Security for smart Electricity GRIDs

An Enhanced Risk Assessment Methodology for Smart Grid – applied to UC2 Sce2

Judith E. Y. Rossebø and Reinder Wolthuis

2nd October, 2017
Risk Management & SEGRID Innovations

Risk assessment

Add new functions to the Power Grid

Development process

Operations

Development

Risk management

Periodic update

Toward dynamic / real-time risk management

Security Operations

Changes in:
- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite

Power Grid Infrastructure

Vulnerability Management, Security Incident Monitoring & Incident Response

SRMM

SEGRID security solutions

Risk Management & SEGRID Innovations

Power Grid Infrastructure

Security & Privacy Architecture

modelled

SRMM overall approach to risk management

Periodic update

Power Grid Infrastructure

Security & Privacy Architecture with SEGRID security solutions

check

Vulnerability Management, Security Incident Monitoring & Incident Response

new system

Development process

time
The SEGRID Risk Management Methodology

- Structured and in-depth methodology designed for Smart Grid risk management
  - To better understand potential threats and vulnerabilities
  - Manage risks
  - Take measures to contain and mitigate risks

Based on ISO/IEC 27005
SEGRID Risk Management Methodology
Segrid enhances existing risk-assessment in 3 ways

HMG Information Assurance Standard No. 1 (IS1) as a foundation

• Extends with Network Risk Management Method
  • for insight in dependency, responsibility and propagation of risks in value chains

• Extends the Impact assessment step
  • To include a practical approach to assessing societal impact in the case of a power outage caused by cyber attack

• Applies an enhancement to ETSI Threat, vulnerability and risk assessment
  • to include assessment of the attacker’s capability and motivation in the risk-estimation step.
The SEGRID Risk Management Methodology

1. Context and scoping
   - Define NRM scopes, obligations and expectations
   - Verify if they match between scopes

2. Impact assessment
   - Assess societal impact
   - Assess impact on Obligations in each Scope
   - Identify FoI

3. Threat and vulnerability assessment
   - Model Threats and vulnerabilities (Attack trees, securiCAD)

4. Risk estimation and prioritization
   - Apply enhanced ETSI TVRA to identify risks and relate these to obligations for prioritization

5. Risk treatment
   - Identify mitigations
   - Structure the report along the Obligations and Expectations

6. Risk acceptance
   - Risk acceptance decision is made, using the ownership of the NRM scope

7. Risk communication and consultation
   - Define NRM scopes, obligations and expectations
   - Verify if they match between scopes
Applying the SRMM: Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment

SEGRID RA scope (DSO)
Applying the SRMM: Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment
# Applying the SRMM: Use Case 2, Scenario 2

## Step 1: Context and Scope of the Risk Assessment

<table>
<thead>
<tr>
<th>Scope</th>
<th>ID</th>
<th>Name</th>
<th>Obligation to scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSO</td>
<td>O1</td>
<td>Avoid failures in the grid</td>
<td>x</td>
</tr>
<tr>
<td>DSO</td>
<td>O2</td>
<td>Avoid failures in the grid</td>
<td>x</td>
</tr>
<tr>
<td>DSO</td>
<td>O3</td>
<td>Avoid failures in the grid</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>O4</td>
<td>Taking the most advantage of distributed generation</td>
<td>x</td>
</tr>
<tr>
<td></td>
<td>O5</td>
<td>Provide correct setpoints to DER RTU</td>
<td>x</td>
</tr>
</tbody>
</table>
Applying the SRMM : Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment

<table>
<thead>
<tr>
<th>Scope</th>
<th>ID</th>
<th>Name</th>
<th>Energy supplier/DER</th>
<th>Private Customer</th>
<th>TSO</th>
<th>SW Vendor</th>
<th>Telco</th>
<th>Society</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSO</td>
<td>E1</td>
<td>Make sensor data available at the DER RTU</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>Generation according to setpoints</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>Deliver reliable forecast data</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>Deliver reliable SW updates</td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>E5</td>
<td>Deliver reliable communication services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
### Applying the SRMM: Use Case 2, Scenario 2

#### Step 2: Impact Assessment

Obligation impact – assessment of maximum impact (worst case) if the obligation is not fulfilled

<table>
<thead>
<tr>
<th>ID</th>
<th>Obligation name</th>
<th>Description maximum impact</th>
<th>Maximum Impact</th>
<th>Financial</th>
<th>Reputation</th>
<th>Operations</th>
<th>L&amp;R compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>O1</td>
<td>Avoid failures in the grid</td>
<td>Financial loss, Reputational damage, large impact on operations, high L&amp;R fines</td>
<td>Very high</td>
<td>High</td>
<td>High</td>
<td>Very high</td>
<td>Very high</td>
</tr>
<tr>
<td>O2</td>
<td>Avoid failures in the grid</td>
<td>Customers receive no financial compensation, Reputational damage but DSO is monopolist</td>
<td>High</td>
<td>Very low</td>
<td>High</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O3</td>
<td>Avoid failures in the grid</td>
<td>No financial compensation for TSO, TSO will not go public</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O4</td>
<td>Advantage of distributed generation</td>
<td>Minimal reputational damage, there are some L&amp;R consequences</td>
<td>Medium</td>
<td></td>
<td>Low</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>O5</td>
<td>Provide correct setpoints to DER RTU</td>
<td>No financial compensation to DER, considerable reputational damage and operational impact</td>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td></td>
</tr>
</tbody>
</table>
Applying the SRMM: Use Case 2, Scenario 2

Step 2: Impact Assessment

- Societal impact—assessment of maximum impact (worst case) if an attack causes an power outage

<table>
<thead>
<tr>
<th></th>
<th>#people affected</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ukraine Cyber Attack 2015</td>
<td>225,000</td>
<td>1 – 6 hours</td>
</tr>
<tr>
<td>Ukraine Cyber Attack 2016</td>
<td>760,000*</td>
<td>1 ¼* hours</td>
</tr>
</tbody>
</table>

* Estimated

SEGRID adopted the approach from FP7 project Viking to plot power outages on Social Impact Magnitude scale and map these to impact scales.
Applying the SRMM: Use Case 2, Scenario 2

Step 2: Impact Assessment

• The outage’s impact can be related to two obligations:

  • O1 - DSO obligation to society – Maximum impact is very high.

  • O2 - DSO obligation to customer – Maximum impact is High.

• Due to the relatively short outage, obligations O3, O4 and O5 are not impacted

Output: identification of the DSO’s critical assets in the Focus of Interest
Applying the SRMM: Use Case 2, Scenario 2

Step 3: Threat and Vulnerability Assessment

Goal: blackout

Ukrainian attack path

Payload(s) execute on timer -
Open breakers at substation by sending legitimate RTU messages

Launcher with knowledge of RTU protocols listens to traffic and identifies addresses of breakers

Macro places the launcher in the SCADA servers or in the Front-End servers.

If opened, a macro in the word document looks for access to the SCADA system

Spear phishing, emails sent with word attachment containing macro to Utility employees

Description of Threat & Vulnerability Scenario

- Threat: Unauthorized, automated operation of high-voltage breakers
- Assets: SCADA servers, remote terminal units, breakers
- Existing controls: access control, FWs
- Threat source: Unidentified group/Nation State
- Threat actor: Team of highly skilled threat actors
- Threat vector: Spear Phishing attacks to get macro installed at the utility, when Word is opened, the macro starts to look for access to the SCADA system
- Vulnerabilities exploited: Insufficient awareness training, insufficient FWs, or no DMZ
- Threat scenario description: Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in parts of a major city of the attacked country.
- Unwanted incident/event: 760,000 customers lose power for 1 hour and 15 minutes, energy supplier, DSO's and TSOs' operations are impacted, and TSOs' reputation damaged
Applying the SRMM: Use Case 2, Scenario 2

Step 4: Risk Estimation \( \text{Risk} = \text{likelihood} \times \text{impact} \)

Based on ETSI TS 102 165 & ISO/IEC 18045 – enhanced for SEGRID

- **Attack Likelihood** estimation –
  - Vulnerability rating (**Opportunity and Required Capability**)

  combined with the

  - Threat level (**Motivation & Capability of the Threat Actor**)

- **Impact** estimation –
  - Combines Obligation Impacts
### Likelihood Estimation

#### Attack Potential

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>4</td>
</tr>
<tr>
<td>Expertise</td>
<td>6</td>
</tr>
<tr>
<td>Knowledge</td>
<td>3</td>
</tr>
<tr>
<td>Opportunity</td>
<td>4</td>
</tr>
<tr>
<td>Equipment</td>
<td>3</td>
</tr>
<tr>
<td><strong>∑</strong></td>
<td><strong>20</strong></td>
</tr>
</tbody>
</table>

#### Vulnerability rating

<table>
<thead>
<tr>
<th>Property</th>
<th>Capability</th>
<th>Motivation</th>
<th>Threat Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>4</td>
<td>3</td>
<td>Moderate</td>
</tr>
<tr>
<td>I</td>
<td>4</td>
<td>5</td>
<td>Critical</td>
</tr>
<tr>
<td>A</td>
<td>4</td>
<td>4</td>
<td>Severe</td>
</tr>
</tbody>
</table>

#### Likelihood of attack

<table>
<thead>
<tr>
<th>Vulnerability rating</th>
<th>Basic</th>
<th>Enhanced Basic</th>
<th>Moderate</th>
<th>High</th>
<th>Beyond high</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Negligible</td>
<td>Low</td>
<td>Moderate</td>
<td>Severe</td>
<td>Critical</td>
</tr>
<tr>
<td>Possible</td>
<td>Likely</td>
<td>Very Likely</td>
<td>Very Likely</td>
<td>Very Likely</td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td>Possible</td>
<td>Likely</td>
<td>Very Likely</td>
<td>Very Likely</td>
<td></td>
</tr>
<tr>
<td>Very Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Likely</td>
<td>Very Likely</td>
<td></td>
</tr>
<tr>
<td>Very Unlikely</td>
<td>Very Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Likely</td>
<td></td>
</tr>
<tr>
<td>Very Unlikely</td>
<td>Very Unlikely</td>
<td>Very Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
<td></td>
</tr>
</tbody>
</table>
Applying the SRMM: Use Case 2, Scenario 2

Step 4: Risk Estimation
Based on ETSI TS 102 165 & ISO/IEC 18045 – enhanced for SEGRID

- **Likelihood** estimation
  - Vulnerability rating (**Opportunity and Required Capability**) is combined with the

- **Threat level** (**Motivation & Capability of the Threat Actor**)

- **Impact** estimation
  - Combines Obligation Impacts

<table>
<thead>
<tr>
<th>Threat Scenario Description</th>
<th>Unwanted Incident or Event</th>
<th>Attack</th>
<th>Factor</th>
<th>Notes</th>
<th>Range</th>
<th>Value</th>
<th>Vulnerability rating</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in parts of a major city of the attacked country.</td>
<td>Power outage. 760 000 people lose electrical power for 1 hour and 15 minutes, no physical damage so recovery is quick. Demonstration of capability by threat source.</td>
<td><strong>Time</strong></td>
<td>Planning, several stages of attack</td>
<td>&gt; 6 months</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td>Beyond High</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Expertise</strong></td>
<td>SCADA experts</td>
<td>Multiple experts</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td>Possible</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Knowledge</strong></td>
<td>Knowledge of SCADA protocols, RTU</td>
<td>Restricted</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>Very high</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Opportunity</strong></td>
<td>Phishing, insider for malware delivery</td>
<td>Moderate</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Equipment</strong></td>
<td>Standard, PC</td>
<td>Standard</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Threat level</strong></td>
<td>Reference threat actor analysis</td>
<td>Critical</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Impact</strong></td>
<td>760 000 customers lost power, no physical damage</td>
<td>Very high</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Applying the SRMM : Use Case 2, Scenario 2

Step 5: Risk treatment

For this risk, we choose to **Reduce the risk**; it exceeds the DSO’s risk appetite. We will **not accept** the risk as-is and there are no possibilities to transfer or avoid this risk.

Security control selection using IEC 62443-3-3 ⇒ Risk Treatment Plan

<table>
<thead>
<tr>
<th>ID</th>
<th>Threat</th>
<th>Likelihood</th>
<th>Impact</th>
<th>Risk</th>
<th>Risk Treatment - Selected Security Controls</th>
</tr>
</thead>
</table>
| UKR 2016 | Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in part of a major city of the attacked country | Possible   | Very high | Critical | **FR 3: Data integrity** - Ensure the integrity of the IACS to prevent unauthorized manipulation.  
**FR 7: Resource availability** - Ensure the availability of the control system against the degradation or denial of essential services. |
| ...   | ...                                                                                                                                                                                                   | ...        | ...     | ...    | ...                                                                                                          |

See SPADE

See Cost assessment
Applying the SRMM: Use Case 2, Scenario 2

Step 6: Risk acceptance

Accept residual risks

- After Risk mitigation plan has been implemented
- By responsible of DSO (DSO director)
Applying the SRMM: Use Case 2, Scenario 2

Step 7: Risk communication and consultation

Communicate residual risks (internally at DSO)

Communicate risks that expectations are not fulfilled (between stakeholders)
The SEGRID Risk Management Methodology

1. Context and scoping
   - Define NRM scopes, obligations and expectations
   - verify if they match between scopes

2. Impact assessment
   - Assess societal impact
   - Assess impact on Obligations in each Scope
   - Identify FoI

3. Threat and vulnerability assessment
   - Model Threats and vulnerabilities (Attack trees, SecurICAD)

4. Risk estimation and prioritization
   - Apply enhanced ETSI TVRA to identify risks and relate these to obligations for prioritization

5. Risk treatment
   - Identify mitigations
   - Structure the report along the Obligations and Expectations

6. Risk acceptance
   - Risk acceptance decision is made, using the ownership of the NRM scope

7. Risk communication and consultation

Network Risk Management
Risk management to support multi-stakeholder

- Define NRM scopes, obligations and expectations
- verify if they match between scopes

- Assess societal impact
- Assess impact on Obligations in each Scope
- Identify FoI

- Model Threats and vulnerabilities (Attack trees, SecurICAD)

- Apply enhanced ETSI TVRA to identify risks and relate these to obligations for prioritization

- Identify mitigations
- Structure the report along the Obligations and Expectations

- Risk acceptance decision is made, using the ownership of the NRM scope
Concluding remarks

• The SRMM builds on state of the art RA methodologies while providing guidance and enhancements for use in smart grids.

• SEGRID enhances risk assessment in three ways:
  • Including societal impact
  • Including NRM for improved insight in dependencies between stakeholders
  • Including the threat actor motivation and capability in the risk estimation step

• The SEGRID enhancement to the ETSI TVRA has been accepted in the next version of the standard.
  • This ensures that the Threat, Vulnerability and Risk Assessment work will be used
You can read more about the SRMM in the April 2017 Issue of IEEE Computer

---

An Enhanced Risk-Assessment Methodology for Smart Grids

Judith E.Y. Rosseel, AAS Norway
Reinder Wolthuis and Pieter Prinsen, TNO
Guimar Bjoerkan, Royal Institute of Technology, KTH
Nicole Molenaar, EDP

Cyberattacks on power grids are pushing threat and risk assessment to another complexity level. As part of its scope, the EU’s Security for Smart Electricity Grids (SEGRID) project was tasked with building on existing methods to address the interdependencies characteristic of a smart grid. The authors describe the resulting methodology.

As society’s electrical needs evolve, smart power grids must be able to adapt to fluctuating demand from renewable energy generation and innovation such as electric vehicles. To remain flexible, utilities need to rethink traditional operational models. From the top-down hierarchical approach to supervisory control and data acquisition (SCADA) systems to a distributed approach with increased heterogeneity of observability, controllability, and automation.

In this new environment, distribution system operators (DSOs) with hour-by-hour support and more responsibility for controlling and influencing power flows in medium- and low-voltage grids. They will use more automatic functions such as self-healing networks, but the cost will likely be a dramatic increase in opportunities for large-scale cyberattacks, which will require deeper risk assessments. Indeed, sophisticated cyberattacks on control systems have already occurred, engineered by highly motivated threat sources and carried out by skilled attackers. For example, in 2010 industrial control systems at the nuclear enrichment facility in Najm, Iran, were damaged by Stuxnet malware, and in 2014 a cyberattack on the Ukrainian electricity distribution network caused a regional blackout. Given the world’s heavily political climate, such attacks can be expected to increase.

Smart power grids pose extreme challenges for risk assessment. The threat and vulnerability landscape continues to change unpredictably as new threat
Thank you

Judith E. Y. Rossebø, PhD
Cyber Security Specialist
ABB AS

Phone: +47 22874725
Mobile: +47 41563062
E-mail: judith.rossebo@no.abb.com

Mail: info@segrid.eu
Website: www.segrid.eu
Telephone: +31 8886 67758

Project type: Collaborative project – small or medium scale focused research project
Grant agreement no: 607109
Thematic Priority: FP7-SEC-2013-1
Start date of project: October 1st, 2014
Duration: 36 months
Coordinator: TNO, The Netherlands

Reinder Wolthuis
+31 6 5191 33 79
reinder.wolthuis@tno.nl