A Resilient Control System maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature.

Resilient Systems

Transformational Solutions from Concept to Deployment

Idaho National Laboratory has envisioned “resilient” systems that ensure control systems are more resistant to interruption from natural or man-made disasters. Through the lab’s Resilient Control and Instrumentation Systems (ReCIS) Program these are being demonstrated for adoption by industry. Complex infrastructure systems with enhanced resilience have the capacity to maintain safe levels of operation in response to natural or man-made threats. INL has led the innovation to improve system resilience and minimize outcomes from unplanned natural disturbances, malicious attacks or new vulnerabilities inherent to critical infrastructure systems. This ReCIS focus anticipates emerging national challenges associated with the efficiency, effectiveness, and security of the Nation’s defense and critical infrastructure systems, including its wired and wireless communications networks. Whether a swarm of unmanned air vehicles or a smart power grid, mission assurance will require the deployment of distributed control systems intended to efficiently, economically and intelligently interact with end user devices. Given the multiple competing demands with which such an interdependent control system must cope, its complexity may well prove to be its Achilles heel. Addressing this vulnerability will require control system technologies that are resilient by nature and remain resilient when interoperating. The development of such technologies will underpin next generation designs for defense and critical infrastructure systems where adversarial threats and benign, but undesirable human responses can create an even greater liability than the loss of use.

Resilience Research

• Resilience Research Leads
  – Interdisciplinary team of individuals representing technical excellence in cyber-physical security, intelligent design and control, and human system applied research, development, demonstration and deployment
  • Select Resilience Papers
    Papers representing several of the resilience research projects associated with ReCIS efforts, vetted by an advisory committee composed of National Academy, National Laboratory, Society Fellows and Industry members.
  • Recognized Resilience Events and Collaborations
    • Resilience Week
      Symposia dedicated to promising research that transforms the resilience of cognitive, cyber-physical systems
    • University Challenge
      Develop a control system design that maintains quantifiable, stable control in spite of threats, including process disturbances, sensor degradation, cyber
ReCIS research covers the following areas: Safeguards and control systems security, sensors, intelligent monitoring, human factors, controls and statistics, and robotics automation.

Facilities
The laboratory can be utilized for complex evaluation of control system designs for cyber security, advanced control, human performance and operational verification and validation. Some of these include:

- SCADA Test Bed (STB) – Vulnerability assessment and risk analysis of energy sector industrial control systems
- High Temperature Testing Laboratory (HTTL) – Dedicated to sensor development, fabrication, and evaluation
- Human System Simulator Laboratory (HSSL) – Supporting human factors design for prioritized and efficient interfaces to nuclear and other critical infrastructure facilities
- Isolated Unmanned Aircraft Systems (UAS) test bed – Airfield for UAS design testing with full radio spectrum authority and authorization from the Federal Aviation Administration, allowing UAS operation.
- Machine Condition Monitoring (MCM) test bed - an engineering-scale environment to verify and validate advanced monitoring and control strategies, including diagnostics, prognostics, data analytics, smart components, resilient controls, and wired/wireless online condition monitoring technologies.