Context-Aware Intrusion Detection in Smart Manufacturing System

Yuru Shao[1], Ruowang Zhang[1], Andrew Ramacher[1], Kira Barton[2], Z. Morley Mao[1]
[1]Deparment of Computer Science and Engineering, [2]Department of Mechanical Engineering
University of Michigan

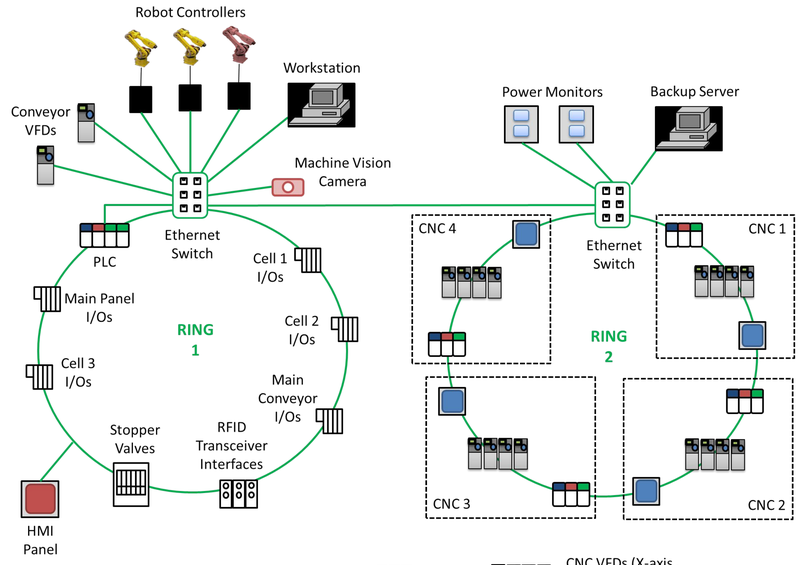
1. The Problem

Smart manufacturing enables high **connectivity**, **interoperability**, and **heterogeneity** in manufacturing systems. Different devices are able to communicate through networks using industrial protocols such as EtherNet/IP. Network-based attack surfaces are inevitably expanded due to the increasing connectivity and interoperability, as well as the integration of Industrial Internet of Things (IIoT). A previous survey of the public IPv4 address space found more than 60,000 publicly accessible industrial control systems [1].

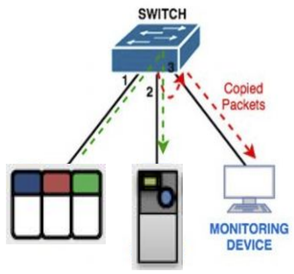
Previous work in anomaly & intrusion detection utilizes only either physical data or network data. It is challenging to tell intrusions from system anomalies without context.

2. What data is available?

- Factory-floor data
  - Machines, sensors, cameras, conveyors, etc
  - Open Platform Communications (OPC) protocol provides data access as tags (*i.e.*, key-value pairs)
- Network traffic
  - All devices are in the same local network. Ethernet switches connect devices together and receive, process, and forward data to the destination device.
  - **Port mirroring** allows us to monitor network traffic on a switch port in real time

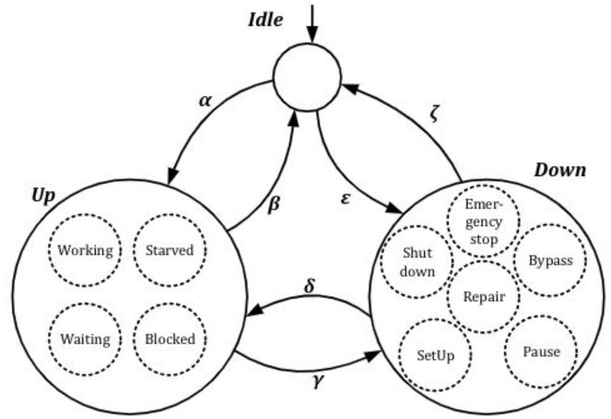


Network topology of the SMART testbed



3. Our Approach

Insights: device data in physical space reveals machine state, from which we can build system-wide context. Network traffic can help with understanding anomaly provenance.

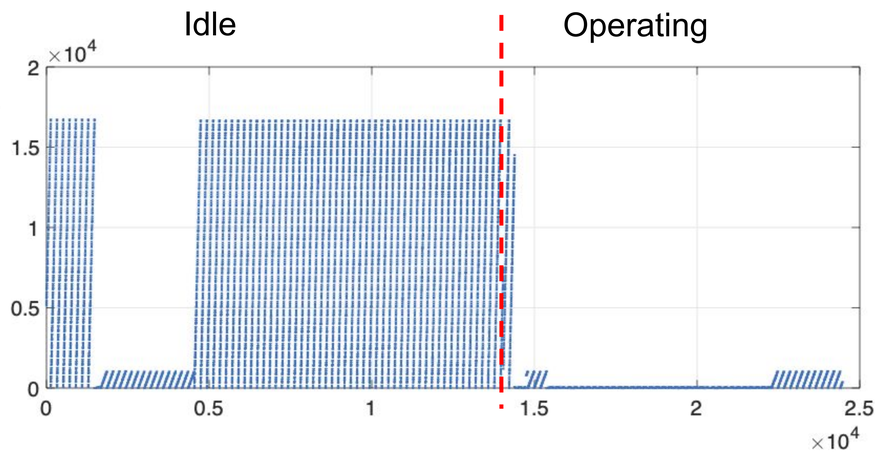


We propose an intrusion detection framework that leverages data analysis techniques to detect intrusions

- Using physical machine data to model system contexts
- Collecting and analyzing a large volume of network traffic in order to identify anomalies and trace their provenance, *i.e.,* whether or not they are caused by attacks.

4. Preliminary Results

- We monitor CNC traffic under **Idle** and **Operating** states
- We extract Ethernet/IP *Connected Data Item*
- Item values are plotted. The difference is obvious, as shown in the figure
- More data items under exploration



[1] Mirian, A., Ma, Z., Adrian, D., et al, 2016, December. An Internet-wide view of ICS devices. PST 2016