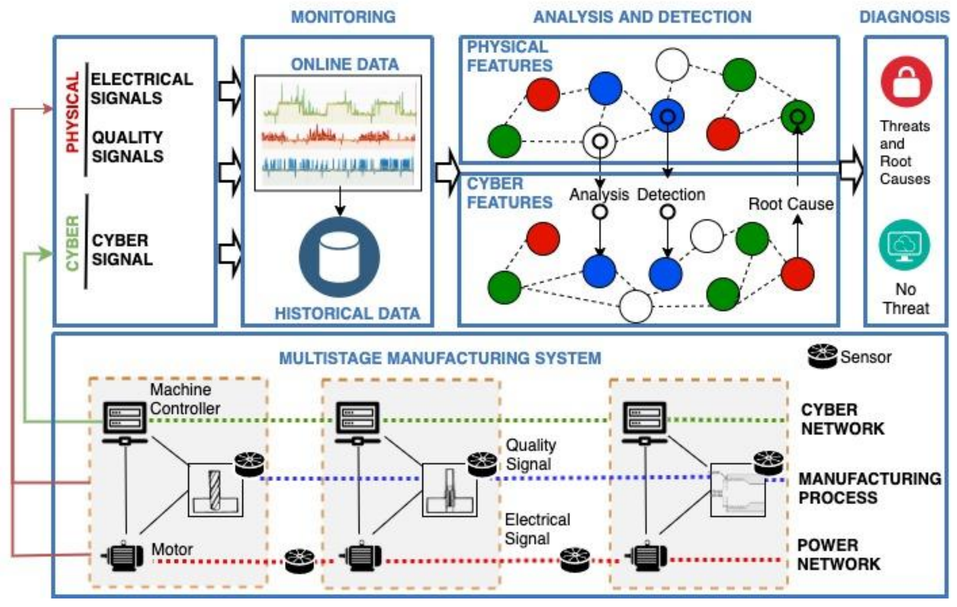
Cyber-threat Detection and Diagnosis in Multistage Manufacturing Systems through Cyber and Physical Data Analytics

Wenzhan Song[1], Jin Ye[1], Jianjun Shi[2], Peng Liu[3],
[1]University of Georgia, [2]Georgia Institute of Technology, [3]Pennsylvania State University

Project URL: https://sensorweb.engr.uga.edu/index.php/cyber-physical-security/

Overview: This project develops cyber-threat detection and diagnosis (CDD) techniques in multi-stage manufacturing systems (MMS) through cyber-physical data analytics. The goal is to enable the prevention and mitigation of potential harms at the early stage, proactive and predictive maintenance, and countermeasures. The idea of integrating cyber and physical signals for cyber-security improvement is an emerging topic of SaTC.



Challenges:

- The cyber-threats may compromise the integrity of machine controllers and manufacturing machines through the communication networks or other means such as Trojan or insider attack. The integrity attacks are stealthy and difficult to detect in the cyberspace.
- There lacks a generalized methodology to detect and diagnose cyber and physical threats in manufacturing systems.
- Stealthy Attack Generation framework that holistically integrates requirements and topology of MMS in the presence of an adversarial insider attacker
- Cyber threat detection and causal identification from cyber and physical MMS sensor data in the presence of stealthy insider attacks

Scientific impacts:

- Innovative approaches for cyber-threat detection and diagnosis are needed for infrastructure security and economic considerations.
- The research results, including source codes and, hardware designs and evaluation testbeds, will be available to the academic community.
- The proposed cyber-threat detection and diagnosis will create a paradigm shift in the security monitoring approaches.
- The proposed cyber-physical spatio-temporal data analysis are fundamental and broadly applicable to many CPS for security and health analysis. The cyber and electrical signals used in CDD are commonly available in most CPS.

Solutions:

The proposed CDD tool will monitor a variety of cyber and physical signals and perform cyber-threat detection and root cause diagnosis through advanced cyber-physical data fusion and taint analysis.

- CDD via data fusion of process and product quality signals. We focused on characterizing the interrelationships between the process signals, and developed the stealthy attack experiments and countermeasures.
- CDD via data fusion of electrical waveform signals. We explored advanced statistical data processing techniques to detect and identify root causes of cyber attacks. We investigated whether the PMU features (voltage, frequency and phase), plus harmonic features THD (Total Harmonic Distortion), are sufficient to construct the feature matrix.
- CDD via cyber-physical dynamic taint analysis. We implemented the intrusion monitoring and diagnosis with a Cyber-Physical information flow model. Then use this model to bridge the monitoring and instrumentation gap.

Broader impacts on society

- The proposed cyber-threat detection and diagnosis will create a paradigm shift in US manufacturing sectors by empowering manufacturing industry to detect cyber threats at an early stage and take preventive actions.
- We collaborated with industry to get industrial needs, data sets, and validation consultation in practice.

Broader impacts on education

- Enrich undergraduate and graduate curriculum and research training. The research results of this project has been incorporated in the undergraduate and graduate course curriculum.
- Several graduate students are supported for thesis research.
- Robins AFB and OGT will also provide student intern opportunities and test the R&D results from this project in industrial settings.

Broader impacts on participation

- Engage minority and female students in STEM research and education. We have applied the REU supplement for undergraduate participation.
- Outreach to K-12 students and broader scientific community. The PI is actively mentoring a high school HackClub and partnering with high school teachers on their computer science and engineering courses.