CREDC Industrial Workshop 2017

Ants on the Grid: Biology–Inspired Monitoring for Incident and Vulnerability Detection

Josephine Lamp, Carlos E. Rubio-Medrano, Ziming Zhao and Gail-Joon Ahn

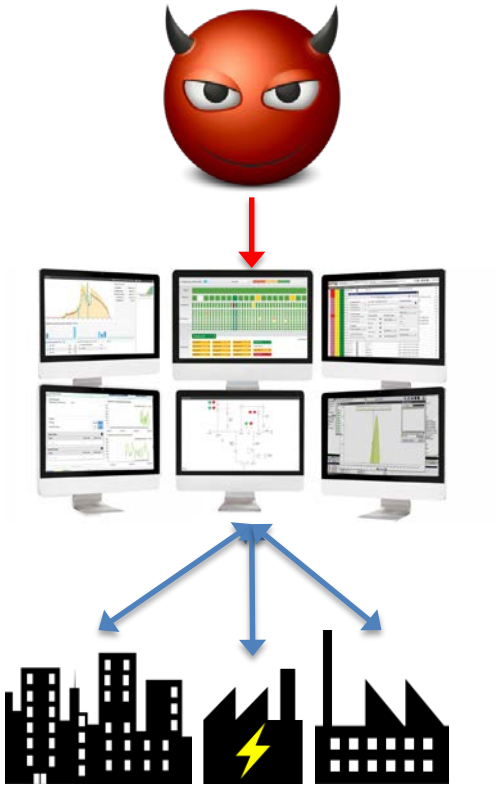
ARIZONA STATE UNIVERSITY

CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

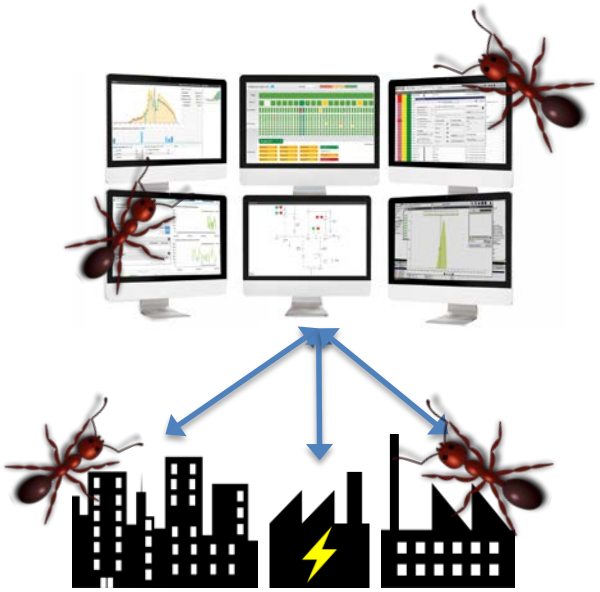
Motivation

- Sophisticated attacks target entire Industrial Control Systems (ICSs):
  - Existing solutions focus on a *small scale*: separate pieces of the system, i.e., end devices
  - Difficult to detect *large-scale* attacks



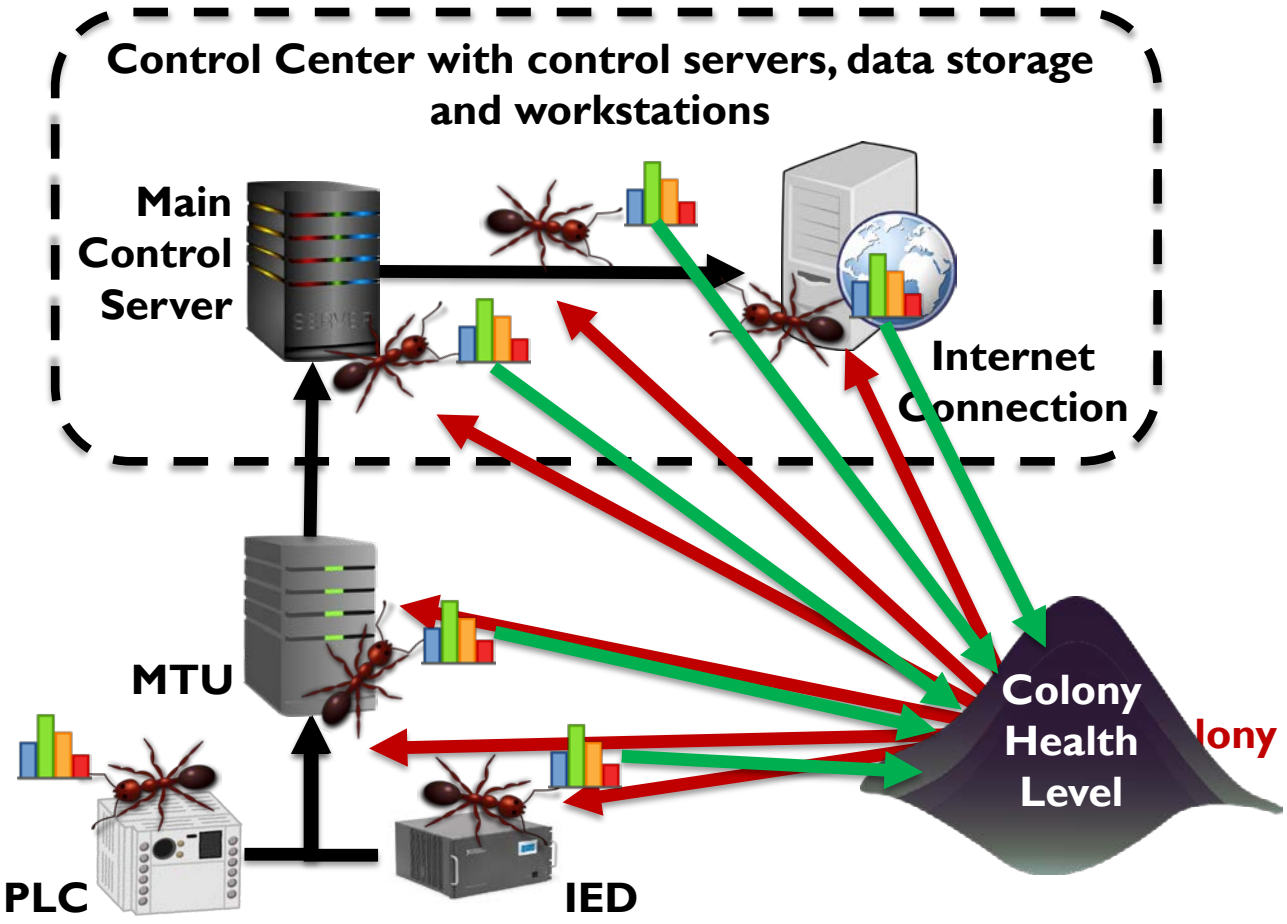
Our Proposal

- A *system-wide* vulnerability and incident detection system that:
  - Places numerous small software/hardware sensors on the grid, aka *ants*[1]
  - Groups them together to link anomalies to vulnerabilities

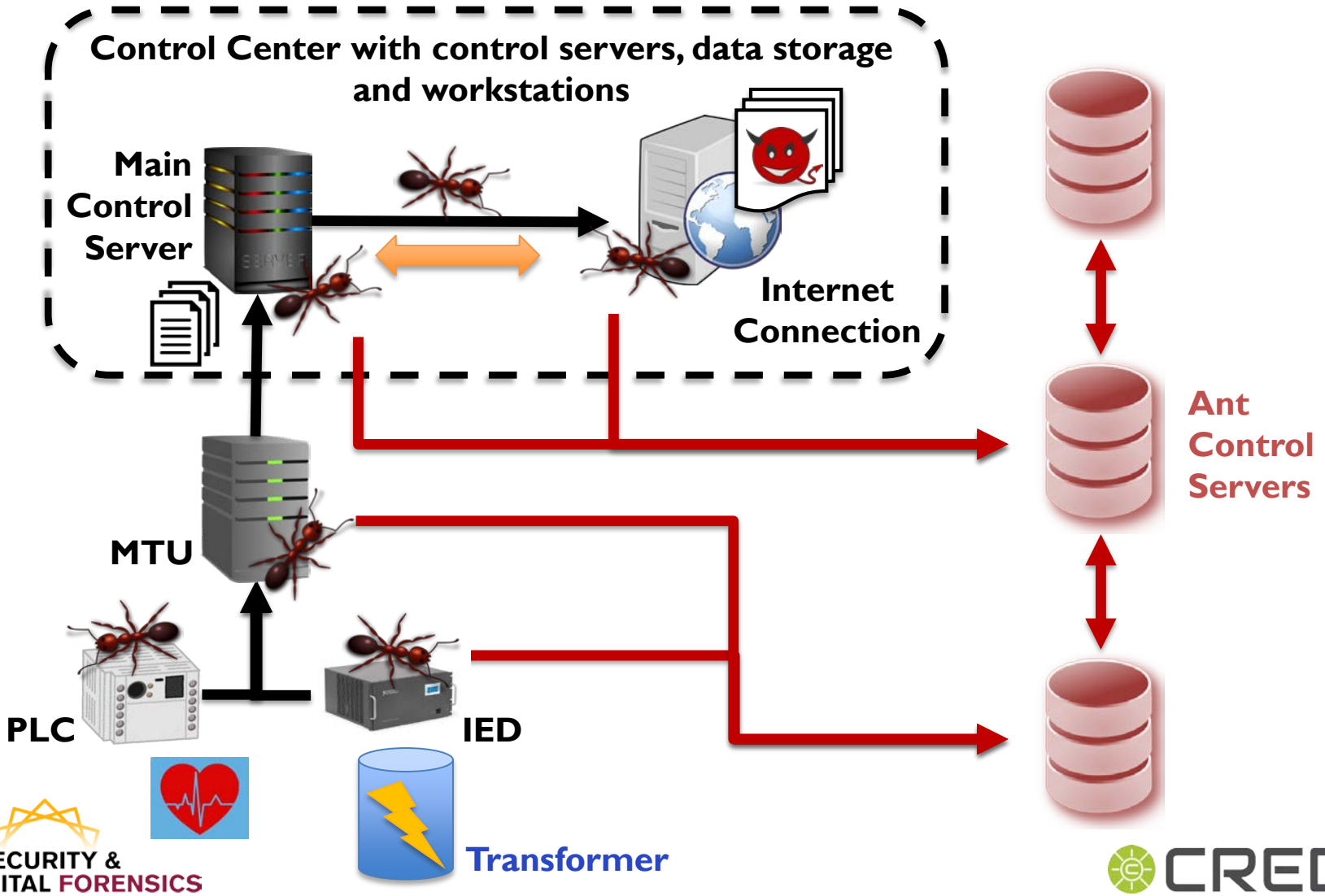


1.) Fink, Glenn A., Jereme N. Haack, A. David McKinnon, and Errin W. Fulp. "Defense on the move: ant-based cyber defense." *IEEE Security & Privacy* 12, no. 2 (2014): 36-43.

Ant Sensors and Architecture



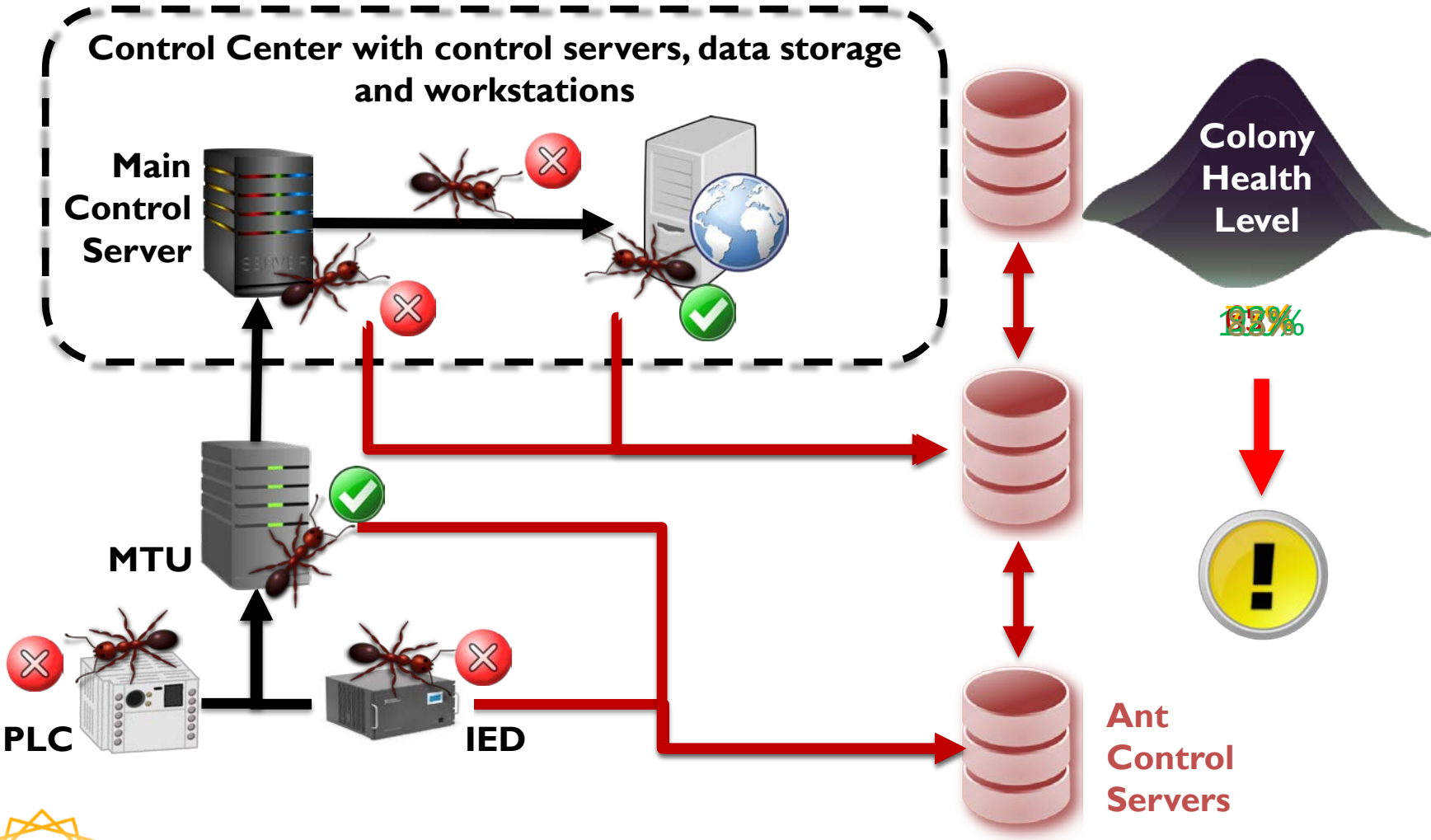
Ant Sensors and Architecture



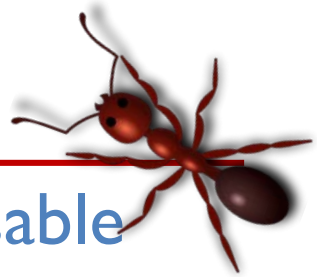
CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

CREDC

Colony Health, Ant Fitness



Advantages of Using Ants



- Ants may be unintelligent and lightweight, reusable and shareable
- Correlate anomalous findings across disparate parts of the grid into a distributed, integrated, and customizable solution
- Provide evidence of incidents and vulnerabilities
- Aid for ICS operators and security officers

Current Work

- Placement and development of ants
- Colony definitions and specializations
- Coordination and correlation of ant finesses with colony health levels

Questions and Contact

- Thank you for listening!

- CDF Website: https://globalsecurity.asu.edu/cdf
- Josephine Lamp: jalamp@asu.edu