Model-Based Cybersecurity Analysis – Extending Enterprise Modeling to Critical Infrastructure Cybersecurity

Yuning Jiang, Manfred A. Jeusfeld, Jianguo Ding, Elin Sandahl

Business & Information Systems Engineering (2023)

Appendix (available online via http://link.springer.com)

Appendix

This appendix presents the questions that led the discussions during the interview-based evaluation study. Summaries of the interview results are presented in sub-section 7.3. Although a list of questions was prepared before the interviews, they were conducted in a semi-structure manner, opening opportunities to both wider and deeper discussions related vulnerability-driven cybersecurity practices and challenges in complicated critical infrastructures.

Question Topic 1: Understanding the Organization

- How do you (or your business partners) get an overview over the assets of your company, i.e. the physical inventory, IT/OT components, the network, software applications and their interdependencies?
- Is there a single person who has the complete overview, or is the knowledge spread among different roles?
- Does your organization treat the cybersecurity of OT components such as RTUs in the same way as the cybersecurity of IT components?
- How frequently do you need to be informed about the vulnerability of your network?
- How frequently do you create reports on the cybersecurity risks in your organization?

Question Topic 2: Evaluating the Usefulness of the Artifacts and Instantiations

- (Before this question, we present to the interviewees how we model and represent different types of components of a CPS.) How could such an overview help in understanding the risks associated to cyber attacks?
- Is the integration of components for IT, OT and the physical power flow potentially useful to your organization beyond the assessment of cyber risks?
- (Before this question, we present to the interviewees how to combine the criticality score of a component with its aggregated vulnerability score.) In which way could such an overview help in understanding the risks associated to cyber attacks?
- (Same precondition as the previous question.) Does it help to make the right investment decisions in cybersecurity?
- The vulnerability score is computed for software assets on IT components but also on OT components that directly control the power flow. How important is it to cover both IT and OT?
- Would you be willing to buy the service of such a tool to get up-to-date cybersecurity assessments?