Transforming the Resilience of Critical Infrastructure Systems and Communities

Resilience Week Objective: A Symposium dedicated to advancing the interdisciplinary dialog on policy and technologies that accelerate critical infrastructure and community resilience to unexpected and malicious threats.

RESILIENCE WEEK WILL BE VIRTUAL THIS YEAR

SUBMISSION SCHEDULE

Call for Special Sessions

- Submissions due: ~~April 22~~ CLOSED
- Acceptance notification: April 29

Call for Papers & White papers/Lightning Talks

- Submissions due: ~~June 3~~ CLOSED
- Acceptance notification: September 9
- Final submissions due: September 23

COST

- $247.50 for registration by October 1
- $297.50 after deadline has passed
- $25 discount for IEEE IES & HFES members
- $37.50 discount for IES members
- 50 percent discount for current students

CALL FOR SPECIAL SESSIONS

Within all topical areas, participants interested in exploring new interdisciplinary approaches or perspectives on resilience are encouraged to complete the special session template with title, paragraph overview, topical areas and chairs.

Sessions or full tracks may be proposed, including invited and paper presentations, panels and facilitated discussions.

CALL FOR PAPERS

Full papers: written following IEEE format and limited to seven double column pages in a font no smaller than 10 points. Note that an extra page fee of $100 for each page (up to three additional pages) will apply to any camera-ready version exceeding the page limit.

Work in progress and industry practice: written following IEEE format and limited to four double column pages, in a font no smaller than 10 points. Work-in-progress papers describe research that has not yet produced the results required for a full paper, but that due to its novelty and potential impact deserves to be shared with the community at an early stage.

Accepted papers and work-in-progress papers will be submitted to IEEE for publication in Xplore.

CALL FOR WHITE PAPERS/LIGHTNING TALKS

White papers shall follow work-in-progress guidelines but not exceed 1,000 words. We welcome research contributions dealing with methodologies and techniques to improve critical infrastructure and communication resilience to all hazards. Case studies from local, state, and federal infrastructure and community protection entities and infrastructure owner-operators are also invited and welcome. Work that has been previously published or presented elsewhere may be suitable provided that it is consistent with the objectives of the conference and these other outlets are referenced appropriately.

CHAIRS

General Chair

- Craig Rieger, Idaho National Laboratory

General Organizing Chair

- Jodi Grgich, Idaho National Laboratory

Workforce Development

- Masood Parvania, University of Utah

Control Systems

- Kevin Schultz, Johns Hopkins App. Physics Lab
- Quanyan Zhu, New York University
- Kris Villez, Oak Ridge National Laboratory

Cyber Systems

- Char Sample, Idaho National Laboratory
- David Manz, Pacific Northwest National Lab
- Nate Evans, Argonne National Laboratory

Cognitive Systems

- Katya Le Blanc, Idaho National Laboratory
- Nathan Lau, Virginia Tech
- Corey Fallon, Pacific Northwest National Laboratory

Communication Systems

- Brad Nelson, Idaho National Laboratory
- Eyuphan Bulut, Virginia Commonwealth University
- Kemal Akkaya, Florida International University

Infrastructures

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

Communities

- Abraham Ellis, Sandia National Laboratories
- Elaina Sutley, University of Kansas
- Ray Byrne, Sandia National Laboratories
- Sara Hamideh, Stony Brook University
- Emma Stewart, Lawrence Livermore National Laboratory

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: anomaly detection, adaptive, fault-tolerant, and resilient control systems; distributed and robust sensing; monitoring/control security; data analytics and machine learning for control and optimization, diagnostic and prognostic tools, computational intelligence; cyber-physical power and energy systems; robotic systems; cyber-physical system security; cybersecurity for industrial control systems; autonomous cyber defense; internet of things; intelligent transportation systems; control of critical infrastructures.

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; 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, situated 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.

Communications 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 for effective provisioning of our societal well-being during major intentional or natural stressors. In addition to infrastructure, human factors such as connections between individuals and groups serve as critical resources for bouncing back from shocks. It is important that resilience planning and policies reflect how communities value resilience, how they respond to events, how the population is disproportionately impacted, what the impact is on the local economy, including business interruption and impact on social institutions, and how availability and distribution of key resources impacts long term recovery and if used effectively, can make communities and populations more resilient to large-scale disruptions. Topical areas include: governance and resilience policy; temporary housing, impacts on affordable housing, and long term housing recovery; effects of human factors in recovery; intersection of social and physical vulnerability; business interruption and interruption of critical social services and institutions; models, metrics and systematic approaches to resilience planning; interdisciplinary approaches to resilience; capacity building and sustainability challenges; and role of distributed community-based assets (utility and customer owned, including social services and the local economy) in recovery.