SEGRID Risk Management Methodology

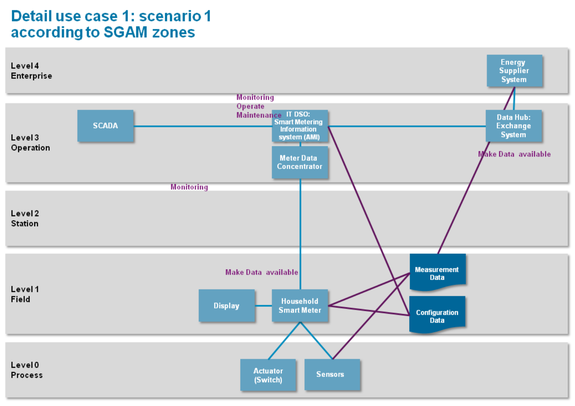
Judith E. Y. Rossebø, PhD[1]; Reinder Wolthuis and Frank Fransen[2];
[1]ABB, [2]TNO
Contact: Judith.Rossebo@no.abb.com

Abstract

The SEGRID Risk Management Methodology (SRMM), builds on the experiences of the SEGRID partners with risk assessment methodologies applied to the energy sector. The SRMM provides the DSOs with a structured and in-depth methodology for Smart Grid risk management that allows the DSOs to better understand the potential threats and vulnerabilities, manage the risks and take the necessary measures to contain and mitigate the risks.

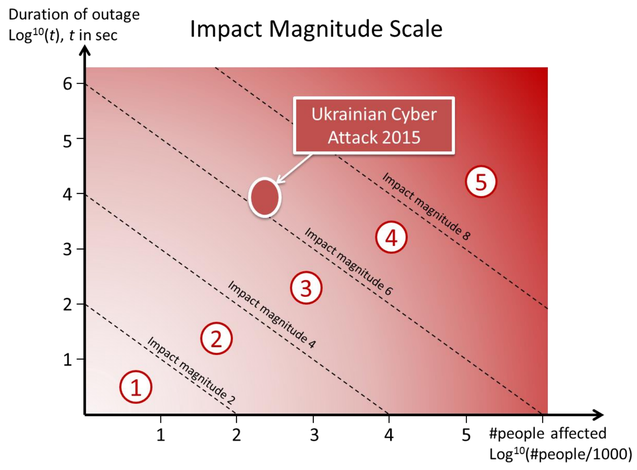
1: context establishment

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

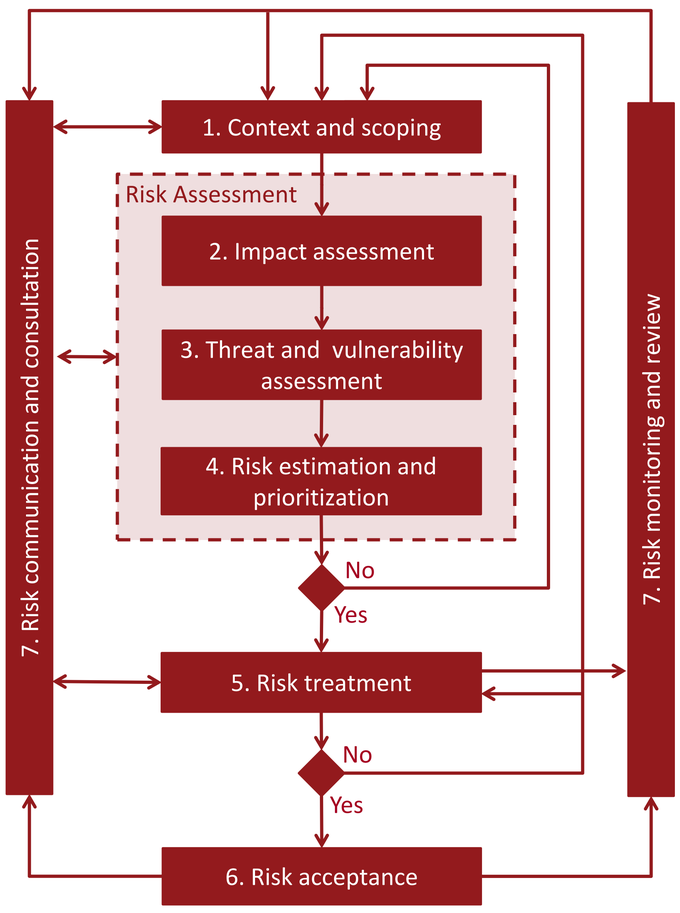


2: Impact assessment

Assess obligation impact for each stakeholder impact category, including society, on all obligations in each scope.

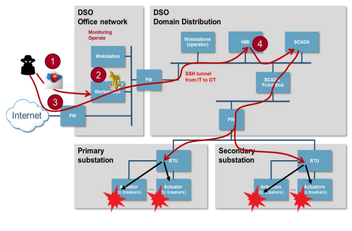


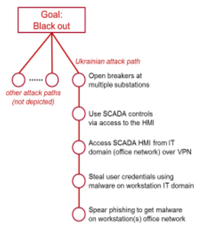
Seven Steps of the SRMM



3: TVRA

Threat and vulnerability assessment - identify threat sources, threat actors, vulnerabilities and threat scenarios.

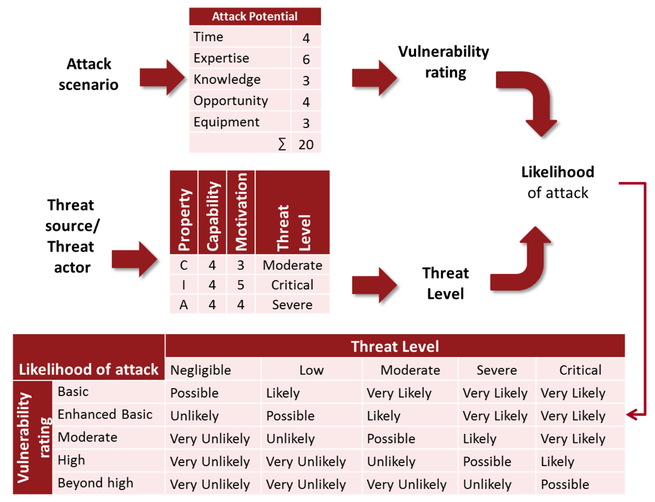




Threat Description	Attack						Impact	Risk
	Factor	Notes	Range	Value	Potential	Likelihood		
Vulnerability: DNP3 inproper input validation, weakness in IP-based network Scenario: An attacker could cause the software to go into an infinite loop, causing the process to crash. The system must be restarted manually to clear the condition.	Time	attack requires careful planning	<= 1 week	1	High	Unlikely	Very high	Critical
	Expertise	communications, protocols	Expert	5				
	Knowledge	AMI, wireless protocols	Public	0				
	Opportunity	Access to the wireless network	Difficult	12				
	Equipment	PC and protocol analyzer	Specialized	3				
	Asset Impact	Loss of power supply	High	4				
	Intensity	Many customers at once	High intensity	2				

4: Risk estimation

Risk estimation and prioritization - estimate the risks in terms of likelihood and impact and prioritize the risks against the risk evaluation criteria



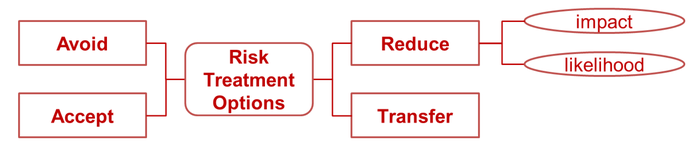
Methodology Enhancements

SEGRID enhances risk assessment in 3 ways:

1. Extends with the Network Risk Management Method (NRM) for insight in dependency, responsibility and the propagation of risks through value chains. This allows DSOs to iteratively evaluate the risks introduced by Smart Grids through a multi-stakeholder impact assessment, with risk dependency, responsibility and propagation in mind.
2. Extends the Impact assessment step to include 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 DSOs to be able to analyse risks with critical impact.
3. Applies and extends 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.

5: Risk treatment

Identify the risks that need to be treated and specify a risk treatment plan in terms of required security controls.

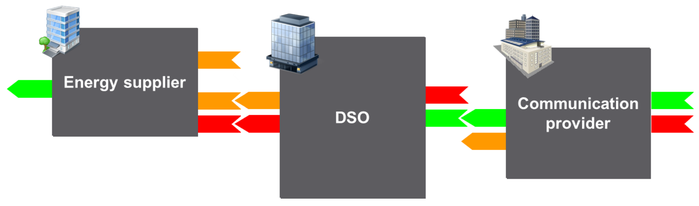


6: Risk acceptance

Based on the risk treatment plan and the residual risk assessment a risk acceptance decision is made, using the ownership of the NRM scope as reference.

7:Communicate results

Document and communicate results, and monitor and review risks (reiterating the assessment when needed).



Reference

- Judith Rossebø et al., "An Enhanced Risk-Assessment Methodology for Smart Grids“, *Computer,* IEEE Computer Society, vol. 50, no. 4, 2017, pp. 62-71.

SEGRID Security for smart Electricity GRIDs

www.segrid.eu info@segrid.eu

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