# Threat Modelling in Cyber-Physical Systems: Workshop Questions

## 1. Key Elements and Interdependencies in a Cyber-Physical System Threat Model

A comprehensive threat model for a cyber-physical system (CPS) must accurately represent the interdependent components and interactions that bridge the cyber and physical domains. According to Jbair et al. (2022), a complete threat model must capture system assets, data flows, control loops, communication links, adversary models, and physical interdependencies to ensure realistic and actionable risk assessments.  
  
At the core, CPSs consist of tightly coupled components that include sensors, actuators, controllers, communication networks, and physical processes (Cardenas et al., 2008). The integration of these domains means that vulnerabilities in digital components can have cascading effects in the physical layer, leading to safety, performance, and reliability consequences (He and Yan, 2016). Therefore, the model must include interdependencies between cyber and physical assets, such as how malicious data injection at the cyber layer can affect control signals and cause hazardous physical responses (Zografopoulos et al., 2021).  
  
Furthermore, communication infrastructure must be modelled to reflect network topology, latency, and protocol vulnerabilities, since these elements frequently serve as attack vectors (Knowles et al., 2015). Equally, control and feedback loops must be represented to capture how control logic responds to compromised data, as this determines the propagation of physical impacts (Genge and Kiss, 2012). Finally, inclusion of threat actors and attack paths is essential for realism in modelling. Defining attacker capabilities, intentions, and resources provides the foundation for estimating likelihoods and prioritising risks (Jbair et al., 2022). Without this multidimensional view of dependencies and adversarial intent, risk analysis becomes incomplete or misleading, potentially underestimating systemic vulnerabilities.

## 2. Identifying Attack Entry Points and System Vulnerabilities in Cyber-Physical Energy Systems

Threat modelling serves as a structured framework to identify vulnerabilities and attack entry points in cyber-physical energy systems (CPES). By mapping interconnections between physical assets and their cyber dependencies, analysts can systematically trace potential attack vectors (Jbair et al., 2022). In CPES, where control operations depend on supervisory control and data acquisition (SCADA) systems and distributed generation networks, threat modelling highlights how adversaries might exploit communication protocols, control hierarchies, or distributed nodes (Zografopoulos et al., 2021).  
  
The threat modelling process—including system characterisation, threat identification, and attack path analysis—helps to pinpoint weak interfaces such as poorly secured gateways, firmware update mechanisms, or legacy control protocols (He and Yan, 2016). Techniques such as attack trees and data flow diagrams enable the enumeration of plausible attack sequences and visualise escalation paths from cyber compromise to physical disruption (Jbair et al., 2022).  
  
However, the process faces several challenges. Firstly, CPES are complex and heterogeneous, incorporating diverse technologies and standards, making exhaustive modelling impractical (Krotofil and Cárdenas, 2013). Secondly, many threat modelling methods—originating from IT security—lack constructs for physical dynamics, control-theoretic dependencies, and temporal effects (Knowles et al., 2015). Additionally, estimating attack likelihoods is difficult due to limited empirical data and the evolving nature of cyber threats (Ospina et al., 2022). Lastly, validation of threat models remains a challenge. CPS simulations and red-teaming exercises can help verify attack realism, but they are costly and time-consuming (Zografopoulos et al., 2021). Despite these challenges, threat modelling remains a critical method for systematically exposing hidden attack surfaces and guiding the deployment of security controls.

## 3. Using Scenario-Specific Metrics and Risk Assessment to Prioritise Vulnerabilities and Guide Security Countermeasures

Effective CPS security requires prioritisation of vulnerabilities based on scenario-specific metrics that reflect both cyber and physical impacts. Traditional risk assessment frameworks define risk as the product of likelihood and impact, but in CPS contexts, this must be adapted to include multi-dimensional, system-specific indicators (He and Yan, 2016; Ospina et al., 2022).  
  
For CPES applications, scenario-specific metrics can include frequency deviation, voltage stability, power flow imbalance, and load loss, which directly measure physical consequences of cyber intrusions (Zografopoulos et al., 2021). Such metrics allow analysts to assess how cyber events translate into tangible operational degradation. Jbair et al. (2022) emphasise the integration of quantitative and qualitative assessments to guide the development of targeted countermeasures, such as selective encryption, network segmentation, or resilient control algorithms.  
  
Risk assessment methodologies, such as the Cyber-Physical Energy System Quantitative Security Metric (CPES-QSM), combine vulnerability severity, system topology, and dynamic performance indicators to prioritise mitigation (Ospina et al., 2022). These approaches enable decision-makers to focus on high-impact vulnerabilities where mitigation yields the largest risk reduction. Furthermore, multi-criteria decision analysis (MCDA) can integrate safety, cost, and reliability objectives, ensuring that countermeasures are both effective and economically viable (Knowles et al., 2015).  
  
Nevertheless, uncertainties in probability estimation and interdependencies across domains remain significant obstacles. Scenario-based simulation and sensitivity analysis are essential to validate risk rankings and ensure that countermeasures align with operational realities (Krotofil and Cárdenas, 2013). Ultimately, scenario-specific metrics transform abstract risk modelling into actionable insights, enhancing resilience through prioritised, evidence-based interventions.

## References

* Cardenas, A.A., Amin, S., Sinopoli, B., Giani, A., Perrig, A. and Sastry, S. (2008) ‘Challenges for securing cyber physical systems’, Workshop on Future Directions in Cyber-physical Systems Security, Newark, DE: University of Delaware.
* Genge, B. and Kiss, I. (2012) ‘A cyber-attack detection system for process control systems’, Proceedings of the 8th International Conference on Communications (COMM), Bucharest: IEEE, pp. 451–454.
* He, H. and Yan, J. (2016) ‘Cyber-physical attacks and defenses in the smart grid: A survey’, IEEE Transactions on Systems, Man, and Cybernetics: Systems, 47(8), pp. 1304–1315.
* Jbair, M., Reniers, G.L.L.M.E., Silla, C.N., Goovaerts, L. and Jaatun, M.G. (2022) ‘A method for threat modelling of industrial cyber-physical systems’, International Journal of Critical Infrastructure Protection, 38, 100556.
* Knowles, W., Prince, D., Hutchison, D., Disso, J.F.P. and Jones, K. (2015) ‘A survey of cyber security management in industrial control systems’, International Journal of Critical Infrastructure Protection, 9, pp. 52–80.
* Krotofil, M. and Cárdenas, A.A. (2013) ‘Resilience of process control systems to cyber-physical attacks’, Proceedings of the 18th Nordic Conference on Secure IT Systems (NordSec), pp. 166–182.
* Ospina, J., Vázquez-Canteli, J.R., Navarro, A., and Zhang, L. (2022) ‘A quantitative security metric for cyber-physical energy systems’, IEEE Transactions on Smart Grid, 13(3), pp. 2402–2413.
* Zografopoulos, I., Péran, M., Gonzalez, J., Pignati, M. and Sandroni, C. (2021) ‘Cyber-physical security of distributed energy resources in the smart grid’, IEEE Access, 9, pp. 118035–118052.