MOSAICS and the Future of ICS Defense

November 5, 2020

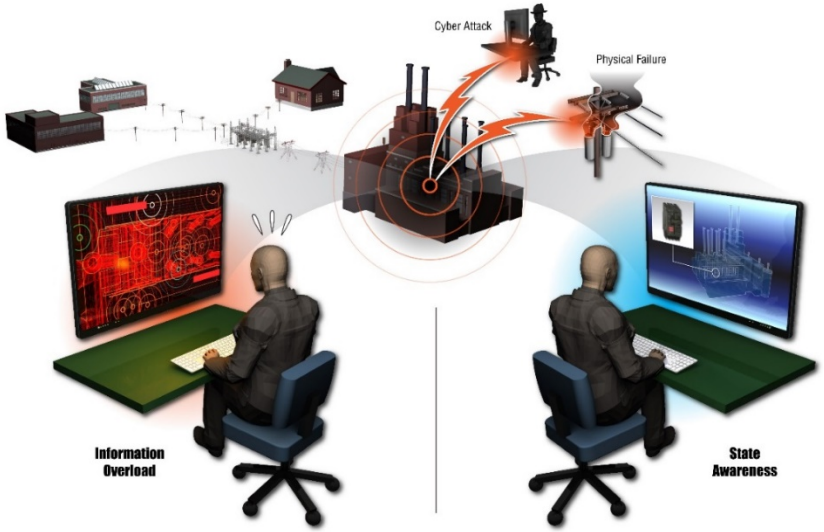
Craig Rieger, PhD, PE

MOSAICS Value Proposition

MOSAICS

2020
INDUSTRY
DAY

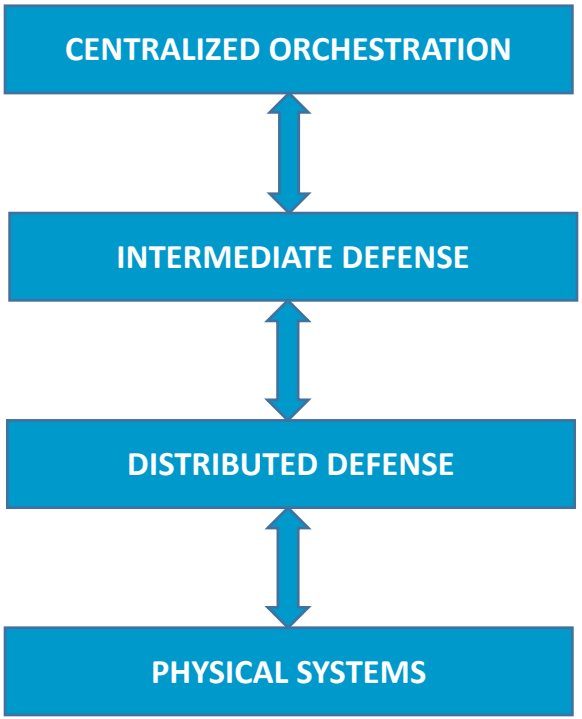
- A multi-phase approach that developed the MOSAICS prototype and applied an increasing robust regime of testing and metrics-based expectations for performance in relevant environments.
- Characterization of the varied cybersecurity roles, and gaps, coupled with the technologies to advancing the appropriate and consistent human in the loop defensive posture at each location.
- A solid foundation for an evolving active, resilient defense, ensuring strong perimeter protections but coupling with human in the loop orchestration and eventual automated response.



Hierarchical Multiagent Dynamical System (HMADS) Layers

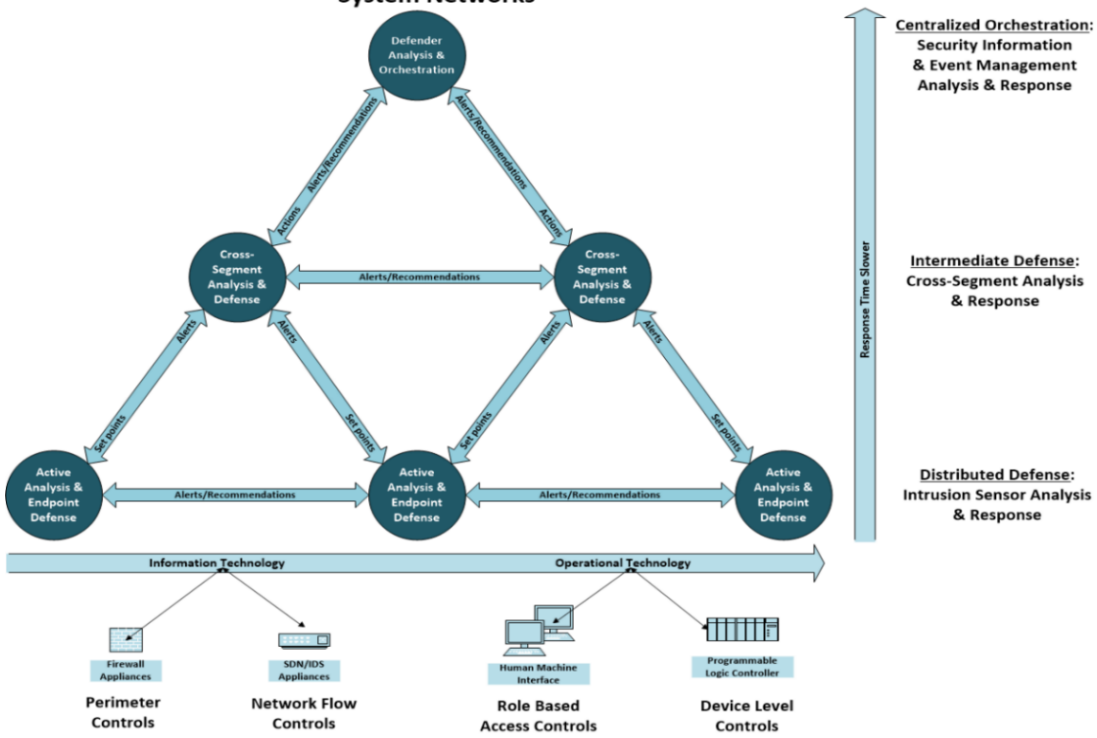
2020 INDUSTRY DAY

- **Upper Layer or Tier—Centralized Orchestration**
  - The Centralized Orchestration Tier includes the overall orchestration actions and defines priorities regarding the cyber defense mechanisms deployed.
- **Middle Layer or Tier—Intermediate Defense**
  - The Intermediate Defense Tier provides network behavioral analysis as well as corresponding response based upon the orchestration dictated by higher layer.
- **Lowest Layer Tier—Distributed Defense**
  - The Distributed Defense Tier provides direct monitoring of IDS and is in charge of remedial actions, and agile response towards completely stopping or mitigating the malicious event.



Detailed HMADS

Hierarchical, Distributed Analytics for Control System Networks



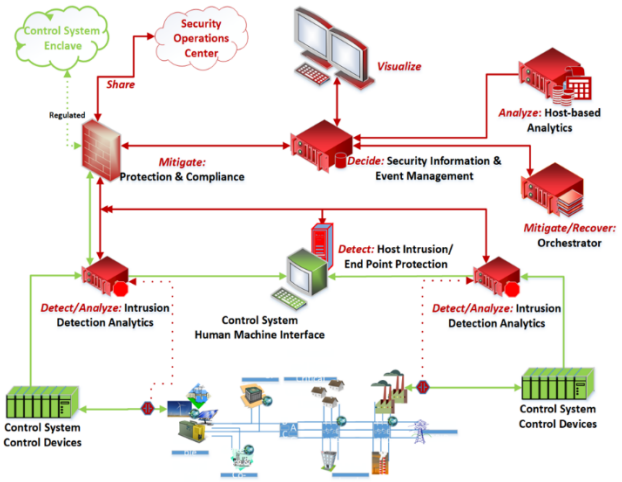
Tier	1	2	3
1	Contains overall security policy and tradeoff space analysis for dissemination.	Provide analytical updates based upon overall system threats and response latitude.	Provide analytical updates based upon overall system threats and response latitude.
2	Transmit cross-segment analytics and event response information.	Maintain cross-segment analysis for anomaly detection and response.	Perform tradeoff space analysis and latitude of autonomous response.
3	Transmit distributed health analysis.	Transmit segment analytics and event response information.	Maintain raw cyber physical analysis and event response strategy in Automated Response Controller.

MOSAICS

2020 INDUSTRY DAY

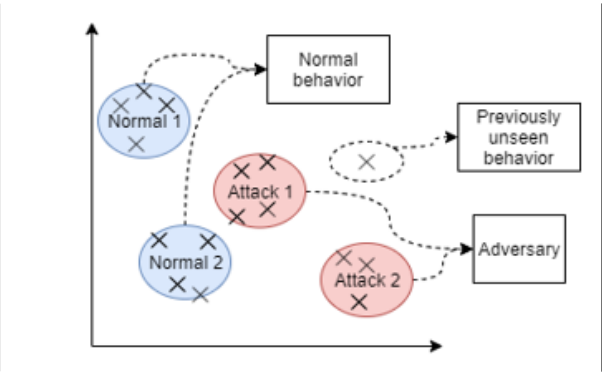
Commercial Off The Shelf (COTS) Hardware Layout

- **Some generalized alignment of COTS to this architecture.**
  - In a COTS security information and event management (SIEM) tool, the orchestrator is an obvious component at the top.
  - Software defined networks (SDN) may operate at the middle layer with a separate sensing/control
  - Distributed intrusion detection systems (IDS) are placed at the bottom layer.
- **However, COTS tools typically do not consider the tradeoff space between cyber mitigation benefit and resulting loss of function assessment.**
- **For example, isolating traffic or a port may cause an instability in a feedback loop creating worse consequences than the initial impact of the cyber-attack.**



Analytics Application to Cyber-Physical Data

- **Cyber-Physical Detection and Analysis of Anomalies**
  - Ingestion of cyber-physical alert data
  - Tradeoff space analysis to validate mitigation benefit and physical impacts that may result
  - Role based actions at the human machine interface or automated actions at the endpoints
- **Cyber-physical Models**
  - Cyber data models based upon statistical or intelligent techniques
    - Techniques baseline data using clustering, where feature sets (e.g., hosts/ports talking, how often, etc.) using live traffic or training sets to inform algorithms
  - Physical data models can be first principles, statistical or intelligent techniques
    - First principles can be exact but are novel to each application and not normally scalable
    - Statistical and intelligent techniques require rich data sets

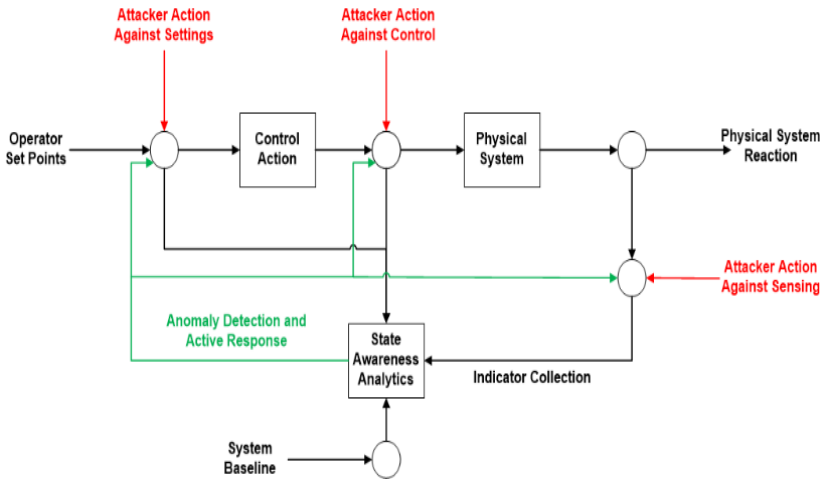


Cyber Physical Feedback Loop and Moving Target Defense

MOSAICS

2020 INDUSTRY DAY

- **A cyber feedback loop can be formed akin to a physical regulator.**
  - This includes both cyber and physical elements and degradation must evaluate both data sets, and responses to mitigate in both areas.
  - To maintain operations, the physical response of a cyber-attack could include use of redundant sensors or actuators or isolating a portion of the facility.
  - From the cyber side, the progression of the attack must be stopped.
- **If failure is only physical and non-malicious, the response would only occur to correct & maintain operation from recognized failure.**
- **Automated Response and Moving Target Defense**
  - Software defined network response actions to redirect or limit traffic for analysis
  - Moving target defenses to deceive actor



Distributed Cyber-Physical State Awareness

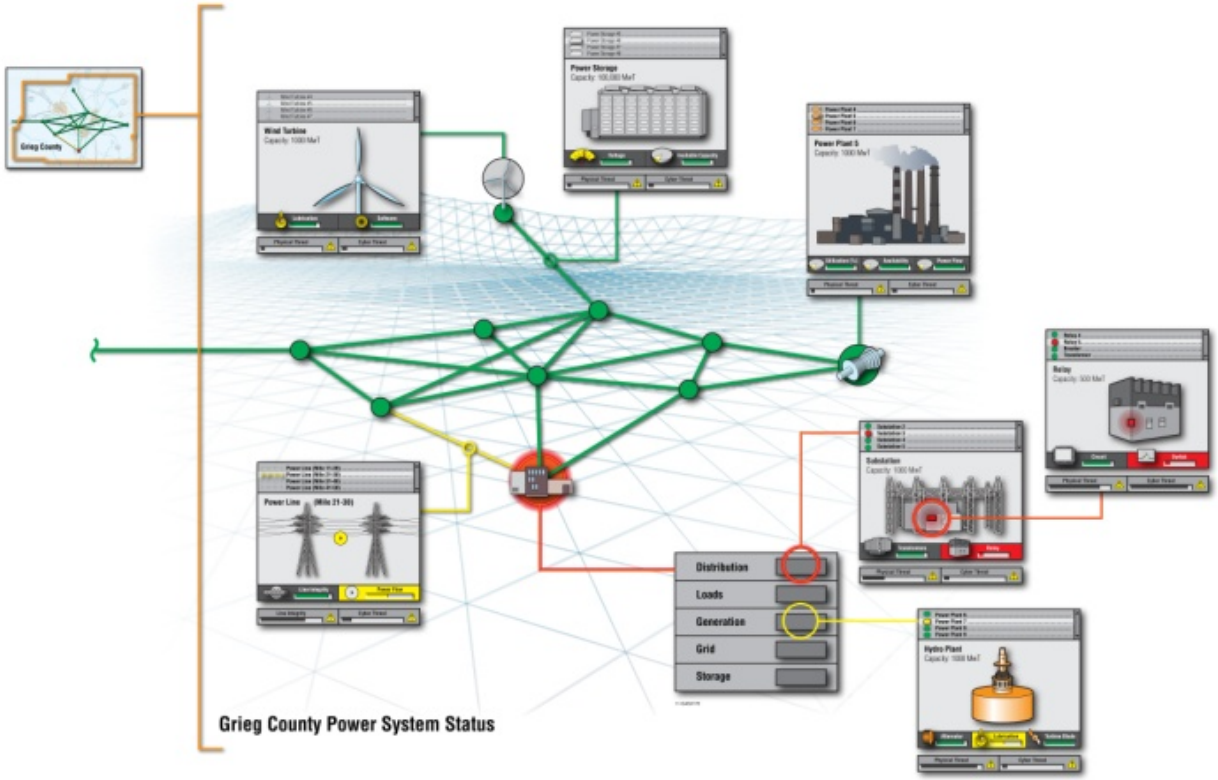
- **Distributed Physical State-awareness**
  - Capability for optimally integrating, monitoring, and controlling the distributed energy systems to prioritize the emergency response to critical infrastructure despite uncertainties.
- **Distributed Cyber State-awareness**
  - Capability for detecting and evaluating cyber threats to allow threat accommodation and reconfiguration of the proposed resilient system against attacks.

Cyber-Physical Common Operating Visualization

MOSAICS

2020 INDUSTRY DAY

- **Integrated Physical and Cyber State Awareness into a Visualization Engine**
  - The visible aspect of this solution is the display interfaces on devices that present information to humans to make more efficient and effective emergency response



Questions and Answers

MOSAICS

2020 INDUSTRY DAY