Resilience Week 2019

Submitted by Anonymous on Tue, 02/05/2019 - 12:54pm
Nov 04, 2019 7:00 am - Nov 07, 2019 6:00 pm CST

Resilience Week 2019

Large disasters may ripple across cities, regions or even nationally through interconnected critical infrastructure systems. Right now, many of those connections are invisible, making it very difficult to put effective mitigation strategies in place. Critical links are often uncovered too late, causing greater impacts to infrastructure and challenging recovery efforts on the ground. Join us for the Resilience Week symposium to discuss how private and public partners can work together to ensure a secure and reliable flow of energy across the nation.

TOPICAL AREAS

ELEMENTS OF RESILIENCE (accepting special session proposals and papers)
CONTROL SYSTEMS
Engineering systems are increasingly subjected to disturbances which are not generally predictable at design time. These disturbances can be man-made or naturally occurring, and they can be physical or cyber in nature. In order to ensure resilient system performance, multidisciplinary control approaches that provide intrinsic state awareness and intelligence are required. Topical areas include: Control Theory; Control Framework; Sensor Architectures, Monitoring/Control Security; Data Fusion, Data Analytics, Predictive Analytics, Prognostics, Computational Intelligence; Cyber-physical power and energy systems; Robotic systems; Cyber-physical system security, and Cybersecurity for industrial control systems.

CYBER SYSTEMS
Engineered systems in use today are highly dependent on computation and communication resources. This includes systems of all kinds, ranging from vehicles to large-scale industrial systems and national critical infrastructures. The resilience of the computational systems and infrastructures underlying these technologies is of great importance for mission continuity, security and safety. Resilience, in this context, is understood as the ability of a system to anticipate, withstand, recover, and evolve from cyberattacks and failures. In this symposium, we will focus on the topic of resilience of cyber-physical systems. Among others, the concepts of cyber awareness, anticipation, avoidance, protection, detection, and response to cyberattacks will be promoted and will help set the tone of the event. A better understanding of the science and engineering of these concepts

and its supporting technologies will help provide some of the key underlying capabilities for the design and development of resilient cyber-physical systems. Topical areas include: Cyber Architecture; Human Machine Interaction and Cyber Social understanding; Human Systems Design, Human and Systems Behavior; Education and Workforce Development; Sensor Architectures; Data Fusion; Computational Intelligence; Resilient Cyber Frameworks and Architectures, Adaptive/ Agile/ Moving Defenses, and Resilient Cyber-physical power and energy systems.

COGNITIVE SYSTEMS
Many environments critical to cyber and physical infrastructure exhibit interplays between engineering systems design and human factors engineering. The Cognitive Systems track will explore how people, individually and in teams, engage in cognitive and cooperative problem-solving in complex, time-critical, and high-consequence settings. We will emphasize technology designs, operating concepts and procedures, and cognitive science research that improve overall human-system performance and increase the resilience and robustness of complex sociotechnical systems. Joint sessions with the Control Systems and Cyber Systems Symposia will explore the functional relations of systems integrating humans, automation, and system management resources. Topical areas include: Selection, training and performance in complex sociotechnical systems; Human performance models of event response; Cognitive readiness in high-consequence environments; Macroergonomics, systems design, and safety; Human factors of security, privacy, and trust; Situation cognition in cyber, physical, and hybrid environments; Procedures, checklists, and skilled performance; Human supervisory control and complex systems performance; Distributed cognition, expertise coordination, and teamwork; Human-machine interaction with automation, computers, and robots, and Autonomous and semi-autonomous systems/technology.

COMMUNICATION SYSTEMS
Many commercial and government applications require reliable and secure communications for effective operations. These communications are often challenged in contested environments - whether from hostile states in a denial of service scenario, degraded infrastructure following a man-made or natural disaster, or !finite spectrum pressure that restrict agility. The symposium will highlight how incorporation of resiliency in communications systems can support a wide range of applications given uncertainty in the communication environment. Topical areas include: Architectures; Threats and Failures; Remediation and recovery; Characterization; Networks and Infrastructure; Military applications, Civil applications, Security, Privacy and trust in communications, Communications for cyber-physical systems (including but not limited to: power transmission and distribution, transportation, autonomous vehicles, industrial automation, building management systems, health care, agriculture, logistics, etc.), Cloud, Edge and Fog Computing.

COMPLEX ENVIRONMENTS (accepting special session proposals, papers, and white papers/lightning talks)

INFRASTRUCTURES

Creating and sustaining resilient critical infrastructure is a diverse and complex mission. Critical infrastructure systems in the United States consist of a diversity of interdependent networks, varied operating and ownership models, systems in both the physical world and cyberspace, and stakeholders from multijurisdictional levels. Methods to improve critical infrastructure resilience are advancing, but much more can be done. Large-scale disasters have revealed that decision-makers often struggle to identify or determine key components and interdependency relationships in infrastructure systems, optimal resource allocation to increase resilience or reduce risk, and optimal response plans. The Resilient Critical Infrastructure Symposium seeks to bridge the gaps among local, city and state entities, infrastructure owner-operators, federal agencies, and researchers to advance a productive discussion of tools, technologies, and policies for improving critical infrastructure resilience. Topical areas include: Modeling, analytical techniques, or decision support tools to determine vulnerabilities in critical infrastructure, assess resilience, and/or inform planning and investment, Adaptations to respond to catastrophic events; Best practices for local, state, federal infrastructure protection entities or infrastructure owner-operators; techniques to improve critical infrastructure resilience to all-hazards; case studies of infrastructure planning and disaster response; Emergency services and regional resilience; Dependency or interdependency examinations of cascading impacts of infrastructure failures; Cyber-physical interdependencies in critical infrastructure analysis; Resilience assessment methodologies and incorporation of sociotechnical approaches; Application of advanced visualization methodologies (e.g., geospatial and virtual reality) that enhance critical infrastructure analysis reports and information sharing processes.

COMMUNITIES

Communities provide the fabric that integrates the provision of our individual needs and support networks. Connections between individuals and groups serve as critical drivers for bouncing back from shocks, including damaging storms and other catastrophic events. Therefore, the role of social networks and cohesion is important in organizational and community resilience. It is also important that as we see increased magnitude and impact of events, consideration of planning and policies that reflect availability and distribution of key resources be in place that will make communities and populations more resilient to large-scale disruptions. Topical areas include: Governance and resilience policy; effectiveness of social networks in recovery; models and systematic approaches to resilience; scientifi!c approaches to resilience, and role of distributed utilities and community-based assets in recovery.

Organizing Committee

EMAIL: RESILIENCEWEEK@INL.GOV

General Chair

- Craig Rieger, Idaho National Laboratory

Organizing Chair

- Jodi Grgich, Idaho National Laboratory

Control Systems

- Frank Ferrese, Naval Sea Systems Command
- David Scheidt, Weather Gage Technologies, LLC
- Kevin Schultz, Johns Hopkins Applied Physics Laboratory

Cyber Systems

- David Manz, Pacific Northwest National Laboratory
- Nate Evans, Argonne National Laboratory
- Nicole Beebe, University of Texas, San Antonio

Communities

- Abraham Ellis, Sandia National Laboratories
- Ray Byrne, Sandia National Laboratories

Infrastructures and Communities

- Cherrie Black, Idaho National Laboratory
- John Hummel, Argonne National Laboratory

Communication Systems

- Krishna Kant, Temple University
- Gurdip Singh, Syracuse University
- Brad Nelson, Idaho National Laboratory

Cognitive Systems

- Ron Boring, Idaho National Laboratory
- Roger Lew, University of Idaho
- Nathan Lau, Virginia Tech
- Phil Bennett, Sandia National Laboratories

Refer to the Resilience Week website for the latest information and submission instructions.

Event Details

Location: San Antonio, TX
URL: https://events.inl.gov/ResWeek2019

Sync this event to your calendar

Conference RESILIENCE WEEK 2019 2019