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

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.

Solutions:

- CDD via data fusion of process and product quality signals. We focuses on characterizing the interrelationships between the process signals
- CDD via Data Fusion of Electrical Waveform Signals. we plan to explore advanced statistical data processing techniques to detect and identify root causes of cyber attacks.
- CDD via Cyber-Physical Dynamic Taint Analysis. We plan to implement intrusion monitoring and diagnosis with a Cyber-Physical information flow model.

#2019311, University of Georgia,
WenZhan Song (wsong@uga.edu)

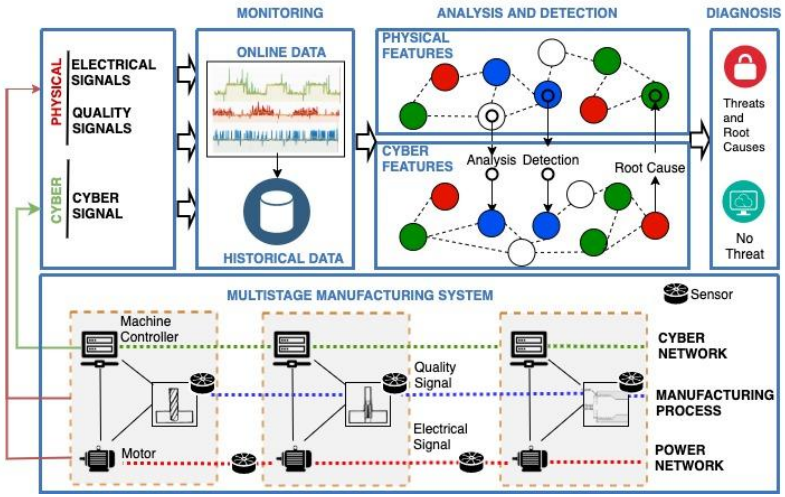

Fig 1: CDD in MMS through cyber-physical data analytics. In MMS, cyber networks, power networks and quality-control signals can be said as its **nervous system**, **circulatory system** and **vital signs**, respectively. In MMS and CPS in general, it is natural and necessary to integrate the signals from both cyber and physical systems to improve cyber-threats detection, as some critical cyber-threats can only be revealed from the physical system measurements or the interdependency analysis of physical and cyber systems. The idea of integrating the cyber and physical measurements in cyber-security improvement is an **emerging** topic for SaTC research and yet to be explored.

Scientific Impact:

- 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, would be available to the academic community.
- The proposed cyber-threat detection and diagnosis methods have been published and cited in top journals and conferences;

Broader Impact and Broader Participation:

- Engage minority and female students in STEM research and education. The PIs will continue our success of engaging underrepresented undergraduate students in the STEM research and education, by collaborating with the Peach State LSAMP.
- Enrich undergraduate and graduate curriculum and research training. The research results of this project will be incorporated in the undergraduate and graduate course curriculum
- Outreach to K-12 students and broader scientific community.