

Toward Integrated Cyber-Physical Security and Resilience in IIoT Manufacturing: Risk, Detection, and Control

BIOGRAPHY

Dan Li is an Assistant Professor in the Department of Industrial and Systems Engineering at the University of Washington. She received her Ph.D. in Industrial Engineering and M.S. in Statistics from Georgia Institute of Technology and her B.S. in Automotive Engineering from Tsinghua University, Beijing, China. Her research interest lies in developing new data-driven algorithms that are tailored for enhancing the cyber-physical resilience and security of critical infrastructures. Dan is the recipient of the NSF CAREER Award and the IISE Transactions Best Application Paper Award. She has also been recognized in multiple Best Track Paper and Best Student Paper Awards in Energy Systems, DAIS, and QCRE divisions at the IISE Annual Meetings, as well as the INFORMS QSR community.



ABSTRACT

The emergence of Industrial Internet of Things (IIoT) technologies has significantly heightened societal and research interest in fortifying the security and resilience of manufacturing systems, especially in the context of industrial control. Within manufacturing systems, cyber-physical attacks exploit cyber network vulnerabilities to compromise operations, ultimately causing physical damage. However, current solutions borrowed from other fields lack a holistic understanding of cyber-physical security resilience in these complex systems, failing to establish the connection between IIoT network vulnerabilities and system dynamics to guide detection and control. In this talk, I will highlight my recent studies and future research directions related to manufacturing cyber-physical security and resilience from the following aspects: (1) Integrated Cyber-Physical Risk Quantification; (2) Data-Driven Cyberattack Identification; and (3) Learning-Based Resilient Control.