JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Self-Aware Industrial Control Systems through Cloud Based Autonomic Computing

Christopher Rouff, Ali Tekeoglu, Joseph Maurio, Alexander Beall

christopher.rouff@jhuapl.edu

Critical Infrastructure Protection Group
Applied Physics Laboratory
Johns Hopkins University

Overview

- Industrial Control Systems
- Industrial Control System Vulnerabilities
- Approach
- Autonomic cloud architecture for ICSs
- Summary

Introduction

- Historically operational technology (OT) has run on private networks
  - Security was through lack of public access and security by obscurity since few people new how to program OT devices
  - Most OT devices have little or no cyber security built into them
- Many OT networks are now connected to enterprise networks
  - This facilitates remote access, updates and monitoring
  - Security of OT networks is now based on enterprise networks
  - ICS and other OT are now vulnerable to malicious actors who can move laterally from the enterprise to the OT networks
- Detecting OT malicious activities is now left to OT operators
  - Detection is often based on experience and anomalous behaviors

Industrial Control Systems Technical Trends

- Panel Based Controls
  - Push Button
  - Stand Alone
  - No Networks
  - No Comms

- Legacy Equipment
  - Proprietary Networks
  - Proprietary OS
  - No Ethernet
  - No Connections
  - Security by Obscurity

- Modern Equipment
  - Ethernet Everywhere
  - Wireless in the Rack
  - Remote Configuration
  - Windows and Linux OS
  - COTs Hardware & Software
  - Security by Obscurity Gone

Bank of Industrial Control Systems

- Limited processing power
- Limited cyber protection
- Often connected to enterprise networks

German Steel Mill and Ukrainian Power Grid

- 2014 Cyber attack on German steel mill inflicted serious damage
  - Demonstrated advanced knowledge of ICS systems
  - Caused multiple components to fail, resulting in physical damage
- Coordinated attack caused outage affecting 80,000 Ukrainians
  - Adversary infected SCADA system computers with malware
  - Were able to remotely open breakers and disconnect 30 substations
  - Acted to blind dispatchers and impede restoration efforts

Water Treatment Plant Hacked

- Verizon Security Solutions' Data Breach Digest from March 2016 identified a hack against an unspecified water utility, referred to by the pseudonym Kemuri Water Company (KWC)
  - A "hacktivist" group exploited unpatched web vulnerabilities in an internet-facing customer payment portal
  - They then accessed KWC's AS/400-based operational control system using login credentials stored on the front-end web server
  - There was evidence that the values controlling the flow of chemicals had been manipulated
    - No significant physical effects were observed
    - Hackers lacked knowledge of ICS systems or the intent to do harm

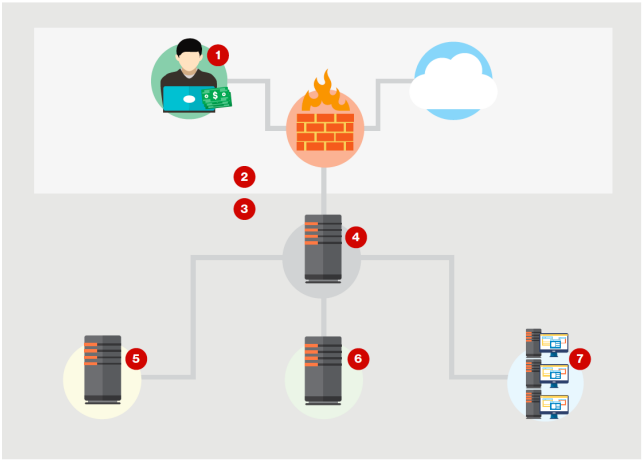
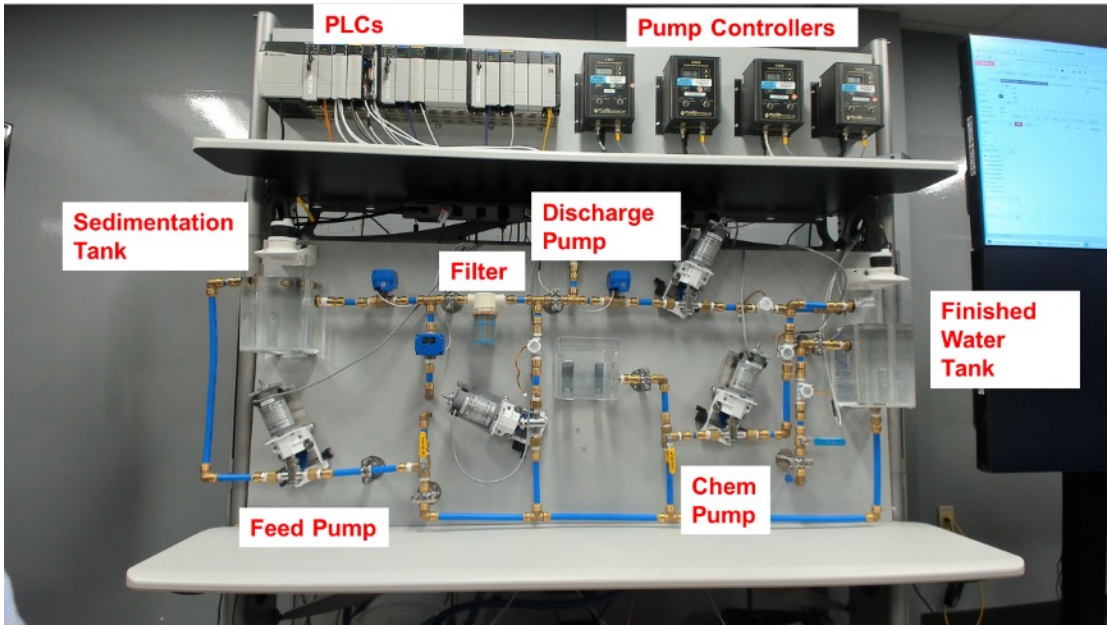


Figure 2

1. Customer access to payment system
2. External (Internet)
3. Internal (Corporate access)
4. AS400
5. PLC management
6. Finance access (PII access)
7. IT management

Industrial Control System Lab

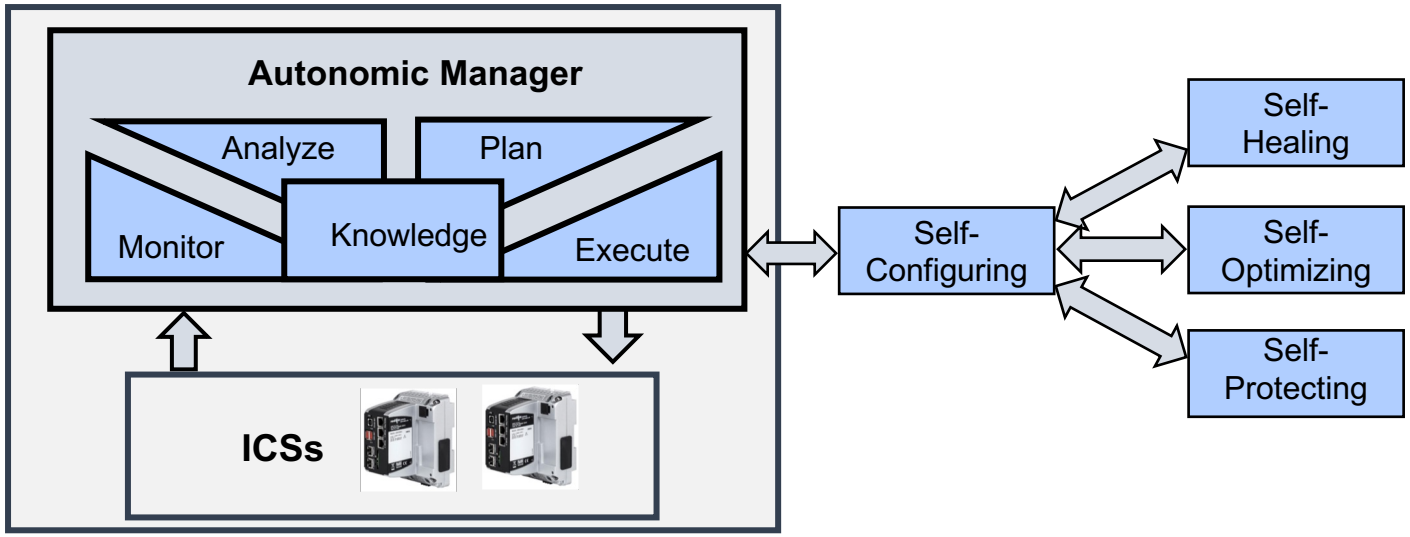
- PLCs in a lab environment
- Models a water treatment system



Approach

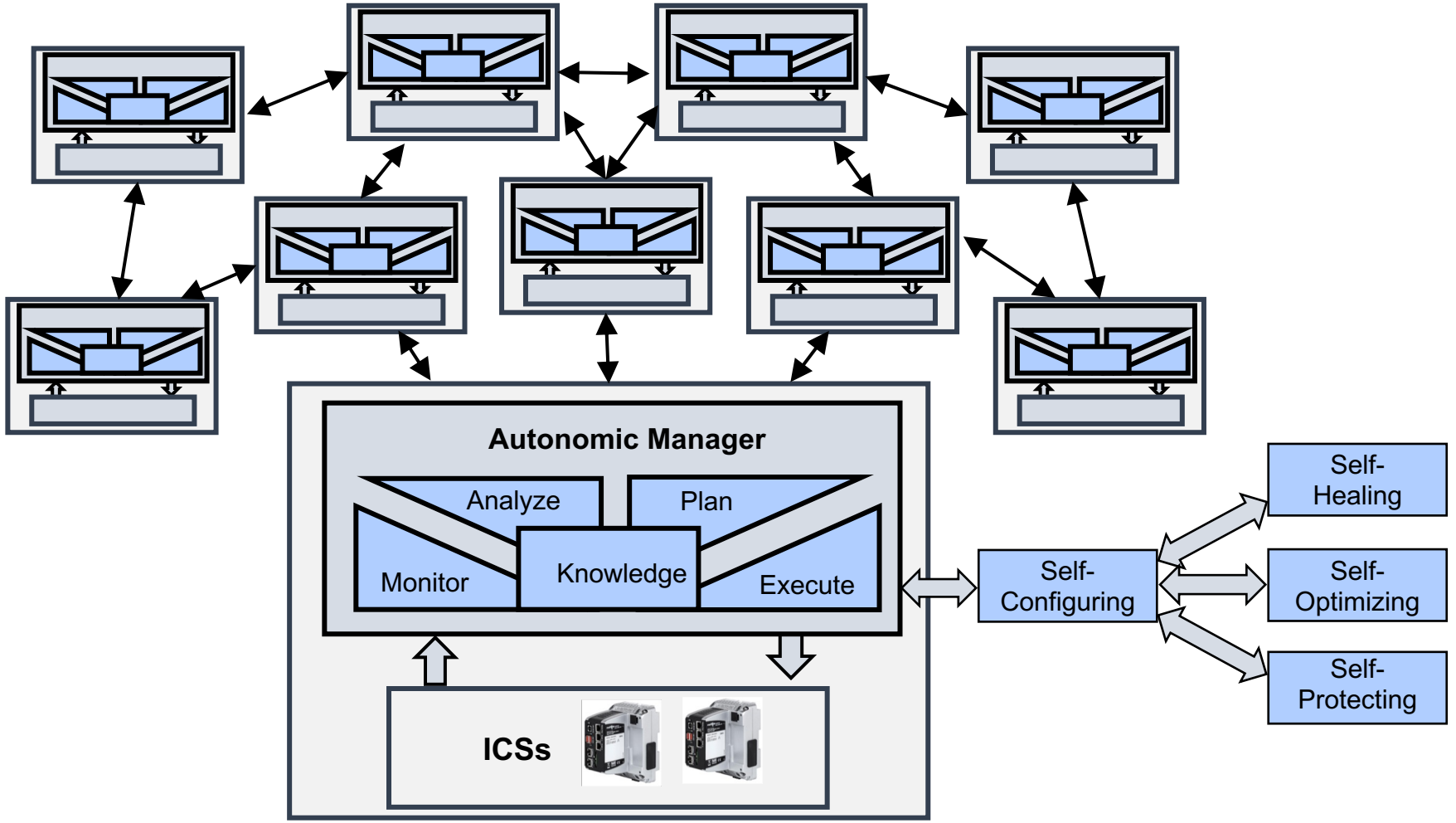
- Provide self-awareness to ICSs using autonomic computing
- Use autonomic self-* constructs to protect ICSs
  - Self-Configuring, Self-Healing, Self-Optimizing, Self-Protecting
- Allow ICSs autonomic managers to communicate threats with each other to cooperate/collaborate
- Use cloud computing to virtualize ICS computations and communicate threats between ICSs

MAPE-K Autonomic Architecture



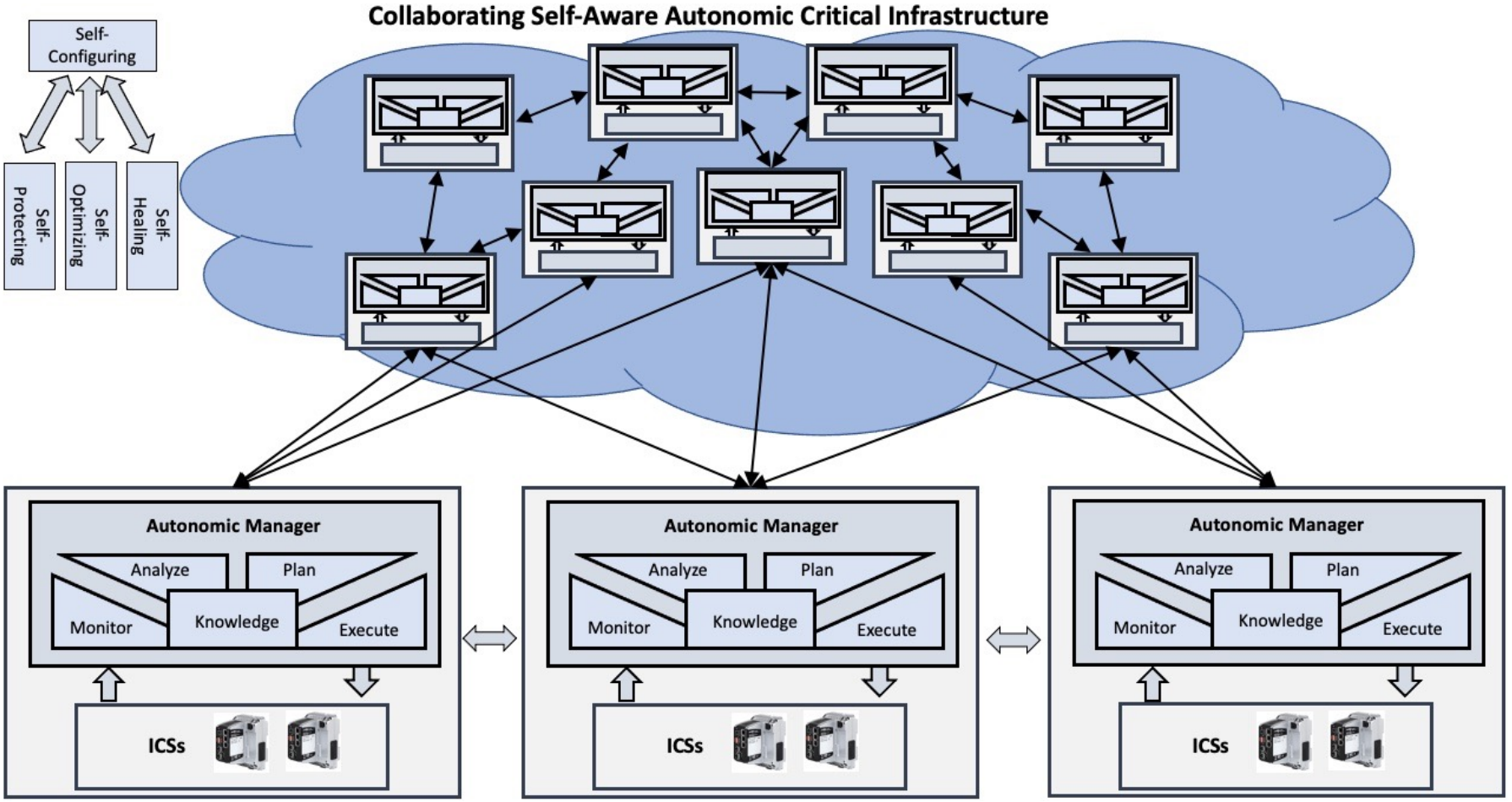
- Individual ICS autonomic Self-* autonomic properties

Collaborating Autonomic Managers



- Autonomic managers collaborating to address attacks on ICSs

Cloud Based Self-Aware Autonomic ICS



Summary

- Critical infrastructure industrial control systems are being connected to enterprise networks which make them vulnerable to cyber attacks
- Several attacks on ICSs have occurred in the recent past and it is expected that more attacks will occur
- Cloud-based autonomics can be used to enhance industrial control systems computation and communications
- Networking autonomic managers can be used to allow cooperation and collaboration across ICSs to thwart and recover from attacks

JOHNS HOPKINS

APPLIED PHYSICS LABORATORY