CALL FOR PAPERS

Critical infrastructure like power grids and transportation systems are the backbones of our modern lives. Moreover, it is becoming increasingly popular for companies to adopt the concept of industry 4.0 for maritime systems as a way to manufacture, improve, and distribute their products. Attacks on critical Infrastructure and maritime systems can cause serious consequences for the manufacturers and the whole society. This workshop aims to bring together researchers interested in critical infrastructure and maritime systems security (CIMSS) to share fresh ideas. It also intends to foster communications between academia and industry to discuss real-world challenges and creative solutions.

Topics of interest include, but are not limited to:

- New Attack Vectors on CIMSS
- Empirical Study of CIMSS
- Formal Treatment of CIMSS
- Authentication and Remote Attestation
- Human Factors in CIMSS
- Intrusion/Anomaly Detection/Prevention
- Forensics in CIMSS
- Novel Security Notions for CIMSS

- Cryptographic Tools for CIMSS
- Vulnerabilities Discovery and Management in CIMSS
- Intellectual Property Protection in CIMSS
- Novel Analysis Tools for CIMSS
- Risk Management
- Control Theoretic Methods for CIMSS
- Ransomware in CIMSS

Important Dates

- **Submission: March 23, 2025**
- **Notification: April 23, 2025**

- **Camera-ready: May 12, 2025**
- **Workshop dates: TBD During June 23-26, 2025**

Workshop Chairs

- Zengpeng Li (Shandong University, China)
- Ahmed Amro (Norwegian University of Science and Technology, Norwegian)

Publicity Chair

- Chenglu Jin (CWI Amsterdam, The Netherlands)

Contact: cimss2025@easychair.org