ReCAS Resilient Control Architectures and Systems

Volume 2, Number 1 AN ICIS NEWSLETTER December 2011

Select Resilience Papers

Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine
www.inl.gov/icis/anomalydetection

Deception Used for Cyber Defense of Control Systems
www.inl.gov/icis/deception

Human Factors and Data Fusion as Part of Control Systems Resilience
www.inl.gov/icis/humanfactors

'Known Secure Sensor Measurements' for Critical Infrastructure Systems: Detecting Falsification of System State
www.inl.gov/icis/knownsecure

Resilient Control Systems: Next Generation Design Research
www.inl.gov/icis/controlsystems

Towards Resilient Critical Infrastructures: Application of Type-2 Fuzzy Logic in Embedded Network Cyber Sensor
www.inl.gov/icis/towardresilient

Boise State University former Dean of Engineering Dr. Cheryl Schrader offers a welcome address to the ISRCS 2011 attendees.

UC Berkeley Dean of Engineering Dr. Shankar Sastry discusses high confidence networked control systems in his keynote address.

Fourth International Symposium on Resilient Control Systems

Idaho National Laboratory, Idaho State University, University of Idaho and Boise State University recently co-sponsored a symposium in Boise to discuss and develop high-level visions and ideas for resilient control systems. IEEE Industrial Electronics Society (IES) was a technical co-sponsor.

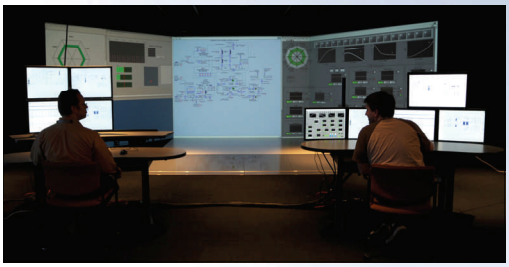
During the three-day event, more than 100 conference attendees participated in a variety of topics and heard from prominent subject matter experts about the need for furthering resilient control systems research.

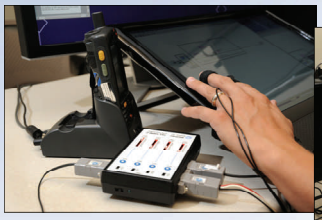
Keynote speakers included College of Engineering Dean Dr. Shankar Sastry of UC Berkeley; Dr. Massoud Amin from University of Minnesota; Dr. Lamine Mili of Virginia Tech; Dr. David Nicol from University of Illinois; and Dr. G. Kumar Venayagamoorthy of Missouri University of Science and Technology. Presentations and discussions consisted of topics related to human systems, cyber awareness, data fusion and complex networked controlled systems.

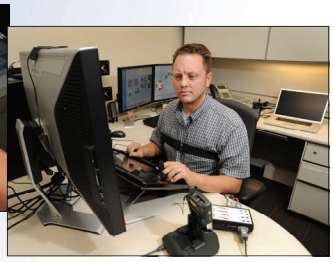
A new workshop offered this year – the 1st Experimental Security Panoramas (ESP) workshop – focused on all forms of experimentation related to cybersystem security, including both software and human vulnerabilities.

"The ESP workshop was created to build a community of researchers whose primary focus was experimentation security," said Miles McQueen, a computer security researcher at INL and the workshop chair. "It was a very successful, first workshop. So much so, that it will be an annual workshop held in conjunction with ISRCS."

INL is a leader in resilient controls research, and sponsors the symposium to support a multidisciplinary approach to the complex nature of control system interdependences that ensure a safe and secure operation of critical infrastructure activities.







INL Human Systems Simulation Laboratory

INL has built a virtual test bed that can be configured to simulate various control room layouts and is compatible with all major reactor designs and software platforms in use at nuclear power plants today. Known as the Human Systems Simulation Laboratory, this innovative facility is the only government-sponsored one of its kind in the United States.

Key components include:

- Operator consoles that can accommodate up to sixteen 30-inch monitors.
- A four-walled computer-assisted virtual environment (CAVE) capable of projecting 3D images that provide an immersive user experience as well as a large overview display.
- An experimenter's workstation which records audio, video and physiological responses including heart rate, breathing and skin conductivity. The data can be synchronized to operational simulations so researchers can identify stress, fatigue and other precursors to operator errors.
- Eye-tracking systems that collect data about an operator's mental and physiological responses to visual stimuli on an operator display.

Human factors researchers work with scientists and operators at the lab and industry to implement design and technological changes that improve efficiency and reduce the risk of human-induced errors. Their approach is to adapt technology to humans, not mold humans to technology.

Focus areas include:

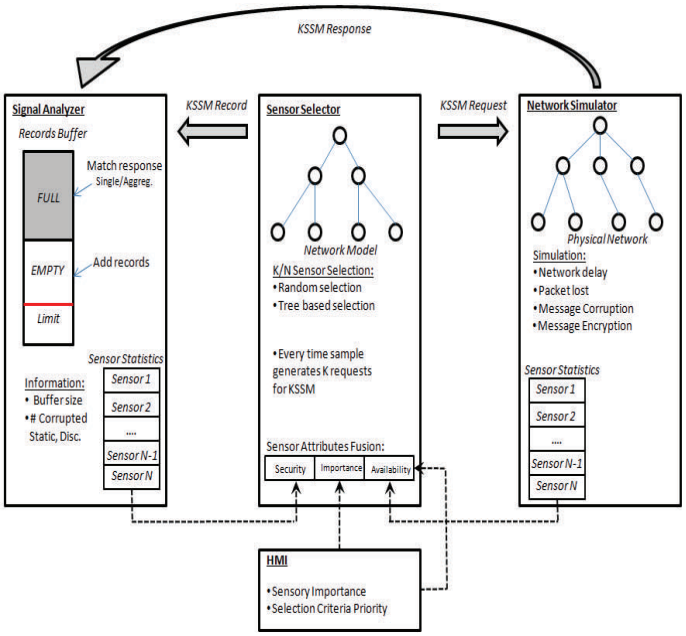
- Studying, designing and testing control room and simulator upgrades at INL's Advanced Test Reactor.
- Studying human performance in various simulations in order to develop guidance and metrics for human performance and human-system interaction for different operating conditions.
- Validating new concepts in control room protocols, staffing, and management through technologies that provide mobile and remote information access and control capabilities.
- Facilitating the design of alarm systems that combine elements of analog annunciator tiles with digital alarm lists.
- Studying and defining conditions that can be modified to improve the overall safety and efficiency of outage control centers at nuclear facilities, such as the format and accessibility of operational and maintenance information.

INL Idaho National Laboratory

ReCAS Resilient Control Architectures and Systems

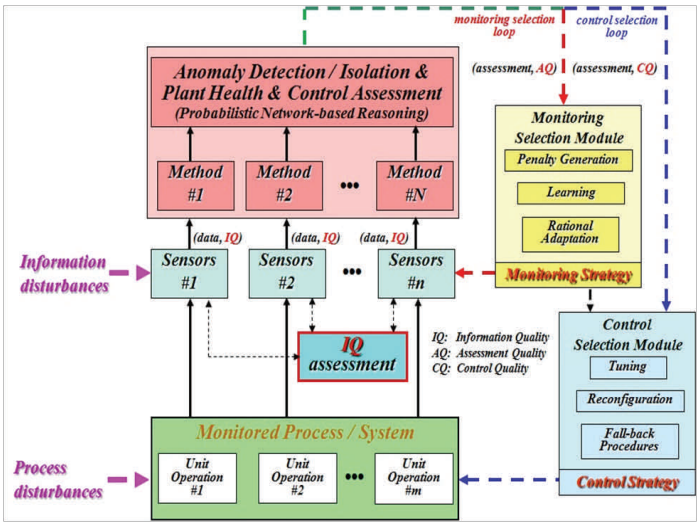
KSSM Resilient Cyber Health Mechanism

INL, in collaboration with both UC Berkeley and U of I are researching integrated mechanisms to integrate cyber security awareness within resilient control system designs. Recognition and response of the physical sensors to malicious attack is a first layer of cyber protection. The cyber health of select sensors provides a basis to normalize the data relative to malicious attack in way that is actionable for assuring continued awareness for varying generation to meet load requirements. This is in stark contrast to cyber detection mechanisms like signature or anomaly -based intrusion detection systems (IDS), which can give some indication of network and host intrusion but not to the type of data being compromised. What might be a reasonable approach for business information systems is not well suited to resilient control systems. In developing mechanisms to provide a first layer of protection from malicious intrusion, known secure sensor measurement (KSSM) algorithms, such as provided in the figure to the right, instead provide a framework for baselining performance and reconfiguring sensors. While multiple methods can be used for sensor selection, the resulting approach provides actionable information regarding cyber health of the sensor system.



Resilient Monitoring, Adaptation, & Control Systems

Being able to robustly assess and control process conditions and operations of critical infrastructures, such nuclear energy systems, oil refineries, electric grids, and computer networks, is crucial for the protection of capital, the public, and the environment. However, this goal is significantly challenging under natural and malicious perturbations. In order to provide reliable operational management under varying conditions of health and controllability, resilient monitoring and control (RMC) systems are being proposed that include varying sets of sensors and actuators. These RMC systems are envisioned to not only dynamically collect information for health assessment at varying levels of fidelity but also adaptively configure its control strategies based on assessed conditions. In addition, in view of ever increasing (physical and cyber) security threats, the sensing, exploitation, and execution of information needs to be achieved in a manner that is both spatially and temporally comprehensive and difficult to attack and defeat. RMC systems should then be rendered with three key properties, namely, resiliency, adaptation, and efficiency. In order to address these challenges, research efforts are on-going to: i) develop innovative architectures and its constituents for implementing RMC systems; ii) develop methodologies for the effective deployment of RMC systems that can accommodate natural and malicious perturbations to both the monitored process and its controllers/actuators and data generation and acquisition systems; and iii) develop RMC approaches that drives data needs and select control strategies according to time-varying requirements and assessment estimations, leading to not only the autonomous selection of monitoring and control strategies but also to a RMC system that gracefully degrades under perturbations, even under severe sensory loss and/or degradation on controllability. The proposed RMC systems are anticipated to significantly contribute to the deployment of modern systems with improved system performance, reliability, availability, and safety.



For more information

Technical Contact:

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

www.inl.gov/icis

A U.S. Department of Energy National Laboratory

Instrumentation Control & Intelligent Systems