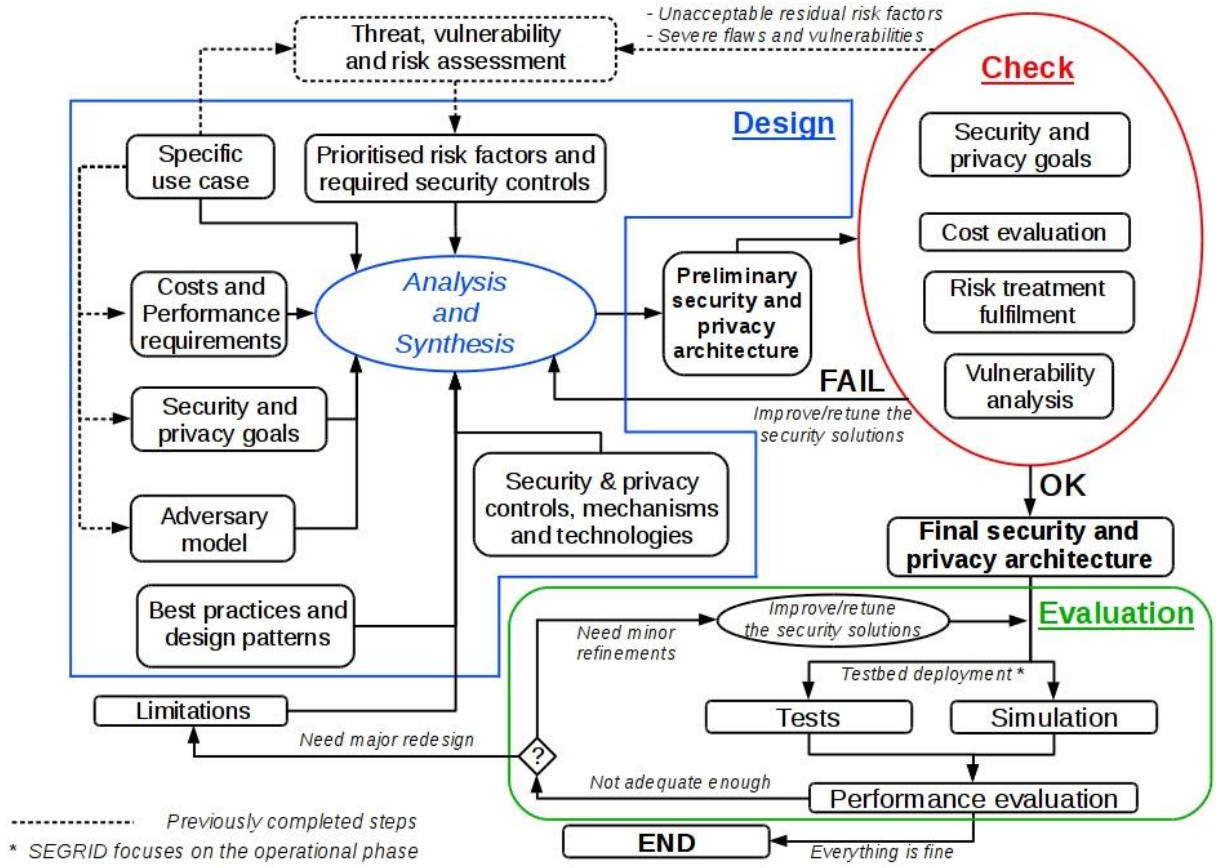


Figure 2: Detailed overview of the SPADE process.

SPADE Phase 1: Design

To produce a security and privacy architecture for a given smart grid use case, the SPADE process starts with the execution of the Design phase. In particular, the goal of the Design phase is to produce a tentative, preliminary, security and privacy architecture to be validated and evaluated in the following SPADE phases.

Specifically, the *Design* phase consists of an "Analysis and Synthesis" procedure, which takes the elements specified below as input, and produces a preliminary security and privacy architecture as output. We provide a step-by-step description of the "Analysis and Synthesis" procedure in Section 3.1.2.The SPADE Design phase considers the following inputs to perform the "Analysis and Synthesis" procedure:

- *Specific use case*. This input is a description of the smart grid use case for which a security and privacy architecture has to be produced. The use case is specified in terms of: i) functional components representing the use case system assets; ii) communication flows between the functional components to exchange instances of information assets relevant in the use case.
- *Cost and performance requirements*. This input is a description of i) the expected and maximum costs that the smart grid system is supposed to result in, even in the presence of security mechanisms and technologies; and ii) the expected and minimum performance that the smart grid system is supposed to show, even in the presence of security mechanisms and technologies. These costs and performance requirements have been previously derived by taking into account the specific smart grid use case.
- *Security and privacy goals*. This input is a description of the specific security and privacy goals that are necessary to fulfil the smart grid use case considered by the SPADE process. The security and privacy goals take into account both information assets and system assets in the use case. In particular, the privacy goals include privacy design strategies that are relevant to adopt for in the considered use case. Readers can refer to [SEGRID-D1.3] and [SEGRID-D1.4] for a list of security and privacy goals related to the five SEGRID Smart Grid use cases [SEGRID-D1.1].
- *Prioritised risk factors and required security controls*. This input has been previously produced as an outcome of a Threat Vulnerability and Risk Assessment (TVRA) process performed on the considered use case. In particular, this input specifies: i) the set of risk factors to be taken into account for the use case, together with their severity level; ii) the planned or implemented security controls and related treatment actions to consider in order to mitigate or neutralise the identified risk and fulfil the use case security and privacy requirements. A comprehensive description of the risk management process can be found in [ISO27005:2011]. Note that prioritisation of risk factors can be further supported by separate (software) tools, and by ranking security attacks according to their quantitative impact on system, application and network performances (see, e.g., [Til16]).
- *Adversary model*. This input considers the adversary able to successfully exploit the identified threats and risk. In particular, the model describes the adversary's capabilities, available resources, and assumed knowledge used to mount cyber-security attacks which put into effect the overall risk for the considered use case.
- *Security and privacy controls, mechanisms and technologies*. This input is a list of basic and compound controls, mechanisms and technologies. In particular, these can be selected, singularly adopted and/or combined in order to provide more complex and specific security solutions aimed at addressing the risk by mitigating or neutralising their effect and fulfilling the use case security and privacy requirements. The privacy controls, mechanisms and technologies include a set of

low-level Privacy Enhancement Technologies (PETs). PETs are specific methods aimed at protecting informational privacy, by eliminating or minimising personal data and hence preventing unnecessary or unwanted processing of personal data. A more detailed review of common security and privacy controls, mechanisms and technologies is reported in Section 3.1.2.

- *Best practices and design patterns*. This input is a collection of widely accepted and adopted best practices, guidelines and approaches to select, combine, deploy, configure and run the security and privacy solutions provided by means of the selected controls, mechanisms and technologies. In particular, this input includes a set of high-level *privacy design patterns*, relevant and applicable from an architectural perspective.

Walk-through of the SPADE Design phase

In this section, we provide a step-by-step description of the "Analysis and synthesis" procedure performed during the SPADE Design phase. In particular, we refer to the provided inputs depicted in Figure 2 and the description reported earlier in this section.

The "Analysis and synthesis" procedure which implements the SPADE Design phase is composed of the following four sequential steps.

Step 0 – *Consider the identified risk factors*. The first concrete step towards the specification of security and privacy solutions consists in taking into account the list of prioritised risk factors and required security controls, which have been produced as part of the previously performed Risk Assessment process. In particular, it is vital that all the highlighted risk factors are satisfactorily addressed (i.e. mitigated or neutralised) and that all the use case security and privacy requirements are fulfilled.

Typical requirements are for instance: implementation of logging functionalities; properly secured communication links; application of privacy (by design) patterns; assurance of platform security properties; support for resilient communication; robust collection, aggregation and processing of information assets; prompt detection and counteraction of intrusions and security attacks; prevention against relevant cyber-security attacks; covering of security and privacy during the different life-cycle phases, spanning from device manufacturing to device de-commissioning.

Step 1 – *Consider the specific use case*. The SPADE process considers the smart grid use case around which the security and privacy architecture will be designed, validated and evaluated. In particular, a specific scenario related to the considered use case is considered and represented as a collection of interconnected functional components with particular emphasis on the related information and communication flows.

Step 2 – *Define a trust boundary*. The goal of this step is to clearly define a trust boundary in the considered use case, in order to partition it into two different portions. That is, all the components and assets lying *above/beyond* the trust boundary can be reasonably assumed to be enough trustable and robust. Therefore, it is not required to explicitly address and guarantee their security, robustness and reliability. Note that, if similar considerations hold, it is possible to specify as lying *above/beyond* the

trust boundary also additional components responsible for providing security and privacy solutions in the considered use case. The trust boundary is established by taking into account the security and privacy goals, list of prioritised risk factors and required security controls, and the adversary model.

Step 3 – *Select the security and privacy solutions*. The goal of this step is to specify an enhanced version of the considered use case, including the security and privacy solutions necessary to make the smart grid system secure. To this end, the main starting points are the pre-defined trust boundary and the list of required security controls provided as input to the SPADE Design phase.

In particular, let us consider the prioritised risk factors and required security controls as a list of entries <*Risk*, *Treatment actions*>. Then, the security solutions to adopt are selected by taking into account costs and performance requirements, the adversary model, and the best practices and design patterns. In particular, the following procedure can be adopted.

For each risk factor in the considered list:

1. Select and consistently combine available security and privacy controls, mechanisms and technologies that are adequate to counteract and mitigate the risk factor, according to the associated treatment actions. A commented list of typical security and privacy controls, mechanisms and technologies is provided in Section 3.1.2.

2. Provide claims and considerations to justify:

    a) Why the chosen controls, mechanisms and technologies are relevant and convenient to address that risk;

    b) How the chosen controls, mechanisms and technologies relate to each other and to the original use case components;

    c) How possible interdependencies and/or conflicts between the chosen controls, mechanisms and technologies are addressed.

After all the risk factors have been considered and treated, the use case includes a set of security and privacy solutions able to address the considered prioritised risk factors. Then, a preliminary high-level validation and evaluation step is performed on the enhanced use case with respect to a set of privacy and performance requirements. If all requirements are satisfactorily fulfilled, the procedure can move forward to Step 4. Otherwise, the selection of security and privacy controls, mechanisms and technologies is revised or repeated, while paying particular attention to the risk factors that were found in need to be better addressed.

Examples of typical privacy requirements that are required to be fulfilled are: minimisation, hiding, separation, aggregation, transparency, control, and demonstration. Examples of typical performance requirements that are required to be fulfilled are: efficiency, graceful degradation, scalability, future-proof, affordability, and timeliness.

Step 4 – *Tune and refine the security solutions*. This final step of the SPADE Design phase considers the enhanced use case in which the security and privacy solutions have been integrated. Then, fine tuning and configuration of the adopted security and privacy controls, mechanisms and technologies are performed. To this end, the preliminary high-level check performed at the end of Step 3 is considered. This results in the preliminary security and privacy architecture for the considered use case to be provided as input to the SPADE Check phase.

Security and privacy controls, mechanisms and technologies

This section lists and briefly describes several security and privacy controls, mechanisms and technologies that are likely to be considered for selection during the SPADE Design phase. In particular, this document does not refer to any specific protocols, approaches or algorithms whose selections and low-level configurations are out of scope.

Trusted third parties (TTPs): This category includes all entities that enable or ease secure interactions between parties. Relevant examples of TTPs include certification authorities, trust anchors, group membership managers, and access control and/or authorisation enforcers. As a particular case, TTPs play a main role as components of Public Key Infrastructures (PKIs).

Monitoring entities and intrusion detection systems: This category includes logical and/or physical mechanism and technologies which are responsible for monitoring the smart grid system, in order to detect and report anomalies, misbehaviours and intrusions.

Key manager entities: This category includes all entities responsible for managing, generating, providing, revoking and (re)distributing cryptographic material. Key manager entities may need to tightly cooperate with dedicated supportive entities, such as intrusion detection systems and TTPs acting as group membership managers.

Redundancy infrastructures: This category includes approaches enabling logical and/or physical redundancy of smart grid entities and functionalities. This practically consists in replicating physical entities or logical/software, and makes it possible to achieve a number of benefits, such as: 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; and iv) practical avoidance of single points of failure (SPoFs).

Security life-cycle management interfaces: This category includes controls and mechanisms allowing system designers, operators and other relevant stakeholders to securely and reliably manage the smart grid system during the different life-cycle phases, ranging from manufacturing to the decommissioning of system components. This comprises, among other things: i) the secure provisioning, distribution, and revocation of cryptographic keys; ii) the management of public certificates; iii) the issue, management,

and revocation of user credentials; iv) the establishment, maintenance and termination of secure communication sessions; and v) the issue, management, enforcement and revocation of any other possible specific permissions, such as the ones related to specific resource access.

Aggregation entities: This category refers to logical and physical entities responsible for collecting single information instances (e.g. data report, management information, status feedback) from individual entities, aggregate them for analysis and storage, and securely forward them to possible different entitled entities.

Logging entities: This category refers to dedicated entities and/or functionalities responsible for logging events and activities in the smart grid system. This includes producing, recording and maintaining information related to the evolution of the system values and attributes over time.

Management console/interface: This category comprises workstation and terminal points that allow administrative or technical authorised personnel to monitor, control, maintain and administer the smart grid system as a whole as well as focusing on single components.

Transparency and Control User Interfaces.: This category comprises 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 category includes all the technologies and mechanisms that can be employed to fulfil platform security requirements on (embedded) devices in the smart grid systems. Platform-security requirements include, for instance: i) trust bootstrapping of operating systems; ii) hardware platform verification; and iii) separation, non-interference and safe execution of software processes.

Secure communication protocols: This category comprises the available security protocols to protect information exchange within the smart grid systems, at different layers of the communication stack. Typical security requirements to be fulfilled include, for instance, confidentiality, message integrity and authentication, and replay protection. Secure communication protocols typically rely on additional supporting entities, including TTPs and key manager entities.

Resilient communication infrastructure: This category includes available technologies and mechanisms that make it possible to quickly and effectively preserve communication availability and performance, in the presence of accidental malfunctioning and/or security attacks. This includes, for instance, the ability to establish new traffic routes on demand, and to isolate suspected sources of malevolent network traffic.

Secure resource discovery: This category refers to available mechanisms that allow any entity 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. Typically, the information and key material necessary to securely interact with entities for secure resource discovery have to be provided far in advance, even at manufacturing time, through out-of-band means.

SPADE Phase 2: Check

The Check-phase takes as input the preliminary security and privacy architecture, in order to verify that it adequately satisfies a pre-defined set of criteria. In particular, the Check-phase considers the following aspects, in order to validate the preliminary architecture and to determine whether the design is ready for the following performance evaluation:

- *Security and privacy goals*. The preliminary security and privacy architecture must be such that, in the presence of the specified security and privacy solutions, all the security and privacy goals for the considered use case are satisfactorily fulfilled.

- *Cost evaluation*. The preliminary security and privacy architecture must be such that, in the presence of its security and privacy services, the expected and maximum costs for the considered use case is not exceeded.

- *Risk treatment fulfilment*. The preliminary security and privacy architecture must be such that, in the presence of its security and privacy services: i) all the prioritised risk factors specified as input to the SPADE *Design* phase for the considered use case are neutralised or satisfactorily mitigated, i.e. the residual risk is acceptable; ii) all the security and privacy requirements for the considered use case are satisfactorily fulfilled; and iii) no new risk factors are introduced in the considered use case. To check that the considered security solutions effectively reduce the identified risk, it is possible to rely on (software) tools such as [Til16].Such tools make it possible to quantitatively evaluate the residual impact of security attacks on system, application and network performance using a scenario which includes the selected security controls, mechanisms and technologies.

- *Vulnerability analysis*. The preliminary security and privacy architecture must be such that the introduced security and privacy solutions: i) are not affected by any vulnerability that can be realistically exploited in a reasonable amount of time by the considered class of adversary in order to compromise their effectiveness and efficiency; and ii) do not introduce any vulnerability to the considered use case that can be realistically exploited in a reasonable amount of time by the considered class of adversary [Bru17].
  To this end, one system-wide tool for vulnerability assessment and analysis that has been used extensively in SEGRID is securiCAD [Sec17]. securiCAD is developed by the company Foreseeti and stems from previous research reported under the umbrella of the Cyber Security Modelling Language (CySeMoL) [Hol15]. In short, securiCAD makes it possible to construct a model of the studied Information and Communication Technology (ICT) infrastructure, manually or by means of automatic import. The resulting model is then used to generate and execute probabilistic cyber-attack/defence graphs to predict time-to-compromise distributions for cyber-attacks related to all the components in the model.
  Tools such as securiCAD can be used during this Check-phase to support the risk treatment fulfilment and vulnerability analysis. If vulnerabilities exploitable in a reasonable amount of time are found on the assessed preliminary security and privacy architecture, the latter should not be further considered for additional checks and later evaluation phases. Instead, the same security and privacy architecture should go through a proper re-design aimed at making the identified vulnerabilities practically infeasible to exploit in a reasonable amount of time.

If not all the validation tests are successfully passed, the SPADE process moves back to the Design-phase. That is, the preliminary security and privacy architecture is redesigned, by improving, replacing, and reconfiguring the adopted security and privacy solutions. In principle, if the validation procedure highlights a number of unacceptable residual risk factors or severe flaws and vulnerabilities, it may be necessary to seriously take into account the validation outcome. One may perform an extensive full TVRA on the smart grid use case at hand one more time before going through the Design-phase once again. When a new version of the security and privacy architecture is ready, it is provided as input to the Check-phase for a new validation process.

If the preliminary security and privacy architecture successfully passes all the validation tests, it can be considered as a final security and privacy architecture[1]. In such a case, the final architecture is provided as input to the next SPADE phase Evaluation (see Section 3.3 below).

SPADE Phase 3: Evaluation

The Evaluation-phase takes as input the final security and privacy architecture from the Check-phase in order to evaluate it in terms of performance. To this end, one is expected to rely on (a combination of) experimental tests with real hardware facilities and/or simulation software and tools. To assess that the considered security and privacy solutions reduce the identified risk also in an efficient way, i.e. their impact on performance is sustainable and affordable, it is possible to rely on (software) tools (e.g. [Til16]).Such tools may consider also the selected security and privacy controls, mechanisms and technologies in the simulated scenario.

A technical report including performance evaluation results is expected to be produced at the end of the Evaluation-phase. Then, three different alternatives are possible:

- The technical report includes overall good results but highlights the possibility of performance improvements. In such a case, it is required to proceed with minor improvements and/or retuning the security and privacy solutions. Thereafter, one can repeat the performance evaluation.
- The technical report includes several severe flaws and limitations. In such a case, the SPADE process moves back to the Design-phase. Major changes are required to be done to the current architecture to take the reported limitations into account. A new preliminary security and privacy architecture is to be produced which can be evaluated in a new instance of the Check-phase.
- The technical report does not include any flaws and limitations, or suggests any particularly significant improvement. In such a case, the SPADE process is completed, and the evaluated final security and privacy architecture is eligible for being implemented and deployed in the considered smart grid use case.

[1] The specific criteria according to which this validation process is performed are out of the scope of the SEGRID project.

References

[Bru17] M. Bruijne et al., “Towards a new cyber threat actor typology”, Delft University of Technology – Faculty of Technology, Policy and Management, 2017.

[Hol15] H. Holm et al., “P2CySeMoL: Predictive, Probabilistic Cyber Security Modeling Language”, IEEE Transactions on Dependable and Secure Computing, 12(6), pp. 626–639, 2015.

[ISO27005:2011] ISO/IEC 27005:2011, "Information technology – Security techniques – Information security risk management", 2011.

[SEGRID-D1.1] SEGRID deliverable D1.1, "Architecture and design for use cases", 2015. Available at https://segrid.eu/results

[SEGRID-D1.3] SEGRID deliverable D1.3, "First report on the security & privacy goals", 2015. Available at https://segrid.eu/results

[SEGRID-D1.4] SEGRID deliverable D1.4, "Final report on the security & privacy goals", 2016. Available at https://segrid.eu/results

[Sec17] Cyber Threat Modeling and Risk Management - www.foreseeti.com

[Til16] M. Tiloca, A. Stagkopoulou and G. Dini, "Performance and Security Evaluation of SDN Networks in OmNET++/INET", OmNET++ Community Summit 2016, pp. 9 – 14, Brno (Czech Republic), 2016.

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 1.

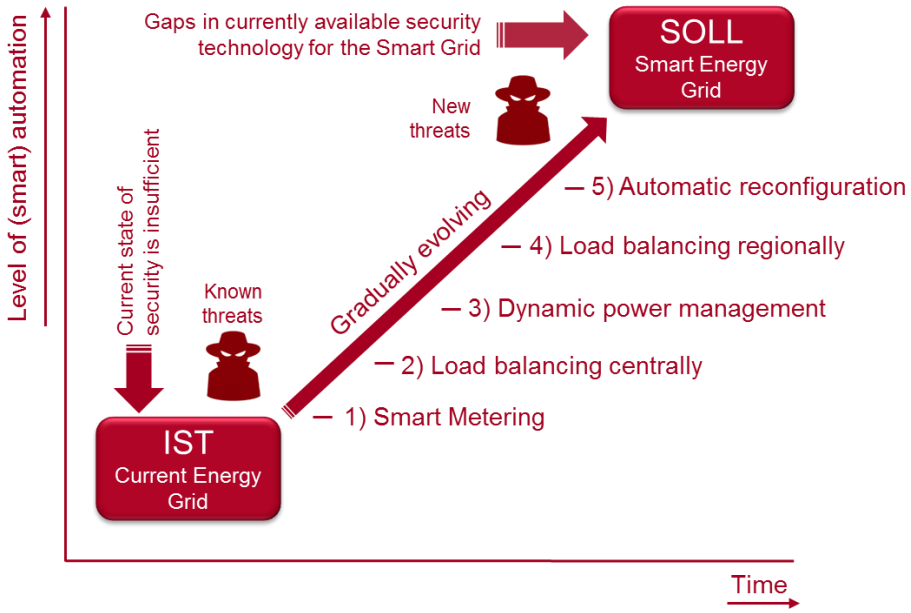


Figure 1 SEGRID storyline

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.