Tutorial

Session 5: Resilience, where do we go from here?

Craig Rieger, PhD
Idaho National Laboratory

Instrumentation, Control and Intelligent Systems,
Signature Lead

August 11-13, 2009
Idaho Falls, Idaho

Control System Research Need

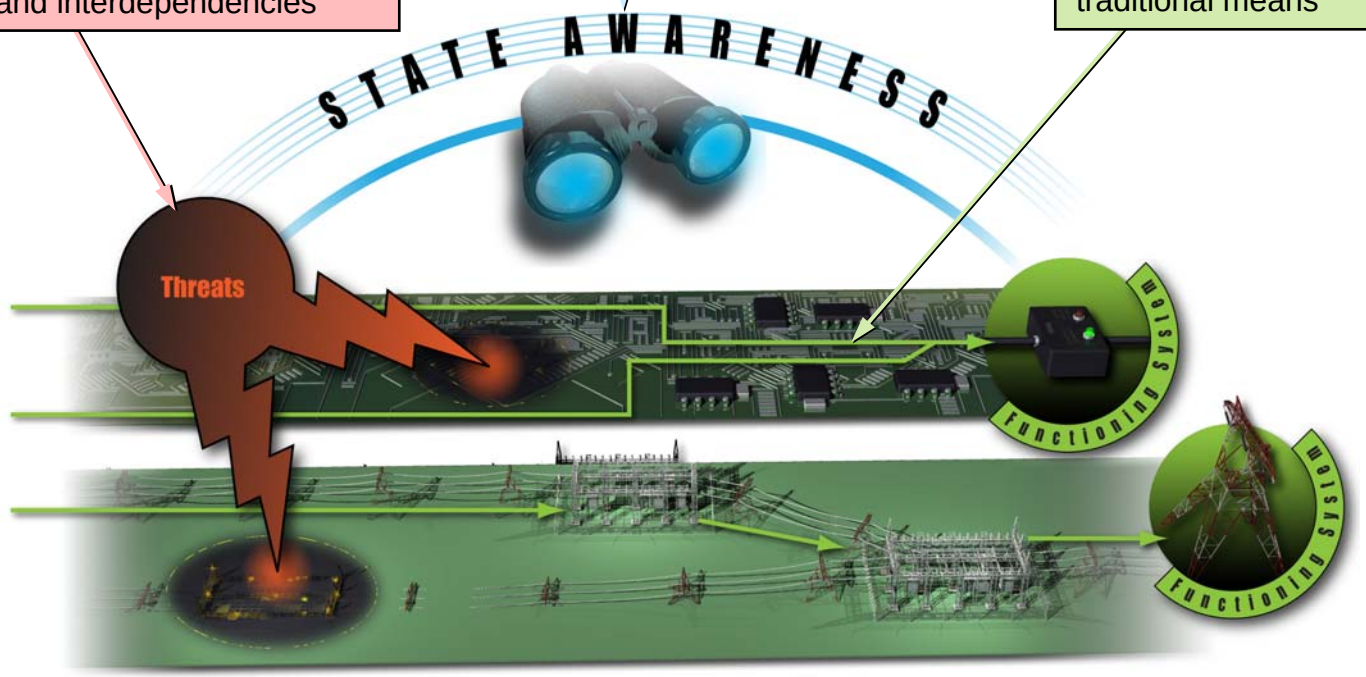
- Sensors and data proliferate, but what does it tell me about my state?
  - Online fusion and analysis of data is required to develop indicators of system performance, status and the basis for response
- It isn't just localized process stability that affects state….
  - Physical security, cyber security, process efficiency, and safeguards are also integral to state awareness, each having similar research needs
- Just tell me what I need to know…..
  - For a manager, the plant information presented and its prioritization is different than that of an engineer
- How can I ensure that the control system responds as expected?
  - Whether cyber or traditional software failure, all failures or threats need to be recognized and addressed for highly interconnected control systems

Next Generation Control Systems: From Reliable to Resilient

Threats are those elements that *counter normalcy* and *destabilize control system* networks – human error and malicious attacks, complex latencies and interdependencies

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

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



Proposed Definition

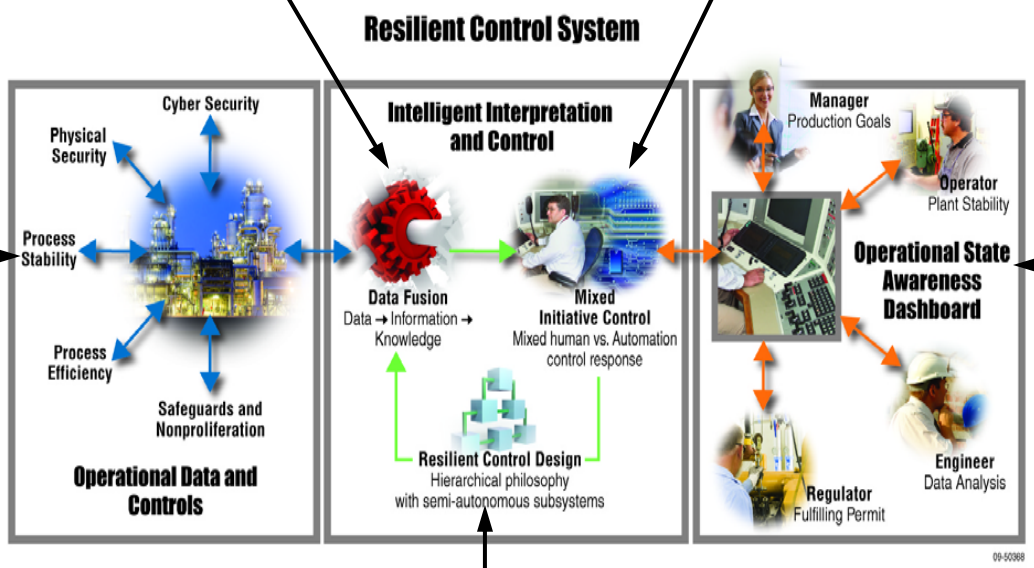
A resilient control system is one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.

A Resilient Control System Framework

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

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



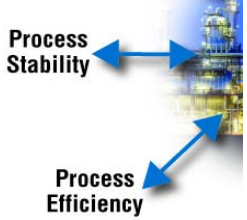
Targeting the consumer of the information, to tailor what is presented and how

Hierarchical Control System Design that provides a *robust and adaptive* mechanism for optimizing control system performance to measures of normalcy

State Awareness:
Cyber & Physical Security

- Development of analytics that identify normal communications behavior for wired and wireless
- Data authentication and diversity to ensure integrity of cyber and physical environment
- Layers of detection fidelity to refine and prioritize discrete targets of interest
- Randomization of system attributes to confound attacks while maintaining determinism for the control application

State Awareness:
Stability and Efficiency



ISRCS 2009

- Prognose and diagnose deviations from nominal behavior, migrating from reactive to proactive design
- Built upon supervisory control that considers the dynamic interactions of plant systems and incorporates advanced control theory
- Performs optimization of subsystems to a global maxima or minima, providing a holistic perspective in ensuring plant safety and efficiency
- Provides adaptive capacity based on an information quality judgment, overcoming brittleness arising from sensor dependencies

State Awareness:
Safeguards and Nonproliferation

Safeguards and Nonproliferation

ISRCS 2009

- Timely knowledge of the location and movement of nuclear material within a nuclear facility
- Real-time knowledge of plant activity to prevent downtime of facilities, and diversion or misuse of nuclear material
- Process accountancy to provide enhanced awareness of the nuclear material inventory and status

Resilient Design:
Data Fusion

- Consideration of human and automation to determine algorithms and methodologies
- Collation of diverse indicators, such as cyber security and process data, performed to determine desired operation
- Proper prioritization of the information provided to the consumer to aid recognition and action
  - Reduction - The reduction of data to provide only that information necessary to achieve the appropriate response
  - Identification - Validation and invalidation of causes for events, e.g., a process upset due to a failed valve and not cyber attack.
  - Improved characterization and knowledge - Development of new information that helps to better characterize state

Resilient Design:
Mixed Initiative

- Interleaving of human and automation responses for optimal reaction
- A control system concept that allows the user to configure autonomy on the fly
- Measurement and adaptation to the user based on current understanding, performance and changing environment
- Provides for prioritization of tasks based on time load and historic resilience

Resilient Design:
Control System

- Hierarchical, multi-agent approach to supervisory design that considers the control system and affected operation holistically
- Independent oversight outside of echelon insures state awareness is accurately communicated up and philosophy is communicated down
- Semi-autonomous operation allowed within defined boundaries for lower echelons
- Traditional concepts are helpful, including redundancy and diversity, but must be extended to consider all threats

Resilient Design:
State Dashboard

- Interactions between the human and the interface form the basis for proper or improper judgments
- Authorizing interaction level by individual certifications and responsibilities, and measured performance
- Presentation of information must reflect the needs of the consumer, whether operator, manager or engineer, and their responsibilities

Area of Resilience:
Human Systems

- The human psyche can have the ability to quickly understand novel situations, with the potential of providing additional control system resilience
- As human behavior is not reproducibly predictable, however, unique measurement and correlations of performance are required
- Bayesian methods provide one method to take into account evidence regarding human response, but one among many approaches
- Defining methods of mixed initiative response, a combination of human and automation, can provide more resilience during complex operations

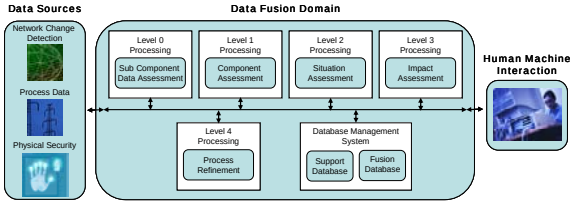
Area of Resilience:
Cyber Awareness

- For the benevolent employee, the goal is to target information to achieve a reproducible response; for the intelligent adversary, a comparable goal is to befuddle the attacker
- Informational mechanisms to understand health, but also feedback mechanisms are needed to tie a sensed attack to a corresponding control system change
- Methods to model the variability of both the objective and motives of the intellectual adversary to provide a basis for feedback
- Atypical architectural design to take away the adversarial advantage, changing system attributes to appear random in response and characteristics

Area of Resilience:
Complex Control Networks

- Ability to characterize interactions, performance and security becomes more critical to ensuring resilience
- No assurance that global stability can be achieved by subsystem minimization
- To provide faster responses, the feedback and response occur close to the point of interaction with the application
- True global optimization coupled with a local interaction can achieve the assurance of a global minima and an acceptable response time

Current Research Projects



- State Awareness
  - Data fusion of system performance data, including cyber
  - Prognostics, diagnostics and supervisory control
  - Intelligent information visualization systems
- Resilient Design
  - Optimal modeling interface to control systems
  - Resilient control system network agents
  - Deterministic wired and wireless communications security
  - Resilient and adaptive condition assessment
  - Automated differential equation-based system identification

Summary

- The discussion presented provides a conceptual framework and brief overview of the architectural considerations for resilient control systems
- The complexity of the control systems and the facilities they are intended to safely and reliably control has increased
- Cyber connectivity, which provides a fairly inexpensive avenue to infiltrate control systems, has increased this complexity
- Research at INL is ongoing under this framework to provide the basis for next generation resilient control systems, a holistic view to ensure a safe and secure critical infrastructure

Questions?

Contact Information

Resilient Control Systems Research

Craig Rieger, Signature Lead	Craig.Rieger@inl.gov	(208) 526-4136