

**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 distinctive signature in **Instrumentation Control and Intelligent Systems (ICIS)** 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 outages from unplanned natural disturbances, malicious attacks or new vulnerabilities inherent to critical infrastructure systems. This ICIS 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 undesir-

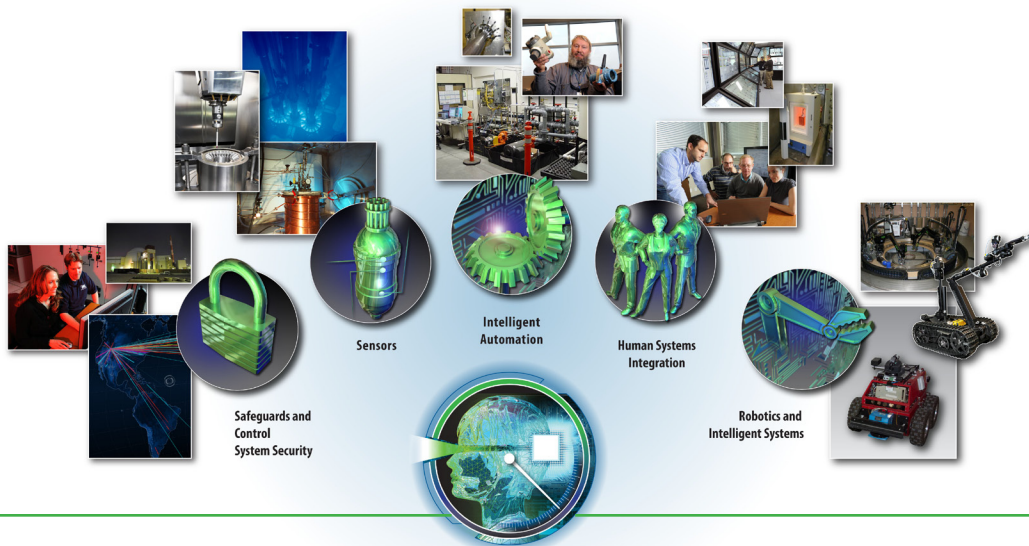
able human responses can create an even greater liability than the loss of use.

#### 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 funded by ICIS since it established a resilient control system grand challenge in 2008, vetted by an advisory committee composed of National Academy, National Laboratory, Society Fellows and Industry members.

*Continued next page*





**ICIS research covers five areas: Safeguards and control systems security, sensors, intelligent automation, human-systems integration, and robotics/intelligent systems.**

practical design performed in support of the operating facilities. Each activity is important to the overall ICIS capability, and provides not only an individual programmatic capability but also a diverse INL capability to meet the challenges of this evolving technological area.

### For more information

#### Technical Contact:

**Craig Rieger**

(208) 526-4136

[Craig.Rieger@inl.gov](mailto:Craig.Rieger@inl.gov)

[www.inl.gov/icis](http://www.inl.gov/icis)

### A U.S. Department of Energy National Laboratory



*Continued from previous page*

#### Recognized Resilience Events and Collaborations

- **Resilience Week** – Symposium 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 intrusion, human error, and related interdependencies
- **Resilience and Security for Industrial Applications (ReSia) Technical Committee** – Engendering threat-resilience into industrial applications through metrics and standards codified by demonstrated technologies with firm scientific underpinnings.

ICIS programmatic research is centered on developing components, programs, systems and individuals for any application that requires monitoring, control, security and human interaction. These capabilities have provided core competencies to address national challenges, and culminated in the development and deployment of cutting edge resilient systems:

- Safeguards and control system security methods to protect digital systems and special

nuclear material from the intelligent adversary

[www.inl.gov/icis/scss](http://www.inl.gov/icis/scss)

- Specialized sensors and sensing systems that are designed to monitor critical infrastructure and withstand demanding environments associated with nuclear facilities and emergency response during natural and manmade events  
[www.inl.gov/icis/sensors](http://www.inl.gov/icis/sensors)
- On-line condition monitoring and prognostics, observational platform design, and advanced supervisory and predictive controls for reliable, efficient and safe operation of industrial and nuclear facilities  
[www.inl.gov/icis/ia](http://www.inl.gov/icis/ia)
- Research to advance human-centered design and operation of complex systems, considering the human interaction with the process in its various forms, including visual, audible and touch  
[www.inl.gov/icis/hsi](http://www.inl.gov/icis/hsi)
- Robotics and intelligent designs for application to autonomous manufacturing, emergency response and defense systems.  
[www.inl.gov/icis/ris](http://www.inl.gov/icis/ris)

#### Expertise

ICIS hosts a team of more than 50 scientists and engineers who specialize in each technological area. Applied research is performed in support of the three research mission areas, and

#### 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
- **Wireless Sensor Test Bed (WSTB)** – Measuring the effects of radio frequency interference on a Wireless Sensor Networks (WSN)
- **Machine Condition Monitoring (MCM) test bed** – Scale, automated hydraulic systems for the evaluation of fault recognition and prognostic response
- **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.