



IEEE Critical Infrastructure Survivability Workshop (CISW) Series

CISW-SG 2010

Smart Grid Survivability Workshop

October 13-14, 2010

<http://www.cert.org/cisw/sg2010/>

"Preventing Catastrophic Impacts from Adverse Cyber-Physical Events"

Venue:

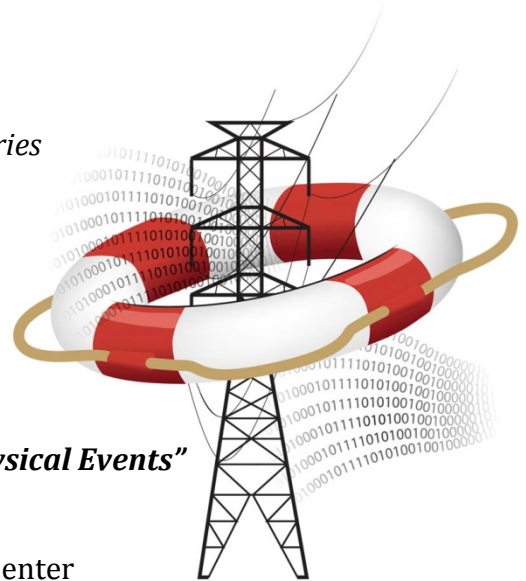
National Rural Electric Cooperative Association Conference Center

Arlington, Virginia USA

(Washington, D.C. area)

Sponsored by: IEEE Systems Council

<http://www.ieeesystemscouncil.org/>



Call for Participation

Are you interested in contributing to advancing the technology, understanding, or applicability of survivability engineering of critical infrastructures? You're invited to participate in the Smart Grid Survivability Workshop, part of the new IEEE Critical Infrastructure Survivability Workshop (CISW) Series, October 13-14, 2010 in the Washington, D.C. area.

Workshop Approach and Objective

Primed by keynotes, invited presentations, panel sessions, and group discussions, participants in this workshop will brainstorm and identify research challenges and strategic approaches in software and systems engineering that will address the ultimate survivability of the smart grid against catastrophic failures induced by malicious or accidental cyber-physical events. Participants will have the opportunity to contribute to a post-workshop report on the proposed set of research topics and strategies to be published by the IEEE Systems Council. We expect that at the end of the workshop, participants will share a better understanding of promising areas for future research and practice in building a survivable smart grid. We also anticipate that participants will have made contacts for future information exchange and possible collaborative research projects.

Registration

A registration discount for IEEE members will apply. Participation in this IEEE workshop will be open, on a space available basis.

Workshop Background

The electric power infrastructure is a primary foundation of contemporary society. Efforts to modernize our nation's electric power infrastructure through the overlay of two-way digital communications and highly automated digital control (to create a so-called "smart grid") are based on the admirable promise of greater energy efficiency, a more reliable self-healing grid, energy conservation, and significant reductions in peak energy usage (thereby reducing the need to continually increase generation capacity to meet increasing demand). Requirements for very high levels of interoperability and cyber security remain major stumbling blocks to progress. The development of interoperability and cybersecurity standards and best practices for the emerging smart grid is proceeding at a breathtaking pace. Nonetheless, despite the standards developers' best efforts, there remain gaps in the software and system engineering foundations necessary to ensure that new smart grid functionality will be secure, safe, survivable, reliable, and resilient.

Many research challenges in software and system engineering need to be addressed for the full vision of the emerging smart grid's benefits to be realized. The most fundamental of these research and engineering challenges is how to design, configure, and operate the smart grid's systems and components in a manner that prevents an adverse cyber-physical event (whether accidental or malicious in origin) from having a catastrophic impact on the grid and on society at large. For examples of the kinds of adverse events we are concerned with, see the "Coordinated Attack Risk" chapter of the recent joint report by the North American Electric Reliability Corporation (NERC) and the U.S. Department of Energy (DOE) on *High-Impact, Low-Frequency Event Risk to the North American Bulk Power System* <http://www.nerc.com/files/HILF.pdf>. Other suggested background reading material for workshop participants includes the *DOE Roadmap to Secure Control Systems in the Energy Sector* http://www.oe.energy.gov/DocumentsandMedia/Roadmap_to_Secure_Control_Systems_in_the_Energy_Sector.pdf, and the Department of Homeland Security (DHS) *Workshop on Future Directions in Cyber-Physical Systems Security* http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf.

CISW-SG Report

To be published by the IEEE approximately three months after the workshop.

Workshop Organization

General Chair/Program Co-Chair

Howard Lipson – CERT, Software Engineering Institute

Program Co-Chair

Michael Assante – NBISE (former CSO, North American Electric Reliability Corporation)

Program Co-Chair

Stacy Prowell – Oak Ridge National Laboratory

Treasurer

Bob Rassa – Raytheon Company

Questions?

For further information, see <http://www.cert.org/cisw/sg2010/>, or write to IEEE CISW-SG 2010 <ieee-cisw-sg2010@cert.org>