SAND2018-11835C

Toward a Multi-Agent System Architecture for Insight & Cybersecurity in Cyber-Physical Systems

PRESENTED BY

William M.S. Stout

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

OVERVIEW

Background

Benefits vs State-of-the-Art

Opportunities

Multi-Agent Systems

Building a MAS

Conclusions

BACKGROUND

Operational Technology (OT) networks existed before the dawn of the internet

- Security by isolation

Convergence of OT and IT networks…

- ICS, IIoT, IoT
- Impending threat/execution of cyber attack
  - MITM/signal emulation
  - Sensor influence/hijack
  - Malware/ransomware
  - D/DoS
  - Device destruction

BACKGROUND

Methods to secure cannot be reasonably implemented due to:

- legacy equipment
- vendor complicity
- cost (resource, monetarily)

New approaches are needed to address past tech, current tech, and still be flexible to accommodate and grow with future tech.

Ref cloud/IT network-security based on agents

- Multi-Agent Systems (MAS)

BENEFITS VS. STATE-OF-THE-ART

Current approaches;

- username/passwords
- embedded certificates
- block-chain

Oft rely on greenfield, proprietary, retrofitting

Disproportionate cost vs. device resources/usage

MAS to provide:

- intelligent, uninfluenced visibility
- extensibility (to other networks)
- interfaces to support additional responses/defenses

OPPORTUNITIES

- Ubiquity/proliferation of OT-networks
  - Address legacy, inject to new technology
    - Augment legacy with "on-the-wire" devices
    - SDN, containers, virtualization for new deployments
  - Cross-pollination of IT/cloud and OT
    - Industrial {Internet|IoT}
    - Io{T|V}
    - Smart{homes|grids}
- Coming soon: Software-defined OT
  - Cyber to the fog and endpoint
  - Intelligent Edge (IT-compatible)

Multi-Agent System (MAS)

- agent (Latin, agree, "to do"): operate autonomously, perceive their environment, persist over a time period, adapt to change, create or pursue goal(s).
- Akin to an organization
  - Departments/operations to support org goals
  - Independent/interfacing/information exchange

- Reactive: react to commands/environments
- Proactive: actively achieve goals thru interaction
- Social: communicate with other (agents)

Multi-Agent System (MAS)

- Sensors: perceive their environment
- Actuators: act upon the environment
- Percepts: perceptual inputs
  - Percept sequence: history of all the agent has perceived

- AI → ability to act autonomously
  - Bridge the gap between sensing and actuating
- Agent view: Micro-perspective
- MAS view: Macro-perspective

Multi-Agent System (MAS)

- Coordination (cooperation): needed to ensure community MAS work together cohesively; coordination due to:
  - agent goals may conflict internally/externally
  - agent goals may be interdependent
  - agents may have different knowledges/capabilities
  - agents goals may be accomplished faster (work together)
- Coordination Approaches:
  - Organizational structuring
  - Contracting
  - Multiagent planning
  - Negotiation

BUILDING A MAS

IT/Cloud operating in untrusted network-space, leveraging agents.

Autonomous Agents (AA)

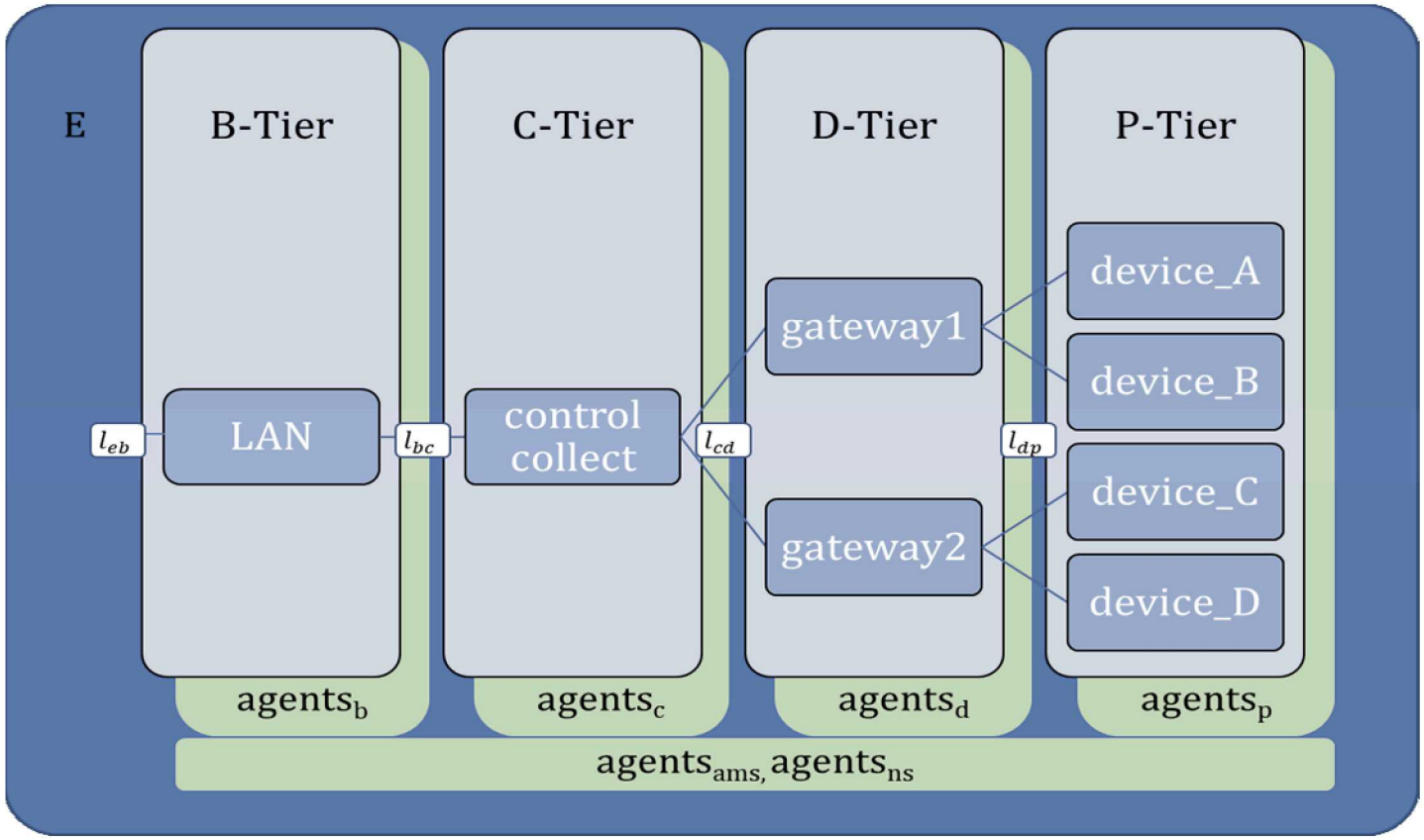
- SW or broadcast-medium based, proving:
  - Passive listening/active probing (where applicable)
  - Data/metadata collection
  - Behavioral analysis and majority voting schemes
  - AA self-policing
  - Active defense techniques
  - Security policy enforcement

BUILDING A MAS

General Categorization for Network Architectures (OT and IT)

Network Model	B-Tier	C-Tier	D-Tier	P-Tier
ICS	Business, Logistics (Level 4)	Control software, HMI, Operations (Level 2/3	Remote devices, collection (Level 1/2)	Physical domain, devices (Level 0/1)
IoT	Business, User Access (Actions)	Storage, Processing, Reporting, Cloud (Insights)	Gateways, Hub	Things, sensors
IIoT	Business Integration	Information, operations, applications	Control	Proximity and physical systems
Enterprise/Cloud	Data center, edge, cloud	Core routing, boundary	Concentrator, distribution	Access, mobile, endpoints

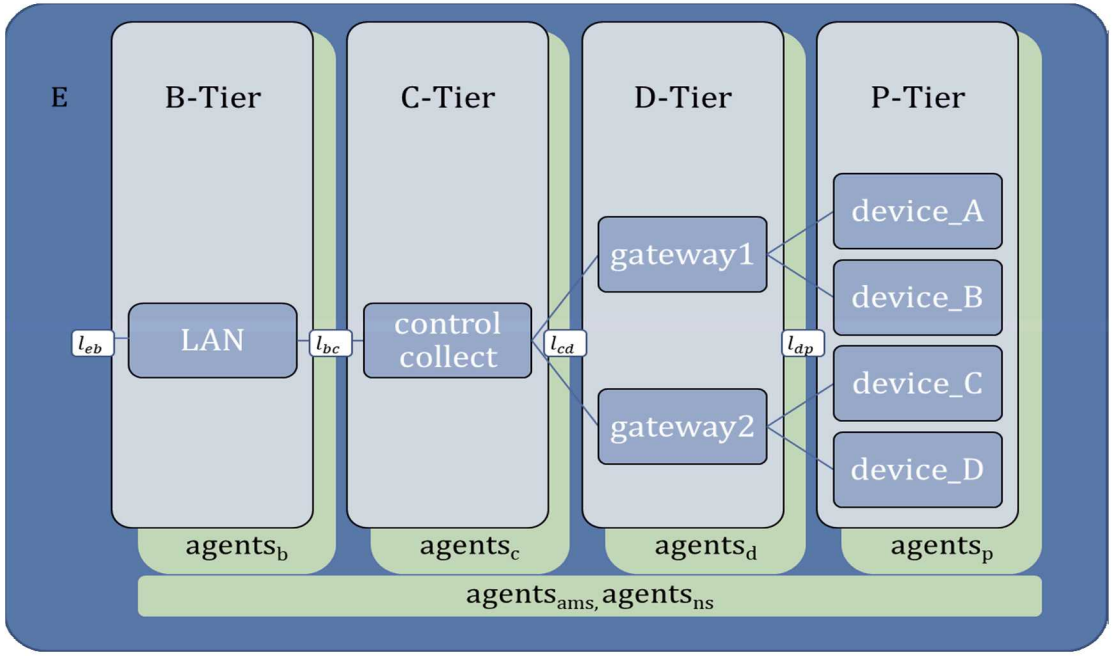
BUILDING A MAS



BUILDING A MAS

$$S_n = \langle E|B|C|D|P\rangle$$
$$L = \langle l_{eb}|l_{bc}|l_{cd}|l_{dp}\rangle$$

$$S_a = \langle a_{\{b,c,d,p\}}|ns_j|ams_k\rangle$$



BUILDING A MAS

$$a_i = \langle \kappa | \sigma | \alpha | \rho | \gamma | kb \rangle$$

$\kappa = developer\ or\ AMS\ knowledge$

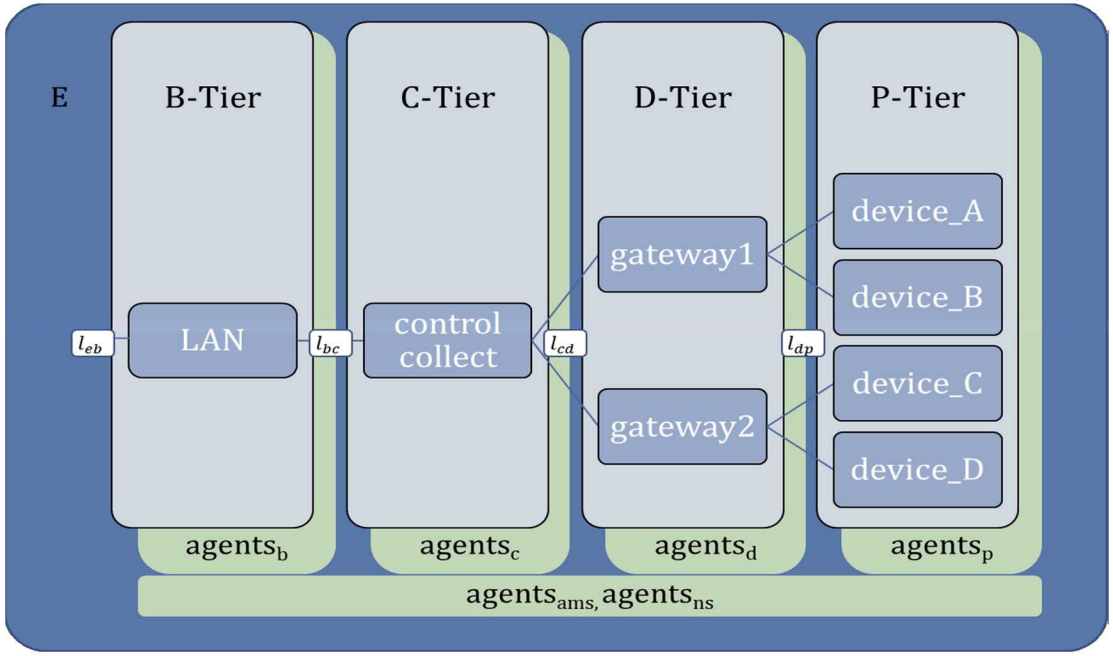
$\sigma = sensors$

$\alpha = actuators$

$\rho = percept$

$\gamma = goals$

$kb = knowledge\ base$

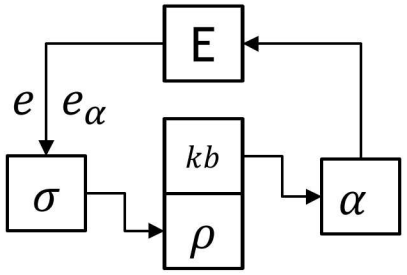


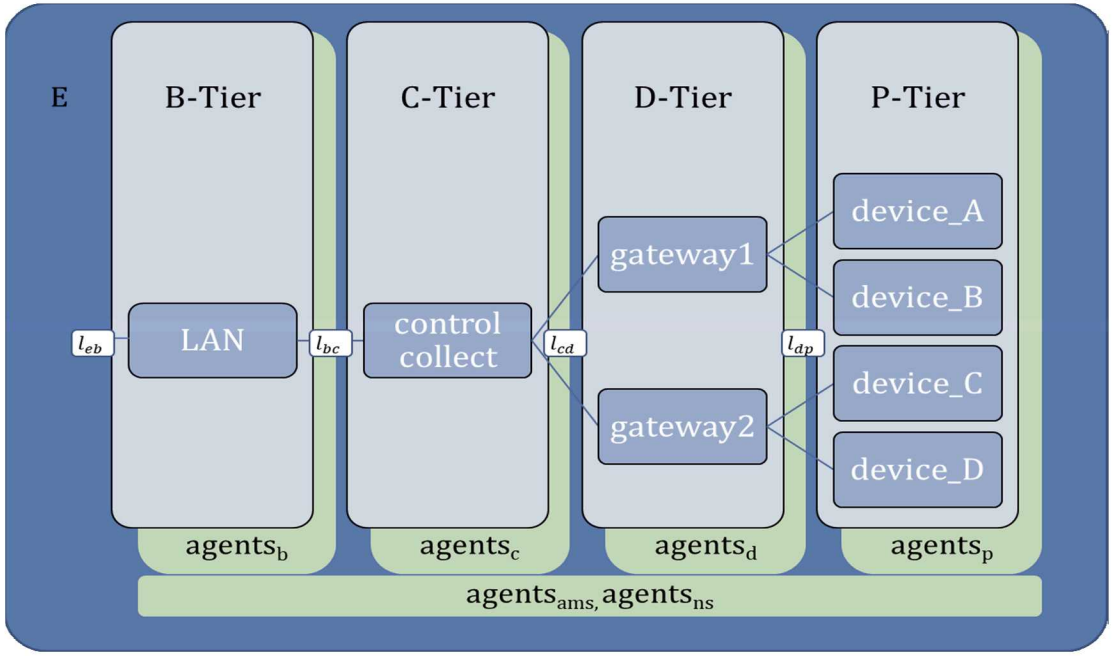
BUILDING A MAS

$$kb = knowledge\ base$$

$$kb = \bigcup_{i}^{n} \rho_i \cup \sigma_\alpha \cup \kappa$$

$$e = event\ or\ observation$$





CONCLUSION

Security in OT is both an old and new paradigm; technology to do so must be flexible to address legacy systems and still grow with new tech and defense mechanism.

We introduced using a Multi-agent System for OT security, further research delve further into coordination and specification of agents.

Toward a Multi-Agent System Architecture for Insight & Cybersecurity in Cyber-Physical Systems

PRESENTED BY

Will Stout

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.