Group work 1: Cybersecurity Testing in Merged Cyber and Physical Spaces

- What are the challenges of risk assessment/management in cyber-physical systems?
- How to increase organizational preparedness?
- What can be learned form observed incidents?
- How does data privacy laws (e.g., GDPR) affect cybersecurity testing?

- How to identify, assess, and mitigate hybrid threats against critical sector systems where the physical space is linked to cyberspace?
- How should organizations prepare for breaches that impact both cyber and physical spaces, and what role does testing play in developing incident response strategies?
- What can be learned from real-world cyber-physical security incidents, and how can cybersecurity testing be improved as a result?
- How do data privacy laws (e.g., GDPR) affect cybersecurity testing, particularly when data is being generated and processed in both the physical and digital realms?

Group work 2: Exploring the Interplay of Safety, Security, Reliability, and Resilience in IT-OT Integration

- How to integrate safety and cybersecurity management in design and in operation? (technical/non-technical)
- How to foster collaboration, knowledge sharing, and mutual understanding to ensure Safety, Security, Reliability, and Resilience in IT-OT Integration?
- To what extent is compliance with standards sufficient to ensure a balanced approach to safety, security, reliability, and resilience?

- What are the best practices for managing conflicting priorities in ensuring safety, security, reliability, and resilience in IT-OT integration, and how can these practices be universally applied across various industries to optimize the interplay between these elements?
- How can safety competence be integrated in cybersecurity management and how can cybersecurity competence be integrated in safety management, in both the design and the operation (deployment) phase?
- How can compliance with standards such as ISO 27001 (information security), IEC 62443 (industrial cybersecurity), and NIST SP 800-82 (cybersecurity for industrial control systems) help ensure a balanced approach to safety, security, reliability, and resilience?
- What strategies can bridge the cultural divide between IT (focused on data security and flexibility) and OT (focused on operational stability and safety) staff, to foster collaboration, knowledge sharing, and mutual understanding?

Group work 3: Secure Industry 5.0 and Industry 6.0: Identifying Emerging Threats and Addressing Needs

- What's new in Industry 5.0 and 6.0?
- What threats are specific for Industry 5.0 and 6.0?
- How to mitigate those threats?
- Are existing cybersecurity standards (e.g., NIST, ISO 27001, IEC 62443) still applicable?
- When humans are collaborating with robots: what are the challenges and dilemmas?

- Based on current trends, what might the future hold for cybersecurity in these emerging industrial paradigms? What threats are on the horizon that we should prepare for now?
- How can organizations proactively identify and mitigate emerging cybersecurity threats specific to Industry 5.0 and 6.0 environments, and what collaborative strategies can be implemented between academia and industry to develop robust security frameworks that address the evolving needs of these advanced industrial paradigms?
- How do existing cybersecurity standards (e.g., NIST, ISO 27001, IEC 62443) apply to Industry 5.0 and Industry 6.0, and what new frameworks may be required?
- What vulnerabilities, legal issues and ethical dilemmas exist in the collaboration between humans and robots, and how can these be effectively addressed?

Group work 4: Trustworthy AI: Balancing Benefits and Risks in Critical Sectors

- How can we use AI to ensure trustworthiness in critical sectors?
- What does it take to make us trust AI?

- What methodologies and frameworks can be applied to evaluate and balance the benefits and risks associated with deploying AI technologies in critical sectors, ensuring trustworthiness?
- What regulatory frameworks are needed to ensure AI is used safely and ethically in critical sectors? Are existing regulations enough, or do new standards need to be created?
- How can AI developers and policymakers ensure that the public trusts AI systems, particularly in high-stakes areas? What role does transparency, accountability, and inclusivity play in gaining trust?
- What is AI's potential role in global geopolitical dynamics, particularly in sectors like defense, cybersecurity, and international trade?