Innovation type:
Tool-supported method

TRL: #5 (Validated in a relevant environment)

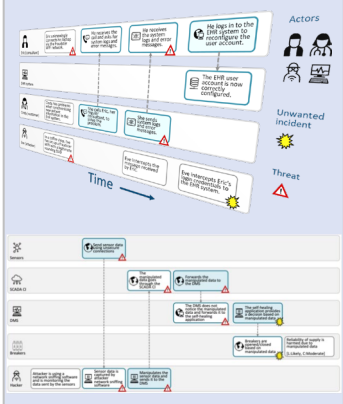
Date: December 2024

Contact:
Susanne Sandell
Susanne.Sandell@sintef.no

Target group:

Actor/ purpose	x
DSO, TSO	X
Technology provider	
Member organisation	
Market operator	
Research/ Consultancy	
Teaching	X

Illustrations



Threat model including threat actor, threat scenario, unwanted incident, asset to protect (e.g. Reliability of supply), and the likelihood and consequence of risk.

Tool-Supported Method for Cyber Risk Assessment in the Planning of Cyber-Physical Smart Grids

The transition to cyber-physical smart grids introduces new cybersecurity challenges, particularly during the early planning phases. To address these, a lightweight, tool-supported method has been developed, enabling grid planners to assess cyber risks with limited information about digital solutions.

Challenge

The integration of active digital measures in smart grids, such as self-healing technologies, brings cybersecurity risks that are difficult to predict during early grid planning. Planners often lack detailed technical information and cybersecurity expertise, creating a need for accessible tools and methods to address potential threats at this stage.

Solution

A six-step, lightweight, tool-supported cyber risk assessment method is developed. It employs the Customer Journey Modelling Language (CJML), extended to include cybersecurity concepts such as assets, threat actors, and unwanted incidents. This method allows planners to:

- Define the scope and analyse the target solution.
- Identify key assets and potential cyber threats.
- Assess risks using expert judgment and likelihood-consequence scales. The open-source tool supporting this method enables graphical threat modelling, facilitating user-friendly visualization and analysis.

Potential

The method empowers grid planners to integrate cybersecurity considerations into grid development processes effectively. By identifying risks early, planners can compare digital and traditional measures, balancing costs, benefits, and risks. Preliminary testing in real-world scenarios has shown promise for broader adoption, potentially enhancing the resilience of future grids. The method was developed and validated in two iterations: first, using the CINELDI-produced Norwegian reference grid system as a real-world application, and subsequently, on a sharp (confidential) case study with one of CINELDI's partners. This dual validation process underscores the method's practical applicability and its alignment with CINELDI's strategic goals of ensuring grid security and reliability.

Reference in CINELDI

G. Erdogan, T.A. Zerihun, I.B. Sperstad and O. Gjerde: "A Light-Weight Tool-Supported Method for Cyber Risk Assessment in the Planning of Cyber-Physical Smart Grids", IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Oslo, Norway, 2024.