Craig Rieger, PhD, PE

December 6, 2022

Resilient Control Systems and the Advancement of the Cyber Feedback Loop

Idaho National Laboratory

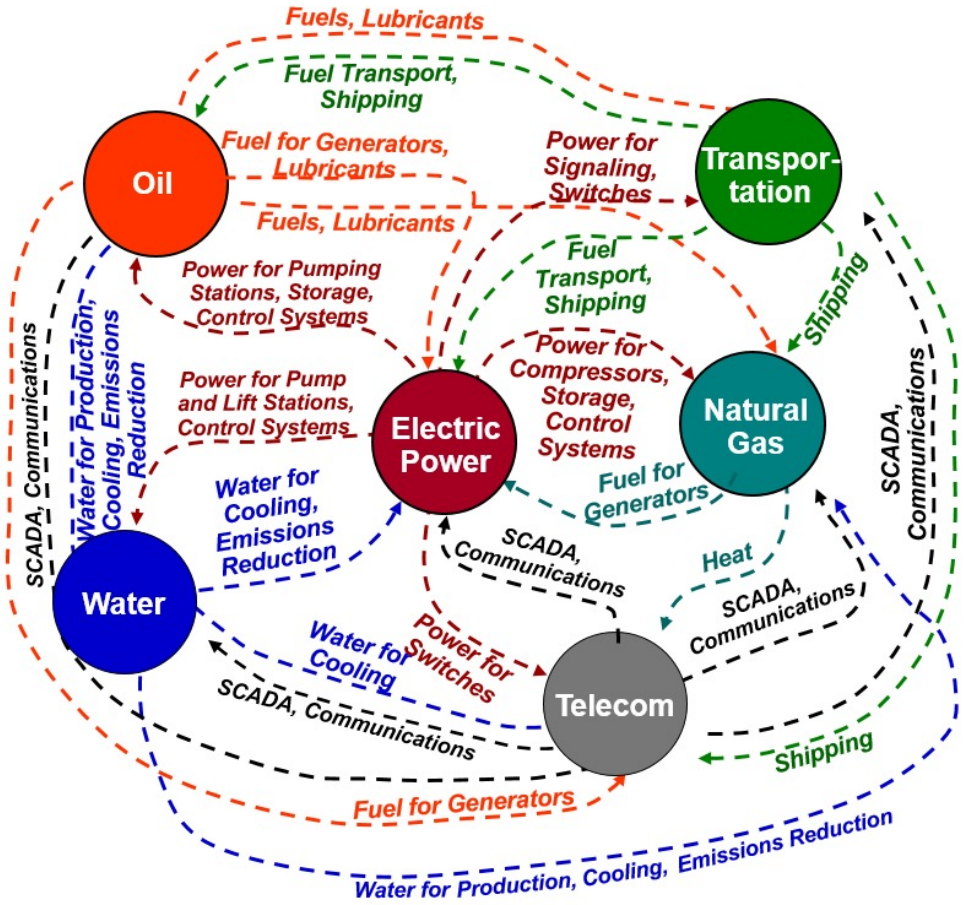
Outline

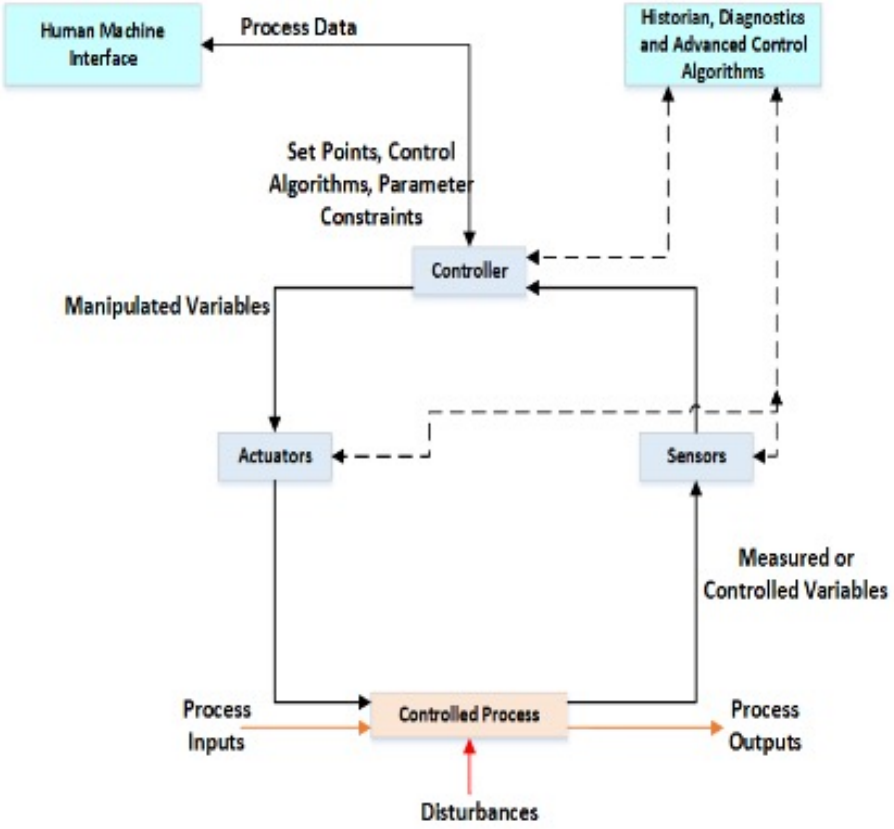
- Resilient Control Systems Background
- Architecture for Resilient Design
- Resilient Control Systems and the Cyber Feedback Loop
- Summary

Resilient Control Systems Background

Control System Complexity

(Ron Fisher, inl.gov)

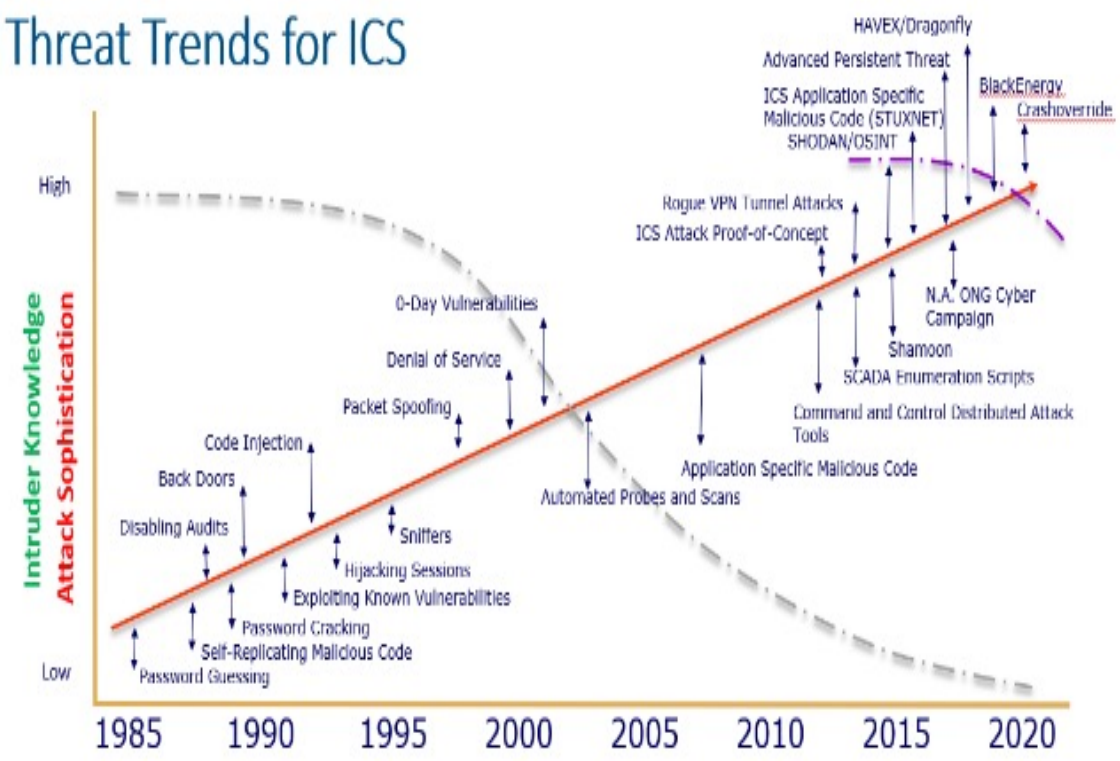


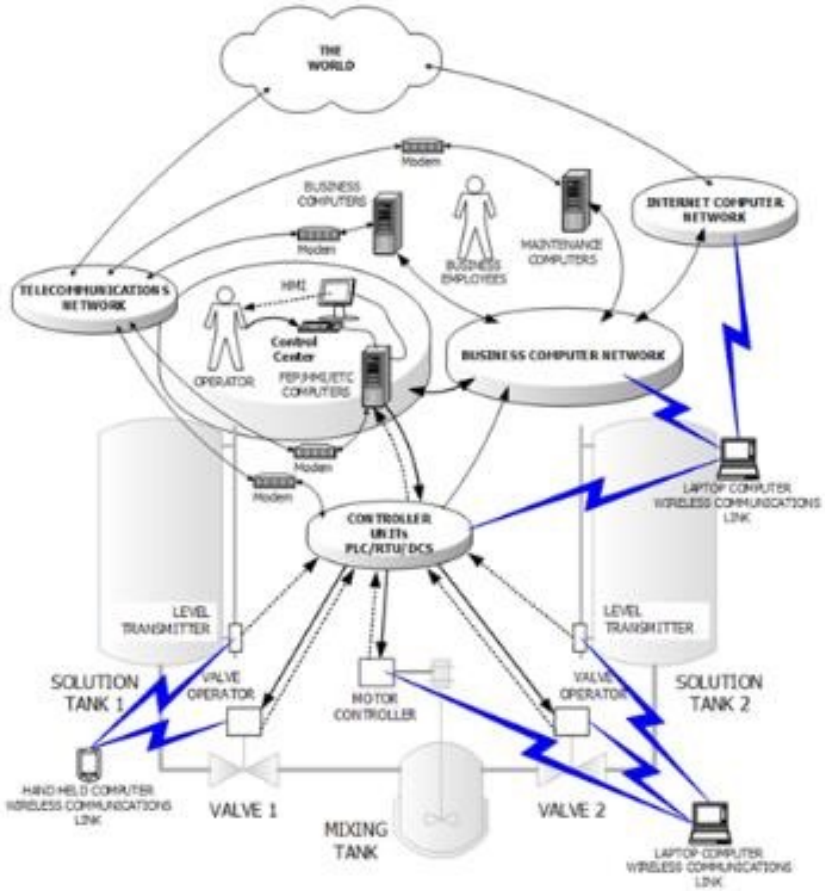


The ability to network control systems has provided a mixed blessing in the ability to interlock systems of systems, even crossing industrial sectors.

Cyber System Complexity

Adapted from Lipson, H. F., Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues, ics-cert.us)

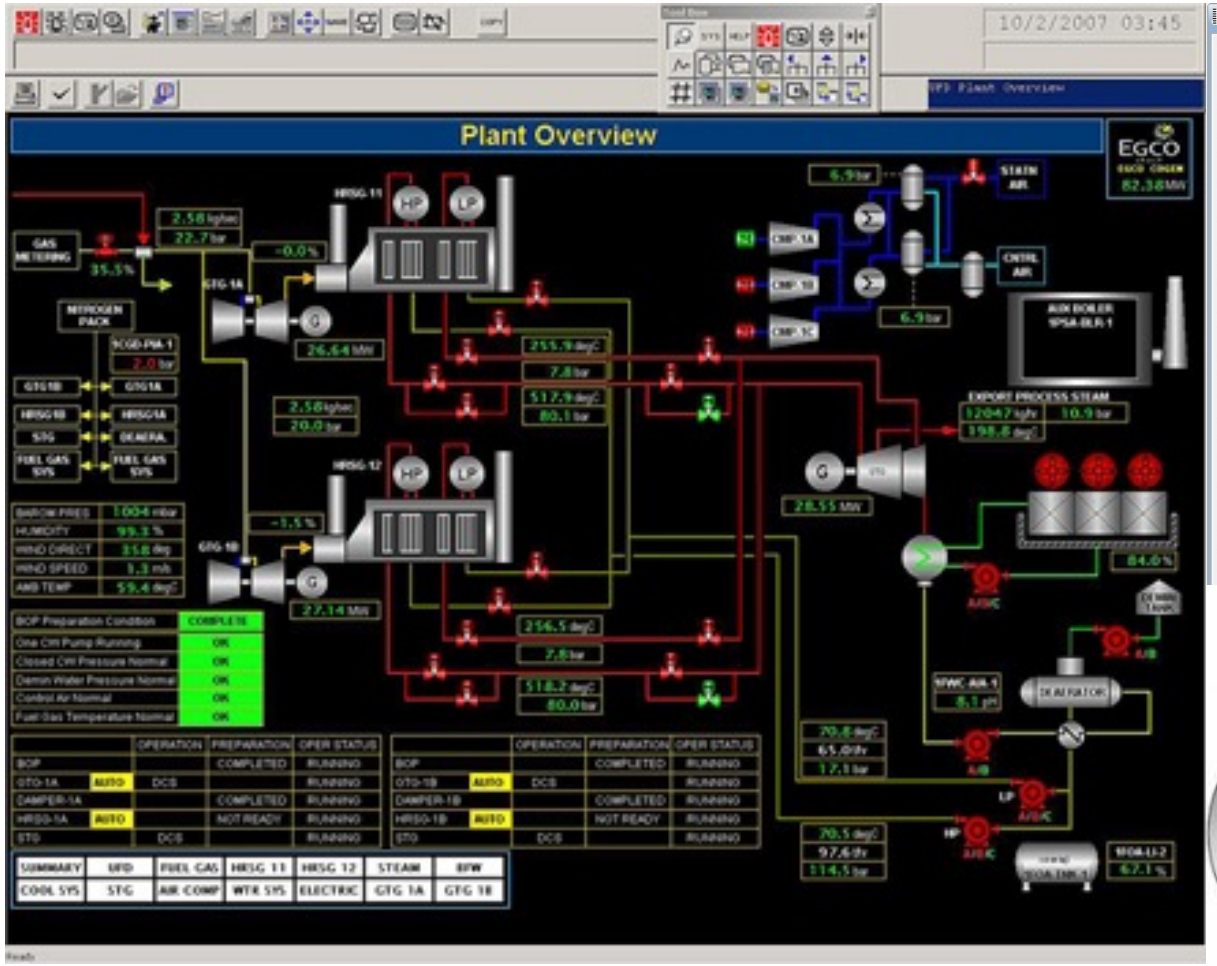


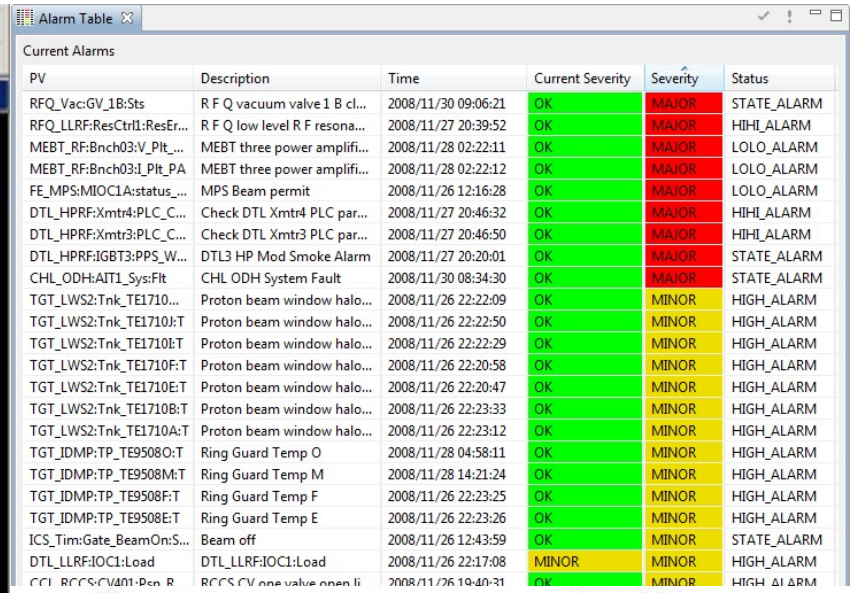


Cyber security attacks are becoming increasingly complex, which includes the targeting of control systems.

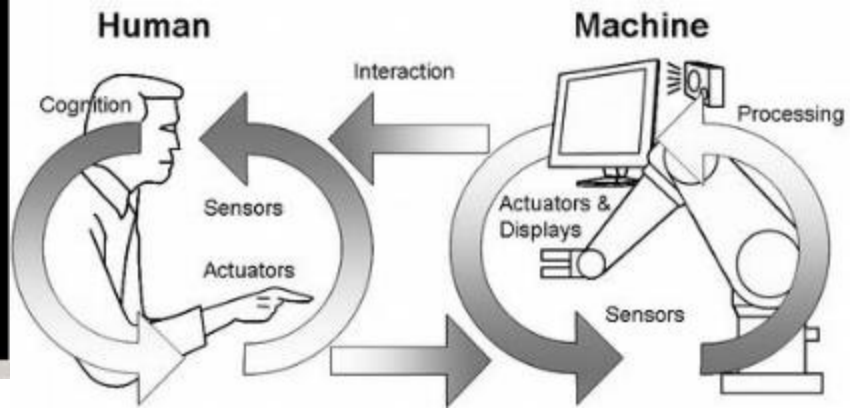
Human System Complexity

(yokagawa.com, cs-studio.sourceforge.net, plantautomation-technology.com)





PV	Description	Time	Current Severity	Severity	Status
RFQ_Vac:GV_1B:Sts	R F Q vacuum valve 1 B cl...	2008/11/30 09:06:21	OK	MAJOR	STATE_ALARM
RFQ_LLRF:ResCtrl1:ResEr...	R F Q low level R F resona...	2008/11/27 20:39:52	OK	MAJOR	HIHI_ALARM
MEBT_RF:Bnch03:V_Plt_...	MEBT three power amplifi...	2008/11/28 02:22:11	OK	MAJOR	LOLO_ALARM
MEBT_RF:Bnch03:I_Plt_PA	MEBT three power amplifi...	2008/11/28 02:22:12	OK	MAJOR	LOLO_ALARM
FE_MPS:MIOC1A:status_...	MPS Beam permit	2008/11/26 12:16:28	OK	MAJOR	LOLO_ALARM
DTL_HPRF:Xmtr4:PLC_C...	Check DTL Xmtr4 PLC par...	2008/11/27 20:46:32	OK	MAJOR	HIHI_ALARM
DTL_HPRF:Xmtr3:PLC_C...	Check DTL Xmtr3 PLC par...	2008/11/27 20:46:50	OK	MAJOR	HIHI_ALARM
DTL_HPRF:IGBT3:PPS_W...	DTL3 HP Mod Smoke Alarm	2008/11/27 20:20:01	OK	MAJOR	STATE_ALARM
CHL_ODH:AIT1_Sys:Flt	CHL ODH System Fault	2008/11/30 08:34:30	OK	MAJOR	STATE_ALARM
TGT_LWS2:Tnk_TE1710...	Proton beam window halo...	2008/11/26 22:22:09	OK	MINOR	HIGH_ALARM
TGT_LWS2:Tnk_TE1710J:T	Proton beam window halo...	2008/11/26 22:22:50	OK	MINOR	HIGH_ALARM
TGT_LWS2:Tnk_TE1710I:T	Proton beam window halo...	2008/11/26 22:22:29	OK	MINOR	HIGH_ALARM
TGT_LWS2:Tnk_TE1710F:T	Proton beam window halo...	2008/11/26 22:20:58	OK	MINOR	HIGH_ALARM
TGT_LWS2:Tnk_TE1710E:T	Proton beam window halo...	2008/11/26 22:20:47	OK	MINOR	HIGH_ALARM
TGT_LWS2:Tnk_TE1710B:T	Proton beam window halo...	2008/11/26 22:23:33	OK	MINOR	HIGH_ALARM
TGT_LWS2:Tnk_TE1710A:T	Proton beam window halo...	2008/11/26 22:23:12	OK	MINOR	HIGH_ALARM
TGT_IDMP:TP_TE9508O:T	Ring Guard Temp O	2008/11/28 04:58:11	OK	MINOR	HIGH_ALARM
TGT_IDMP:TP_TE9508M:T	Ring Guard Temp M	2008/11/28 14:21:24	OK	MINOR	HIGH_ALARM
TGT_IDMP:TP_TE9508F:T	Ring Guard Temp F	2008/11/26 22:23:25	OK	MINOR	HIGH_ALARM
TGT_IDMP:TP_TE9508E:T	Ring Guard Temp E	2008/11/26 22:23:26	OK	MINOR	HIGH_ALARM
ICS_Tim:Gate_BeamOn:S...	Beam off	2008/11/26 12:43:59	OK	MINOR	STATE_ALARM
DTL_LLRF:IOC1:Load	DTL_LLRF:IOC1:Load	2008/11/26 22:17:08	MINOR	MINOR	HIGH_ALARM
CCL_RCCS:CV401:Pos_R	RCCS CV one valve open li	2008/11/26 19:40:31	OK	MINOR	HIGH_ALARM



Human interfaces are loaded with data, generating complexity for the operator or dispatcher to interpret.

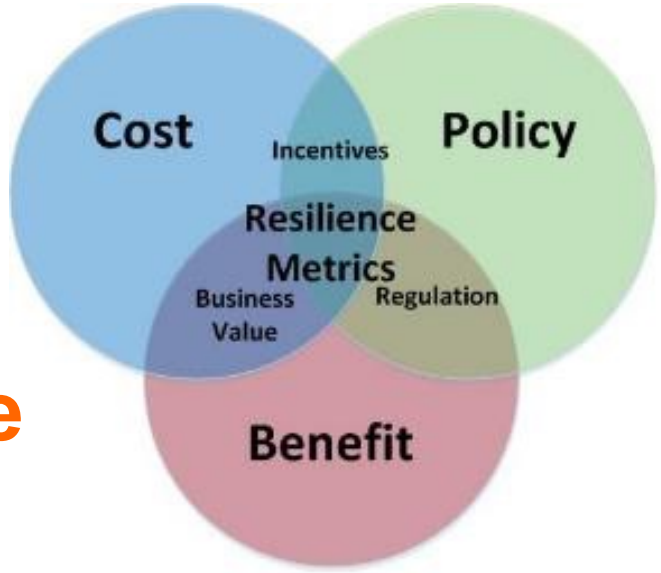
Resilience Considerations Arising From Complexity

- **Unexpected condition adaptation**
  - **Achievable hierarchy with semi-autonomous echelons**: The ability to have large scale, integrated supervisory control methodologies that implement graceful degradation
  - **Distributed control to address complex interdependencies and latency**: Decomposition of interdependent control system elements to simpler, stabilizable agents to reduce impacts from latency and failure propagation
- **Goal conflicts**
  - **Recognize performance goals**: Besides stability, security, efficiency and other factors influence the overall criteria for performance of the control system and must be prioritized with appropriate tradeoff analysis
  - **Increase state awareness**: Raw data must be translated to information on the condition of the process and the control system components
- **Human interaction challenges**
  - **Human performance prediction**: Humans possess great capability based upon knowledge and skill, but are not always operating at the same performance level
  - **Cyber awareness and intelligent adversary**: The ability to mitigate cyber attacks is necessary to ensure the integrity of the control system

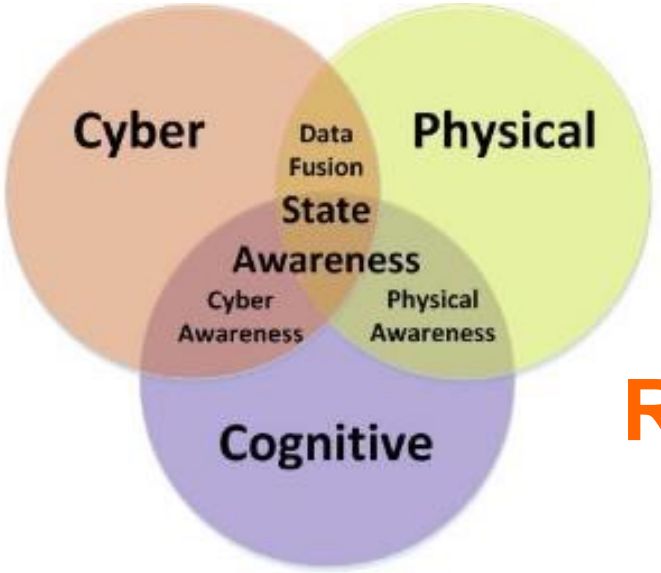
Disciplinary Approaches to Resilience Research

Discipline	Research Area	Limitation
Control Engineering	• Full autonomy or advanced supervisory control • Evolution of state space modeling, such as introducing a malicious disturbance • Application of game theoretic adversarial contests to consider malicious intentions	• Applications are very specific due to complexity, brittleness, etc. • Assumes malicious disturbances can be entirely recognized by physical anomalies and thresholds • Assumes attackers follow rational behaviors and probabilities can be accurately assigned to behaviors
Computer Science	• Evolution of anomaly detection mechanisms, such as intrusion detection systems with machine learning • Evolution of defense methods with adversarial modeling • Application of architectural deception, such as randomization and moving target	• Dependent on recognition of anomalies and tradeoffs between “big data” false positives & negatives • Models and scripted, open-loop methods of randomization can be recognized and bypassed
Cognitive Psychology	• Application of cognitive modeling to human process resilience and safety • Recognition of human fatigue and behaviors that may impact desired response • Presentation of cyber detection data for recognition of malicious attack	• Heavy emphasis on safety and not security or control systems • Evaluations based upon human effects and not the ability to selectively automate response • Visualizations targeted to security engineers only

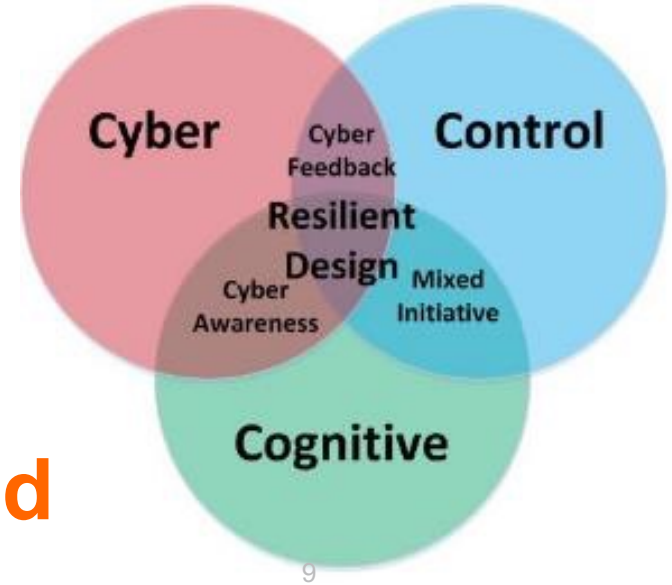
Disciplinary and Application Alignment



Measure



Recon



Resist/
Respond

Resilience

Resilient Control Systems Science/Engineering Foundation and Community

Symposia

Resilience Week

ISRCS

IEEE

1951-2011 ICS 60th anniversary

Publications

IEEE TRANSACTIONS ON CYBERNETICS, VOL. 44, NO. 11, NOVEMBER 2014

Guest Editorial:
Introduction to the Special Issue on Resilient Control Architectures and Systems

HSI 2009 — Catania, Italy, May

Resilient Control Systems:
Next Generation Design Research

Craig G. Rieger†, *Senior Member, IEEE*, David I. Gertman†, Miles. A. McQueen†, *Member*.
†Idaho National Laboratory, Idaho Falls, Idaho, USA

Abstract — Since digital control systems were introduced to the market more than 30 years ago, the operational efficiency and stability gained through their use have fueled our migration and ultimate dependence on them for the monitoring and control of critical infrastructure. While these systems have been designed for functionality and reliability, a hostile cyber environment and uncertainties in complex networks and human interactions have placed additional parameters on the design expectations for control systems.

Keywords —resilience, control systems, complex networks, cyber security, data fusion.

I. Introduction

A preeminent objective for corporate and government organizations is state awareness, a comprehensive

IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, VOL. 15, NO. 7, JULY 2019

Guest Editorial:
Resilience in Energy Industries—Recent Advances, Open Challenges, and Future Directions

THE transformation of energy infrastructure is making the resilience a fundamental topic for the definition of future configuration of the energy systems. This is due to the increased penetration of renewable energy sources (RES), the distributed energy management, the change in the power demand, the integration between energy and mobility sectors, the progressive liberalization of energy markets, the increased probability of extreme weather events, and the occurrence of errors in the interaction between humans and machines.

Resilience is the capacity of critical infrastructure systems to proactively maintain a safe level of operational normalcy in response to anomalies, including threats of a malicious and un-

or in subsystems). On the other hand, the active resilience enhancement measures include all those actions and devices allow the active management of the system during its operation These systems include the definition of the optimal management schemes of RES, energy storage systems or backup systems, implementation of measurement and/or control systems, and implementation of islanding procedures.

Also, it should be interesting to investigate passive approaches to improve the impact of active resilience enhancement measures. As an example, this can include an optimized placement of monitoring systems or the optimal placement of energy storage systems, which can be identified during the planning phase

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Current events
Random article
About Wikipedia
Contact us
Donate

Contribute
Help
Learn to edit
Community portal

Article Talk

Resilient control systems

From Wikipedia, the free encyclopedia

For other

In our mode … automate many of the industrial operations that we take for granted, from the power plant … how the designers integrate them, the roles and responsibilities of the humans that interact with the systems, and the cyber security of those highly networked systems have led to a new paradigm in research philosophy for next-generation control systems. **Resilient Control Systems** consider all of these elements and those disciplines that contribute to a more effective design, such as cognitive psychology, computer science, and control engineering to develop interdisciplinary solutions. These solutions consider things such as how to tailor the control system operating displays to best enable the user to make an accurate and reproducible response, how to design in cybersecurity protections such that the system defends itself from attack by changing its behaviors, and how to better integrate widely distributed computer control systems to prevent cascading failures that result in disruptions to critical industrial operations. In the context of cyber-physical systems, resilient control systems are an aspect that focuses on the unique interdependencies of a control system, as compared to information technology computer systems and networks, due to its importance in operating our critical industrial operations.

Advances in Information Security 75

Craig Rieger
Indrajit Ray
Quanyan Zhu
Michael A. Haney Editors

Industrial Control Systems Security and Resiliency

Practice and Theory

Springer

IEEE Press Series on Power and Energy Systems

Resilient Control Architectures and Power Systems

Craig Rieger, Ronald Boring, Brian Johnson, Timothy McJunkin

WILEY

Patents and Copyrights

Provisional/full patents and copyright assertions, three of which have been licensed as provided below:

1. **Systems and methods for control system security, CG Rieger, TR McJunkin, M Manic, K Amarasinghe, US Patent 10,896,261. (2021) Commercially licensed in 2021 to Nanotronics.**
2. **Targeted Energy Management System Toolset (TEMST). Copyrighted. (2020). Evaluation licensed to Trust Automation.**
3. **Gas Emulation Demo (GasED) for the Autonomic Intelligent Cyber Sensor (AICS). Copyrighted. (2018) Commercially licensed to Trust Automation.**

Other copyright assertions and open-source software releases:

1. **Copyright: Industrial Control System Diagnostics (ICSD) Web Scraper**
2. **Copyright: Cyber-physical Architecture for Automated Responses (CyPhAAR) In Adversarial OT Environments**
3. **Open Source: Power Distribution Designing For Resilience Application (PowDDeR) (2 releases)**
4. **Open Source: Scalab … is (SPEMMCRA)**
5. **Cyber State Awarene**

Patent applications in pro

1. **Systems And Method … reaty**
2. **Systems And Method … on**
3. **Systems And Method**
4. **Systems And Method**
5. **A Computer-aided Te … d Related Systems, Methods, And Device**
6. **A Computer-aided Technique For Assessing Infrastructure Reliability And Resilience And Related Systems, Methods, And Devices, PCT/US19/47 253, Patent Cooperation Treaty**
7. **A Computer-aided Technique For Assessing Infrastructure Reliability And Resilience And Related Systems, Methods, And Devices, 62/720,618, United States**
8. **Anomaly Detection For Cyber- physical Systems, 17/027,463, United States**
9. **Systems And Methods For Cyber- physical Anomaly Detection, 62/902,885, United States**
10. **Systems And Methods For Control System Security, 16/990,972, United States**
11. **Systems And Methods For Control System Security, 62/885,520, United States**
12. **Tracking Of Health And Resilience Of Physical Equipment And Related Systems, 63/203,146, United States**
13. **Distributed Automated Response Control Networks And Related Systems And Methods, 63/262,598, United States**
14. **Detection Of Behavior Anomalies In Control Systems And Related Systems, Methods, And Devices, 63/262,600, United States**

Project Sponsors

Department of Energy — United States of America

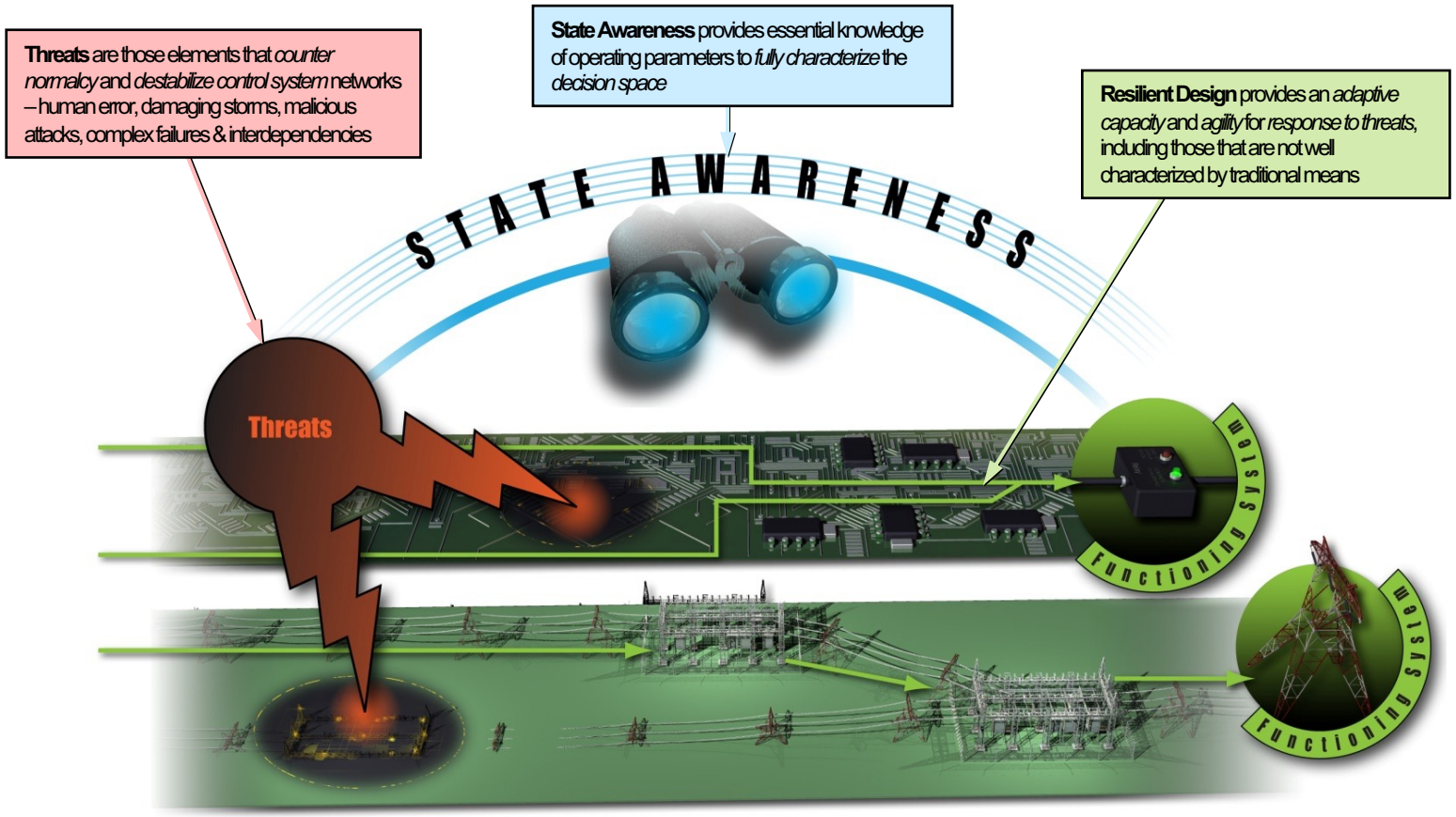
U.S. Department of Homeland Security

DARPA

Office of Naval Research — ONR — Science & Technology

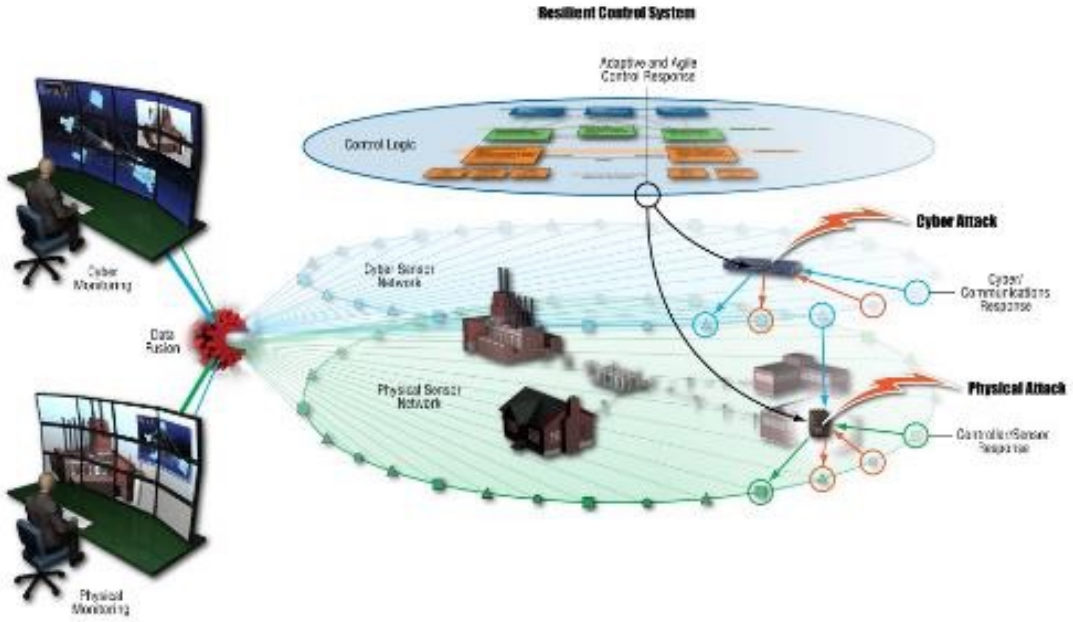
Architecture for Resilient Design

Next Generation Control Systems: From Reliable to Resilient



"Resilience" is the capacity of a control system to maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. (2009)

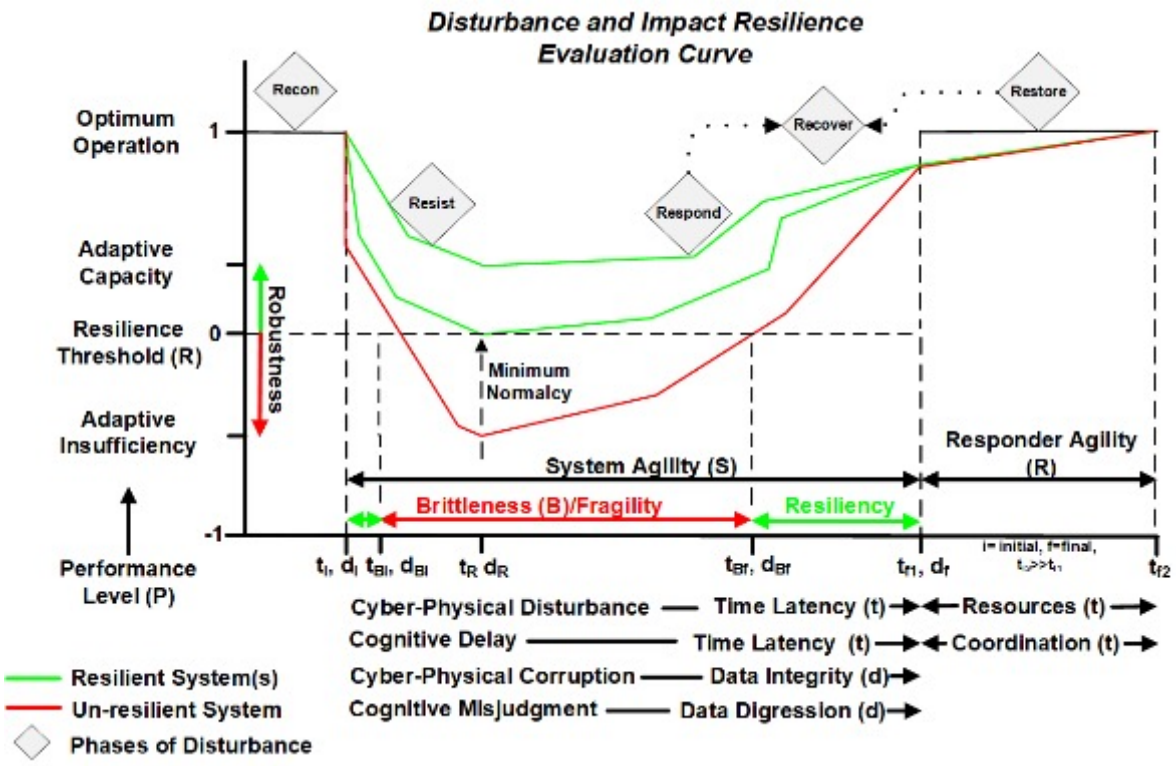
Transformational Threat-Resilient Control Systems



- **National Challenges**
  - **Cascading failure**: Increasingly networked control systems create correspondingly increased control/human interdependencies
  - **Cyber security**: Cyber vulnerability is a new dynamic systems failure paradigm
- **Outcomes Addressing Challenges**
  - **Minimizing impact to infrastructure and mission**
    - Intelligent architectures integrate expert knowledge with supervisory control
    - Diverse detection and response protections at each level of control system architecture
  - **Maximizing operational efficiencies**
    - Advanced control designs assess degradation and proactively control
  - **Enabling rapid response to all threats**
    - Cyber security and human factors-based degradation state awareness for operators and pilots

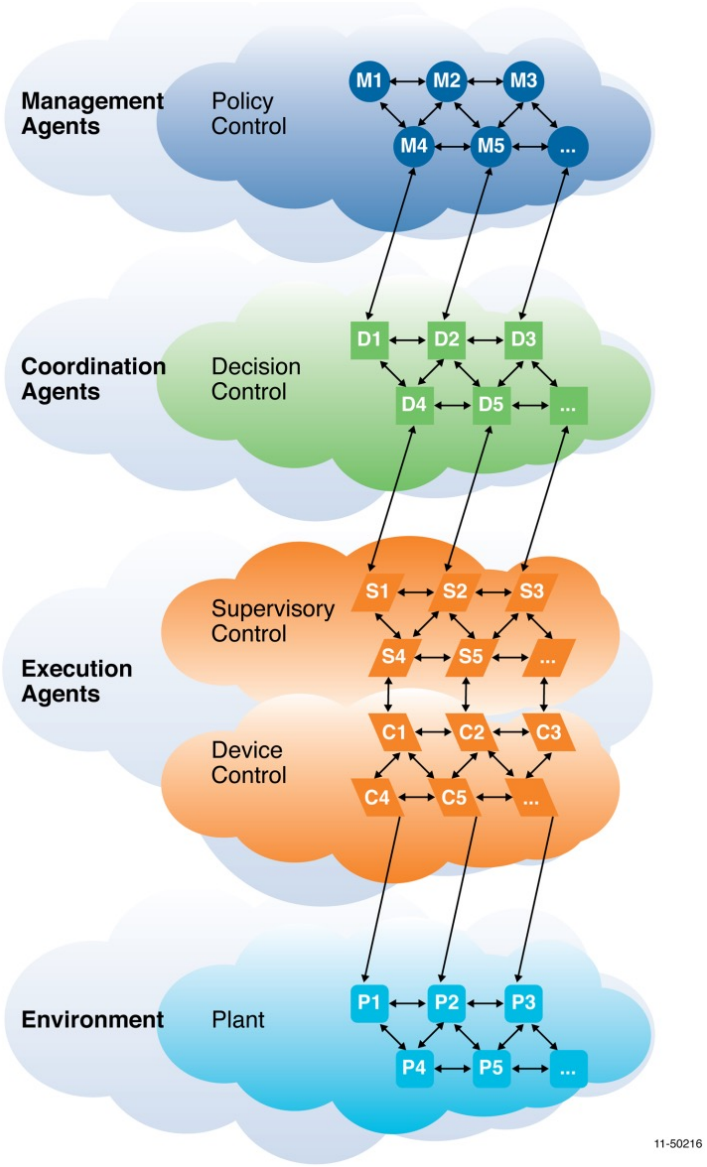
Disturbance and Impact Resilience Curve

- **Red curve** indicates the trajectory of a system that is **not** particularly **resilient** and falls below some predefined normalcy criterion
- **Green curves** are systems that maintain a minimum level of **acceptable** operation during this crisis, indicating resilient (as opposed to fragile/brittle) systems
- To provide context that will be relevant for evaluating the trade-off space, **a decomposition of the timing and data considerations** must be defined in terms of control system functionality
- **Timing issues** include considerations that revolve around latency
- **Data issues** involve the types **of physical parameters** for monitoring and control that are shared on a control system network
- Roles consider **human monitoring and response**



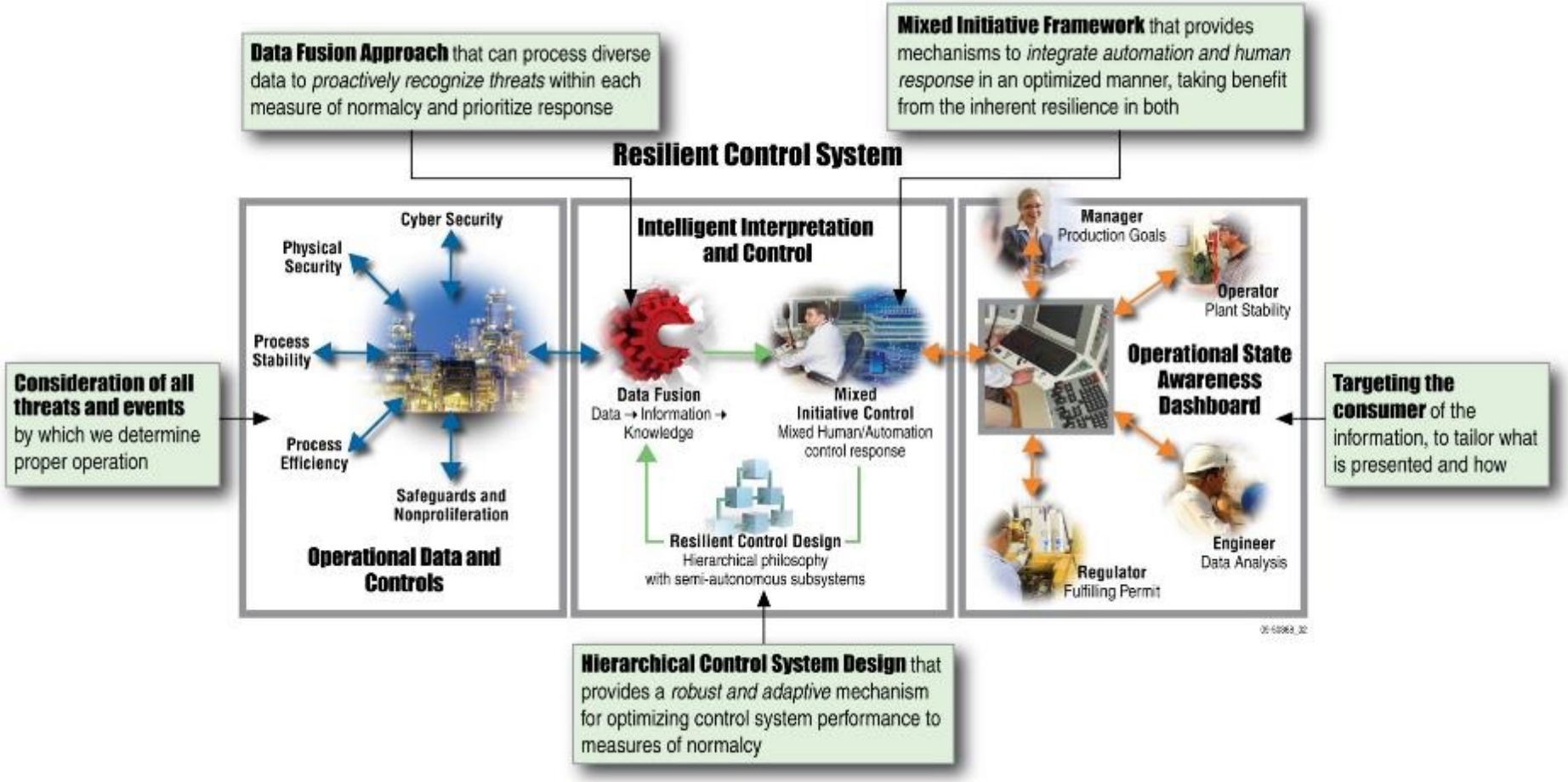
From Reliable Centralized to Resilient Distributed Control Systems

- **Unexpected condition adaptation**
  - Centralized monitoring and control interactions that are brittle to unexpected failures
  - Complex interdependencies and latencies of interaction that cause emergent behaviors
- **Human Interaction**
  - Complex human performance variables and variations
  - Multiple performance goals not uniquely correlating resilience
- **Malicious Action**
  - Lack of state awareness of malicious action and physical context



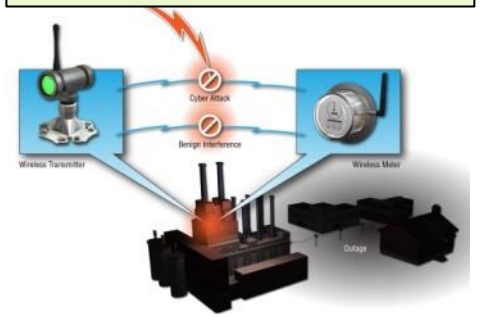
- **Unexpected condition adaptation**
  - Decomposed dynamics to achievable hierarchy with semi-autonomous echelons
  - Tiered metrics to confirm performance and root cause
  - Negotiated tradeoff analysis to disturbance conditions to ensure mission resilience over efficiencies and cost
  - Intelligent behavior learning for transformational response
- **Human Interaction**
  - Prediction of human performance and autonomy interdiction
  - Fusion and prioritization of response based upon resilience priorities
- **Malicious Action**
  - Active defenses for deception and environment modification confuse and deflect adversaries

A Resilient Control System Architecture

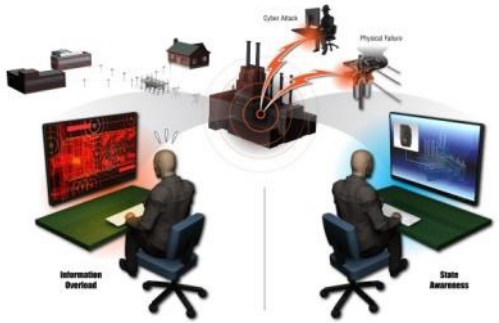


Transformative Research and Deployable Solutions for Inherent Infrastructure Resilience

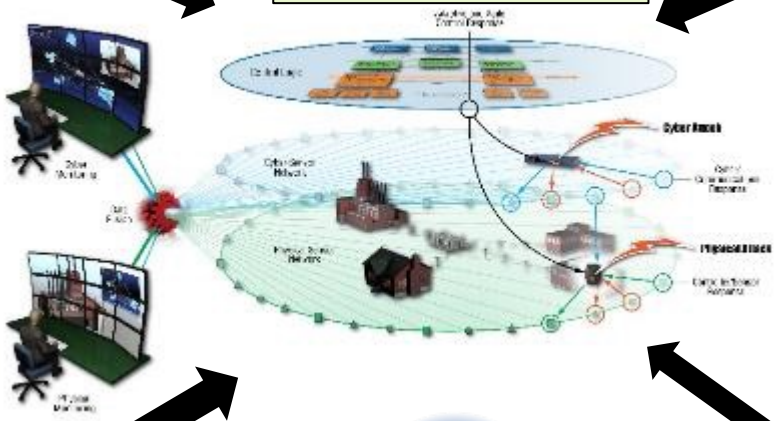
Intelligent Cyber Detection & Feedback Mechanisms



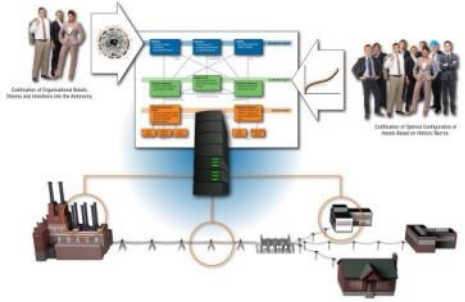
Role-based, Cyber-Physical State and Context Awareness



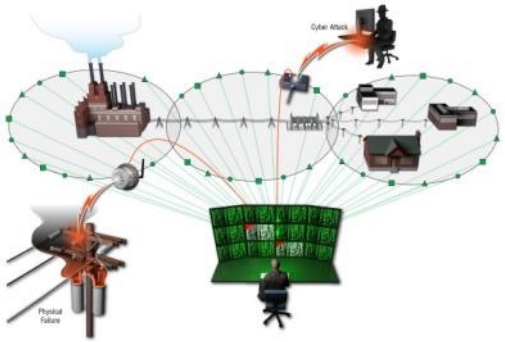
Resilient Control System Architecture



Adaptive and Agile Resilience Control Architectures

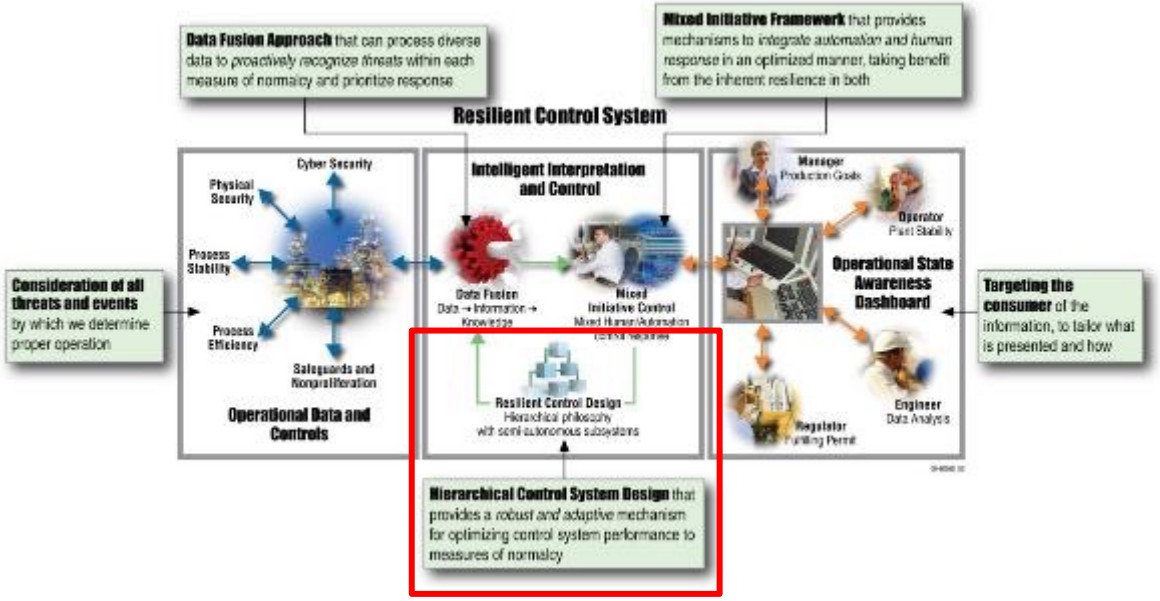


Infrastructure Trustworthiness Assessment & Proactive Control



Resilient Control & Instrumentation Systems

Hierarchical, Multi-agent Dynamical System Design for a Physical System

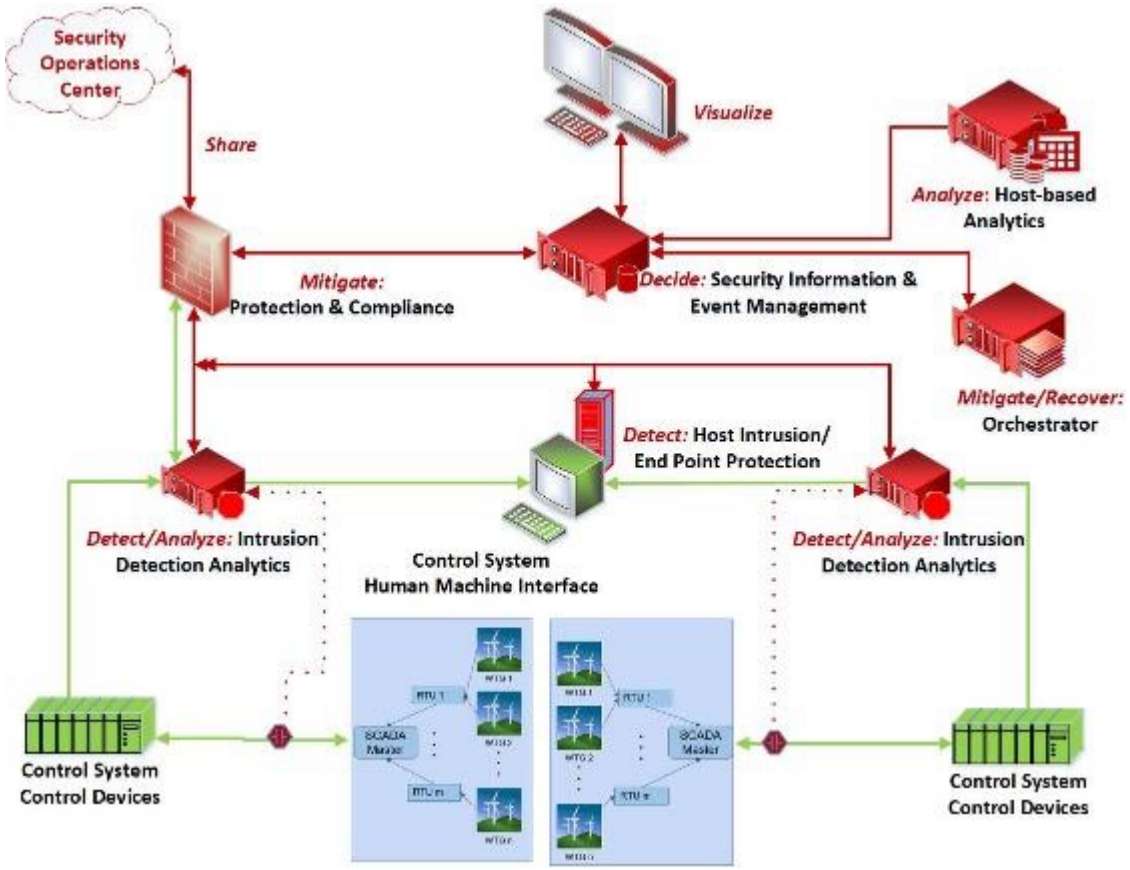


- **Management and Coordination Layers Reflect Policy & Coordination**
  - **Human intrinsic decisions** and desires currently performed outside of control system
  - Integrated using computational intelligence, **codifying human interactions and decisions**
  - **Performance targets and decisions** integrated directly in the design to increase resilience through **rapid configuration and reduced operator burden**
  - **Security and complex interdependencies** are key elements in ensuring the ultimate architecture of the design, requiring a perspective on normal behaviors and interactions
- **Execution Layer Reflect the Time-based Control Theory of Operation**

Resilient Control Systems and the Cyber Feedback Loop

General Security Reference Architecture

- **Detect:** Includes methods and systems for the monitoring and analysis of network traffic to recognize anomalies and undesirable traffic
- **Analyze:** Comprises of methods, including machine learning, for acquiring details regarding the nature and gaining insight in the execution methodology of the attack
- **Decide/Visualize:** Encompasses methods for the presentation of information to cyber-defenders for quick recognition and response
- **Mitigate/Recover:** Incorporates a set of methods to stop a cyber-attack and reverse any negative affects
- **Share:** Refers to a set of tools that describe details of a seen cyber-attack. This information can be securely shared to benefit the defenses of other organizations in the future



Normalizing Physical and Cyber Inputs/Outputs for Feedback Considerations

Plant Physical Feedback: Operator

- **Human Monitoring**
  - Raw Analog Plant Information
  - Raw Digital Plant Information
  - System State
  - Raw Physical Data Analytics
- **Human Response**
  - Plant Controller Set Points
  - Plant Hand Switch Positions
  - Plant Tuning Parameters
- **System State**
  - Ctrl Sys Device Health Status
  - Ctrl Sys Network Health Status
- **Time**
  - Loss of Determinism
  - Packet Not Delivered

Cyber-Physical

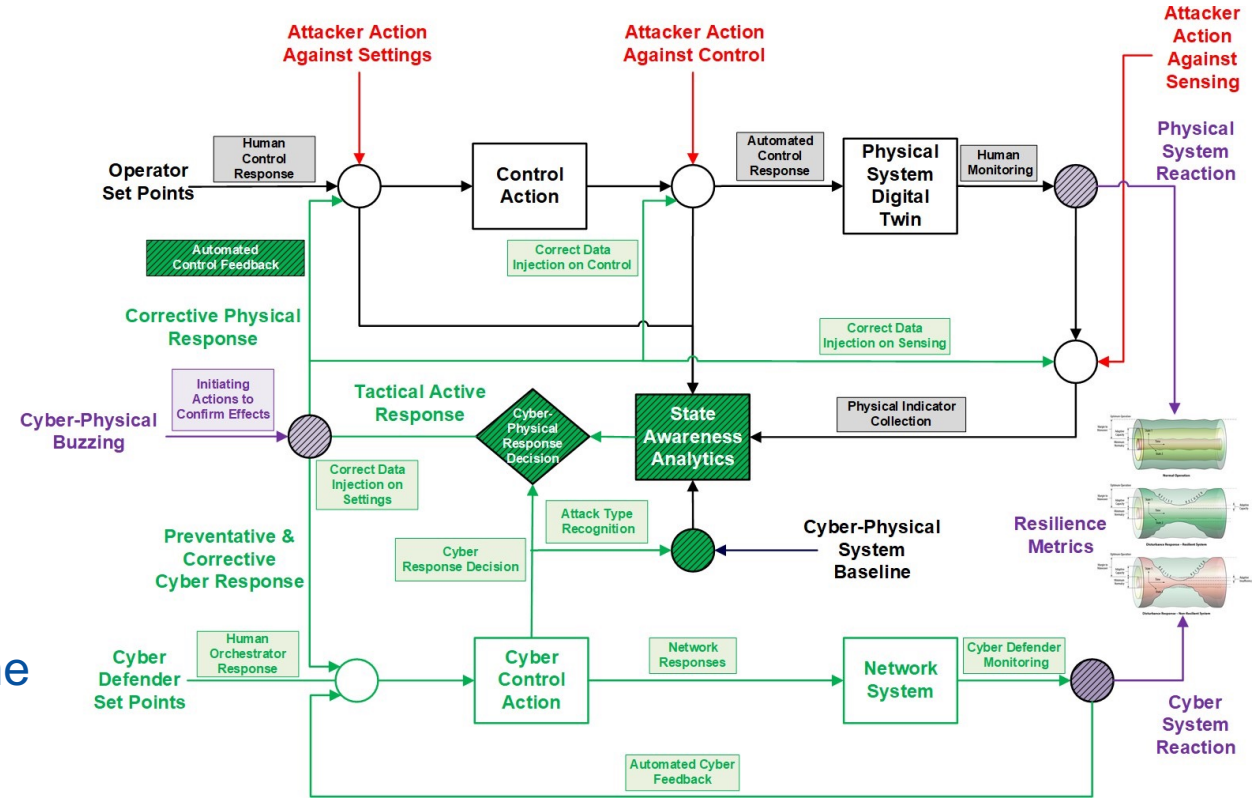
Feedback Taxonomy Crossover

Cyber Feedback: Cyber Defender

- **Human Monitoring**
  - Raw Log Information
  - Raw IDS Information
  - System State
  - Raw Cyber-Physical Data Analytics
- **Human Response**
  - Software Defined Net Controller Set Pts
  - Security Appliance Parameter
  - Data Correction
- **System State**
  - Security System Device Status
  - Security System Network Status
- **Time**
  - Latency of Packet Delivery
  - Packet Not Delivered

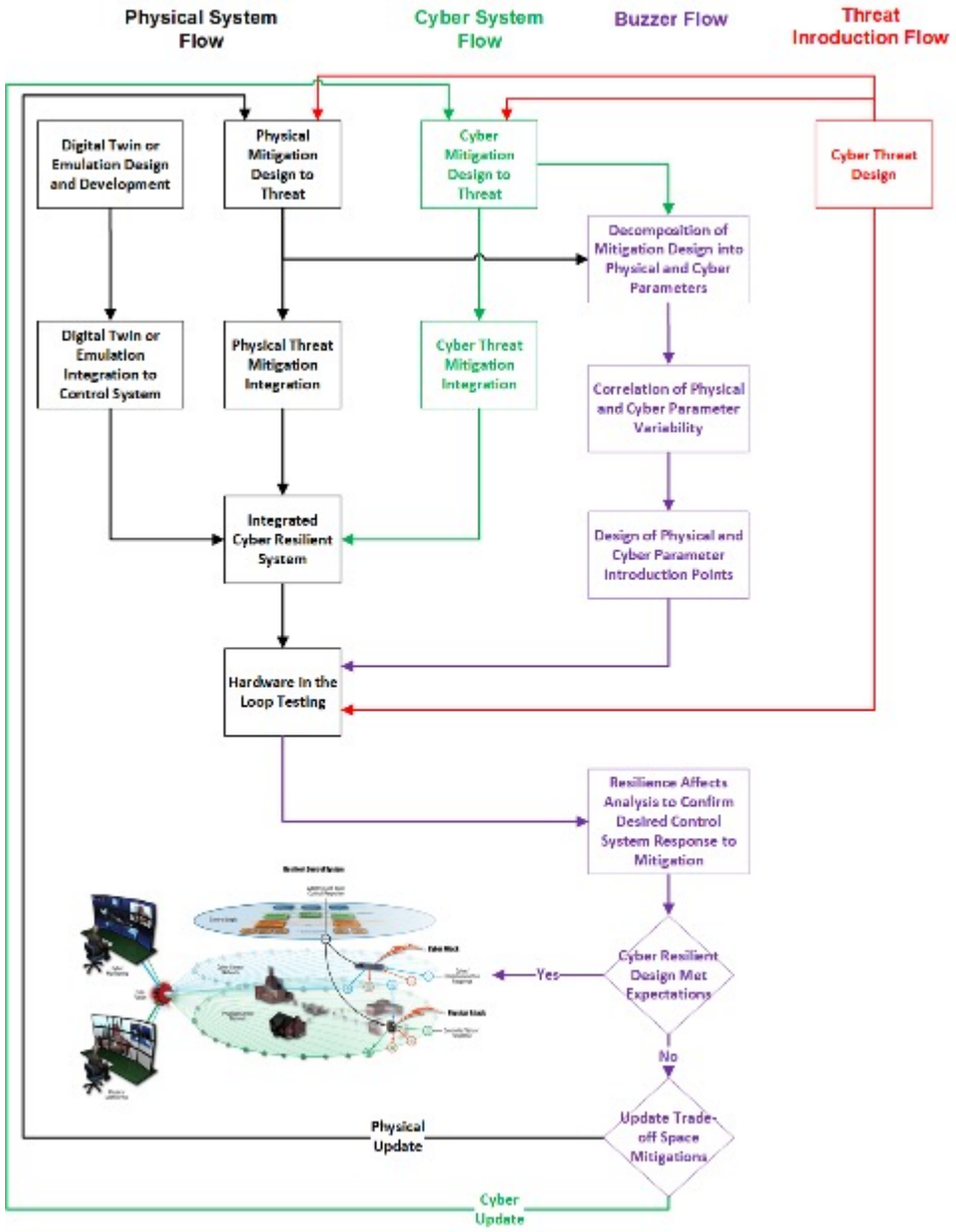
Cyber Feedback Tradeoff Analysis to Vet Mitigative Benefit

- **Hypothesis: A prototype for tradeoff space analysis can be developed, to confirm/refine the concept and demonstrate to Asset Owners:**
  - A **buzzer** can be effectively designed and integrated to successfully **test all desired mitigation steps** and boundaries of execution
  - **Emulation of physical components**, specifically, that will allow for **observing** and evaluating the **impact** of alternative mitigation decisions
  - Besides traditional **emulation** strategies our efforts will capitalize on the **digital-twins technology** to emulate important aspects of the plant system
  - An **efficient mutation process**, which given a set of inputs to certain components of the system it can **automatically generate alternative** mitigation **sequence of steps**



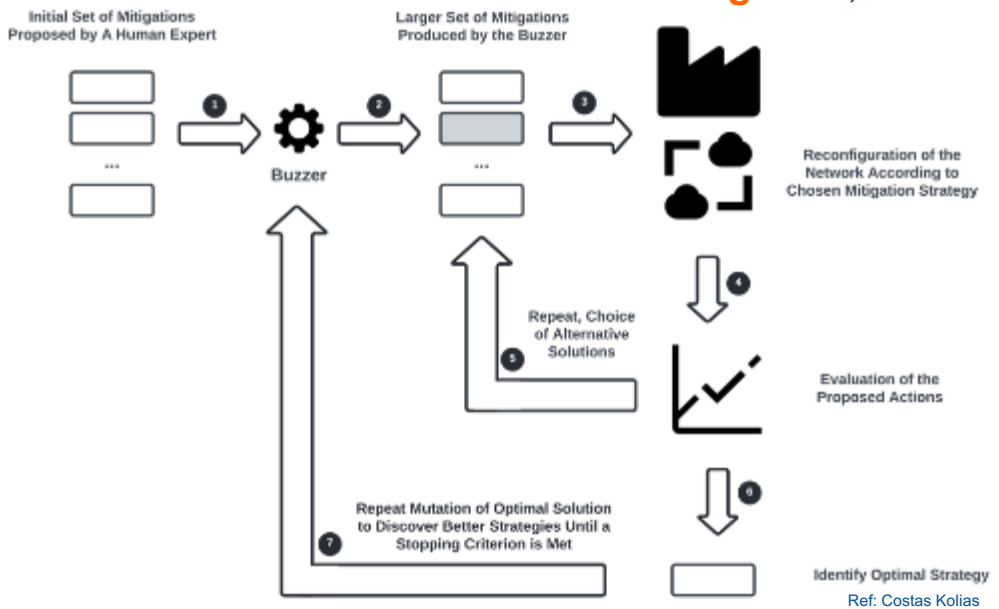
Tradeoff Space Evaluation Flow

- **Setup for Testing**
  - **Establish software defined network controller and network segmentation** to accept buzzer inputs for evaluating cross-segment responses
  - Establish **control and plant emulation system interfaces to accept buzzer inputs** to evaluate corrective actions from buzzer inputs
- **Buzzer Design**
  - **Decomposition** of distributed, **cyber-physical mitigations** and **allowances**
  - **Develop methodologies for informing/updating** the physical system **settings** and **cyber system controllers** with mitigative updates
- **Experimentation**
  - The **individual tradeoff aspects** will be reviewed through experimentation
  - **Resilience metrics** will be used for **assessing impact** and preferred options
  - **Scalability based** in **emulation**



Scenario Training Examples (Human Expert Input)

- **Starts with Human Inputs**
  - **Starting** set of **alternative mitigation strategies** as a seed
  - **Buzzer system** will **generate alternative** mitigation strategies
- **Refinement Using Optimization**
  - Extending **principles of genetic programming** and evolutionary computation that are today considered de-facto in conventional fuzzing systems
  - Thus, by **iteratively applying cross-over and mutation operations** and evaluating them against a set of user defined criteria, **new strategies** will be **proposed**
  - Evaluates **resilience relative to mitigation**, undesired affects

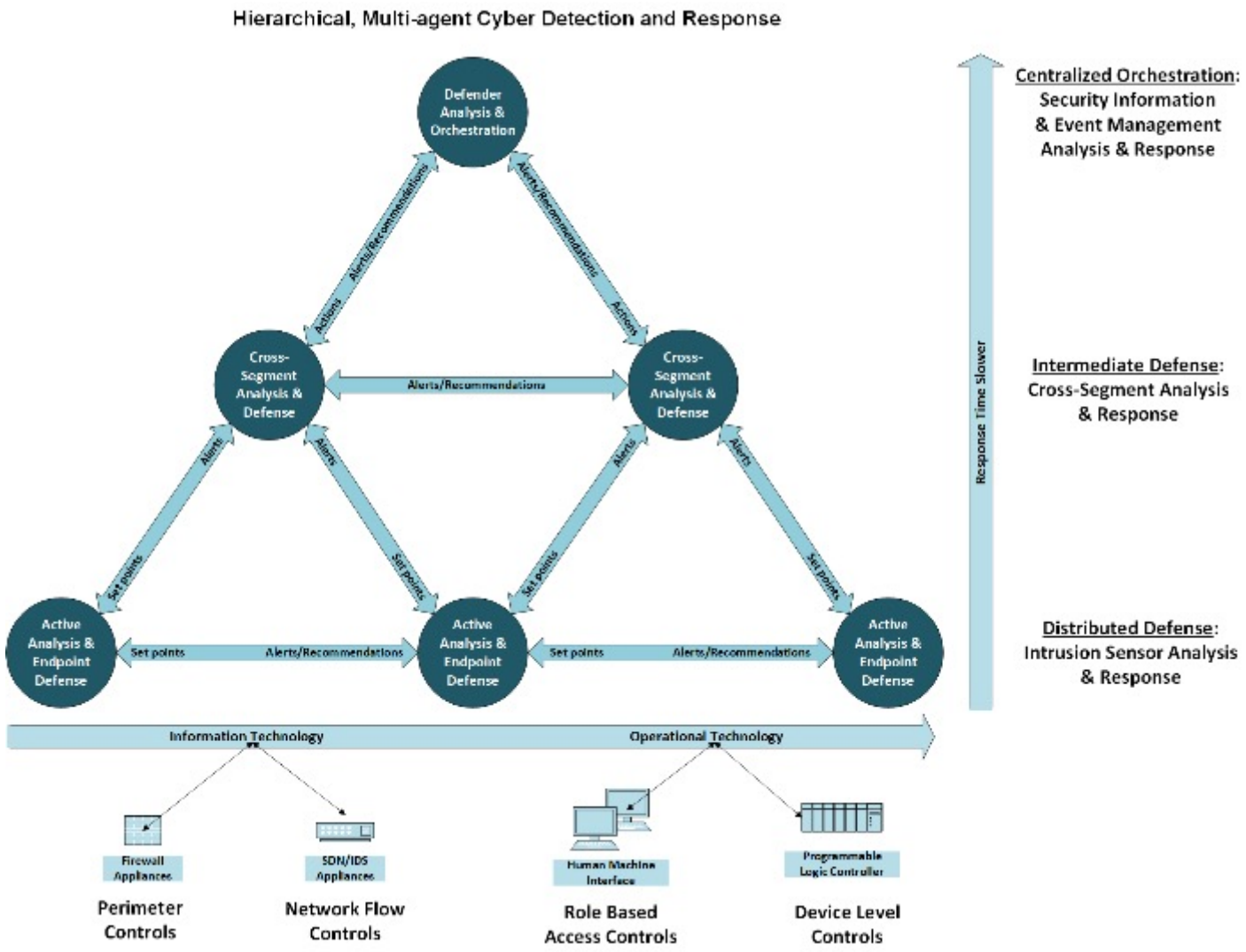


Ref: Costas Kolias

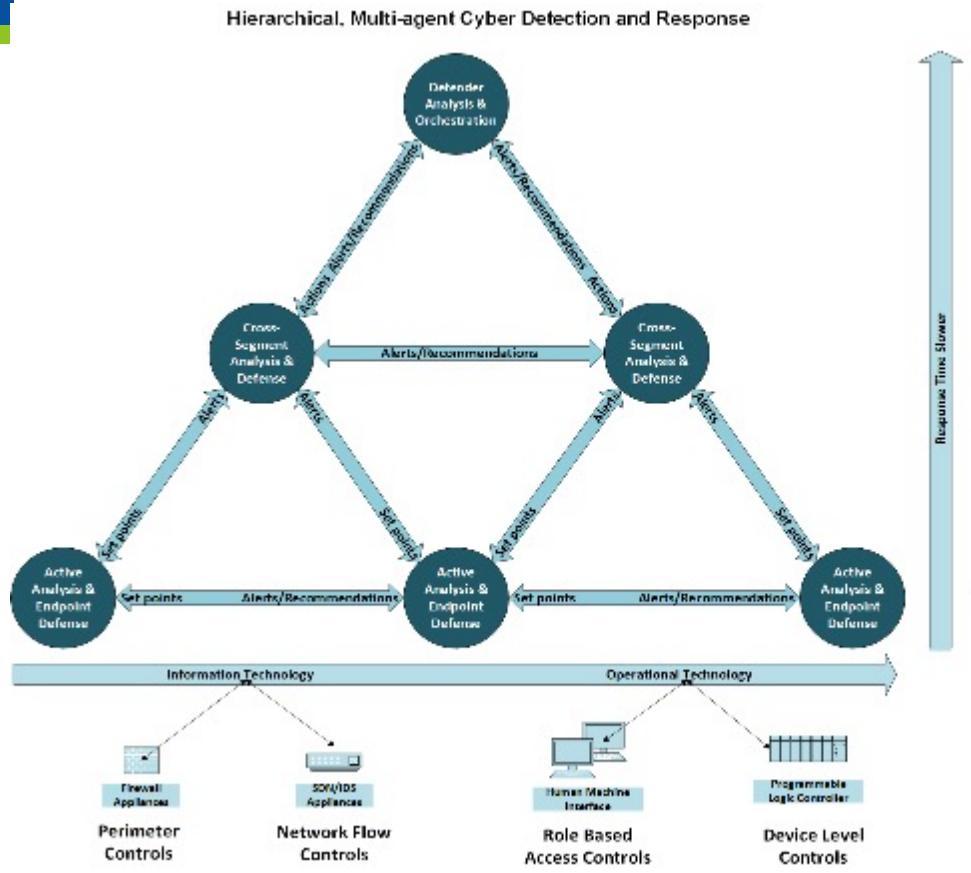
Attack	Attack Taxonomy	Possible Target	Network Impact	Cyber Response	Cyber Mitigative Benefit (Greater Mitigation = Better)	Physical System Impact (Less Impact = Better)	Physical Response	Physical Mitigative Benefit (Greater Mitigation = Better)
Active Network Scanning/ Enumeration	Protocol Based	Controller HMI Servers Switches Routers	Increases network traffic latency	1. Block scanning ARP\IP\TCP session using SDN 2. MTD 3. Return false results 4. Stand up a honeypot/honeynet	1. Stops scan, warns attacker of detection 2. Provides attacker with inaccurate results, makes targeting difficult 3. Can aid in detection of further attacks if falsified data is detected in the future 4. Prevents additional targeting of active devices, aids in attribution	None if the blocking doesn't affect ICS communications	None Needed	N/A
Passive Network Scan/Enumeration	Protocol Based	All Network Devices	No Effect	None	None	None	None Needed	N/A
SSH/Account Compromise	Traffic Based	HMI Controller Servers Switches Routers	Prevent remote management of devices	1. Block source IP using SDN 2. Deactivate account 3. MTD	1. Stops brute force attack 2. Prevents attack on device, aids in attribution 3. Prevents exploitation of that device 4. Prevents targeting of SSH/Account service	May not affect an ICS item unless the node compromised is an ICS device through compromised account. Telnet like communications not normally real time activity, but more for set points.	None, unless compromised, and specific attack response discussed below according to affect	N/A
Buffer Overflow	Protocol Based	Controller HMI Servers	Shutdown controller or HMI Remote code Execution	1. MTD 2. Drop packets from SDN using DPI 3. Drop packets with unknown MAC/IP at SDN 4. Startup secondary controller using SDN	1. Prevents targeting of end device 2. Drops packets of death before effecting controller 3. drops packets of unknown senders 4. Continues service after standing up second controller	Would impact affected ICS controller, and interruption until this is affected.	Switch to a isolated, preferably diverse backup	Switch to a backup that is not vulnerable to the same attack. If only redundancy is possible, then a cyber block and a redundant switch can return normal conditions.
DNP3 Flood	Traffic Based	HMI Controller	Breaks control feedback loop	Block incoming packets by source address using SDN	Blocks attackers' access to send packets on network	Mitigation should help recover the system and not create new problems.	Depending upon packets being read by HMI or controller and affects, data should be flagged by distributed analytics and corrected.	Data flagged as malicious to the operator and dropped before control action.
Denial of Service (DoS)	Traffic Based	HMI Controller Routers Servers Switches	Breaks control feedback loop Halts routing and switching to multiple devices	1. MTD 2. Block incoming packets by source address using SDN 3. redirect traffic to virtual network 4. Disable system processes if coming from known host	1. Prevents targeting of end devices 2. Blocks attackers' access to send packets on network 3. Allows attack to continue a non-critical network 4. Stops attack from insider threat or compromised device	Mitigation may generally save the system but rerouting the traffic will cause potential loss of monitoring or response, i.e., inability to send new set points or controller responses out of date due to bad data.	Cyber response should provide primary response, but a redundant system in place could be brought to bear.	Redundant system that is not impacted by DoS takes over to maintain operation.
DNP3/Modbus replay attack	Header Based	HMI Controller	Control loop is compromised; old control values resent	1. Place controller and HMI on new network segment using SDN 2. Detect and block physical port of attacker using SDN 3. MTD	1. Restore the control loop 2. Removes man in the middle 3. Prevents attacker from targeting control loop	Mitigation will resolve potentially instable or degrading operation based upon bad data. The scale of the ancillary affects would depend on what is blocked to know good ICS devices.	Depending upon packets being read by HMI or controller and affects, data should be flagged by analytics and corrected.	Data flagged as malicious to the operator and dropped before control action.
DNP3/Modbus integrity attack	Header Based	HMI Controller	Control loop is compromised; false control values resent	1. Place controller and HMI on new network segment using SDN 2. Detect and block physical port of attacker using SDN 3. MTD	1. Restore the control loop 2. Removes man in the middle 3. Prevents attacker from targeting control loop	Mitigation removes compromised data, which could be acted upon, but may have ancillary affects and would require an assurance that any controller, logic or HMI that uses it is placed in a good state. This good state could still be a degraded state.	Corrections in the logic recognized through distributed analytics recognition and response or switching to an isolated controller or HMI required.	The switch to an isolated and preferably diverse controller or HMI with full or subset capability maintains operation.
XSS Scripting/markup injection	Protocol Based	HMI Servers	Remotely execute unauthorized control commands	1. Block incoming packets by source address using SDN 2. MTD	1. Stops individual attacks 2. Makes targeting of web apps difficult (HMI could be a web app)	Would prevent monitoring and control, and depend on whether an OPC server has redundancy, or for a common exploit, all were compromised.	Response through switching to an isolated HMI required.	A secondary, diverse HMI would be a good solution to maintain monitoring.

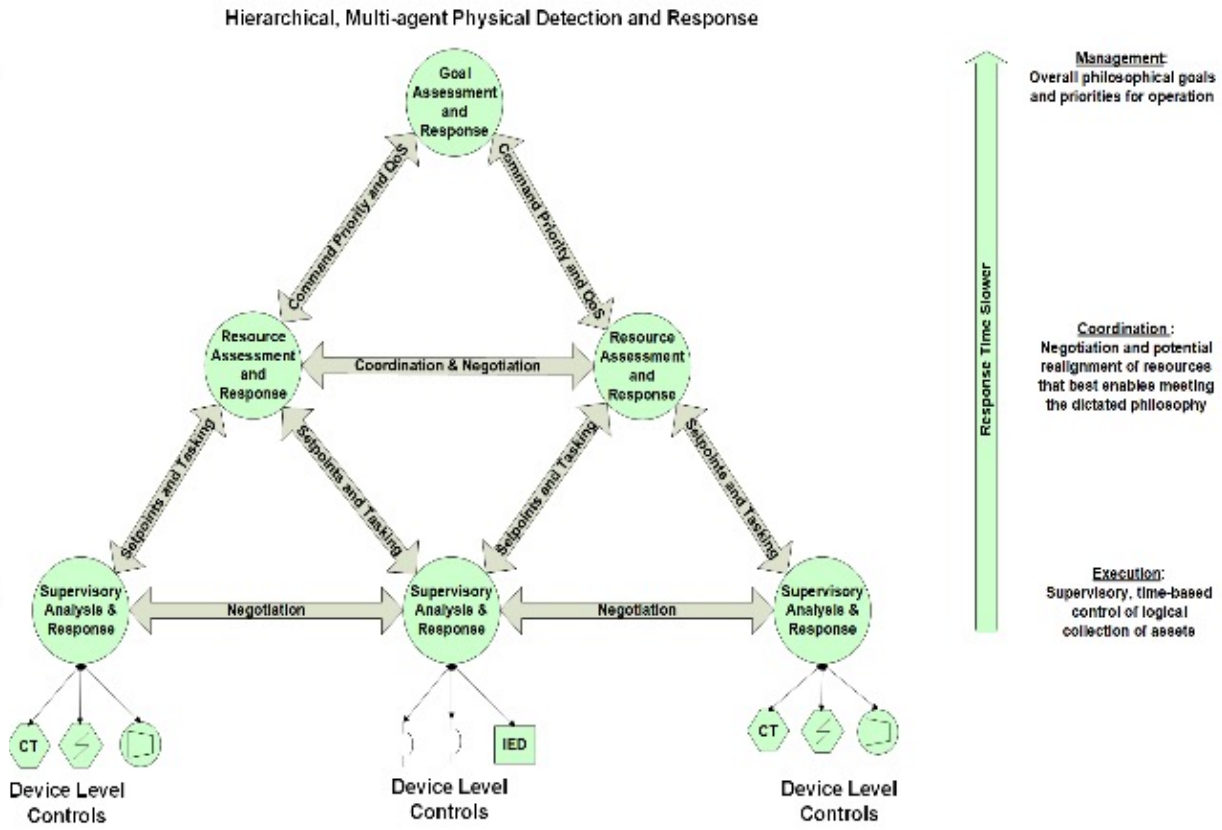
The Future: A Tiered Application of a Cyber Feedback Loop

Tier	1	2	3
1	Contains overall security policy and tradeoff space analysis as the coordinating authority for the generation and transmission assets.	Provide analytical and signature updates based upon overall system threats and level of latitude in isolating networks, ports and types of communication between substations and within/across generators.	Provide analytical and signature updates based upon overall system threats and level of latitude in isolating physical devices and traffic.
2	Transmit generator or substation analytics, event response information and threat comparisons between substations and within/across generators.	Maintain cross-segment analysis for anomaly detection and response within/across generators and substations.	Perform tradeoff space analysis and latitude of autonomous response in generators and substations versus human intervention.
3	Transmit distributed health analysis for generators and substations to allow overall system wide threat analysis and threat response strategy update.	Transmit segment analytics and event response, to inform impact and future tradeoff analysis and cross-segment threat analysis for update considering an ongoing substation or generator cyber-attack.	Maintain raw cyber-physical analysis and event response strategy in Automated Response Controller for the substation segment or within a generator.



The Future: Cyber vs Physical Multi-agent Hierarchical Architecture Concepts

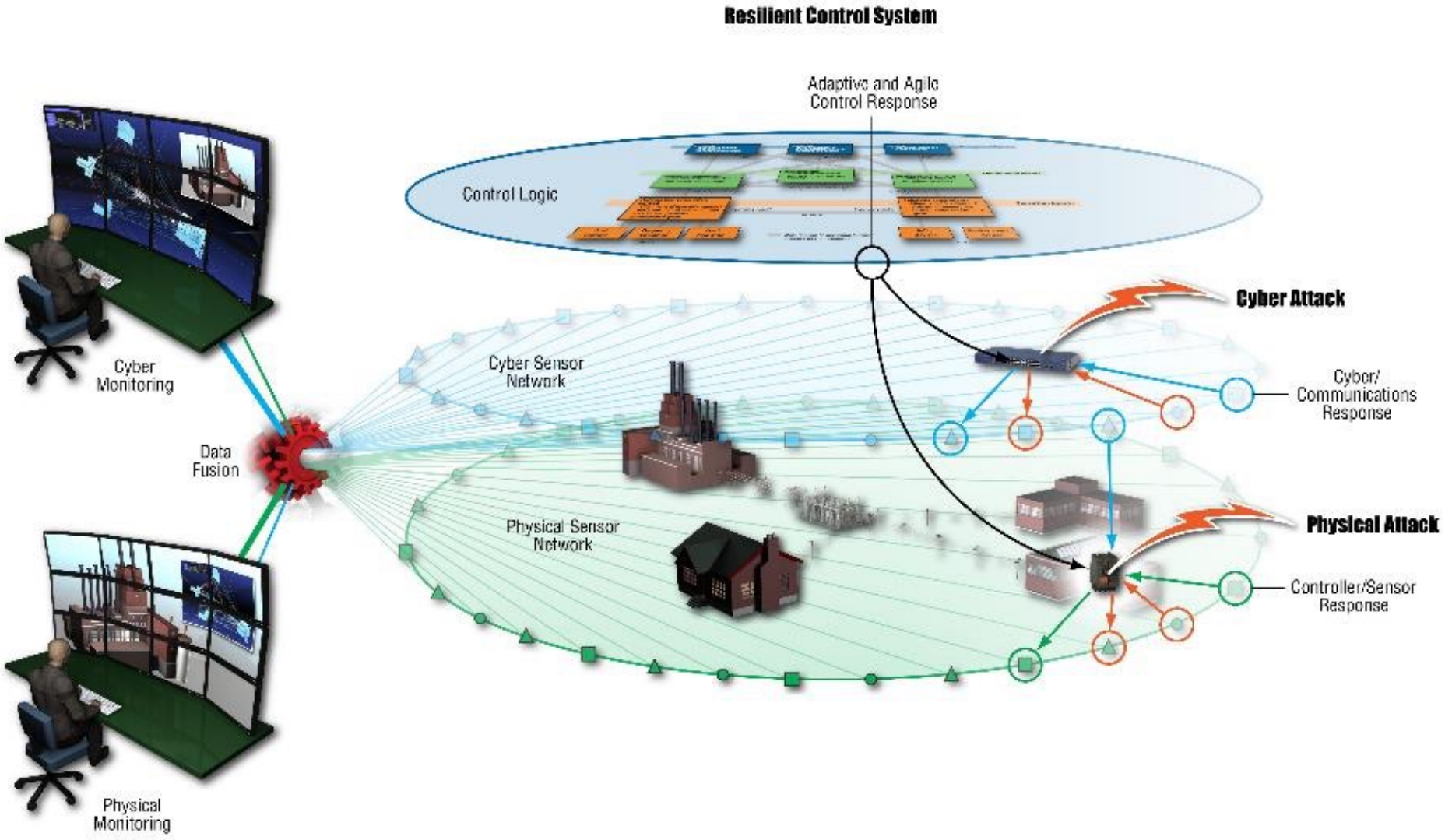




- **Commonalities**
  - Three Tiers of Agents
  - Recognizes a centralized authority with semi-autonomous echelons
  - Recognizes faster response occurs in a distributed response
  - Top tiers provides ongoing tradeoff space analysis

- **Differences**
  - Cyber is all event-based
    - Physical is time-based on bottom tier
  - Cyber anomalies are network-based, but can also include physical data
    - Physical anomalies are based on physical sensors alone
  - Cyber response actions are network-based
    - Physical response actions are host-based

A Resilient Control System Integrates Cyber-Physical Recognition & Response



Summary

Summary

- **Resilient Control Systems has been a Research Area Since 2008**
  - Founded Resilience Week, but also other conferences, symposia and workshops
  - Considers State Awareness and Resilient Design to recognize and counter affects
  - Must be judged by accepted metrics of resilience
- **Resilient Control Considers Manmade and Natural Threats**
  - Both malicious and benign, unintended human actions
  - Unexpected, cascading affects to complex control systems
- **Advent of the Active Cyber Feedback Loop to Reduce Mitigation Time**
  - Currently considers human in the loop, but the future includes autonomous
  - For acceptance, asset owners must understand first the benefits and affects of the mitigations
- **Acceptance Requires Confirming Responses and Resilience before Application**
  - Hardware in the Loop coupled with a Digital Twin, but emulation for scaling could be cyber-physical
  - Optimized approach that starts with Human Mitigation Input
- **Hierarchical Multiagent Architecture for Cyber-Physical Response**
  - Three tiers of influence, allowing for decentralized response but benefited by centralized considerations
  - Cyber anomalies network-based but can include physical data, while physical anomalies based upon sensors alone
  - Cyber responses are network-based and physical responses are host-based

QUESTIONS?

CyPhRe Triad™

Idaho National Laboratory