UNIVERSITY OF NORTH DAKOTA

# Resilience Basis, Definition, and Interdisciplinary Application

Craig Rieger, PhD, PE

November 27, 2023

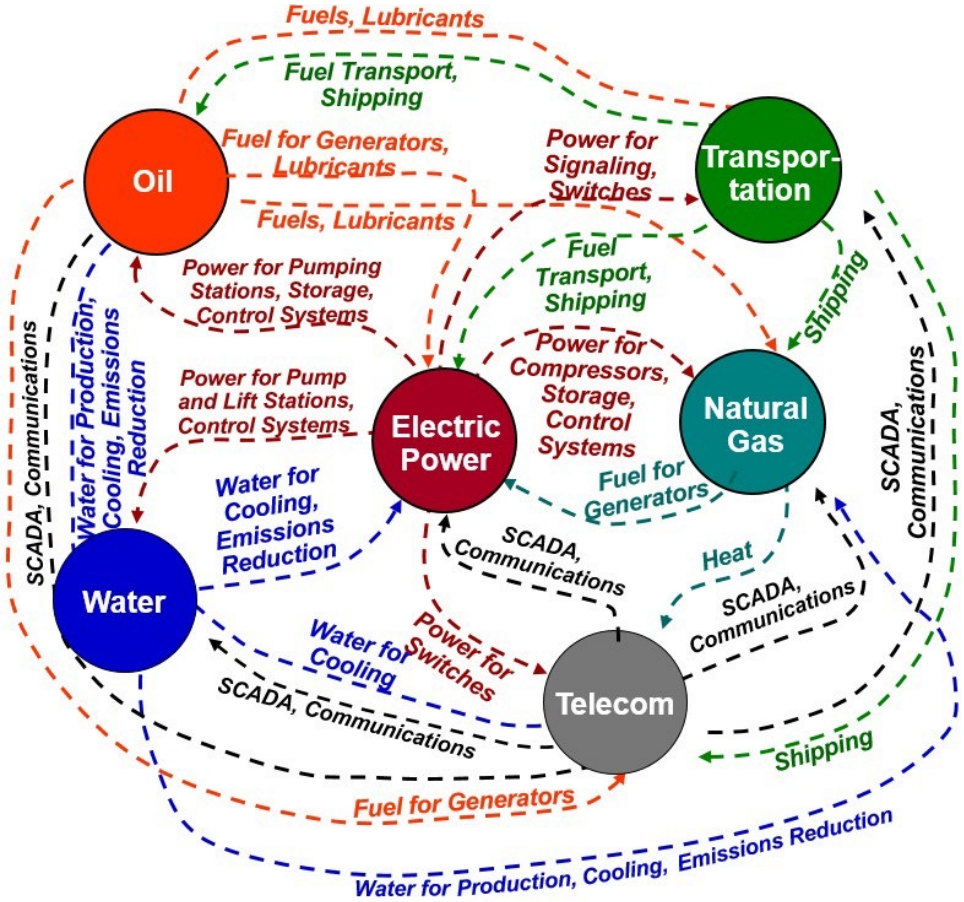
# Outline

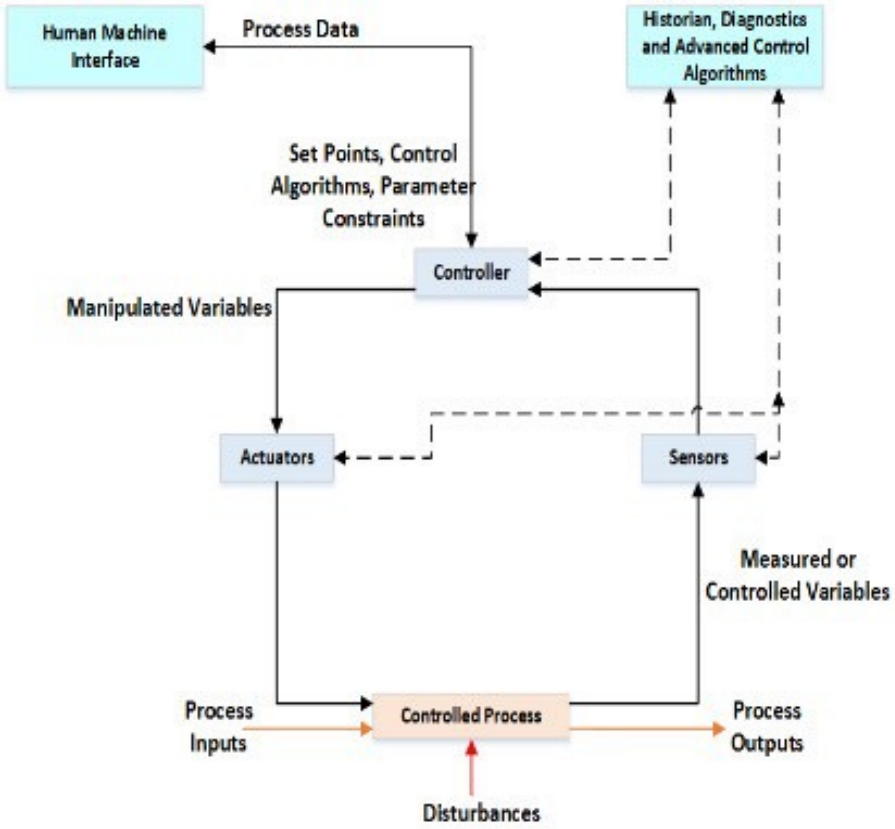
- Resilient Control Systems Background
- Resilient Control Systems Precepts
- Architecture for Resilient Design
- Summary

# Resilient Control Systems Background

# Control System Complexity

(Ron Fisher, inl.gov)



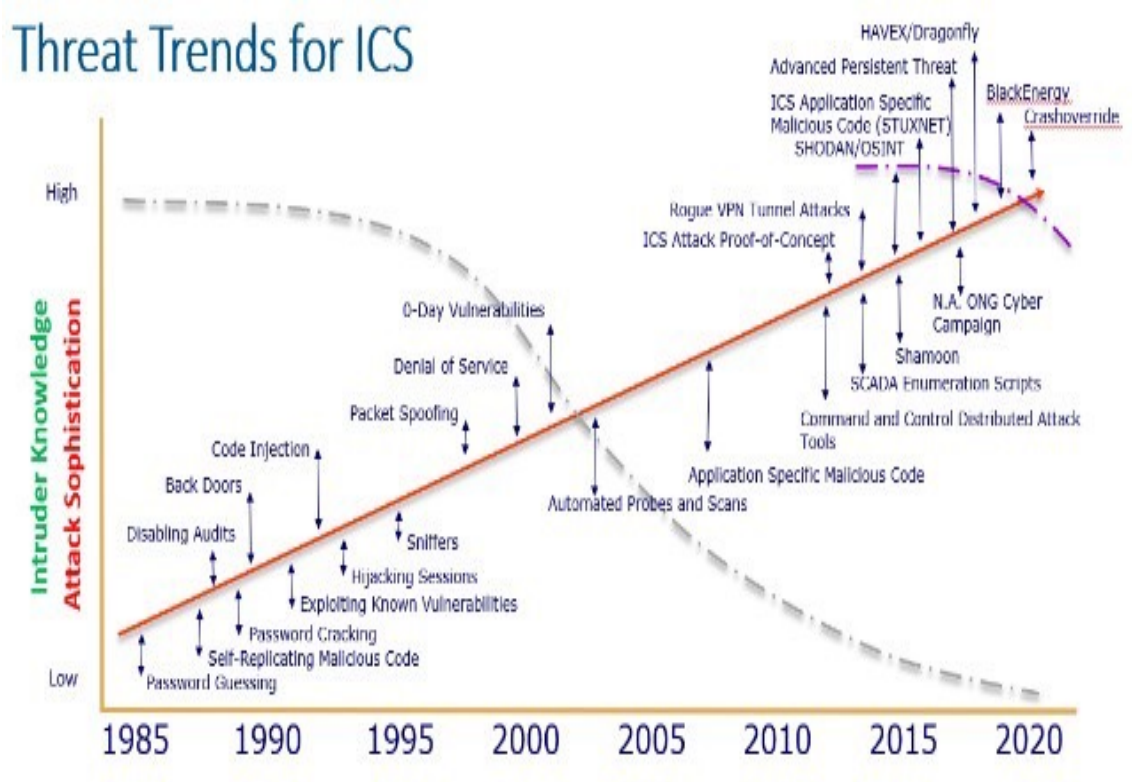

***The ability to network control systems has provided a mixed blessing in the ability to interlock systems of systems, even crossing industrial sectors.***

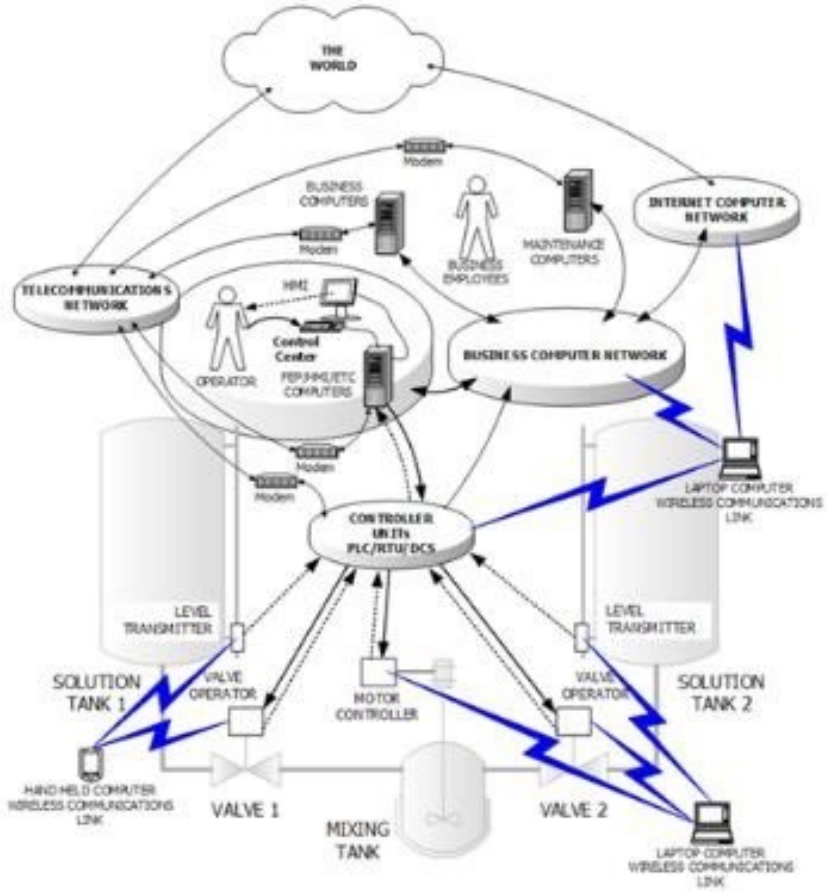
C2SR
CENTER FOR CYBER SECURITY RESEARCH

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

# Cyber System Complexity

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



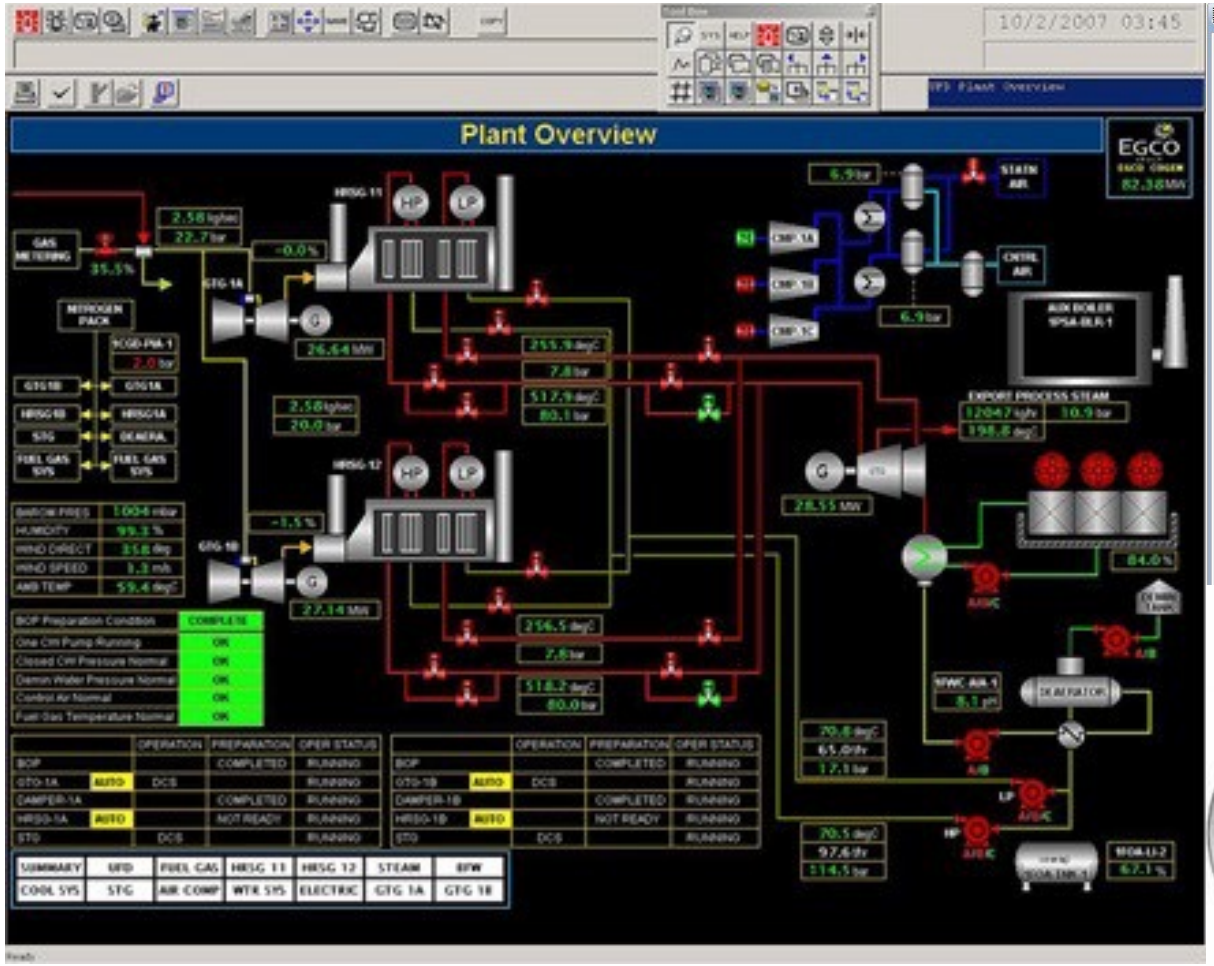

***Cyber security attacks are becoming increasingly complex, which includes the targeting of control systems.***

C2SR
CENTER FOR CYBER SECURITY RESEARCH

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

# Human System Complexity

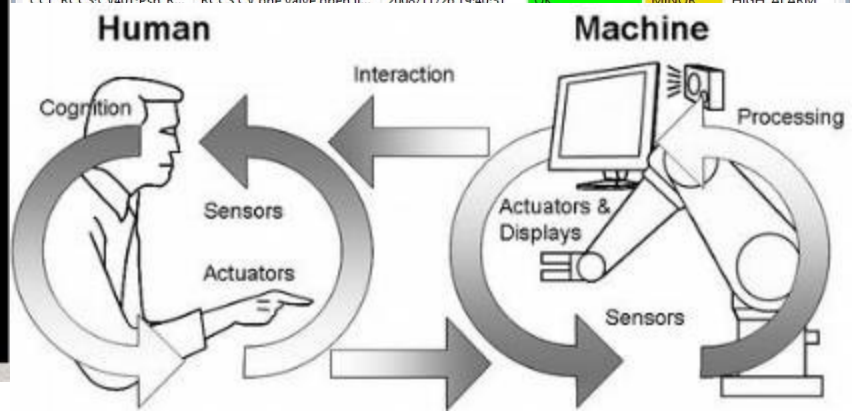
(yokagawa.com, cs-studio.sourceforge.net, plantautomation-technology.com)




Alarm Table

Current Alarms

| 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.***

C2SR
CENTER FOR CYBER SECURITY RESEARCH

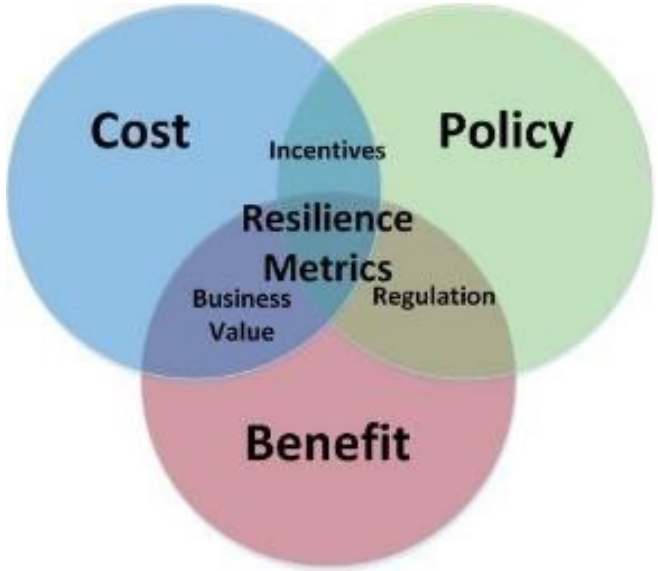
UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

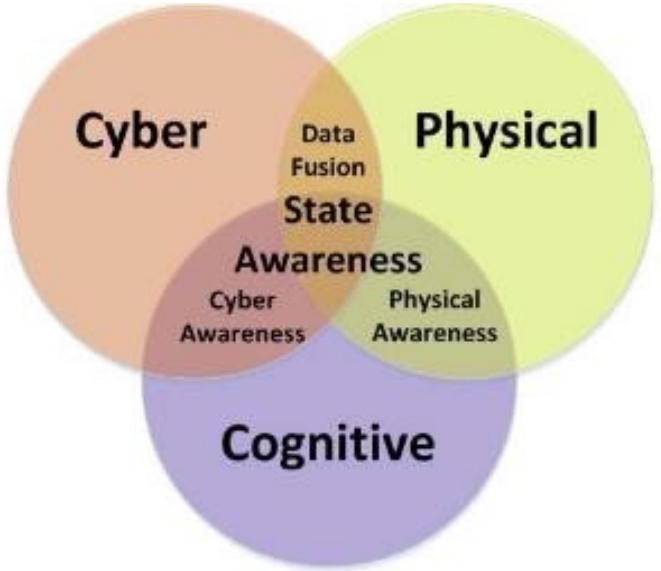
# Resilience Considerations Arising From Complexity

- **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 and Application Alignment

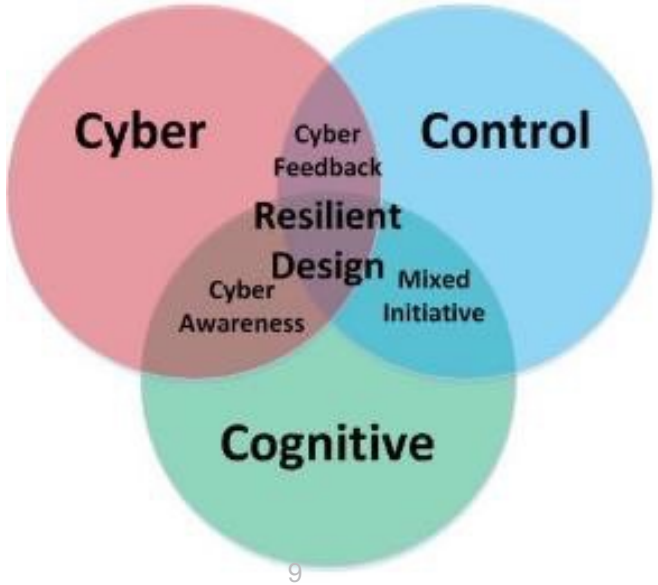
**Measure**




**Recon**

**Resist/ Respond**





**Resilience**



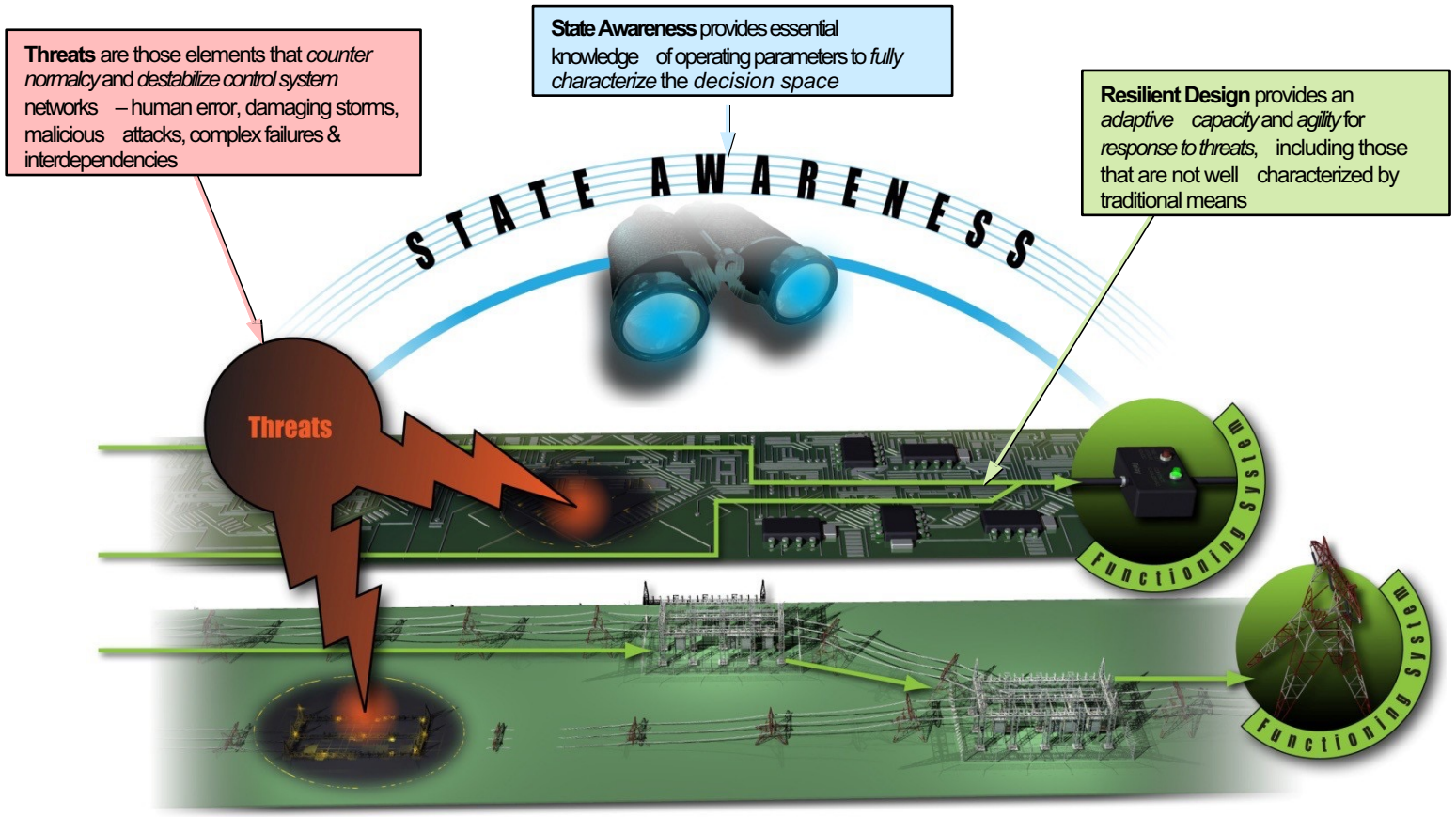
UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

# Resilient Control System Precepts

C2SR

CENTER FOR CYBER SECURITY RESEARCH

# Next Generation Control Systems: From Reliable to Resilient



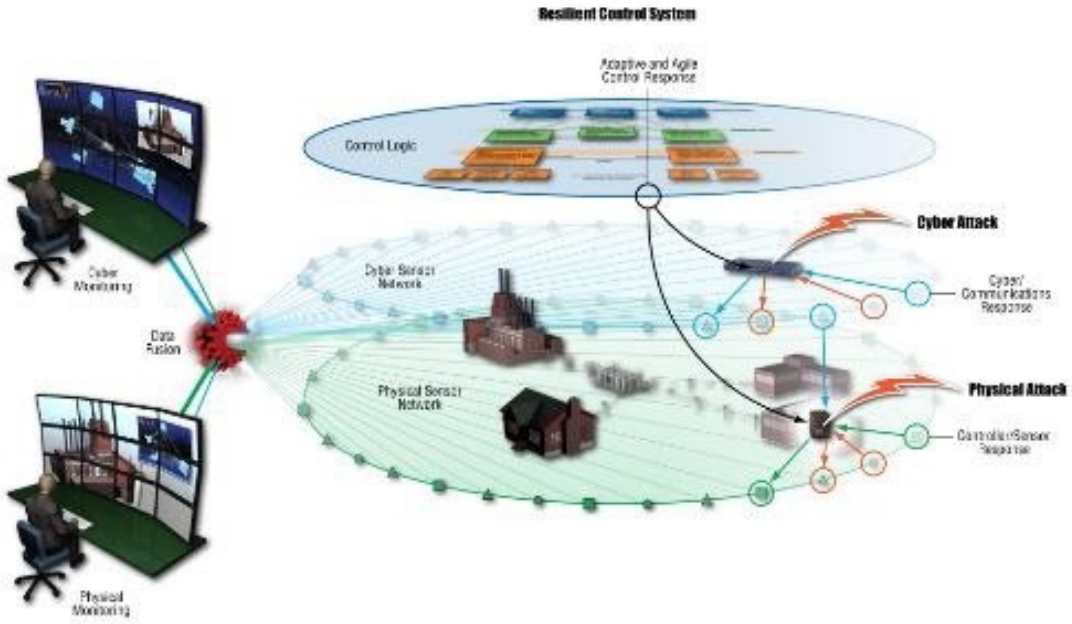

***"Resilience" is the capacity of a control system to maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. (2009)***



UNIVERSITY OF NORTH DAKOTA

# 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

C2SR CENTER FOR CYBER SECURITY RESEARCH

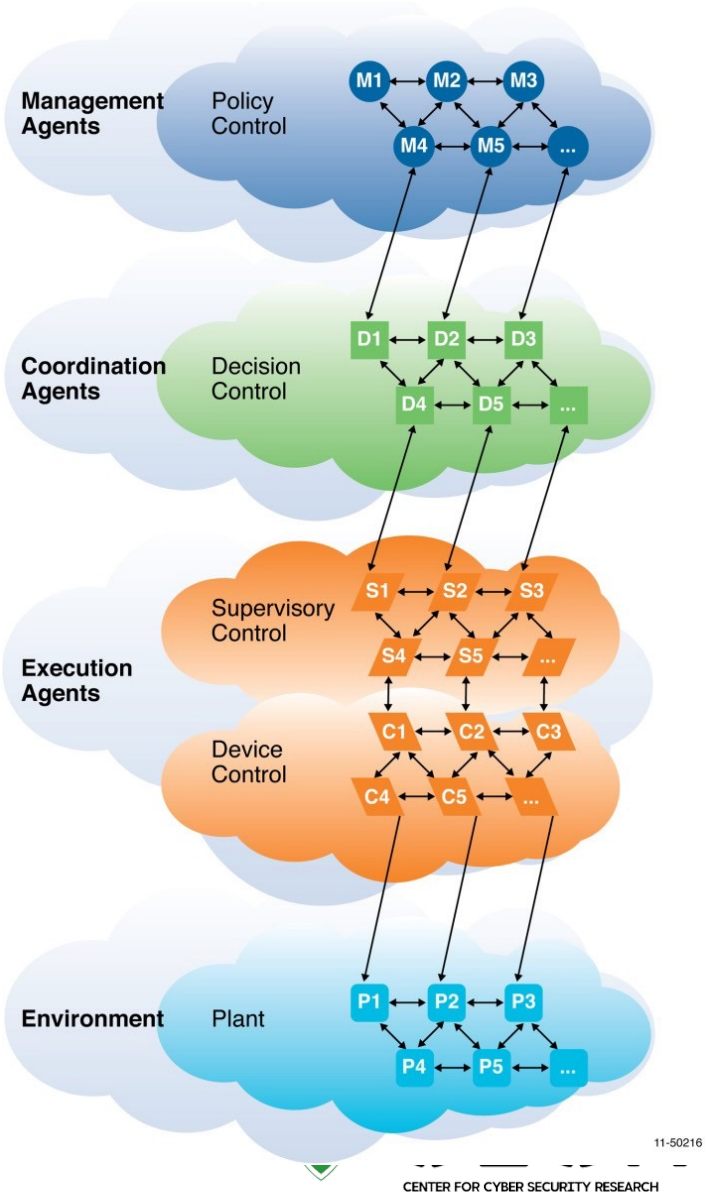
UND UNIVERSITY OF NORTH DAKOTA COLLEGE OF ENGINEERING & MINES



Infosecurityinc.net.com

# 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

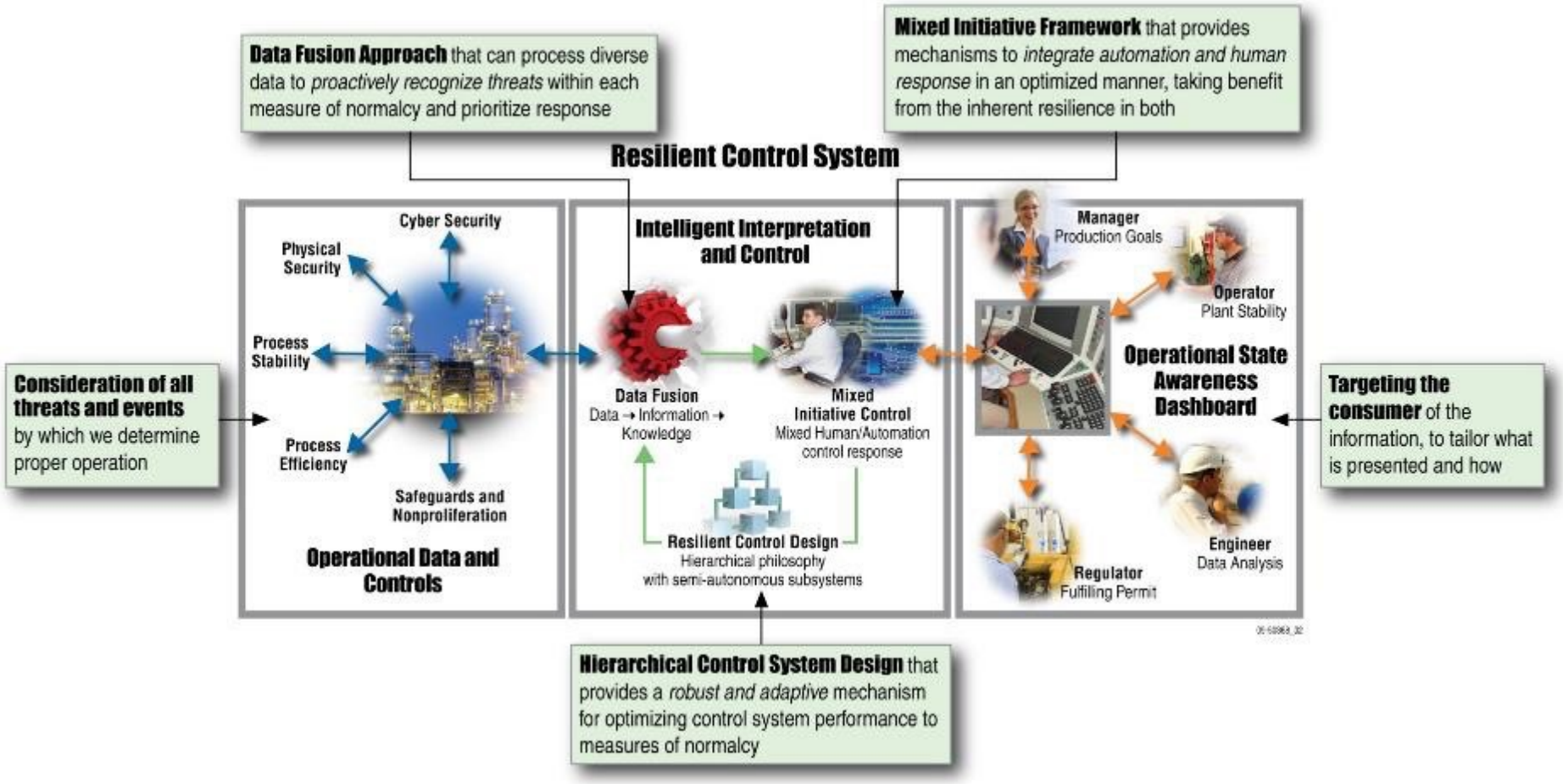



- **Unexpected condition adaptation**
  - Decomposed dynamics to achievable hierarchy with semi- autonomous echelons
  - Tiered metrics to confirm performance and root cause
  - Negotiated tradeoff analysis to disturbance conditions to ensure mission resilience over efficiencies and cost
  - Intelligent 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

UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

# Architecture for Resilient Design

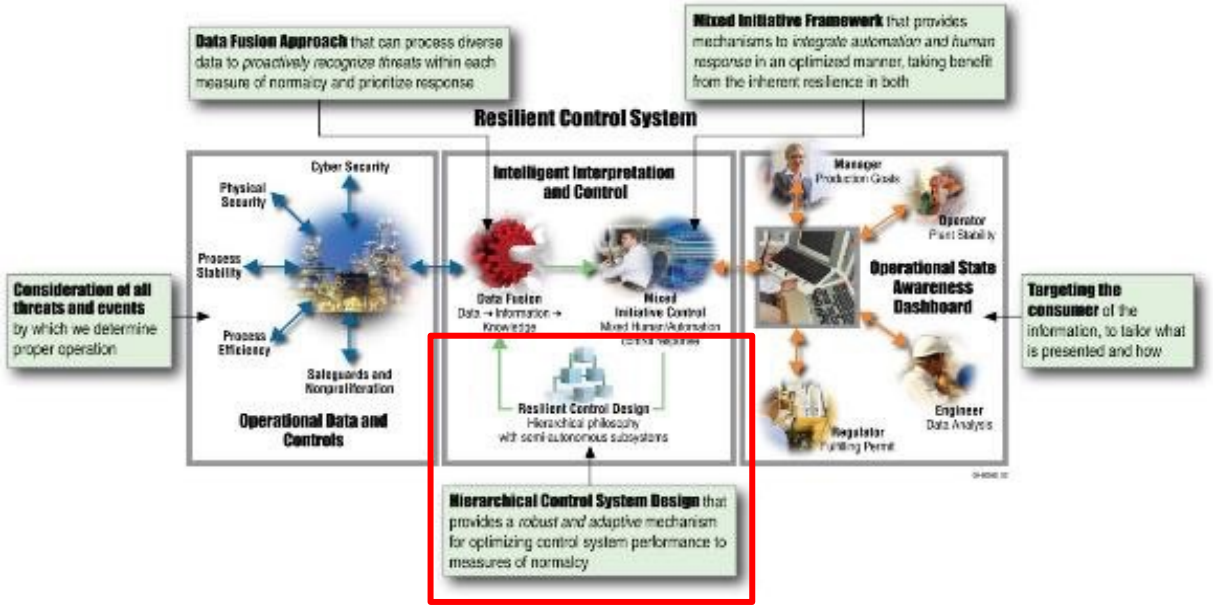
# A Resilient Control System Architecture




C2SR
CENTER FOR CYBER SECURITY RESEARCH

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

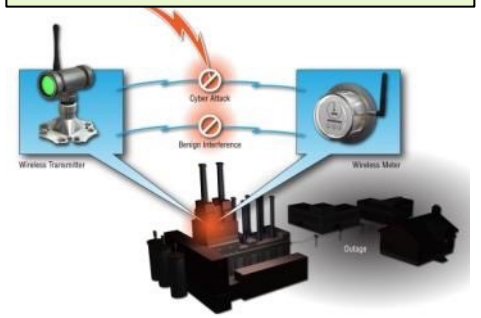
# Hierarchical, Multi-agent Dynamical System Design for a Physical System




- **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**

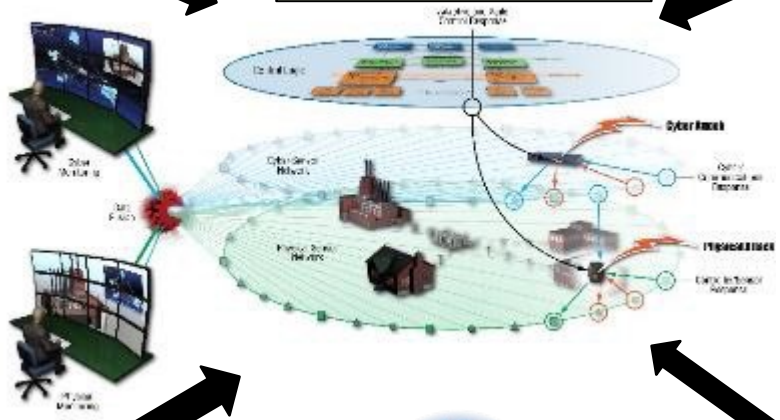
# Transformative Research and Deployable Solutions for Inherent Infrastructure Resilience (from inl.gov)

**Intelligent Cyber Detection & Feedback Mechanisms**

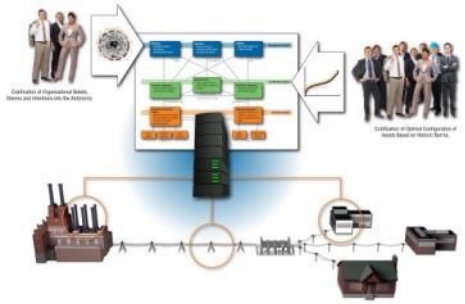



**Role-based, Cyber-Physical State and Context Awareness**

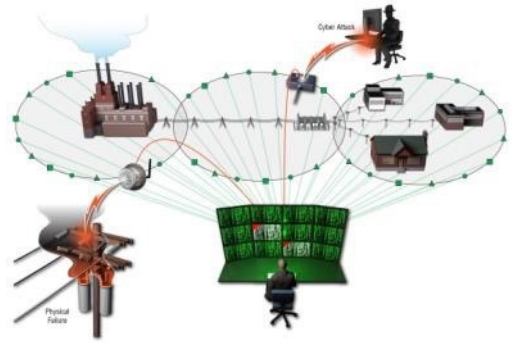

**Resilient Control System Architecture**




**Adaptive and Agile Resilience Control Architectures**



**Infrastructure Trustworthiness Assessment & Proactive Control**




Resilient Control & Instrumentation Systems

C2SR
CENTER FOR CYBER SECURITY RESEARCH

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

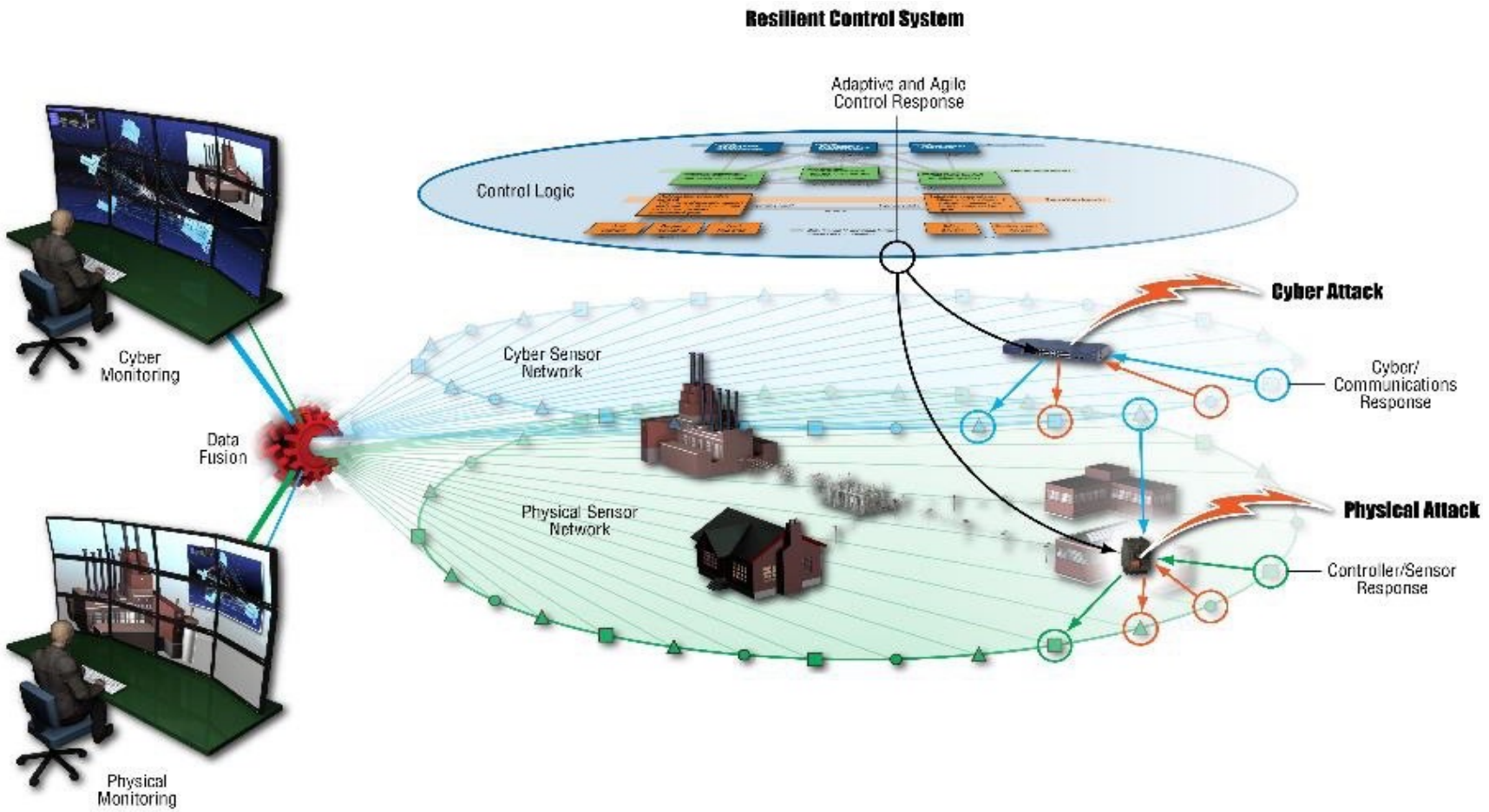
# Summary

# 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
- **Architecture for Human-Cyber-Physical Response**
  - Infrastructure Cyber-Physical Trustworthiness Assessment & Adaptive, Proactive Control
  - Role-based, Cyber-Physical State and Context Awareness for Human Response
  - Hierarchical, Multiagent Distributed Recognition and Response to Cyber-Physical Threats

UNIVERSITY OF NORTH DAKOTA

# QUESTIONS?




C2SR
CENTER FOR CYBER SECURITY RESEARCH