Resilient Control Systems and the Advancement of the Cyber Feedback Loop
Outline

• Resilient Control Systems Background
• Architecture for Resilient Design
• Resilient Control Systems and the Cyber Feedback Loop
• Summary
Resilient Control Systems Background
The ability to network control systems has provided a mixed blessing in the ability to interlock systems of systems, even crossing industrial sectors.
Cyber security attacks are becoming increasingly complex, which includes the targeting of control systems.
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

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

Resilient Design provides an adaptive capacity and agility for response to threats, including those that are not well characterized by traditional means.

State Awareness provides essential knowledge of operating parameters to fully characterize the decision space.

Threats are those elements that counter normalcy and destabilize control system networks – human error, damaging storms, malicious attacks, complex failures & interdependencies.

“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**
    o Intelligent architectures integrate expert knowledge with supervisory control
    o Diverse detection and response protections at each level of control system architecture
  – **Maximizing operational efficiencies**
    o Advanced control designs assess degradation and proactively control
  – **Enabling rapid response to all threats**
    o 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

- **Data Fusion Approach**: that can process diverse data to proactively recognize threats within each measure of normalcy and prioritize response.

- **Mixed Initiative Framework**: that provides mechanisms to integrate automation and human response in an optimized manner, taking benefit from the inherent resilience in both.

- **Resilient Control System**
  - **Operational Data and Controls**
    - Physical Security
    - Cyber Security
    - Process Efficiency
    - Safeguards and Nonproliferation
  - **Intelligent Interpretation and Control**
    - Data Fusion
    - Intelligent Interpretation
    - Mixed Initiative Control
  - **Operational State Awareness Dashboard**
    - Manager
    - Operator
    - Engineer
    - Regulator
  - **Hierarchical Control System Design**: that provides a robust and adaptive mechanism for optimizing control system performance to measures of normalcy.

- **Consideration of all threats and events**
  - by which we determine proper operation.

- **Targeting the consumer**
  - of the information, to tailor what is presented and how.
Transformative Research and Deployable Solutions for Inherent Infrastructure Resilience

Intelligent Cyber Detection & Feedback Mechanisms

Adaptive and Agile Resilience Control Architectures

Resilient Control System Architecture

Role-based, Cyber-Physical State and Context Awareness

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 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 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

---

**Feedback Taxonomy Crossover**
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

  Initial Set of Mitigations
  Produced by A Human Expert

  Initial Set of Mitigations
  Produced by A Human Expert

  Initial Set of Mitigations
  Produced by A Human Expert

  Initial Set of Mitigations
  Produced by A Human Expert

  Initial Set of Mitigations
  Produced by A Human Expert

  Initial Set of Mitigations
  Produced by A Human Expert

  Initial Set of Mitigations
  Produced by A Human Expert
# The Future: A Tiered Application of a Cyber Feedback Loop

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

---

**Diagram:**

- **Defender Analysis & Exploration**
- **Cross-Segment Analysis & Defense**
- **Alerts & Recommendations**
- **Security Information & Event Management Analysis & Response**
- **Intermediate Defense - Cross-Segment Analysis & Response**
- **Distributed Defense - Intrusion Sensor Analysis & Response**

---

**Legend:**

- **Information Technology**
  - Perimeter Controls
  - Network Flow Controls
  - Human Machine Interface
  - Programmable Logic Controller

- **Operational Technology**
  - Role Based Access Controls
  - Device Level Controls

---

**IDAH0 NATIONAL LABORATORY**
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

• 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™