Adoption of computing devices in Critical Infrastructures (CIS) render these systems susceptible to physical and/or cyber security threats. The KIOS CoE Cyber-Physical Security testbed aims to model, identify, and control security vulnerabilities and attacks in a wide class of CIS. The testbed integrates and exploits the interoperability between Software and Hardware components.

ARCHITECTURE
- Software Emulators of several Critical Infrastructure Systems
- Virtual PLCs implemented on small computing devices (e.g., RPis)
- Hardware in the Loop (HIL) PLCs
- Integration of Virtual (simulated) and Real Network Infrastructures
- Use of Industrial grade Control and Security Systems

CAPABILITIES
- Model and implement attacks in different CIS
- Identify vulnerabilities in existing CIS and their individual components
- Deploy and test attack detection and mitigation algorithms
- Design and implement vulnerability control mechanisms for attack prevention

IMPACT
- Education and training activities on various types of attacks
- Provide solutions for attack detection, prevention, and mitigation for various CIS
- Demonstrate security vulnerabilities of current CIS
- High-quality research in the security of cyber-physical systems
- Provide an exercise ground for CIS operators to facilitate attack identification and forecast