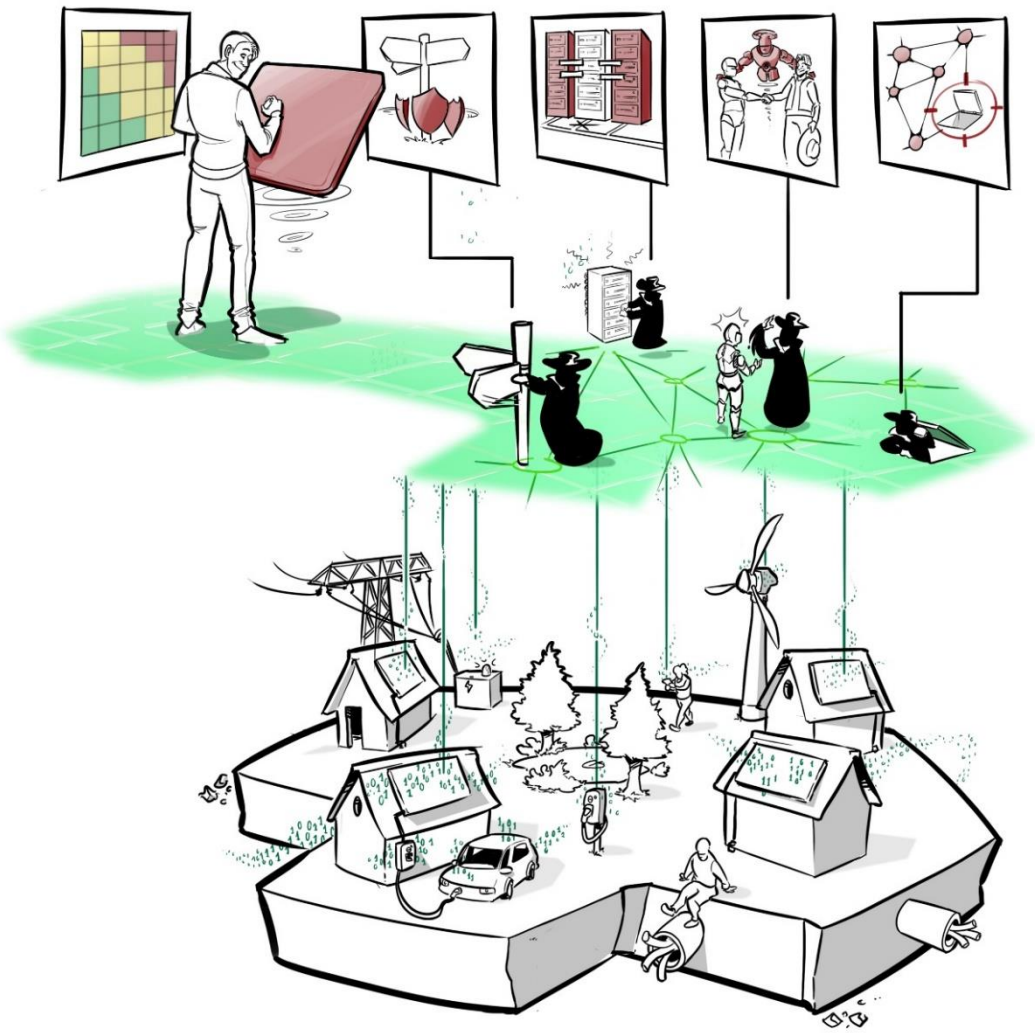
SEGRID

SEGRID Risk Management Methodology (SRMM)



This white paper describes an enhanced Risk Management approach for smart grids, the 'SEGRID Risk Management Methodology (SRMM)'. The SRMM is meant to be applied in the context of smart grids, e.g. by risk managers and security officers of Distribution System Operators (DSOs) and Transport System Operators (TSOs). This white paper provides improved insights in risk in smart grid environments. SRMM was developed by the 'Security for smart Electricity GRIDs (SEGRID)' project. SEGRID has been an EU Framework 7 security project (2014-2017) with the objective of enhancing the protection of smart grids against cyber-attacks.

List of Contributors

Judith Rossebø (ABB)
Gunnar Björkman (ABB)
Johan Rambi (Alliander)
Rick van Dijk (Alliander)
Nuno Medeiros (EDP)
Maarten Hoeve (ENCS)
Mathias Ekstedt (KTH)
Frank Fransen (TNO)
Reinder Wolthuis (TNO)
Eric Luiijf (TNO)

Editors: Reinder Wolthuis & Frank Fransen (TNO)
Version: 2017
Classification: Public

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.

1 Contents

List of Contributors 2
Acknowledgment & disclaimer 2
1 Contents 3
2 Introduction 5
3 Step 1: Context establishment 8
3.1 Summary 8
3.2 Guidance 8
3.2.1 The threat and risk assessment team 8
3.2.2 Define the basic criteria 9
3.2.3 Risk Evaluation Criteria 11
3.2.4 Define the RA scope 11
3.2.5 Break down the model in SRMM scopes 12
3.2.6 Define obligations and expectations 12
3.2.7 Link obligations to internal and external expectations 13
3.2.8 Identify personal data 13
4 Step 2: Impact assessment 14
4.1 Summary 14
4.2 Guidance 14
4.2.1 Impact assessment 14
4.2.2 Obligation impact assessment 14
4.2.3 Personal data impact assessment 15
4.2.4 Define Focus of Interest (FoI) 15
5 Step 3: Threat and vulnerability assessment 16
5.1 Summary 16
5.2 Guidance 16
5.2.1 Assessment of threats related to personal data 18
6 Step 4: Risk estimation and prioritisation 19
6.1 Summary 19
6.2 Guidance 19
6.2.1 Attack likelihood estimation 19
6.2.2 Attack impact estimation 20

6.2.3 Obligation risks 22
6.2.4 Prioritising the risks 22
7 Step 5: Risk Treatment 24
7.1 Summary 24
7.2 Guidance 24
8 Step 6: Risk acceptance 25
8.1 Summary 25
8.2 Guidance 25
9 Step 7: Document and communicate the results and monitor and review risks 26
9.1 Summary 26
9.2 Guidance 26
References 27
Appendix 1 – The SEGRID Project 29
Appendix 2 – SRMM background 31
Appendix 3 – Supporting MS Excel tooling 33

2 Introduction

The Smart Grid is a system-of-systems involving a conglomerate of stakeholders, each representing their own interests. 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) with more intelligence will be placed in distribution substations. The increased automation will provide a better view of how electricity flows to the medium and low voltage grids, provide grid operators with increased control to influence that flow and include more automatic functions, i.e. self-healing networks. But the increased automation also has major consequences for the cyber security of the electricity grid. Not only does it add new attack vectors through which cyber attackers can enter and attack the networks of grid operators, the automation itself also offers other possibilities to do damage to the electricity grid itself.

It is important to protect the smart grid; the Smart Grid is a significant part of the critical infrastructure and new regulation such as the directive on Network and information systems (NIS) [NIS] and the new European Commission data protection regulation, General Data Protection Regulation (GDPR) [GDPR] is mandating protective measures.

One of the first things that needs to be done is implementing a structured approach to risk management, to identify, analyse, evaluate and treat the risks to ensure that the Smart Grid is sufficiently protected. Risk assessment (RA) in smart grids is challenging. The threat and vulnerability landscape is increasing in complexity, both due to the emergence of new threat sources and threat actors capable of exploiting vulnerabilities. It is increasingly observed that the attacker's capability and motivation plays a significant role in both the likelihood of cyber-attacks being carried out and the impact on the infrastructure.

This document provides a description of the full version (including guidance) of the SEGRID Risk Management (SRMM) methodology. The SRMM is designed for application in the smart grid domain and builds on the experiences of the SEGRID partners with risk assessment methodologies applied to the energy sector. The SRMM provides stakeholders in the smart grid domain, such as DSOs, with a structured and in-depth methodology for smart grid risk management that allows them to better understand the potential threats and vulnerabilities, manage the risks and take the necessary measures to contain and mitigate these risks. The SRMM is based on the ISO/IEC 27005 framework [ISO27005], but tailored for application in the smart grid domain. The SRMM contains three innovative elements that specifically fulfil the needs of smart grid risk assessment (see also Appendix 2 for a more detailed background of the SRMM)). Firstly, many smart grid use cases involve multiple stakeholders, and the methodology specifically addresses this issue by providing insight in dependency, responsibility and the propagation of risks through value chains. This allows smart grid stakeholders to iteratively evaluate the risks introduced by smart grids through a multi-stakeholder impact assessment, with risk dependency, responsibility and propagation in mind. Secondly, since smart grids are part of the critical infrastructure, the methodology also integrates a practical approach for societal impact assessment. Any disturbance of the power supply has a very significant impact on society, making it a critical for smart grid stakeholders to be able to analyse risks with critical impact. Thirdly, the methodology applies an enhanced version of the ETSI Threat Vulnerability and Risk Analysis (TVRA) methodology to include an assessment of the

motivation and capability of the attacker in the risk estimation step. This is relevant because we expect attackers that target smart grids to have higher motivation and capabilities than the average attacker.

The SRMM is conducted according to the seven steps depicted in **Figure 1**. These seven steps are:

1. Context establishment
    a. Define criteria necessary for performing the risk assessment and managing the risks.
    b. Identify the scope, boundaries and context of the Risk Assessment (RA), including stakeholders, processes, assets, and existing security controls. The assets need to be linked with stakeholder processes.
    c. Identify the SRMM scopes and sub scopes. These are demarcations based on organisational responsibilities. Each SRMM (sub)scope has an identifiable responsible person.
    d. Define SRMM obligations and expectations and verify if they match between scopes
    e. Link external obligations with internal and external expectations
    f. If personal data is included in the RA scope, conduct the pre-assessment step of the Data Protection Impact Assessment (DPIA) [DPIA] and if needed, the full DPIA, and ensure that the DPIA and SRMM are aligned.

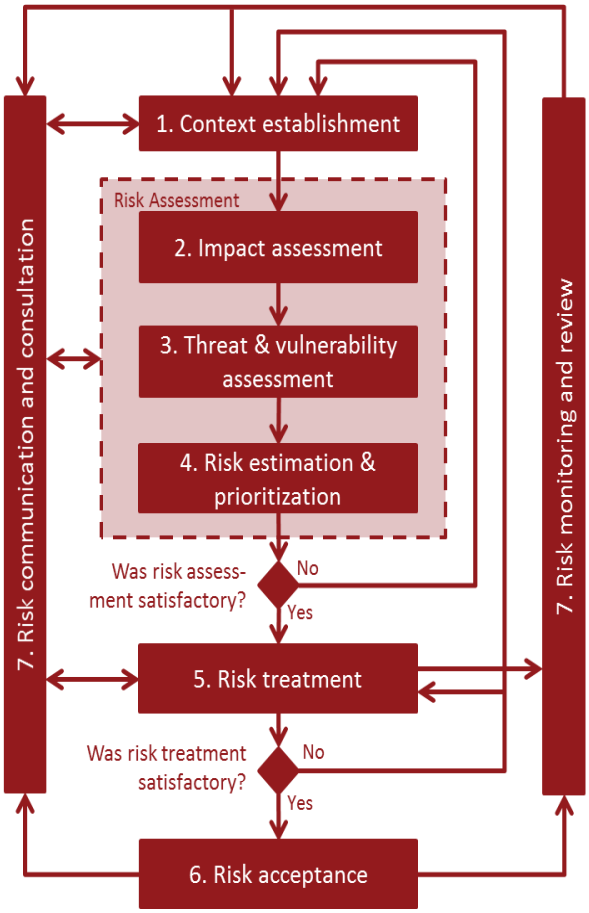


Figure 1 SEGRID Risk Management methodology

2. Impact assessment
    a. Assess impact on obligations in each scope
    b. Assess personal data impact using the DPIA, if personal data is in the RA scope.
3. Threat and vulnerability assessment - identify threat sources, threat actors, vulnerabilities and threat scenarios.
4. Risk estimation and prioritisation - estimate the risks in terms of likelihood and impact and relate these to obligations for prioritisation 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. Structure the report along the Obligations and Expectations.
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 SRMM scope as reference.
7. Document and communicate results and monitor and review risks (reiterating the assessment when needed). Communicate the likelihood that obligations are not fulfilled to relevant other stakeholders.

The steps will be further elaborated in the following chapters, including some guidance to perform these steps.

3 Step 1: Context establishment

3.1 Summary

Input: All information necessary to conduct the risk assessment and the environment of relevance to establishing the context.

Action: Establish the team responsible for conducting the assessment and managing the process. Establish the context for the risk assessment. This includes setting the criteria necessary for performing the risk assessment and managing the risks, and identifying the Risk Assessment (RA) scope. Defining the RA scope includes establishing the boundaries for what is in scope and what is not, defining the stakeholder processes and assets, and linking assets with stakeholder processes. Identification of assets includes identifying the existing security controls in place, in order to assess the effectiveness of these controls during the threat and vulnerability step. Identify whether personal data is included in the RA scope. Also, the SRMM scopes are defined including obligations and expectations for each scope.

Output: The team identified for conducting the assessment, the identified basic criteria and the description of the RA scope.

3.2 Guidance

3.2.1 The threat and risk assessment team

A dedicated multidisciplinary team needs to be selected for conducting the threat and risk assessment and managing the process. This team should include as a minimum a facilitator who is familiar with the SRMM and its (MS Excel-based) tools, and include cyber security/ICT experts, smart grid system architecture and operations experts as well as experts with technical knowledge about the stakeholder systems in the RA scope. If personal data is involved, then a personal data expert/officer needs to be a member of the team. The roles and responsibilities of the team members need to be clearly defined, e.g., who is leading the risk assessment, who is responsible for recording the results from each activity, etc.

The team performing the threat and risk assessment needs to have a strong background and knowledge about the RA scope and access to relevant expertise concerning cyber security and privacy. It is recommended to establish a team consisting of representatives that include the following expertise:

- Vulnerability, threat and risk assessment
- Industrial automation and control system security
- Electrical power generation and distribution systems, in particular expertise in the areas that are included in the RA scope
- Privacy and data protection
- IT and network security
- Systems management
- Legal

3.2.2 Define the basic criteria

During the context establishment, the following needs to be defined by the dedicated risk assessment team:

- Stakeholder Impact Criteria – Stakeholder impact categories and the definition, for each of those, of the impact levels;
- Risk Scales –
    - Consequence (impact) scales – in the SRMM, these are based on the stakeholder impact analysis, which is then used in the Threat & Vulnerability Risk Assessment (TVRA) spreadsheet;
    - Likelihood scales – in the SRMM, these have already been defined for use in the TVRA spreadsheet;
- Risk Levels (which are given by a function of likelihood and consequence) – in the SRMM, these have already been defined for use in the TVRA spreadsheet, using a risk matrix. These risk levels form a basis for defining the risk evaluation criteria;
- Risk Evaluation Criteria – the risk evaluation criteria can be used to set priorities for the risk treatment. The risk evaluation criteria provide the terms of reference for evaluating the criticality of the identified risks;
- Risk Acceptance Criteria – defines the risk acceptance criteria for accepting risks and identifying the acceptable level of residual risk.

In general, an organisation should establish criteria for the whole organisation (e.g. based on the corporate risk requirements). Then, it is still possible to deviate per application of the risk assessment method; however, these deviations should be carefully documented.

Guidance for establishing each of these criteria is given in the following.

3.2.2.1 Stakeholder Impact Criteria

Business impact is, by definition, the impact that a compromise has on the operations or efficiency of the organisation or on customers or citizens [HMGIS109]. The RA team needs to define the stakeholder specific impact categories and the impact levels for each category.

To support this activity, SEGRID provides a template for specifying the impact categories and scale to be used in the impact assessment. The templates and results of risk assessment (in MS Excel) are provided as addenda to this report. The tools are listed and described Appendix 3.

Below, we provide some general guidance for defining the impact categories (note that each category will be detailed differently for different stakeholders).

For each obligation, the obligation impact will need to be assessed on a risk impact classification scale from 1 (Very low) to 5 (Highly Critical). Impact classification scales are therefore defined for each impact category. The following are examples of consequences that may be considered when defining the stakeholder impact categories and scales:

- Reduction or loss of energy supply at one site/regional area or multiple sites/regions simultaneously;
- Injury or death of employees;
- Injury or death of persons in the community;
- Damage to equipment;

- Environmental damage;
- Violation of regulatory requirements;
- Product contamination;
- Criminal or civil legal liabilities;
- Loss of proprietary or confidential information;
- Loss of brand image or customer confidence;
- Economic loss.

While ideally the scales should be defined in such a way so that they can be in some sense comparable, there are some challenges. For example, impact categories for the Safety category will address risks to individuals' safety, with High and Very High categories addressing damages of loss of one life and multiple deaths respectively due to a compromise. On the other hand, damages defined in the legal and regulatory compliance category will address the impact of legal claims on the organisation due to a compromise. While not comparable, clearly, in both cases, it is relevant to avoid incidents leading to compromise resulting in High and Very high impact in both cases. For each stakeholder and for each category, the range of limits that can be tolerated needs to be defined in terms of Very low to Very high.

The RA team should agree on the impact levels per category.

- A stakeholder shall define the impact categories that are important from his/her perspective;
- For each category, defining the range of incidents resulting in impact for the stakeholder, from least critical to most critical, grouping these stepwise into five levels from Very low to Very high;
- The activity shall be based on existing knowledge, previous assessments, documented incidents with business impact, etc.

The results should be recorded in the template for impact and threat assessment, see Appendix 3.

3.2.2.2 Consequence and Likelihood scales

Likelihood definition

For a threat to be exploitable, there should be at least one threat source/threat actor possessing the required attack potential to attack one or more vulnerabilities of an asset. Therefore, we need to assess the likelihood that the threat source/threat actor succeeds in enacting the threat and subsequently cause an unwanted incident. The estimation of likelihood considers both the likelihood that a threat is enacted and the likelihood that there are one or more vulnerabilities that enable the threat to be enacted. In the SRMM the likelihood range is divided into five levels: Very Unlikely, Unlikely, Possible, Likely and Very Likely. This is described in more detail below.

Risk Levels and the Risk Matrix

Regarding the risk scales, the risk level is the magnitude of a risk, expressed in terms of the combination of consequences and their likelihood [ISO27005]. Risk levels are established based on a function of likelihood and consequence and shall be documented using a risk matrix with likelihood on one axis and consequence (i.e., obligation impact in the SRMM) on the other axis.

The risk levels and the risk matrix in the SRMM tooling (see Appendix 3) are based on input from the different SEGRID project partners. These risk levels form a basis for defining the risk evaluation criteria.

3.2.3 Risk Evaluation Criteria

The risk evaluation criteria are used to specify priorities for risk treatment. As such, the risk evaluation criteria provide the terms of reference for evaluating the criticality of the risks. These may be defined differently for different types of obligations. Typically, the maximum acceptable impact when an obligation is not fulfilled is determined, which can be used to define the focus of Interest (FoI) in step 2.

Another criterion that should be defined is at what impact level the Society will be impacted. We express this as a Societal Impact Magnitude (SIM) value, which is explained in paragraph 6.2.2.1.

3.2.4 Define the RA scope

During this step of the risk assessment, a comprehensive description of the RA scope is established, where the stakeholders are identified, and their assets documented.

The steps taken in the RA scope definition are:

- Model the RA scope using the Smart Grid Coordination Group (SGCG) Smart Grid Architectural Model (SGAM) and define assets
- Break down the model in SRMM scopes and sub scopes and assign assets to scopes
- Define obligations and expectations between scopes and within one scope, between sub scopes
- Identify personal (privacy sensitive) data

3.2.4.1 Modelling the RA scope using the SGAM

In this sub-step, assets and components are represented according to the SGAM interoperability layers [SGAM12], see in Figure 2 . This process is described in Chapter 3 of “SEGRID Architecture and design for use cases” [SEGRID D1.1].

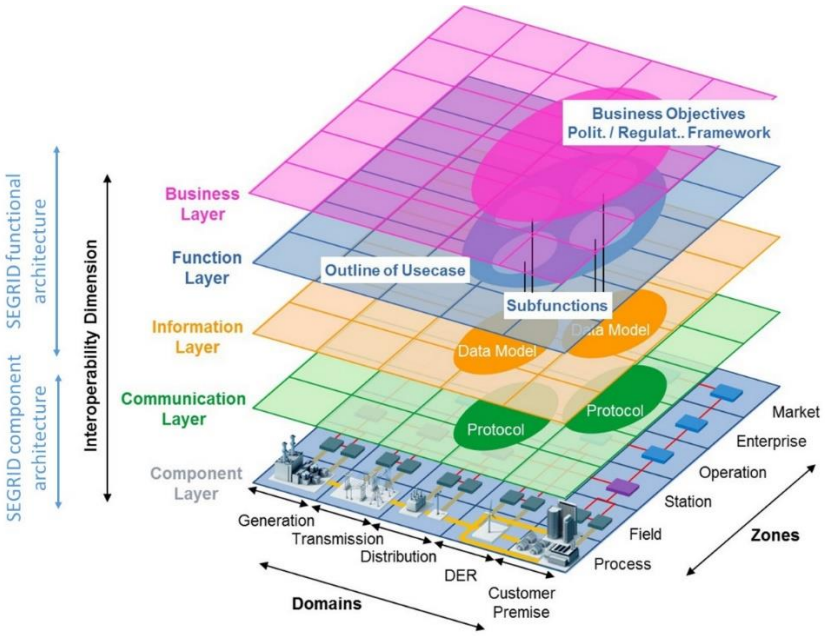


Figure 2 SGAM framework (source: [SGAM12])

The scope and boundaries of the RA scope are identified. The involved actors are identified, and the RA scope is modelled as diagrams using the SGAM.

The scenarios (flows of execution within the RA scope) are identified and described step-by-step. This includes modelling the flows involving personal data.

The SGAM model contains the relevant assets for the RA; the RA team needs to define these assets, the elements of the system (e.g., the advanced metering infrastructure (AMI), smart meters, substation RTU, etc.), which need to be protected, and which represent any value.

First, the assets as elements of the system are identified, based on the description of the RA scope. Asset as element of a system is a broad term. The definition of assets is important. What kind of assets are defined? The number of assets may be very large, if one zooms in at a deeper level. From the perspective of system components, one can distinguish probably hundreds of elements. But the point is that it should be transparent and clear. The IS1-methodology [HMGIS109] therefore tries to distinguish only the most important assets.

3.2.5 Break down the model in SRMM scopes

During this step, the SRMM scopes for the RA scope that is assessed are defined; SRMM scope on the highest level typically is the scope of one stakeholder. It is important to notice that SRMM scoping is scoping of responsibilities rather than functional or technical scoping. Each asset that is relevant in the RA scope, including information assets, is assigned to exactly one SRMM (sub)scope. If a scope contains many assets, it is recommended to group them into sub-scopes (e.g. a business process, as defined in the previous paragraph, or a department). Then we define ownership for each scope (it is important that also for sub-scopes, clear ownership can be defined): a scope has exactly one 'scope owner' that is responsible for this scope. The results of these steps are documented in the worksheet that is called 'Step 1 scoping' in the impact and threat assessment worksheet, see Appendix 3.

3.2.6 Define obligations and expectations

The next step is to define the obligations that each scope has to other scopes and are specific for the RA scope that is assessed. These should be formulated as precisely as possible. Then we define the expectations that each scope has from other scopes and are specific for the RA scope that is assessed. These steps are documented in the worksheet called 'Step 1 oblig. & expect.' in the impact and threat assessment worksheet.

When these steps have been done, the impact and threat assessment worksheet contain: the SRMM scopes, the scope owners, the obligations and expectations for each scope.

At this stage, we can then discuss whether each obligation that is put upon a scope is related to an expectation of another scope. This currently is a manual inspection; the tool does not automatically do a check on these relations. But by performing this step, we already can establish if there are any discrepancies in the mutual expectations of the stakeholders.

See **Figure 3** for a hypothetical example how this can be pictured.

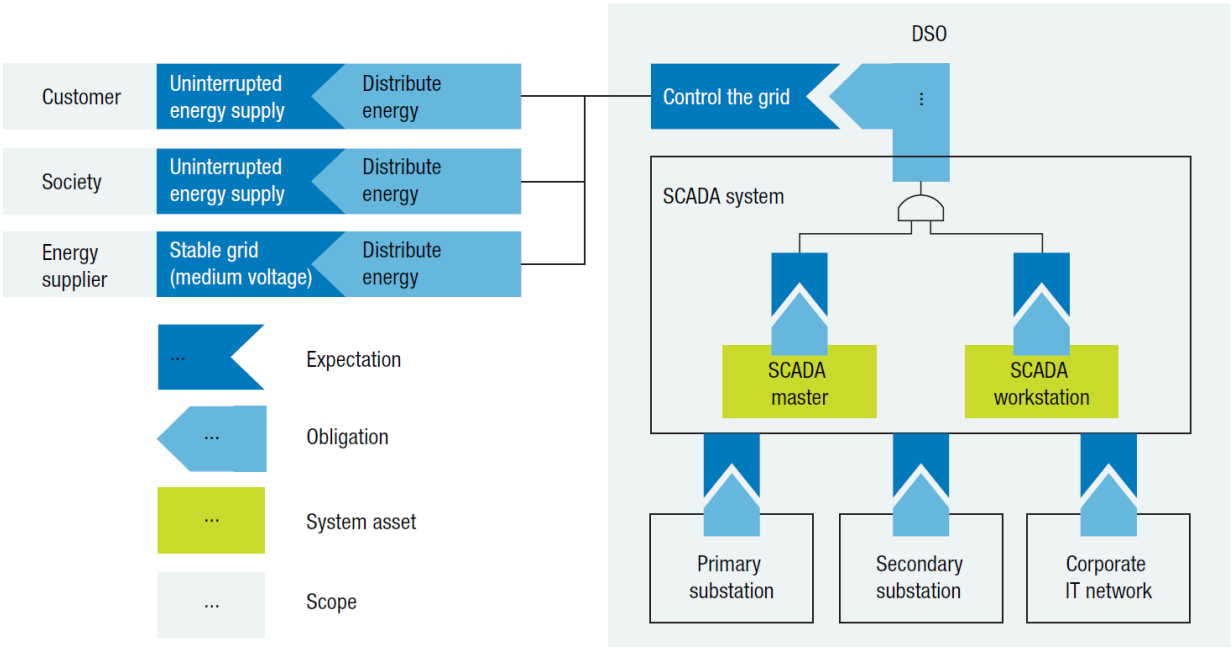


Figure 3 – Example of the DSO scope (source: [IEEE2017])

The scope 'DSO' has an owner that is the DSO director. It also has three obligations, one to the scope Customer ('Distribute energy') one to the scope 'Society' ('Distribute energy') and one to the scope Energy supplier ('Distribute energy'). The scope DSO has one internal expectation ('Control the grid') on the SCADA system. To fulfil the resulting internal obligation ('Control the grid'), the SCADA system has two Internal expectations to the SCADA master and the SCADA workstation. But the SCADA system also has internal expectations on the sub scopes Primary substation, Secondary substation and Corporate IT network.

3.2.7 Link obligations to internal and external expectations

In the simplest case, an external obligation of a scope is only fulfilled by its assets and the scope is not divided in sub scopes. But if the scope is divided in sub scopes and an obligation is depending on expectations on these internal sub scopes and on external expectations, a link should be made between obligation and in- and external expectations. See **Figure 3** for an example of such internal sub scopes, in which the scope 'DSO' is divided into four sub scopes (SCADA system, Primary substation, Secondary substation and Corporate IT network) and the sub scope SCADA system is divided in the sub scopes SCADA master and SCADA workstation.

3.2.8 Identify personal data

If during the definition of the RA scope it is identified that personal data is included in the RA scope, then a data protection impact assessment [DPIA] needs to be performed. It is recommended to perform the personal data impact assessment as described in [DPIA] and using the template as provided in [DPIAtemplate]. It is strongly advised for the SRMM team to collaborate with the DPIA team on this e.g., regarding the SGAM modelling and the analysis of the RA scope.

4 Step 2: Impact assessment

4.1 Summary

Input: All information from step 1:

- The information about the RA scope;
- The breakdown in SRMM scopes, the obligations and expectations of the SRMM scopes;
- Stakeholder impact categories and scales;
- Hazardous scenarios and societal impact scales for societal impact;
- The result of the analysis on presence of personal data.

Action: For each obligation, assess the maximum impact for a scope owner if the obligation is not fulfilled, using the impact categories and scales. The impact is assessed per impact category and the maximum obligation impact is the highest category impact. If a DPIA has to be conducted, synchronise between the obligation impact assessment and DPIA task 5.1.

Output: Identification of the potential maximum obligation impacts for each scope. Identification of the Focus of Interest (FoI), for which the next steps in the SRMM will be taken. If personal data is involved, output of the DPIA.

4.2 Guidance

4.2.1 Impact assessment

In this step the obligation impact is assessed for each scope and if personal data is involved, a Data Privacy Impact Assessment (DPIA) is conducted.

The impact assessment is carried out in a workshop with cyber security/ICT experts, as well as smart grid experts and people representing business departments. In the case that personal data is involved, a Personal Data Protection Expert/Officer needs to be involved.

4.2.2 Obligation impact assessment

An obligation is directly related to the external stakeholder to whom the obligation is contracted and the task of fulfilling this obligation is the responsibility of the scope owner. For each stakeholder obligation, the maximum impact (worst case scenario) if the obligation is not fulfilled is defined in qualitative terms of 'very low' to 'very high' for each impact category. Existing impact analyses, such as the National Electric Sector Cybersecurity Organisation Resource (NESCOR) impact analyses [NESCOR], should be considered as input to the 'obligation impact' assessment. In the obligation impact analysis, there is no distinction between the aspects of confidentiality, integrity and availability. The analysis purely focusses on the resulting potential impact if the obligation is not fulfilled.

Within each SRMM scope and for each obligation, define the maximum impact if the obligation is not fulfilled per impact category. The maximum obligation impact is the highest category impact; this is the impact that will be used in the TVRA spreadsheet.

For this step, we use the impact assessment table in the template for impact and threat assessment (see Appendix 3), and the result can be documented in the same template, in the worksheet that is called *'Step2 Obligation impact'*.

4.2.3 Personal data impact assessment

For RA scopes involving personal data, the DPIA is used to perform an *Assessment of Severity/Impact* as a task in *Step 5 – Data Protection Risk Assessment'*. In DPIA *"Task 5.1 – Assessment of Severity/Impact"* the Severity/Impact of the Primary Assets (i.e. personal data and processing operations dealing with personal data) is determined, based on the *Level of Identification* of the Primary Assets and *Prejudicial Effect* when a threat becomes real.

The results of SRMM step 2 can be used for the DPIA task 5.1, and vice versa. Moreover, as the DPIA template is specifically focussed on personal data and privacy aspects, it is recommended to align the SRMM with the results from DPIA template task 5.1 at this point.

4.2.4 Define Focus of Interest (FoI)

Based on the output of the previous step, and the risk evaluation criteria that were defined in step 1, the FoI is determined. The FoI contains all obligations for which the potential impact, when not fulfilled, exceeds the maximum impact as defined in the risk evaluation criteria.

5 Step 3: Threat and vulnerability assessment

In the previous step, the Focus of Interest (FoI) was identified as output from the Impact Assessment. The FoI identifies the obligations that, when not fulfilled due to a security breach, have critical impact on the stakeholder scope. The scope of the threat and vulnerability assessment is therefore narrowed down to the obligations that are critical for the stakeholder processes.

5.1 Summary

Input: The information about the RA scope from step 1, the identified existing controls in the RA scope, and the Focus of Interest (FoI) from step 2.

Action: Based on the stakeholder impact assessment, for assets that are linked to the obligations in the FoI, identify attack paths, threat attack scenarios. Identify threat sources and threat actors, and assess the threat level.

Output: List of potential threat scenarios. Overview of expected threat sources and threat actor combinations, with their threat level based on the anticipated capability and motivation.

5.2 Guidance

Identifying threat attack scenarios

Threat attack scenarios are identified during this step. For this, it is important to understand the component architecture of the RA scope and the potential attacks and attack paths (to compromising assets in the FoI).

Identification of threat scenarios is left to expertise of the person or team performing the threat assessment. Several methods exist to assist in the identification of threat scenarios and attack paths. Potential methods include:

- *Threat lists / attack libraries*
  Lists of known threats and attacks can be used by the analysist to identify threat scenario. In addition, these lists are useful to make sure that the assessment is done thoroughly. Example of a threat list for smart grids is [Luiijf2012]. A common (general) attack library is CAPEC[1] from MITRE. Do note that CAPEC contains a large number of detailed attack descriptions.
- *STRIDE*
  STRIDE is a method for structuring Threat Modelling developed by Microsoft [Shostack2014]. It is the abbreviation for six threat categories: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege. The method was designed for threat modelling software development, and is therefore too limited for application in the context of smart grids.
  Note that the ETSI TVRA [TVRA2011] also contains a similar kind of threat categorisations structured in a threat tree with the branches: Interception, Manipulation (with leaves Masquerade ("spoofing"), Loss of information, Corruption of information, Unauthorised access, and Forgery), Repudiation, and Denial of service.
- *Attack Trees*
  Attack trees are graphs showing how an asset might be attacked. Attack trees provide a structured approach to identify, analyse and document threats and attack paths. Tree-based risk

[1] https://capec.mitre.org/

assessment methods (e.g. fault tree, attack tree, event tree, vulnerability tree and various combinations of the above) as well as other risk assessment methods based on directed graphs are the most widespread risk assessment methods cited in the literature [Cherdantseva16].

- *Cyber Kill Chain*
  The Cyber Kill Chain is initially developed by Lockheed Martin and is based on the military kill chain [Lockheed Martin]. The Cyber Kill Chain consists of seven steps that can help an analyst understand adversary's tactics, techniques and procedures (TTP), in particularly the so-called Advance Persistent Threats (APTs) type of attacks. As attacks in Industrial Control Systems (ICS) may consist of a jump from the IT domain (e.g. enterprise network) to the ICS domain, the SANS institute devised an ICS cyber kill chain [ICS killchain]. The ICS cyber kill chain consists of two stages:
  - stage 1 – contains basically the seven attack steps of the Cyber Kill Chain
  - stage 2 – contains an additional five attack steps in the ICS domain

  The ICS cyber kill chain can be used during a threat assessment to identify the necessary steps that an attacker needs perform to achieve a particular goal
- *SecuriCAD*
  SecuriCAD is a commercial system-wide automated vulnerability assessment tool that was based on CySeMoL [Sommestad13], developed by KTH. SecuriCAD was developed by the spin-off company Foreseeti. It can be used to identify threat scenarios and attack paths. As securiCAD requires a rather detailed description of the configuration of a system in order to compute the attack paths, we recommend the use of such a tool only for detailed threat and risk assessment (when a detailed design of the infrastructure is available).

Threat source and threat actor analysis

To facilitate the stakeholder impact analysis, key threat sources are identified and assessed. The key threat sources are individuals or groups of individuals that would see a gain in compromising the assets and are identified based on available threat assessment information for example from CERTS, such as The Industrial Control Systems Cyber Emergency Response Team [ICS-CERT] or other authorities.

An example, excerpt of such a table, based on a SEGRID threat source/threat actor analysis can be found in Table 1.

The threat source and threat actor analysis is not only important for the risk estimation step, but is useful for analysing the different mitigations needed to counter the threats as well. In the case that a threat source and the threat actor are one and the same, this cell can be left blank.

Table 1 IS1-based threat source and threat actor analysis

Threat Actor ID	Threat Source name	Description (and rationale)	property	Capability	Motivation	Threat level	Source(of information about threat source)	Threat actors (employed)
Ex 1	Organised Crime Group	The aim is to gain financially from causing outages	C	4	3	Severe	Business Blackout report	hackers
			I	4	5	Critical	Business Blackout report	hackers
			A	4	4	Severe	Business Blackout report	hackers
Ex 2	Hacktivists	libertarianism, anti-establishment ideology, freedom of information and anti-surveillance, environmentalism, and anti-capitalism	C	2	4	Low	media	N/A
			I	3	4	Moderate	media	N/A
			A	3	4	Moderate	media	N/A
Ex 3	Unidentified group	motivated to cause significant disruption of an entire region in a coordinated cyber-attack	C	3	3	Moderate	ICS-CERT (attack on Ukrainian DSOs)	group of hackers/ programmers
			I	5	5	Critical	ICS-CERT (attack on Ukrainian DSOs)	group of hackers/programmers
			A	5	5	Critical	ICS-CERT (attack on Ukrainian DSOs)	group of hackers/ programmers

The process for completing the table is as follows. Identify each threat source that is applicable to the threat, vulnerability and risk assessment and create a new row in the table as follows:

- The name given to the identified threat source that is applicable to a threat should be entered in the first column, with a description and rational given in the second column.
- If the threat source described is known or expected to employ threat actors, these are entered in the last column. In the case that a threat source and the threat actor are one and the same, this cell is left blank.
- For each property, C, I, A (confidentiality, integrity, availability respectively) discuss the threat source Capability and threat source Motivation respectively and determine the level for each. The scales given in the IS1 standard for Threat Source Capability and Threat Source Priority [HMGIS109] can be used as a reference. In the spreadsheet, Capability and Motivation are then combined to obtain the Threat level that this threat source/threat actor presents. If knowledge about the threat source is obtained externally, it is good practice to record the source (of information about threat source) in the Source column.

A template for such a table is included as tab '*Step 2 Threat Actor Analysis'* in the Impact and Threat Actor Assessment Worksheet, see Appendix 3.

5.2.1 Assessment of threats related to personal data

The assessment of threats to personal data also includes very different threats compared to cyber security threat assessment, such as threats related to the regulatory requirements. Therefore, it is important to align or collaborate on performing the assessment of cyber security threats against personal data with the threat assessment tasks done in the DPIA for the RA scope.

6 Step 4: Risk estimation and prioritisation

6.1 Summary

Input: The information about the RA scope from step 1, the results of the impact assessment from step 2 and the results of the threat assessment step 3. Information from other stakeholders on which expectations exist, about the probability that these expectations will not be fulfilled (or if this information is missing, an estimation of this probability).

Action: For each threat scenario, estimate the likelihood to obtain the obligation risks. The risks should be identified and prioritised against the risk evaluation criteria and the stakeholder objectives.

Output: A list of risks prioritised according to the risk evaluation criteria. Identification of the critical risks as input to the risk treatment step.

6.2 Guidance

During the workshop for conducting this step, for each obligation from Step 2 in the focus of interest, all threats identified in Step 3 are analysed.

The risk estimation is carried out using the Threat & Vulnerability Risk Assessment (TVRA) spreadsheet tool; see for the list of tools Appendix 3.

Based on an understanding of the threat attack scenarios and the potential attacks and attack paths on the functional architectures, for each threat, the obligations that are affected are determined and the likelihood is estimated in the excel tool by filling all the relevant fields.

The risk for the threat is then calculated by multiplying the likelihood with the highest impact of the obligations that are affected by the threat (using the impact and threat actor assessment sheet). The method is supported by an excel-based tool which automates the risk estimation step.

6.2.1 Attack likelihood estimation

The TVRA includes an estimated likelihood that a potential attack will be successful. To estimate the likelihood of attack, there are several steps. First, the attack potential is estimated and mapped to the vulnerability rating. The vulnerability rating is an indication of the effort required to perform the attack. This is then combined with the threat level to arrive at the likelihood of attack.

6.2.1.1 Estimating the attack potential to obtain the vulnerability rating

The attack potential is estimated based on the Common Methodology for Information Technology Security Evaluation (CEM) [CEM]. With the CEM, the difficulty for the attacker of mounting an attack is rated based on five factors: time, experience, knowledge, opportunity and equipment. For the attack scenario, these five factors are assessed and combined as shown top left in Figure 4. The resulting attack potential rating is a weighted sum of these factors, which indicates how difficult it would be to carry out the attack. The attack potential rating is then mapped to a vulnerability rating of between Basic, and Beyond High based on the numerical value of the attack potential. The vulnerability rating is an indication of the effort required to perform the attack.

6.2.1.2 Estimating the threat level

For a threat to exist, there should be at least one threat source/threat actor possessing the required attack potential to attack one or more vulnerabilities of an asset. The TVRA excel-based tool includes the

Threat Level obtained during the threat source and threat actor analysis (described in the previous step) as part of the likelihood estimation. The Threat Level is a function of threat source capability and threat source motivation.

6.2.1.3 Combing the vulnerability rating with the threat level to obtain the likelihood estimation

The Threat Level is combined with the Vulnerability Rating to obtain the likelihood estimation as illustrated in Figure 4. Likelihood is a function of the vulnerability rating obtained from the attack potential rating and the threat level from the threat source and threat actor analysis. For each threat scenario, the highest Threat Level is taken from the threat source and threat actor analysis performed in Step 3 'Threat Assessment' of the method. Since the Threat Level in SRMM is determined per information security property (i.e. confidentiality, integrity and availability), it is necessary to consider what security property is breached by the threat scenario.

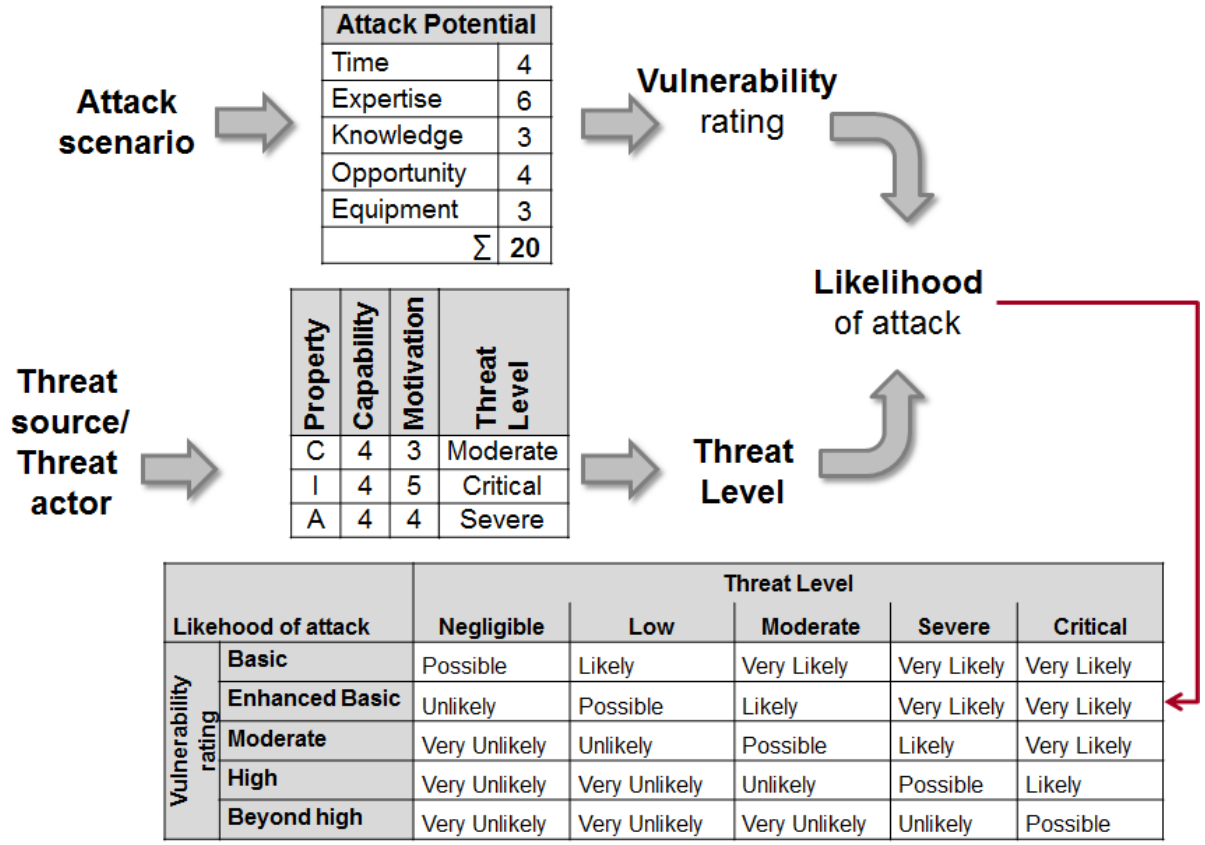


Figure 4 Estimation of the likelihood of an attack scenario

6.2.2 Attack impact estimation

The impact is derived from the impact assessment of Step 2. A threat is related to an asset, which is part of a (sub)scope, which has obligations to other scopes. If a threat becomes reality, it should be examined which obligations of the (sub)scope cannot be fulfilled. The impact for a threat is the highest obligation impact of these obligations.

A specific case of the attack impact estimation is when the threat could cause major power outages, as this will have impact on society. In that case the societal impact estimation approach, described in the next section, can be used as a practical approach to determine the extent of the societal impact. If the societal impact is higher than a predefined level as defined in step 1, we assume that the obligation to society will be impacted.

6.2.2.1 Societal impact estimation

In SRMM the stakeholder 'Society' has been introduced to include an assessment of the potential societal impact of a power outage. Typically, one of the obligations towards society is a stable and uninterrupted electricity supply. To estimate the impact when this obligation is not fulfilled, i.e. when a threat could cause a power outage / electricity blackout, Societal Impact Magnitude (SIM) is used mapped to a scale from 1 (Very low) to 5 (Very high), see Figure 5.

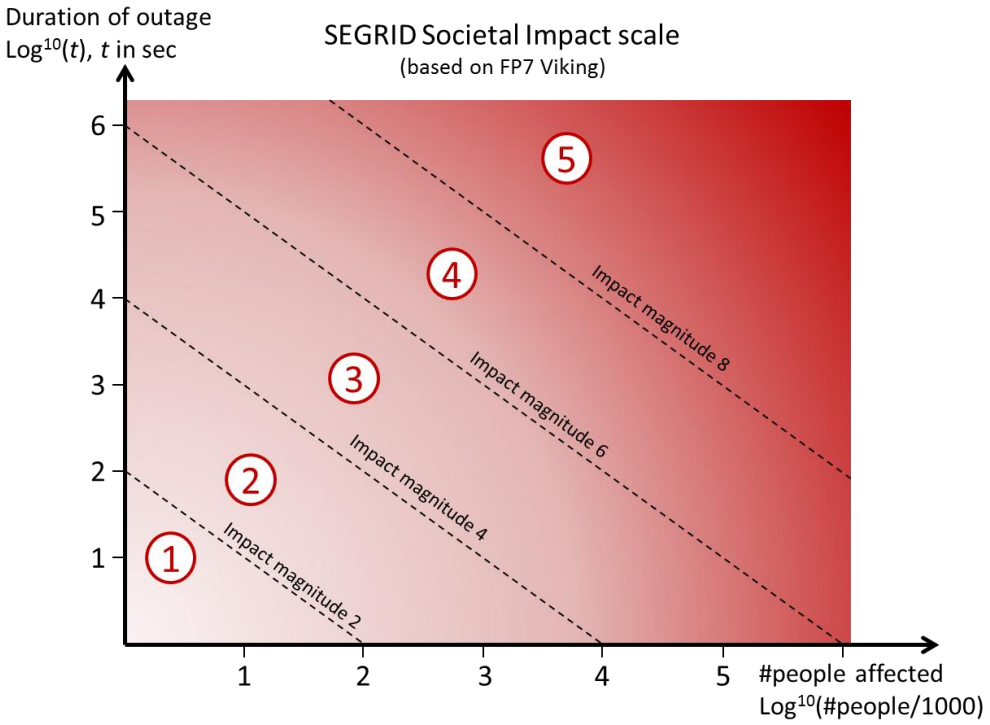


Figure 5 SEGRID Societal Impact scale**.**

SIM is determined based on the potential scale of an incident in terms of *duration* and *number of people affected*[2]:

$$Social\ Impact\ Magnitude = \mathrm{Log}_{10}(\mathrm{A}_{\mathrm{people}} * \mathrm{A}_{\mathrm{length}}) = \mathrm{Log}_{10}(\mathrm{A}_{\mathrm{people}}) + \mathrm{Log}_{10}(\mathrm{A}_{\mathrm{length}})$$

where

$\mathrm{A}_{\mathrm{length}} = \mathrm{Average\ Disturbance\ Length\ (in\ seconds)}$

[2] Note that the number of people affected is different and typically higher than the number of customers affected.

$$A_{people} = \text{Number of impacted people } /1000$$

The definition of A_{people} is the number of impacted people /1000. The reason for the division by 1000 is to create similarities with the Richter Magnitude Scale, used for measuring earthquakes. The similarities with the Richter Magnitude Scale are designed to give an intuitive feeling for the scale of the societal disturbance but should not be over-emphasized.

In the figure below the application of the SIM in SRMM is depicted.

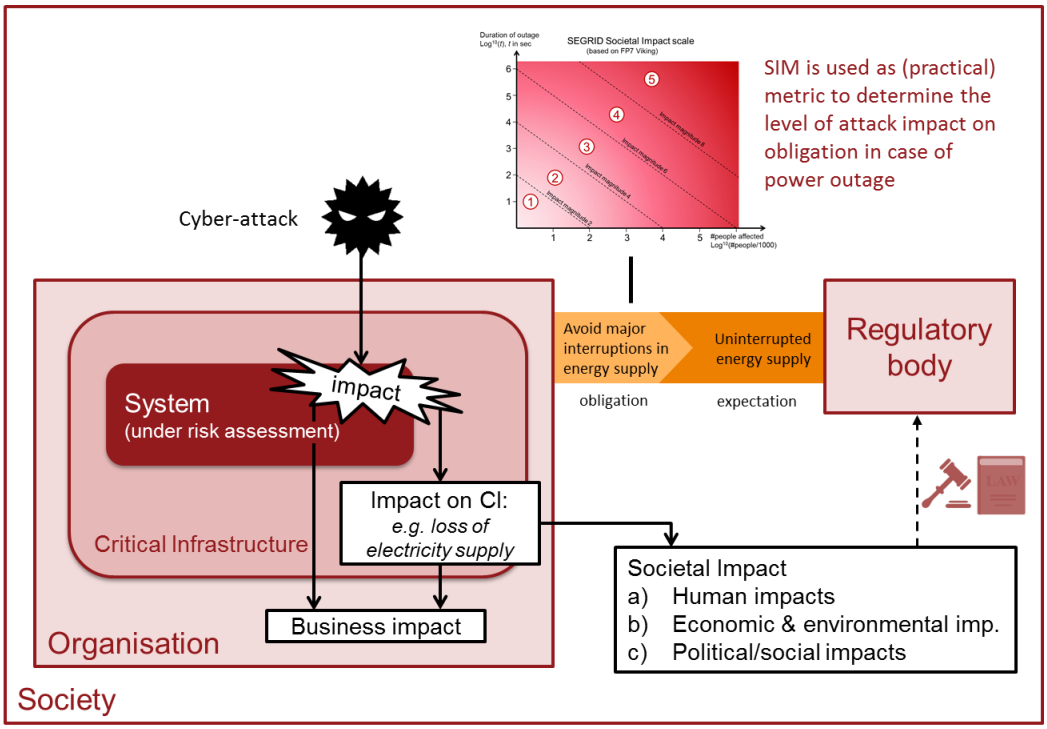


Figure 6. Depiction of the application of SIM in SRMM.

6.2.3 Obligation risks

The risk for each obligation is estimated by considering all the risks (established in the previous step) that affect the obligation and combine them with the external risks. The external risks are established by multiplying the likelihood that an external expectation is not fulfilled with the maximum impact that an obligation is not fulfilled. The maximum impact can be looked up in the impact and threat assessment sheet and the likelihood should have been communicated by the stakeholder on which the expectation is set. If information on this likelihood is missing, the RA team has to estimate it.

6.2.4 Prioritising the risks

During this step the risks are prioritised against the risk evaluation criteria that were defined during the Context establishment step. The risks to obligations with risk level 4 (Critical) or 5 (Highly critical) are prioritised for risk treatment.

For RA scopes involving personal data, the risk estimation and prioritisation of the cyber security related threats involving personal data should be aligned with the identified risks to Primary Assets in the DPIA.

7 Step 5: Risk Treatment

7.1 Summary

Input: The list of risks prioritised according to the risk evaluation criteria, identifying the critical risks that need to be treated in relation to the threat scenarios leading to those risks. If personal data is in scope, the list of Personal Data Protection Targets of the DPIA needs to be considered.

Action: Select controls to reduce, retain, avoid or share the risks. Define a risk treatment plan.

Output: A risk treatment plan and a list of the residual risks.

7.2 Guidance

This step involves defining a risk treatment plan. Risk treatment has to be done by the person or team performing the threat assessment, complemented by a person that is familiar with the responsibilities and budgets of the stakeholder. The resulting risk treatment plan and residual risks still have to be accepted by persons having the proper authority to do so (risk owners), in the next step - risk acceptance.

The list of prioritised risks has to be analysed, taking into account the risk evaluation criteria. For each risk, an assessment has to be made to either:

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

The risk reduction step will involve a gap analysis on controls and technical measures to determine which controls and technical measures are needed to reduce risk but are missing today. For these missing controls, budget indications have to be provided and an implementation roadmap has to be defined. The Security and Privacy Architecture DEsign (SPADE)[SPADE] methodology can also be used in this step.

For RA scopes involving personal data, the identified controls to treat the risks related to (cyber security related threats against) personal data should be aligned with the List of Personal Data Protection Targets of the DPIA. Possibly, the risk treatment steps may be collaboratively performed.

8 Step 6: Risk acceptance

8.1 Summary

Input: The risk treatment plan and the list of residual risks. The pre-defined risk acceptance criteria.

Action: Evaluate the risk treatment plan and the residual risks against the pre-defined risk acceptance criteria. Assess the acceptability of the plan and provide justification for those residual risks that do not meet the pre-defined risk acceptance criteria.

Output: A list of accepted (residual) risks with justification for those that do not meet the pre-defined risk acceptance criteria.

8.2 Guidance

This step will have to be done by each individual stakeholder. Risk acceptance has to be done by persons having the proper authority to do so (risk owners), which usually is related to the potential impact that a risk can induce. The risk owner has to verify whether the necessary budget is available to implement the required controls, whether the proposed planning to implement controls is acceptable in relation to the risks and whether the residual risks match the pre-defined risk acceptance criteria.

If all checks are positive, then the risk treatment plan and residual risks can be accepted, and the implementation of controls can start. The risk owner has to track the implementation on progress and results. If there are issues, the risk treatment plan has to be revised by taking the previous step again (risk treatment).

Use the ownership that is defined for each scope (see worksheet *'Step1 scoping'* in the impact and threat assessment sheet) to clearly assign the responsible party that has to accept each risk.

For RA scopes involving personal data, the results of SRMM *'Step 6. Risk acceptance'* need to be mapped to and aligned with the DPIA *'tasks 6.3 - Final Resolution'*.

9 Step 7: Document and communicate the results and monitor and review risks

9.1 Summary

Input: The risk assessment results, risk treatment plan, accepted risks and all information obtained about the risks during the risk management activities.

Action: Share the information about the risks with relevant internal parties. Review the results and discuss plans for improvement, if needed. Determine when the process should be re-iterated. Share the probability that obligations to another scope cannot be fulfilled with that scope, so they can use this information in their risk assessment.

Output: Documented risks, risk treatment plans and risk acceptance decisions. Continuation of the monitoring and review of the risks and recommendations for when to update the process.

9.2 Guidance

Ideally this process is managed by a risk manager that involves other relevant people where necessary. All risk assessment results, risk treatment plans, and risk acceptance decisions have to be stored safely. Preferably, there is a central risk register in which (residual) risks are registered so they can be monitored. If personal data is included in the RA scope, it is important that the documented results of the SRMM risk management process is shared with and aligned with the documented results of the DPIA. Risk treatment plans and (residual) risks have to be reviewed on a regular basis and re-assessed if needed. The risk management process and associated tooling has to be evaluated regularly, and updated if necessary. The probability that an obligation to another scope cannot be fulfilled would ideally be communicated to that other scope. They can use this information in their risk assessment (as probability that their expectation on another scope will not be fulfilled), thereby making the risk assessment a multi stakeholder risk assessment in which the risk progresses through the value chain.

References

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, September 2012, Version 3.1, Revision 4. Also published as: ISO/IEC 18045. Available at: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R4.pdf.

[Cherdantseva16] Cherdantseva et al. A review of cyber security risk assessment methods for SCADA systems. Journal of Computers and security 56. 2016. P. 1–27.

[DPIA] Smart grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the smart grid Environment, DPIA Editorial Team Draft version 1.7, September, 2017.

[DPIAtemplate] http://ec.europa.eu/energy/en/content/dpia-template-smart-grid-and-smart-metering-systems.

[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 April 2016, Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679.

[HMGIS109] HMG IA Standard No. 1, Technical Risk Assessment, Issue No: 3.51, October, 2009.

[ICS-CERT] Industrial Control Systems Cyber Emergency Response Team, https://ics-cert.us-cert.gov/.

[ICSkillchain] Michael J. Assante and Robert M. Lee "The Industrial Control System Cyber Kill Chain"; SANS Institute; October 2015, Available at: https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297.

[IEEE2017] 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.

[ISO27005] International Organisation for Standardization: ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management (second edition), 2011.

[Lockheed Martin] Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin; "Intelligence - Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains"; Lockheed Martin; 2011, Available at: http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

[Luiijf2012] Work Package 1.2, Threat Analysis Expert Group on the security and resilience of Communication networks and Information systems for smart grids; 14 March 2012.

[NESCOR] Nat'l Electric Sector Cybersecurity Org. Resource, Electrical Sector Failure Scenarios and Impact Analyses, v1.0, NESCOR Technical Working Group 1, 2013.

[Netbeheer] Netbeheer Nederland, http://www.netbeheernederland.nl/, 2013.

[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. Available at:http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:32016L1148&from=EN.

[SGAM12] CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture, November 2012.

[SGIS14] CEN-CENELEC-ETSI smart grid Coordination Group Final Report – smart grid Information Security, December 2014.

[Shostack2014] Adam Shostack; "Threat Modeling: Designing for Security"; April 2014; ISBN: 978-1-118-80999-0.

[Sommestad13] Sommestad, T. E. (2013). The cyber security modeling language: A tool for assessing the vulnerability of enterprise system architectures. IEEE Systems Journal, 7(3), 363-373.

[SPADE] Security & Privacy Architecture Design,

[TVRA2011] ETSI TISPAN; Methods and Protocols; Method and proforma for Threat, Risk, Vulnerability Analysis, ETSI TS 102 165-1 V4.2.3 (2011-03). Available at: http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf.

[TVRA2017] ETSI TISPAN; Methods and Protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA), ETSI TS 102 165-1 V5.2.3 (2017-10). Available at: http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf.

[Wolthuis11] 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.

Appendix 1 – The 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 7.

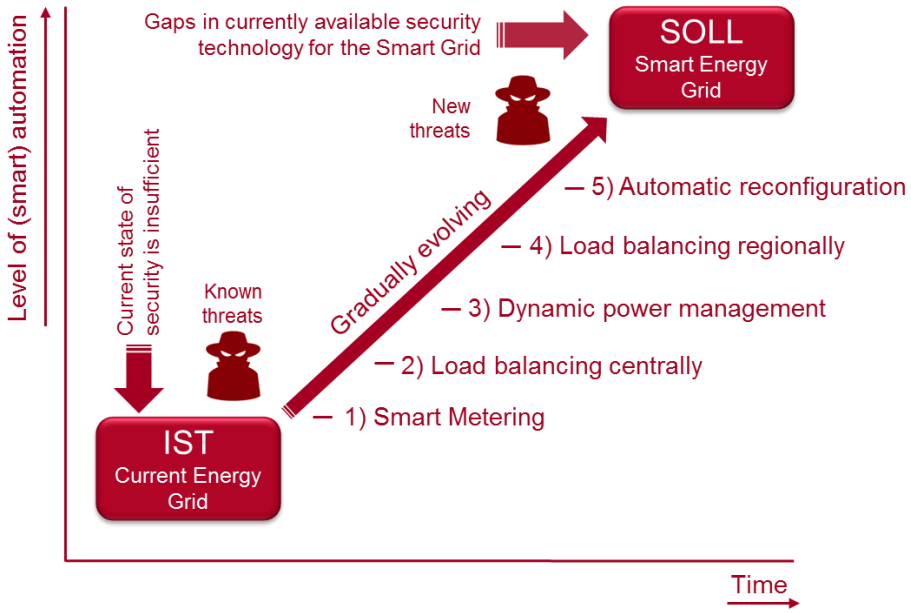


Figure 7 SEGRID storyline

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.

Appendix 2 – SRMM background

Risk assessment (RA) in Smart Grids is challenging. The threat and vulnerability landscape is increasing in complexity, both due to the emergence of new threat sources and threat actors capable of exploiting vulnerabilities. It is increasingly observed that the attacker's capability and motivation plays an important role in both the likelihood of cyber-attacks being carried out and the impact on the infrastructure. The Smart Grid is a system-of-systems involving a conglomerate of stakeholders, each representing their own interests and with different perceptions of the risks. Furthermore, the Smart Grid is an important part of the critical infrastructure. This means that a structured approach to risk management is needed to identify, analyse, evaluate and treat the risks to ensure that the Smart Grid is sufficiently protected.

One of the SEGRID project goals was to evaluate current risk assessment methods and further develop enhanced risk-assessment and risk-management approaches tailored for application to smart grids. First, a set of requirements was established and used to evaluate the existing risk-assessment methods. Second, based on this evaluation and practical insights into application of risk-assessment methods from the SEGRID partners, several methods were selected to serve as the basis for further enhancements to create a risk assessment and risk management method tailored for smart grids. We now refer to this method as the SEGRID Risk Management Methodology (SRMM).

Brief descriptions are given below of the methodologies that formed the basis for the SRMM.

- HMG *IA Standard No. 1 (IS1)*
  The HMG IA Standard No. 1 (IS1) [HMGIS109], was developed as the UK government's technical risk assessment methodology. Netbeheer NL [Netbeheer] 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. The method includes support for graphical modelling standardized to the interoperability layers of the smart grid architecture model (SGAM) [SGAM12].

- *ISO/IEC 27005*
  The ISO/IEC 27005 standard [ISO27005] provides a framework for information security risk management. The risk management process includes context establishment, risk assessment, risk treatment, risk communication, consultation, monitoring and review.

- *Network Risk Management (NRM)*
  NRM [Wolthuis11] 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 business interests. The SRMM integrates elements from NRM to provide insight on dependencies and responsibilities between systems and/or stakeholders in a system-of-systems environment. This enables further enhancement of the multi-stakeholder view of the smart grid domain. In particular, this concerns the understanding of the responsibilities and obligations each of the stakeholders have to other stakeholders in the event of a cyber-attack. This is an important enhancement to support risk assessment of the multi-stakeholder view as negative effects of cyber-attacks can transfer from one stakeholder domain to another.

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. In ETSI TS 102 165-1 [TVRA2011], a series of steps are applied for evaluation and estimation of the factors that affect the risks posed by the threats. The ETSI TVRA method is supported by a MS Excel-based tool, which automates the risk estimation step. The ETSI TVRA has been enhanced by the SEGRID project with respect to impact and likelihood scales, as well as an assessment of the motivation and capability of the attacker in the risk estimation step. The enhancement of the TVRA by SEGRID resulted into an update of the ETSI TS 102 165-1 [TVRA2017].

Appendix 3 – Supporting MS Excel tooling

The SRMM comes with two supporting MS Excel template to support the SRMM steps and to register the results:

1. **The SRMM Impact and Threat Actor Assessment sheet (SRMM Impact and Threat Actor Ass. Template – version 1.0 – Public.xlsx).**

- This template is designed to be used as a tool in carrying out steps 1, 2 and 3 of the SRMM. Several of the sheets have been filled in with information already to provide examples.
- There are several sheets to support Step 1:
    - Step 1 - Scope - identify RA scope using the SGAM. The architectural and flow diagrams should be included in this sheet.
    - Step 1 - Assets - This sheet is provided to compile an inventory of the assets
    - Step 1 Stakeholder Impact Class - classification of stakeholder impact. This needs to be discussed during the workshop
    - Step 1 SRMM scoping - define SRMM scopes and sub scopes and assign clear responsibilities
    - Step1 SRMM obligations & expectations - define obligations and expectations per scope and verify if they match between scopes
- Sheets to support Step 2:
    - Step 2 - Stakeholder Impact: The stakeholder impact assessment will be used as input to steps 3, and 4
    - Step 2 - SRMM obligation impact: Assess impact on obligations in each scope
- Sheets to support Step 3:
    - Step 3 -Threat Actor Analysis: this will be used as input to step 4 Risk estimation using the SEGRID TVRA spreadsheet template

2. **The SRMM Threat & Vulnerability Risk Assessment sheet (SRMM TVRA template – version 1.0 – Public.xlsx)**

- This template is designed to be used as a tool in carrying out steps 1, 2 and 3 of the SRMM. Several of the sheets have been filled in with information already to provide examples.
- When using the template to support the SRMM, the following Input to the SRMM TVRA is needed for carrying out Step 2 of the SEGRID approach to threat and risk assessment:
    - The identified Focus of Interest, that is the obligations that, when not fulfilled due to a security breach, have critical impact on the stakeholder scope. The Focus of Interest was identified when conducting the Obligation Impact Assessment (ref sheet Step 2 Obligation Impact in the SRMM Impact and Threat Actor Assessment Worksheet). The Obligation Impact (from the Step 2 Obligation impact) will be a basis for the Impact estimation. The obligation impact for a threat is the highest obligation impact of the obligations impacted."
    - The identified possible threat actors/threat sources from carrying out Step 2 using the sheet Step 2 Threat Actor Analysis in the SRMM Impact and Threat Actor Assessment Worksheet. The threat actor analysis provides input to the threat level Factor of the Likelihood estimation step.