# Unit 4 Seminar: Risk Identification Modelling

## Workshop Questions

### a. Key Elements and Interdependencies in a Cyber-Physical System (CPS) Threat Model

Cyber-Physical Systems (CPS) integrate computational, networking, and physical processes, forming the foundation of smart infrastructures such as energy grids, transport systems, and industrial control systems. A comprehensive threat model must capture key elements such as sensors, actuators, communication channels, control logic, data flows, and human operators. Equally important are their interdependencies, since a compromise in one domain—such as a communication protocol—can cascade into the physical system (Zografopoulos et al.,2021).

These elements are critical for accurate risk analysis because CPS threats often exploit cross-domain weaknesses. For instance, an attacker might manipulate sensor data (cyber domain) to alter actuator behaviour (physical domain), leading to system failure. Capturing such dependencies enables security engineers to evaluate both direct and indirect risks, supporting more resilient system design (Adamos et al., 2024).

### b. Identifying Attack Entry Points and Vulnerabilities in CPS through Threat Modelling

Threat modelling helps organizations systematically identify attack vectors and vulnerabilities within CPS architectures. Frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) and MITRE ATT&CK enable analysts to map threats to specific components, functions, or data flows (Huang,Poskitt & Shar, 2024).

For cyber-physical energy systems, threat modelling exposes potential entry points such as insecure communication links, weak authentication, or unpatched embedded software (Tatam et al., 2021). However, challenges arise due to the heterogeneity and complexity of CPS environments, where numerous devices operate with differing protocols and real-time constraints. Additionally, many legacy systems lack modern security features, making integration of threat data and mitigation strategies difficult (Castiglione & Lupu,2023).

To overcome these limitations, hybrid threat modelling approaches that combine attack tree analysis with data-driven AI simulations can improve predictive capability and vulnerability visibility (Lee et al.,2021).

### c. Using Scenario-Specific Metrics and Risk Assessment to Prioritise Vulnerabilities

Scenario-specific metrics—such as exploit likelihood, system criticality, and potential impact—are essential in ranking vulnerabilities and allocating mitigation resources. For CPS, quantitative methods like the Common Vulnerability Scoring System (CVSS) can be combined with qualitative expert assessments to balance precision with contextual understanding (Khalil et al., 2023).

Incorporating scenario-based evaluation, such as analyzing energy flow disruptions or sensor data falsification, allows security teams to develop targeted countermeasures. These can include real-time anomaly detection, redundancy mechanisms, or secure communication protocols. By aligning

these measures with the most critical risks, organizations enhance both operational continuity and system resilience.

Ultimately, scenario-specific modelling transforms threat identification from a static checklist into a dynamic prioritization process that evolves with system and threat landscape changes (Badawy Sherief & Abdel-Hamid, 2024).

# References


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.

Adamos, K., Stergiopoulos, G., Karamousadakis, M. and Gritzalis, D., 2024. Enhancing attack resilience of cyber-physical systems through state dependency graph models. *International Journal of Information Security*, *23*(1), pp.187-198.

Huang, S., Poskitt, C.M. and Shar, L.K., 2024. Security modelling for cyber-physical systems: A systematic literature review. *arXiv preprint arXiv:2404.07527*.

Tatam, M., Shanmugam, B., Azam, S. and Kannoorpatti, K., 2021. A review of threat modelling approaches for APT-style attacks. *Heliyon*, *7*(1).

Castiglione, L.M. and Lupu, E.C., 2023. Which attacks lead to hazards? Combining safety and security analysis for cyber-physical systems. *IEEE Transactions on Dependable and Secure Computing*, *21*(4), pp.2526-2540.

Lee, C.C., Tan, T.G., Sharma, V. and Zhou, J., 2021, June. Quantum computing threat modelling on a generic cps setup. In *International Conference on Applied Cryptography and Network Security* (pp. 171-190). Cham: Springer International Publishing.

Khalil, S.M., Bahsi, H., Ochieng'Dola, H., Korõtko, T., McLaughlin, K. and Kotkas, V., 2023. Threat modeling of cyber-physical systems-a case study of a microgrid system. *Computers & Security*, *124*, p.102950.

Badawy, M., Sherief, N.H. and Abdel-Hamid, A.A., 2024. Legacy ICS cybersecurity assessment using hybrid threat modeling—An oil and gas sector case study. *Applied Sciences*, *14*(18), p.8398.