*Resilience* is the capacity of energy and other infrastructure systems to proactively maintain a safe level of operational normalcy in response to anomalies, including threats of a malicious and unexpected nature. Threats to normal operation are those elements that *destabilize control and communications system* networks. These threats include human error and malicious human attacks, complex latencies and interdependencies. For instance, control systems need to provide greater human in the loop recognition based upon the roles and responsibilities of the individual. This ensures that the human interaction provides the required and most accurate state awareness information for the unique requirements of an individual formulating a judgment. In addition, control system performance indices are not just physics-based, but include event-based cyber security measures, as cyber exploitation can degrade systems and require some human response to mitigate. Ultimately, the control system architecture must engender a holistic design that includes all performance indices affecting the resilience of the infrastructure.

**Track Chairs**

* Craig Rieger, USA
* Ron Boring, USA
* Todd Vollmer, USA
* Tim McJunkin, USA
* Anshul Rege, USA

To advance the interdisciplinary discussion on resilience, the Idaho National Laboratory organized the IES technically co-sponsored Resilience Week over a decade ago. Since that time, a large community has developed that are focused on the challenges, solutions and policy to achieve cognitive, social and cyber physical resilience. This established community has a number of initiatives have been advanced to engender resilience in infrastructures such as the power grid, which include education.

Within this track, focused on resilient control architectures and systems, we will overview the challenges that exist, particularly with the control system environments and the energy facilities operated. The track will be concluded with a competition using the GridGame, allowing attendees to experience interdisciplinary interaction. Peer reviewed papers will accepted for presentation. In particular, we look at the aspects that holistically shape resilience in understanding the interdisciplinary nature of addressing these issues. General topics of interest for papers include:

* Control Theory: intelligent, reconfigurable, optimal
* Control Framework: supervisory, multi-agent, distributed intelligence
* Monitoring/Control Security: decoys, randomization, diversity, training and cognition, decision making, measurement
* Cyber Architecture: health indicators, defense optimization
* Data Fusion: data reduction, security characterization, data diversity, anomaly detection, response prioritization
* Computational Intelligence: machine learning, neural networks, fuzzy logic, evolutionary computation, Bayesian belief networks
* Cyber-physical power and energy systems: real-time communication, protection, control, resilience, reliability, sustainability, efficiency
* Distributed intelligence: Failure/error tolerance and recovery, adaptable/flexible architectures, multi-level/agent systems

**Program Plan**

|  |  |
| --- | --- |
| **Session** | **Plan** |
| **AM-1**  | **Keynote** |
| **AM-2** | **Panel Discussion of Research Challenges in Resilience** |
| **PM-1** | **Paper Session (Full & Extended Abstracts)** |
| **PM-2** | **Facilitated Discussion on Research Challenges** |
| **PM-3** | **Demonstration of the Grid Game** |