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
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.
### Applying the SRMM: The Ukraine Case

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

<table>
<thead>
<tr>
<th>Customer</th>
<th>Energy supplier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uninterrupted energy supply</td>
<td>Stable (MV) grid</td>
</tr>
<tr>
<td>Distribute energy</td>
<td>Distribute energy</td>
</tr>
</tbody>
</table>

- **DSO**
  - Control the grid

- **SCADA system**
  - SCADA master
  - SCADA workstation

- **System assets**
  - Primary substation
  - Secondary substation
  - Corporate IT network

- **Expectation**
- **Obligation**
- **System asset**
- **Scope**
Applying the SRMM: The Ukraine Case

Step 2: Impact Assessment

- Obligation impact – assessment of maximum impact (worst case) if the obligation is not fulfilled
- Societal impact – assessment of maximum impact (worst case) if an attack causes an power outage

Ukraine Cyber Attack 2015:
- 225,000 Customers lost power on Dec 23rd, 2015 (for 1 to 6 hours)
- Societal impact HIGH

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: The Ukraine Case

Step 2: Impact Assessment

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

  • DSO obligation to customer – Brief outage (1 – 6 hrs) the obligation impact rating would be low to medium.

  • DSO obligation to society – high societal impact, impact due to fines and additional regulations on the DSO. The estimation of the impact if this obligation is not fulfilled is rated to high.

  • DSO obligation to energy supplier. The energy supplier cannot supply energy and loses income. Obligation impact rated medium to high.

Output: identification of the DSO’s critical assets in the Focus of Interest
Applying the SRMM: The Ukraine Case

Step 3: Threat and Vulnerability Assessment

Goal: blackout

Ukrainian attack path

- Open breakers at multiple substations
- Use standard SCADA dialogues in the SCADA workstation
- Access SCADA workstations from IT domain (office network) over VPN
- Steal user credentials using malware on workstations in the office network
- Spear phising to get malware on workstations in the office network

Description of Threat & Vulnerability Scenario

- Threat: Unauthorized operation of medium-voltage breakers
- Assets: SCADA workstations, remote terminal units, breakers
- Existing controls: access control (username/password), FWs
- Threat source: Unidentified group
- Threat actor: Team of highly skilled threat actors
- Threat vector: Phishing attacks to get credentials, remote access to SCADA workstations using virtual private network (VPN) access as corporate users
- Vulnerabilities exploited: insufficient protection of credentials, insufficient training
- Threat scenario description: Attackers leverage legitimate credentials to obtain access to three DSOs, use remotely operated breakers to disconnect power, and wipe additional systems using KillDisk malware at the end of the attack. Firmware of serial-to-Ethernet devices at substations is corrupted, call centers are flooded, and follow-up attacks interfere with restoration efforts
- Unwanted incident/event: 225,000 customers lose power, energy supplier and DSOs’ operations are impacted, and DSOs’ reputation damaged
Likelihood estimation
- With TVRA we estimate the likelihood that the attack will be a success

Impact estimation
- Intensity of the attack is a factor of the Impact

Step 4: Risk Estimation

Motivation
- Opportunity
- Capability

What about Motivation?

Applying the SRMM: The Ukraine Case

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

(Risk = likelihood \times \text{impact})
Likelihood depends also on level of **Motivation** & **Capability** of the attacker.

**Examples:** Stuxnet, the **Ukrainian power outage** are real examples that demonstrate that threat actor capability and motivation influence likelihood.

Applying the SRMM: The Ukraine Case

**Step 4: Risk Estimation**

What about motivation?

- Likelihood depends also on level of **Motivation** & **Capability** of the attacker.

**Examples:** Stuxnet, the **Ukrainian power outage** are real examples that demonstrate that threat actor capability and motivation influence likelihood.

(Risk = likelihood \( \times \) impact)
Including threat actor capability and motivation

Starting point: Likelihood Estimation in the ETSI TVRA
Based on the CC CEM (ISO/IEC 18045)

<table>
<thead>
<tr>
<th>Attack Potential $\sum$</th>
<th>Vulnerability rating</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 to 9</td>
<td>Basic</td>
<td>Very likely</td>
</tr>
<tr>
<td>10 to 13</td>
<td>Enhanced Basic</td>
<td>Likely</td>
</tr>
<tr>
<td>14 to 19</td>
<td>Moderate</td>
<td>Possible</td>
</tr>
<tr>
<td>20 to 24</td>
<td>High</td>
<td>Unlikely</td>
</tr>
<tr>
<td>&gt;24</td>
<td>Beyond high</td>
<td>Very Unlikely</td>
</tr>
</tbody>
</table>

Factor

<table>
<thead>
<tr>
<th>Factor</th>
<th>Value</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>
</tbody>
</table>

Attack Potential $\sum = 20$

Required Attack Potential

Likelihood of attack

Depends also on level of Motivation & Capability of the attacker
Likelihood Estimation Enhanced

---

**Attack Potential**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</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>
</tbody>
</table>

∑ 20

---

**Vulnerability rating**

**Likelihood of attack**

<table>
<thead>
<tr>
<th>Vulnerability rating</th>
<th>Negligible</th>
<th>Low</th>
<th>Moderate</th>
<th>Severe</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
<td>Possible</td>
<td>Likely</td>
<td>Very Likely</td>
<td>Very Likely</td>
<td>Very Likely</td>
</tr>
<tr>
<td>Enhanced Basic</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Likely</td>
<td>Very Likely</td>
<td>Very Likely</td>
</tr>
<tr>
<td>Moderate</td>
<td>Very Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Likely</td>
<td>Very Likely</td>
</tr>
<tr>
<td>High</td>
<td>Very Unlikely</td>
<td>Very Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
<td>Likely</td>
</tr>
<tr>
<td>Beyond high</td>
<td>Very Unlikely</td>
<td>Very Unlikely</td>
<td>Very Unlikely</td>
<td>Unlikely</td>
<td>Possible</td>
</tr>
</tbody>
</table>

---

**Threat actor**

<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>

---

**Threat Level**

C43
I45
A44
Risk Estimation enhanced

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 Impact with Attack Intensity

---

### Threat scenario description

<table>
<thead>
<tr>
<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 leverage legitimate credentials to obtain access to three DSOs, use remotely operated breakers to disconnect power, and wipe additional systems using KiliDisk malware at the end of the attack. Corruption of firmware of serial-to-Ethernet devices at substations, flooding of call centers, and follow-up attacks to interfere with restoration efforts.</td>
<td>Time</td>
<td>Attack requires some planning</td>
<td>&gt; 6 months</td>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Expertise</td>
<td>Expert in these systems</td>
<td>Multiple experts</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Knowledge</td>
<td>Knowledge of SCADA, RTUs</td>
<td>Restricted</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opportunity</td>
<td>Remote and inside access</td>
<td>Moderate</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Equipment</td>
<td>PCs, VBR and ICS client software</td>
<td>Standard</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threat level</td>
<td>Reference threat actor analysis</td>
<td>Severe</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impact</td>
<td>Many customers lose power</td>
<td>High</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Intensity</td>
<td>Three DSOs, customers at once</td>
<td>High intensity</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Motivation and Capability of the Threat Actor

Opportunity
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, CySeMoL)

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
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
Concluding remarks

You can read more about the SRMM in the April 2017 Issue of IEEE Computer.
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