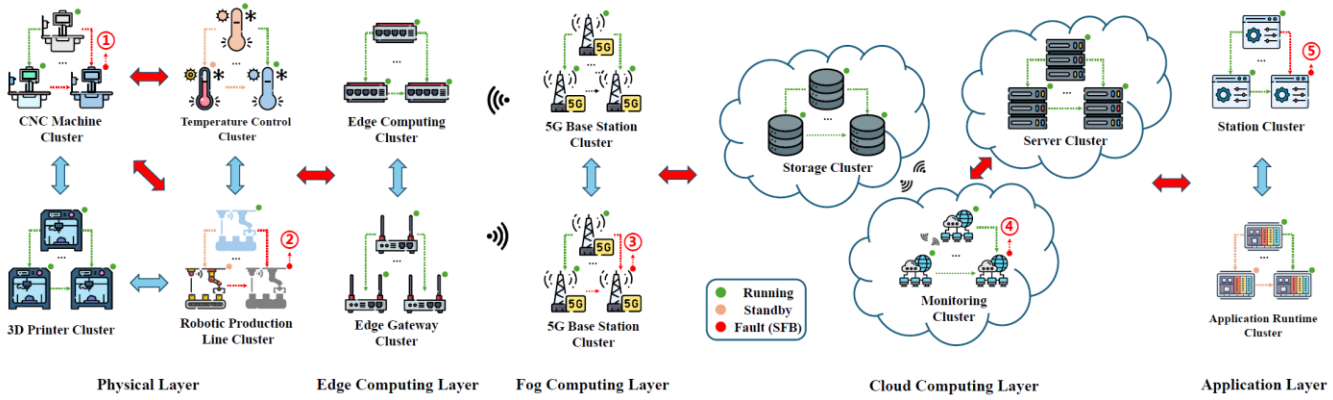
A Systematic Review of Semantic Firmware Bugs and Security Challenges in Distributed Industrial Cyber-Physical Systems

Hao LIU, Yucheng LIU, Bruno SILVA, Raphael Elikplim NKROW, Dutliff BOSHOFF, Lu ZHOU, Liquan CHEN, Gerhard Petrus HANCKE

Frontiers of Computer Science, DOI: 10.1007/s11704-026-51802-9

Problems & Ideas

- Problems of conventional stereo matching approaches:
  - Traditional security analyses primarily focus on memory corruption vulnerabilities, often overlooking complex **semantic and logic bugs**.
  - The distributed and heterogeneous nature of Distributed Industrial Cyber-Physical Systems (DICPS) makes semantic bug detection highly challenging.
- Ideas: A systematic review that categorizes semantic firmware bugs, analyzes the unique attack surfaces in DICPS, and provides a comprehensive overview of current detection methodologies.



The architecture of Distributed Industrial Cyber-Physical Systems (DICPS) and the potential attack surfaces for semantic firmware bugs.

Main Contributions

- Contributions:
  - A novel taxonomy: Proposes a systematic classification of semantic firmware bugs specifically tailored for Distributed Industrial Cyber-Physical Systems.
  - Comprehensive analysis: Evaluates state-of-the-art vulnerability detection techniques, highlighting their strengths and limitations in industrial contexts.
  - Future directions: Identifies critical security challenges and outlines promising future research directions for mitigating semantic vulnerabilities in DICPS.