Call for Submissions: Resilience Week 2019

Submitted by Anonymous on Mon, 06/03/2019 - 10:07am

CALL FOR SUBMISSIONS - EXTENDED to JULY 1

Resilience Week 2019

Call for Special Sessions

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

Call for Papers & White papers/Lightning Talks

- Submissions due: ~~June 3~~ **July 1 EXTENDED**
- Acceptance notification: September 9
- Final submissions due: September 23

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.

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.

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 react to events, and how availability and distribution of key resources will make communities and populations more resilient to large-scale disruptions. Topical areas include: Governance and resilience policy; effects of human factors in recovery; models, metrics and systematic approaches to resilience planning; scientific approaches to resilience, capacity building and sustainability challenges, and role of distributed community-based assets (utility and customer owned) in recovery.

COST

- $495 for registration by September 16
- $595 after deadline has passed
- $50 discount for IEEE IES & HFES members
- 50 percent discount for current students

VENUE/ACCOMMODATIONS

The Westin Riverwalk | 420 W Market Street, San Antonio, Texas

CHAIRS

General Chair

- Craig Rieger, Idaho National Laboratory

General Organizing Chair

- Jodi Grgich, Idaho National Laboratory

Elements of Resilience

Control Systems

- Frank Ferrese, Naval Sea Systems Command
- David Scheidt, Weather Gage Technologies
- Kevin Schultz, Johns Hopkins App. Physics Lab

Cyber Systems

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

Cognitive Systems

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

Communication Systems

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

Complex Environments

Infrastructures

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

Communities

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

? CfP:12th International Conference on Graph Transformation (ICGT 2019) Call for Position Papers: 1st International Workshop on Next-Generation Operating Systems for Cyber-Physical Systems ?

Calls for Papers
