Cyber-risk assessment in grid planning

CINELDI/NORCICS workshop on
cyber security in cyber-physical electricity grids

Gencer Erdogan
SINTEF Digital
28 March 2023

Outline

- Motivation, challenges and needs
- Grid planning and cyber-risk assessment
- Self-healing case
- Identifying high-level risks using CJML
- Further work

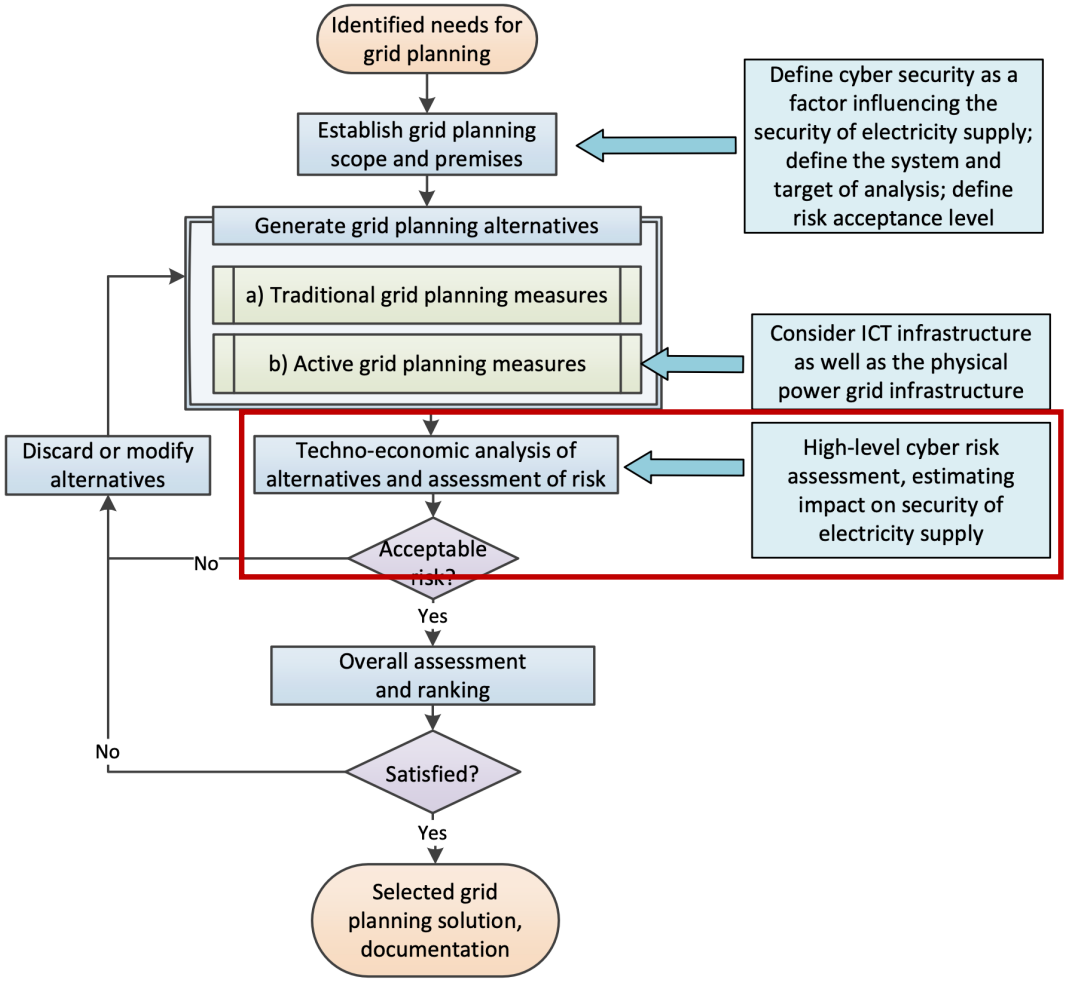
Motivation, challenges and needs

- Smart electricity distribution grids are cyber-physical systems with mutual dependencies between power and cyber parts
- Lack of cybersecurity may jeopardise security of supply
- Grid planning has several challenges

- The target of analysis is not implemented
- Information about the target of analysis is at an conceptual level (high-level)
- The information about the final grid is therefore uncertain
- Non cyber-experts have to assess cyber risks with very limited knowledge about the grid under development

There is a need for a low-threshold risk assessment method to identify high-level cyber risks in the planning phase

CINELDI



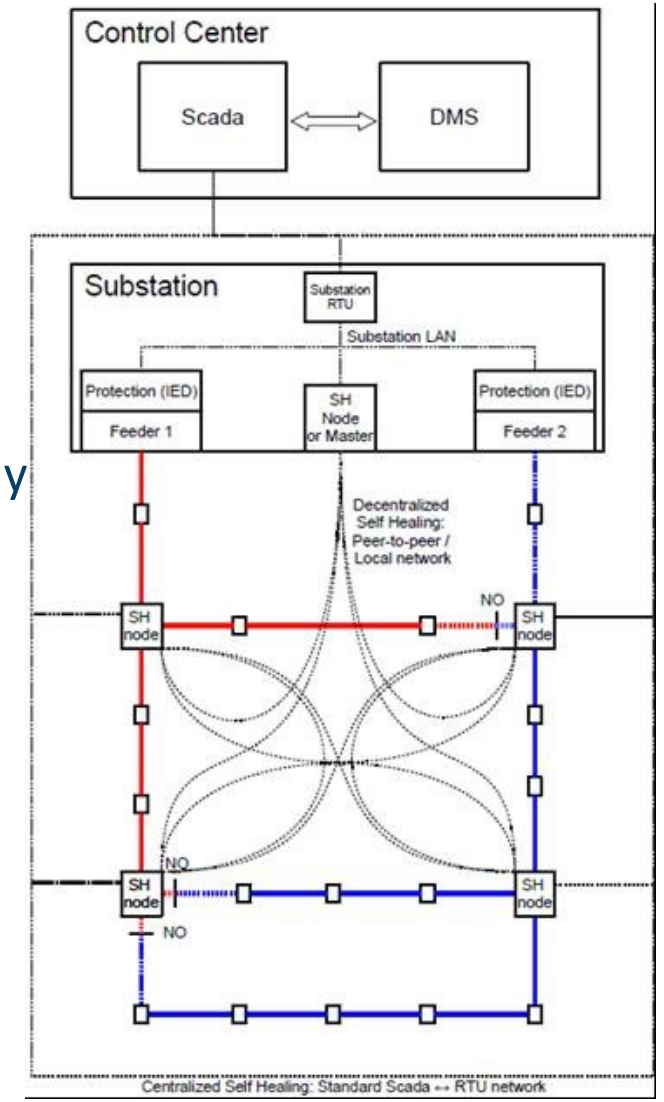
Grid planning and cyber-risk assessment

- Identify needs for grid planning
- Assess grid planning alternatives and associated risks
- Select the most optimal solution
- Cyber-risk assessment fits in many steps of this process
- Our focus: cyber-risk assessment of the potential alternatives including ICT

CINELDI

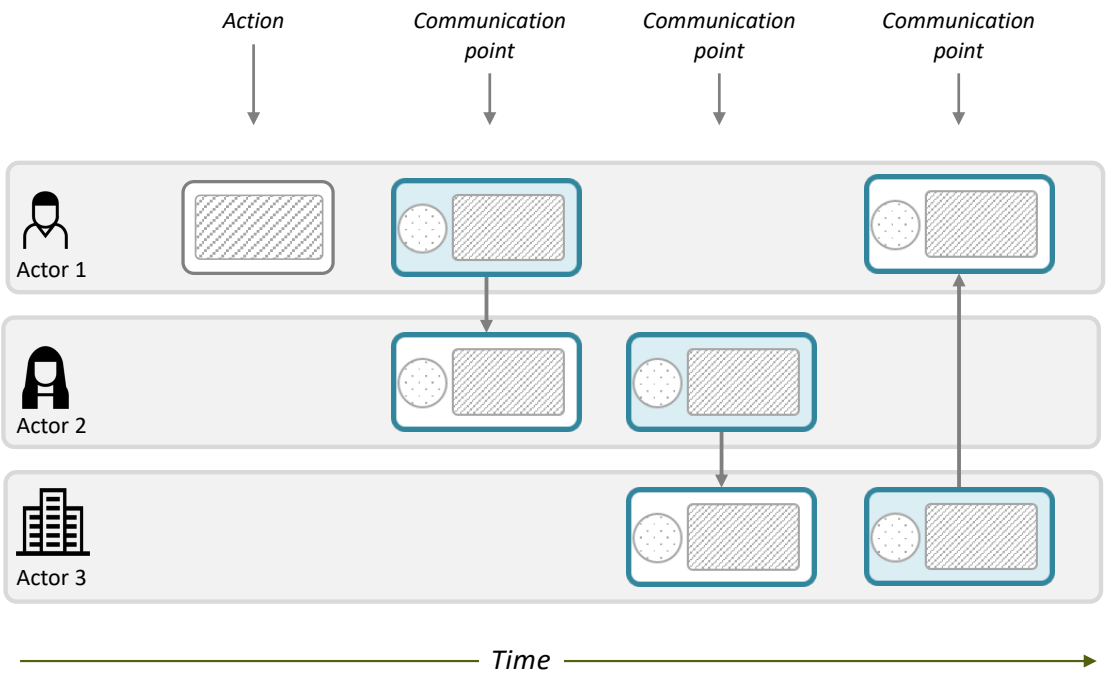
Self-healing case

- A grid company wants to explore the possibilities of implementing self-healing grids as part of grid planning
- In self-healing grids, digital solutions are used to reconfigure the network and to restore the power supply
- Digital solutions, e.g. SCADA, are vulnerable to cyber attacks (Supervisory Control and Data Acquisition)
- One possible attack: a hacker gains unauthorized access to the SCADA system and changes switches in the self-healing grid, which further leads to power outages (attack on security of supply)

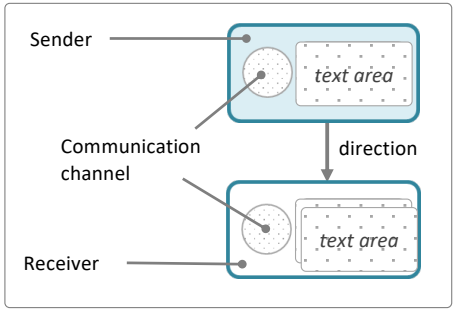


One possible approach to model high-level risk is to use the Customer Journey Modelling Language

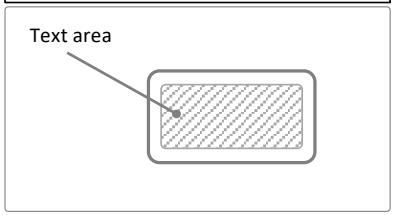
All the actors involved in the journey has a separate swimlane.



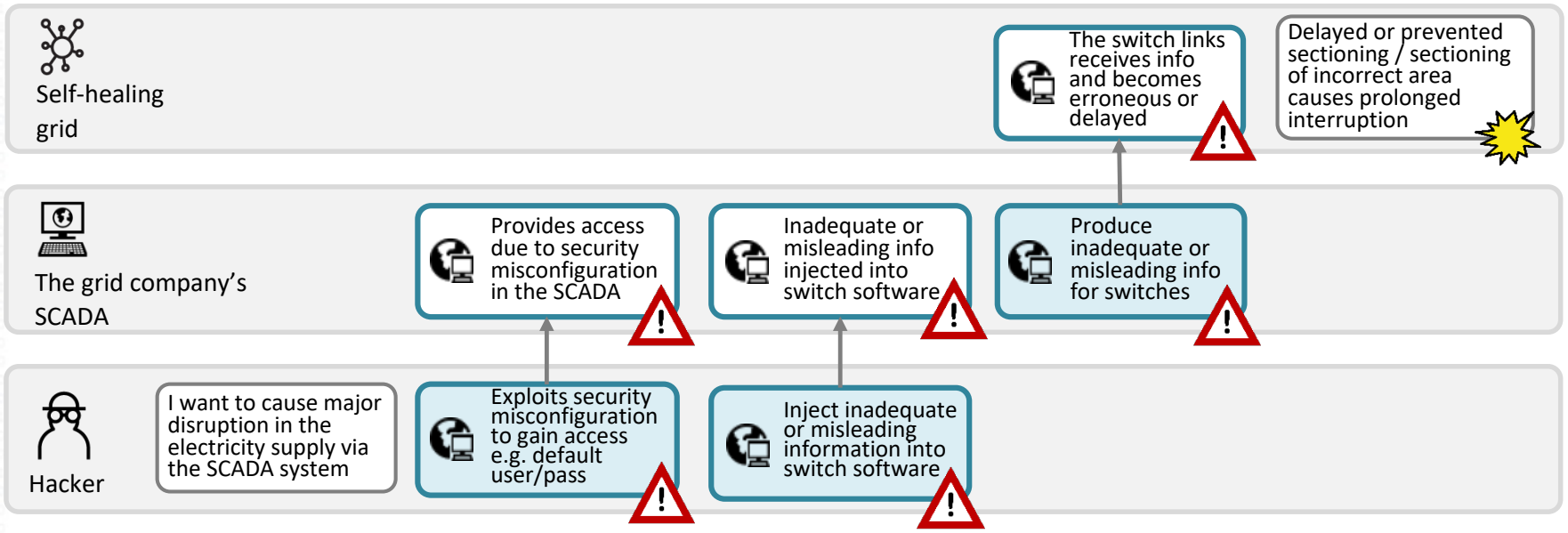
A communication point has a sender and a receiver that must be positioned in the corresponding swimlanes of the actors.



An action element is used for non-communicating events



Hacker attacking switches in the self-healing network leads to disruption of electrical supply



Further work

- Continue to develop and test the risk assessment method in industrial cases
- Adapt the risk assessment method for other steps in the planning phase
- Include guidelines to identify interdependencies between power and ICT systems as part of the risk assessment method
- Identify scenarios that could harm security of supply

References

[1] A. Omerovic, H. Vefsnmo, G. Erdogan, O. Gjerde, E. Gramme, S. Simonsen. *A Feasibility Study of a Method for Identification and Modelling of Cybersecurity Risks in the Context of Smart Power Grids.* In Proc. 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS'19), pages 39-51, SCITEPRESS, 2019.

[2] R. Halvorsrud, C. Boletsis, E. Garcia-Ceja. *Designing a Modeling Language for Customer Journeys: Lessons Learned from User Involvement.* In 2021 ACM/IEEE 24th International Conference on Model Driven Engineering Languages and Systems (MODELS) (pp. 239-249). IEEE. 2021.

[3] G. Erdogan, I.B. Sperstad, M. Garau, O. Gjerde, I.A. Tøndel, S. Tokas, M.G. Jaatun. *Adapting Cyber-Risk Assessment for the Planning of Cyber-Physical Smart Grids Based on Industrial Needs*. CCIS, Springer, 2023 (to appear).

CINELDI

Centre for intelligent electricity distribution
- to empower the future Smart Grid

Gencer Erdogan
Senior Research Scientist
SINTEF Digital
Gencer.Erdogan@sintef.no
https://gencer.no/

www.cineldi.no

This work is funded by CINELDI - Centre for intelligent electricity distribution, an 8 year Research Centre under the FME-scheme (Centre for Environment-friendly Energy Research, 257626/E20). The authors gratefully acknowledge the financial support from the Research Council of Norway and the CINELDI partners.

CINELDI