Unit 4 Seminar SEMINAR PREP

Title: Risk Identification and Modelling - Case Study

Please carry out this activity before joining the seminar this week. Your answers will be discussed during the seminar.

Workshop Activity

Review Jbair, M. et al.(2022).

Workshop Questions

1. What are the key elements and interdependencies in a cyber-physical system that must be captured in a comprehensive threat model, and why are they critical for accurate risk analysis?

Key element	**interdependency**	**Criticallity**
Threat actor	Initiates cyber-attacks by exploiting vulnerabilities in assets.	Determines the likelihood and sophistication of attacks
Cyber-attack	Depends on threat actor capabilities and asset vulnerabilities.	Defines potential harm
Asset	Targeted by attacks; asset level influences impact severity.	Asset criticality affects the prioritisation of mitigation
Vulnerability	Enables threats and attacks; linked to asset type and exposure.	Identifies entry points
Attack impact	Determined by asset level and type of attack.	Quantifies the loss event
Attack likelihood	Influences risk level; linked to threat actor behaviour and asset exposure.	Prioritising threats
Threat	Comes from vulnerabilities leads to risk when combined with impact and likelihood.	Connects vulnerabilities to actual consequence(s)
Risk	depends on all previous elements.	Critical for decision-making and resource allocation
Mitigation	Implemented based on assessed risk	Rreduces risk

2. How can threat modelling help identify attack entry points and system vulnerabilities in cyber-physical energy systems, and what are the challenges in doing so effectively?

How threat modelling can help:

- Helps to pinpoint which components are most critical and likely targets for attacks.

- Reveals how attackers might exploit vulnerabilities and where they could enter the system.
- By evaluating vulnerabilities and threats it identifies weakness in the system that can be exploited
- It helps prioritise which vulnerabilities pose the greatest danger.
- Helps to propose mitigation controls to ensure vulnerabilities are addressed before they can be exploited

Challenges:

- Most existing threat modelling approaches often fail to connect with the tools used to design and build CPES.
- They don't take into account new technologies like digital twins and smart manufacturing tools.
- Most existing threat modelling methods don't cover cybersecurity at every stage of a system's life.

(Jbair, M. et al., 2022).

- CPES consist of multiple layers and assets. It can be challenging (due to extensive time, modelling efforts, resources, and cost) to examine all the possible scenarios that could arise as system vulnerabilities (Zografopoulos et al., 2021, p. 29784). If the system isn't modelled correctly, it can hide how parts are connected, which leads to wrong risk calculations
- Threat modelling is often done manually, which is time-consuming, error-prone, and not scalable for complex CPES environments (Jbair, M. et al., 2022).

3. In the context of CPS threat modelling, how can scenario-specific metrics and risk assessment methodologies be used to prioritise vulnerabilities and guide the development of targeted security countermeasures?

Jbair et al. (2022)

- Uses scenario-specific metrics: Attack Vector (AV) and Attack Likelihood (AL), calculated from asset value, vulnerability rating, threat actor capability, and impact severity.
- Combines AV and AL to calculate quantitative and qualitative risk scores**,** which are then used in a risk matrix that helps prioritiing vulnerabilities based on severity and likelihood.
- Helps automatically create technical and policy-based security measures that fit each scenario, using data from digital twin models and engineering tools**.**

References

Jbair, M., Ahmad, B., Maple, C. and Harrison, R. (2022) 'Threat modelling for industrial cyber physical systems in the era of smart manufacturing', *Computers in Industry*, 137, p.103611. Available at: https://doi.org/10.1016/j.compind.2022.103611 (Accessed: 11 August 2025).

Zografopoulos, I., Ospina, J., Liu, X. and Konstantinou,C. (2021) 'Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies', *IEEE Access*, 9, pp.29775–29818. Available at: https://doi.org/10.1109/access.2021.3058403 (Accessed: 13 August 2025).

Limitations of Jbair et al.

1. The methodology is tailored to smart manufacturing and demonstrated using a Festo Test Rig, which limits its generalizability to other CPS domains such as healthcare or autonomous vehicles (Jbair, 2023).

2. Relies heavily on digital twin models for early-stage threat modelling. However, many organisations lack the infrastructure or maturity to implement digital twins effectively, making the approach less practical in broader industrial contexts (Jbair, 2023; Jamil et al., 2021).

3. The methodology emphasises early design-stage modelling, but it does not fully address threats that emerge during deployment, operation, or system evolution →problem when updating threat models over time (Jamil et al., 2021).

4. It may not scale well especially when integrating legacy systems with modern technologies (Saurabh et al., 2024).

5. It is not clear how well it aligns with other established cybersecurity standards like NIST SP 800-82, which could hinder adoption in regulated industries (Saurabh et al., 2024).

6. Although it incorporates both qualitative and quantitative methods, the method lacks metrics for evaluating risk interdependencies across subsystems (Jbair, 2023).

References

Jamil, A.-M., Lotfi ben Othmane, and Valani, A. (2021) ‘Threat Modeling of Cyber-Physical Systems in Practice’. Available at: https://arxiv.org/pdf/2103.04226 (Accessed: 13 Aug. 2025).

Jbair, M., Ahmad, B., Maple, C. and Harrison, R. (2022) 'Threat modelling for industrial cyber physical systems in the era of smart manufacturing', *Computers in Industry*, 137, p.103611. Available at: https://doi.org/10.1016/j.compind.2022.103611 (Accessed: 11 August 2025).

Saurabh, K., Gajjala, D., Kaipa, K., Vyas, R., Vyas, O.P. and Khondoker, R. (2024) ‘TMAP: A Threat Modeling and Attack Path Analysis Framework for Industrial IoT Systems’, *Arabian Journal for Science and Engineering*, 49, pp. 13163–13183. Available at:](https://link.springer.com/article/10.1007/s13369-023-08600-3) (Accessed 13 Aug. 2025).