**Unit 4: Risk Identification and Modelling – Case Study**

**Seminar Title:** Risk Identification and Modelling – Case Study

**Reference Paper:** Jbair, M. et al. (2022) Threat Modelling in Cyber-Physical Energy Systems

**Workshop Activity Questions and Answers**

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

According to Jbair et al. (2022), effective CPS threat modelling must capture **physical components, communication channels, control logic, and human–machine interactions**. These elements represent the layered architecture of energy systems where digital operations directly influence physical processes.

Interdependencies — such as the link between sensors, controllers, and actuators — are vital for accuracy because they reveal how a single point of failure can cascade through the entire system. For example, if a compromised sensor feeds manipulated data into a Supervisory Control and Data Acquisition (SCADA) subsystem, operational safety and power stability can both be jeopardised.

Recognising these dependencies helps analysts predict not just isolated incidents but also **propagating attack chains**, a core concept in modern cyber-physical risk assessment (Humayed et al., 2017).

**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?**

Threat modelling provides a **structured approach** to map entry points such as communication interfaces, control ports, wireless links, and third-party integrations. Techniques like **Data Flow Diagrams (DFDs)** and **STRIDE** enable analysts to visualise how data moves across the system and where potential breaches could occur (Microsoft, 2023).  
In CPS, this process reveals how attackers might exploit insecure protocols (e.g., Modbus TCP or DNP3) to manipulate control logic or inject false data. However, challenges arise from system **complexity**, legacy infrastructure, and the **real-time nature** of industrial controls, where downtime for testing or patching may be unacceptable (Knowles et al., 2015).  
Additionally, interconnectivity with IT systems increases the attack surface, requiring analysts to coordinate across engineering and cybersecurity disciplines to ensure comprehensive coverage.

**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?**

Scenario-based metrics allow organisations to quantify the **impact and likelihood** of threats in context — for example, energy distribution disruption or operational downtime. Risk frameworks such as **NIST SP 800-30** and **ISO/IEC 27005** can be adapted to the CPS environment by integrating domain-specific parameters like system criticality, fault propagation rate, and detection latency (NIST, 2012; ISO, 2018).

By assigning scores or weights to these metrics, analysts can **prioritise vulnerabilities** that pose the greatest business or safety risk. For example, a control system exposed to unauthenticated commands may receive a higher risk score than a low-impact monitoring node.  
Jbair et al. (2022) highlight that these methodologies not only enhance technical accuracy but also help allocate resources efficiently and design **targeted mitigation strategies** such as redundant control paths, anomaly detection mechanisms, or automated isolation protocols.

**Reflection**

This case study reinforced the importance of **holistic threat modelling** in cyber-physical environments. I learned that true resilience depends not only on defending digital assets but also on understanding physical interconnections and operational dependencies.  
By analysing CPS systems, I realised that cybersecurity must integrate engineering perspectives — something I can apply directly in managing critical infrastructure projects at MBZUH. The workshop also improved my analytical thinking and my ability to link risk metrics with real-world operational outcomes, bridging the gap between theory and practice.

**References**

* Humayed, A., Lin, J., Li, F. and Luo, B. (2017) ‘Cyber-physical systems security — A survey’, *IEEE Internet of Things Journal*, 4(6), pp. 1802–1831.
* ISO (2018) *ISO/IEC 27005:2018 — Information Security Risk Management.* Geneva: International Organization for Standardization.
* Jbair, M., Al-Awadi, A., Al-Hammadi, F. and Al-Nashif, Y. (2022) ‘Threat modelling in cyber-physical energy systems: A risk-driven perspective’, *International Journal of Critical Infrastructure Protection*, 39, pp. 1–14.
* Knowles, W., Prince, D., Hutchison, D., Disso, J. and Jones, K. (2015) ‘A survey of cyber security management in industrial control systems’, *International Journal of Critical Infrastructure Protection*, 9, pp. 52–80.
* Microsoft (2023) *STRIDE Threat Modelling Framework.* Redmond: Microsoft Security Docs.
* NIST (2012) *SP 800-30 Rev. 1 — Guide for Conducting Risk Assessments.* Gaithersburg, MD: U.S. Department of Commerce.