Resilience Week 2013

Transforming the Resilience of Cognitive, Cyber-physical Systems

August 13-15, 2013

Table of Contents

Resilience Week Sponsors and Organizers

Organizers
- Idaho National Laboratory
- Purdue University
- Temple University
- Team for Research in Ubiquitous Secure Technology, University of California Berkeley
- Florida Institute for Human & Machine Cognition

Technical Sponsors
- Institute of Electrical and Electronics Engineers, Industrial Electronics Society
- Center for Advanced Energy Studies
- Human Factors and Ergonomics Society

Platinum Sponsors
- Fujitsu

Gold Sponsors
- Enterasys Secure Networks
- Access Data
- Intelligent Decisions

Silver Sponsors
- SAS
- Trend Micro
- Symantec
- Network Instruments
- CenturyLink Governmnt

Control Systems Technical Sponsors and Organizers
- Idaho National Laboratory
- Temple University
- Industrial Electronics Society
- Institute of Electrical and Electronics Engineers
- Center for Advanced Energy Studies
- Team for Research in Ubiquitous Secure Technology, University of California Berkeley

Cognitive Systems Technical Sponsors and Organizers
- Idaho National Laboratory
- Purdue University
- Center for Advanced Energy Studies
- Human Factors and Ergonomics Society

Cyber Systems Technical Sponsors and Organizers
- Idaho National Laboratory
- Florida Institute for Human & Machine Cognition
- Industrial Electronics Society
- Center for Advanced Energy Studies
- Team for Research in Ubiquitous Secure Technology, University of California Berkeley

Communication Systems Techncial Sponsors and Organizers
- Idaho National Laboratory
- Air Force Research Institute
- Industrial Electronics Society
- Center for Advanced Energy Studies

At-a-Glance

Tuesday, August 13 - Tutorials & Workshops

7:30 a.m.	**Coffee and Registration** *(Grand Ballroom Foyer)*				
8:00 a.m.	**Opening Welcome:** Shankar Sastry, University of California, Berkeley *(Grand Ballroom)*				
8:15 a.m.	**Introductions and Logistics:** Jodi Grgich *(Grand Ballroom)*				
	CONTROL		**COGNITIVE**	**CYBER**	**COMMUNICATION**
8:30 a.m.	**Keynote:** Piero Bonissone, General Electric Global Research *(Mason I/II)*		**Keynote:** Kyle Hultgren, Center for Medication Safety Advancement *(Columbus I/II)*	**Keynote:** Vipin Swarup, MITRE *(Jackson)*	Open to attend keynotes
9:30 a.m.	**Morning Break**				
10:00 a.m.	**Control Session 1a:** *Mason I/II* Cyber Security for Industrial Control Systems Chair: Frank Ferrese, NSWC	**Control Session 1b:** *Montgomery* Chair: Frank Ferrese, NSWC	**Cognitive Session 1:** *Columbus I/II* Concepts and Processes of Resilient Cognitive Operations *(Columbus I/II)* Chair: Barrett Caldwell, Purdue University	**Cyber Session 1:** *Jackson* Cyber Resilience Theory Chair: Nick Multari, PNNL	**Communication Session 1:** *Pine* Learning from Disasters: Sandy, Communciations, and Manifold Resiliency Chair: Juan Deaton, INL
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Norman Whitaker, DARPA *(Grand Ballroom)*				
1:00 p.m.	Test-Driven Development of Physics-Based Models Chair: Frank Ferrese, NSWC	ReSia Technical Committee Chairs: Milos Manic U of Idaho Craig Rieger, INL	Teams in Resilient Performance Settings Chair: Ron Boring, INL	Cyber Resilience Applications Chair: Marco Carvalho, Florida Institute of Technology	Resilience, Survivability and Disruption Tolerance for the Future Internet and Global Information Grid Chair: Juan Deaton, INL
2:30 p.m.	**Afternoon Break**				
3:00 p.m.	Resilient Consensus Control of Dynamic Systems Chair: Frank Ferrese, NSWC	ReSia Technical Committee (Cont.) Chairs: Milos Manic, Craig Rieger	History of Resilience Metrics Discussion Chair: Barrett Caldwell, Purdue University	Cyber Resilience Metrics Chair: Sean Peiser, UC Davis	Resilience, Survivability and Disruption Tolerance for the Future Internet and Global Information Grid (Cont.) Chair: Juan Deaton, INL
4:30 p.m.	**Adjourn**				

At-a-Glance

Wednesday, August 14 - Papers & Presentations

7:30 a.m.	**Coffee and Registration** *(Grand Ballroom Foyer)*					
8:00 a.m.	**Opening Remarks and Daily Agenda:** Jodi Grgich *(Grand Ballroom)*					
	CONTROL			**COGNITIVE**	**CYBER**	**COMMUNICATION**
8:30 a.m.	**Keynote:** Massoud Amin, University of Minnesota *(Mason I/II)*			**Keynote:** Stephen Rottler, Sandia National Laboratories *(Columbus I/II)*	**Keynote:** Thomas Longstaff, National Security Agency *(Jackson)*	**Keynote:** Rangam Subramanian, Idaho National Laboratory *(Pine)*
9:30 a.m.	**Morning Break**					
10:00 a.m.	**Control Session 1a:** *Mason I/II* Complex Networked Control Systems Chair: Chika Nwankpa, Drexel University	**Control Session 1b:** *Montgomery* Sensor Design / Networks Chair: Li Bai, Temple Uniersity	**Control Session 2:** *Washington* Mixed Initiative Response Chair: Zaruhi Mnatsakanyan, Johns Hopkins University	**Cognitive Session 1:** *Columbus I/II* Path to Autonomous, Resilient Systems Chair: David Woods, The Ohio State University	**Resilient Cyber Systems:** *Jackson* Chair: Marco Carvalho, FIT	**Systems Intelligence for Resilience:** *Sansome* Chair: Dipankar Dasgupta, Memphis University	**Communication Session 1:** *Pine* Efficient Resilient Communication in Error-prone Wireless Networks Chair: Juan Deaton, INL
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Dane Egli, The Johns Hopkins University *(Grand Ballroom)* *Sponsored by* ***TRUST, UC Berkeley***						
1:00 p.m.	Complex Networked Control Systems Chair: Chika Nwankpa, Drexel University	Data Fusion Chair: Jeff Bradshaw, Florida Institute for Human & Machine Cognition	Complex Networked Control Systems Chair: Frank Ferrese, NSWC	Path to Autonomous, Resilient Systems Chair: David Woods, The Ohio State University	Resilient Cyber Systems Chair: Marco Carvalho, FIT	Cyber Resilience Theory Chair: Nick Multari, PNNL	Communication Session 2 Chair: Juan Deaton, INL
2:30 p.m.	**Afternoon Break**						
3:00 p.m.	**Poster Session**				Resilient Cyber Systems Chair: Marco Carvalho, FIT	Cyber Resilience Theory Chair: Nick Multari, PNNL	
4:30 p.m.	**Adjourn**						
6:00 p.m.	**Hoster Dinner with Plenary Speaker** Declan Ganley, Rivada Networks *(The Dining Room)*						

Thursday, August 15 - Panel Discussions

7:30 a.m. **Coffee and Registration** *(Grand Ballroom Foyer)*

8:00 a.m. **Opening Remarks and Daily Agenda:** Jodi Grgich *(Grand Ballroom)*

8:30 a.m.

CONTROL	COGNITIVE	CYBER	COMMUNICATION
Keynote: David Scheidt, Johns Hopkins University APL *(Mason I/II)*	Open to attend keynotes	**Keynote:** Doug Tygar, UC Berkeley *(Grand Ballroom)*	Open to attend keynotes

9:30 a.m. **Morning Break**

10:00 a.m. **Panel Discussion** - open to all attendees *(Grand Ballroom)*

Moderator: Juan Deaton (Idaho National Laboratory)
Declan Ganley (Rivada Networks), Dave Hutchison (Lancaster University), David Woods (Ohio State University), Li Bai (Temple University), Marco Carvalho (Florida Institute of Technology)

11:30 a.m. **Concluding Remarks:** Craig Rieger, Idaho National Laboratory

11:40 a.m. **Adjourn**

1:30 p.m. **Tour -** UC Berkeley *(Optional)*

3:30 p.m. **End of Tour**

Resilience Week Plenary Speakers

Beyond the Storms--Operationalizing Critical Infrastructure Resilience

Dr. Dane S. Egli, Johns Hopkins University

Bio

Dr. Dane Egli is a national security senior advisor at Johns Hopkins University and career Coast Guard officer who served on the White House National Security Council staff from 2004-06 as a director for counterterrorism, and as the President's advisor on hostages and global counternarcotics. He holds master's degrees from George Washington University and National Defense University in National Security Studies, and a doctoral degree from University of Colorado in public policy. He served as the senior maritime advisor to the COCOM Commander at NORAD/USNORTHCOM from 2006-08 and speaks nationally on maritime security, national preparedness, and critical infrastructure resilience issues. He is the author of the strategic report, "Beyond the Storms: Strengthening Security & Resilience in the 21st Century."

Abstract

Less than one year ago, Hurricane Sandy caused $19 billion in damages to New York City alone, reminding us that disasters are inevitable and the subsequent costs will dwarf our available resources. So what are the lessons we can learn and where can we find refuge? In response to these vexing questions this presentation offers an adaptive framework for action to operationalize resilience in the face of unprecedented complexity and uncertainty.

Perfect prevention and security are unrealistic, but by facing the inevitability of coming storms, pandemics, and man-made disasters, we can mitigate the impact of these destructive forces. Multiple converging trends suggest the nation is at a strategic inflection point that requires America to rethink our current approach to preparedness. The consequential impacts of globalization, eroding infrastructures, climate change, and persistent threats of terrorism require innovative solutions to address these historic challenges. And the need for visionary and empowered leadership across the public and private sectors has never been greater.

Preparing America for the demands of the 21st century will require systematically integrating resilience into our systems, education, and culture as an active virtue--and it starts by looking Beyond the Storms of current disasters events and tactical responses to make investments in long-term hazard mitigation.

Delivering Innovation in Public Safety Communications

Declan Ganley, Rivada Networks

Bio

Declan Ganley, Irish Entrepreneur, Chairman & CEO Rivada Networks, a leading public safety communications business with operations in the US and Europe. Declan has built a number of businesses in the telecommunications and natural resources sector including Broadnet, which rolled out wireless networks in ten European countries. He rolled out a cable TV network, Cabletel, in Eastern Europe, and from 1991-1997 built what became the largest private forestry company in the Former Soviet Union. Declan is Founder & Chairman of The Libertas Institute, which has campaigned on European issues, starting with its successful referendum campaign against the first Libson Treaty in 2008. As a European federalist, he has campaigned for a democratic, solvent and federal European Union. He is a regular commentator/op-ed contributor on business and European affairs for international print and broadcast media.

Declan is a recipient of the Louisiana Distinguished Service Medal for what was cited as his life saving actions; leading Rivada Networks' delivery of communications capability for emergency responders post Hurricane Katrina. In 2008 he was awarded the Frode Jacobson Prize for Courage in Copenhagen and the Czech Republic's Michal Tosovsky Prize. He served for over twenty years with the 54th Field Artillery Regiment, Irish Army Reserve. Declan is co-author of 'What If Ireland Defaults' (Orpen Press 2012). He was the subject of media columnist Bruce Arnold's 2009 book 'The Fight for Democracy'. He is also the patented co-inventor of Dynamic Spectrum Arbitrage technology.

Abstract

Mr. Ganley's remarks will address the potential of a revolutionary new technology developed and pioneered by Rivada Networks. "Dynamic Spectrum Arbitrage/Tiered Priority Access" allows, for the first time, bandwidth to be allocated to users on a the basis of clear user priority, guaranteeing public safety officials access to high quality, uncongested bandwidth during a public safety emergency.

Mr. Ganley will address the challenge of providing a nationwide, dedicated public security communications network, and how such a network can fund itself, and dramatically increase competition in the commercial wireless network, through the commercial provision of excess bandwidth to commercial carriers through a dynamic auction process.

Overcoming National Security Challenges Posed by Threats to Critical Infrastructure

Dr. Norman A. Whitaker, DARPA

Bio

Dr. Norman A. Whitaker serves as Deputy Director of the Information Innovation Office at DARPA. DARPA is the principal Agency within the Department of Defense for research, development, and demonstration of concepts, devices, and systems that provide highly advanced military capabilities.

Dr. Whitaker previously served as Special Assistant to the DARPA Director and was the Program Manager for the DARPA Urban Challenge autonomous vehicle program. He was also centrally involved in planning the 2005 Grand Challenge. Prior to his work at DARPA, Dr. Whitaker was CEO of the Escher Research Institute, which he co-founded in 2003, CTO of Puritan Research, and a program manager at DARPA. From 1986 to 1997 he was on the research staff at AT&T Bell Laboratories.

Dr. Whitaker received his Bachelor of Science (1979), his Master of Science (1983) and his Ph.D. (1986) in Electrical Engineering and Computer Science from Massachusetts Institute of Technology. He is a member of the Institute of Electrical and Electronics Engineers (IEEE).

Abstract

The Defense Advanced Research Projects Agency (DARPA) was established in 1958 to prevent strategic surprise from negatively impacting U.S. national security and create strategic surprise for U.S. adversaries by maintaining the technological superiority of the U.S. military. To fulfill its mission, the Agency relies on diverse performers to apply multi-disciplinary approaches to both advance knowledge through basic research and create innovative technologies that address current practical problems through applied research.

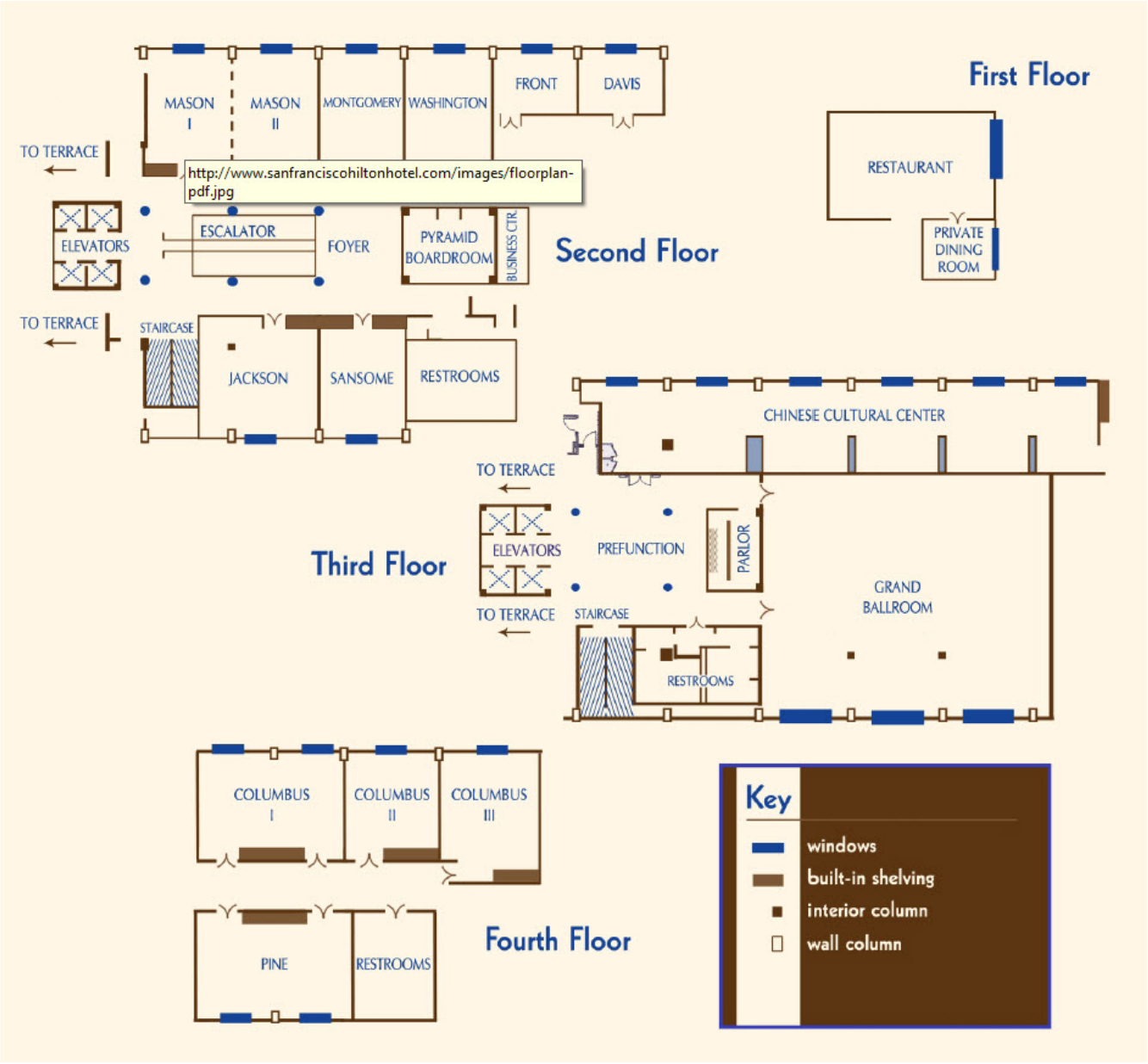
The presentation will review DARPA's research programs to address the national security challenges posed by threats to our critical infrastructure.

ReSia Technical Committee

Tuesday, August 13, 1:00 p.m.-4:30 p.m. Montgomery
Chairs: Milos Manic, Craig Rieger

The Technical Committee aims to serve as an interdisciplinary forum and source of reference for the development, implementation, assessment and dissemination of novel and effective methods to enhance, modernize and improve resilient technologies.

Venue Map



Poster Session

- Investigating the Application of Moving Target Defenses to Network Security, Scott DeLoach, Kansas State University
- Intruder detection based on graph structured hypothesis testing, Joseph Sexton, LANL
- Tele-manipulation of Robot Arm with Smartphone, Wen Yu, CINVESTAV-IPN
- Mixed/Fault Detection Filter Design based on Probabilistic Robustness, Young-Man Kim, University of Michigan- Flint
- Cloud Resiliency and Security via Diversified Replica Execution and Monitoring, Nathan Evans, Symantec
- Testing Human-Auto Cyber Team Resilience: Uncovering latent failures with a novel, decision-centered approach, Jay Peffer, Resilient Cognitive Solutions
- Adaptive Strategies for Evolutionary Algorithm Monitoring, Hector Lugo-Cordero, University of Central Florida
- The Case for Distributed Data Archival Using Secret Splitting with Percival, Thomas Kroeger, Sandia National Laboratory
- LINEBACkER: bio-inspired data reduction toward real time network traffic anomaly detection Jeremy Teuton, Pacific Northwest National Laboratory

Panel Discussion

Thursday, August 15, 10:00 a.m.-11:30 a.m.
Grand Ballroom

Moderator: Juan Deaton, Idaho National Laboratory

Panel: Declan Ganley (Rivada Networks), Dave Hutchison (Lancaster University), David Woods (Ohio State University), Li Bai (Temple University), Marco Carvalho (Florida Institute of Technology)

Like the blind men and the elephant, inter-disciplinary views to quantify, qualify, and describe resilience exist. In this session, panelists will explore and describe their own perspectives of resilience. Specifically, how do they model and measure resilience within their own domain of expertise. With respect to critical infrastructure, networks, organizations, and security protocols, panelists will describe aspects of resilience. This inter-active discussion seeks to contrast and compare modeling and the qualitative and quantitative techniques for describing resilience between domains.

Tours

Visitors to the Electrical Engineering and Computer Science Department at UC Berkeley may have the opportunity to:

- see graduate students demonstrate research being conducted in the Robotics Lab, the central location for robotics and intelligent machines at UC Berkeley;
- suit up to get a view of the Nanofabrication Laboratory, a shared research center that provides more than 100 Principal Investigators and over 500 academic and industrial researchers a complete set of micro- and nano-fabrication tools;
- learn about achievements at the Parallel Computing Lab, a multidisciplinary research project exploring the future of parallel processing;
- speak to representatives from the Berkeley Sensor and Actuator Center, which is devoted to interdisciplinary engineering research on micro- and nano-scale sensor that take advantage of progress made in integrated-circuit technology.

Tours are dependent on availability and it is possible that not all of the centers will be open for visitors.

CONTROL

Overview

The major purpose of this symposium is to extend and endorse particular concepts that will generate novel research and codify resilience in next generation control system designs.

Energy security and sustainability are important concerns to individuals and industry alike, but even with the promise of a smart grid, increasing research will be necessary to ensure that what is achieved is more resilient in nature. As mobile and industrial robotics form an ever increasing role in both national defense and plant automation, the dependence on these systems elevates a need to ensure continued operability in spite of hazardous environments. Through appropriate sessions and presentations, the symposium will highlight resilience in light of the power system and robotics, bringing to light resilience perspectives important to these applications.

Symposia: Control

Control Systems At-A-Glance

Tuesday, August 13 - Tutorials & Workshops

8:30 a.m.	**Keynote:** Piero Bonissone, General Electric Global Research *(Mason I/II)*	
9:30 a.m.	**Morning Break**	
10:00 a.m.	**Control Session 1a:** *Mason I/II* Chair: Frank Ferrese, US Navy NAVSEA	**Control Session 1b:** *Montgomery*
	Cyber Security for Industrial Control Systems - Wayne Cantrell, Siemens Corporation	Open
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Norman Whitaker, DARPA *(Grand Ballroom)*	
1:00 p.m.	Test-driven Development of Physics-based Models - Damian Rouson, Sourcery, Inc.	ReSia Technical Committee Chairs: Milos Manic, U of I and Craig Rieger, INL
2:30 p.m.	**Afternoon Break**	
3:00 p.m.	Resilient Consensus Control of Dynamic Systems - Saroj Biswas, Temple University	ReSia cont.
4:30 p.m.	**Adjourn**	

Wednesday, August 14 - Papers & Presentations

8:30 a.m.	**Keynote:** Massoud Amin, University of Minnesota *(Mason I/II)*		
9:30 a.m.	**Morning Break**		
	Complex Networked Control Systems: *Mason I/II* Chair: Chika Nwankpa, Drexel University	**Sensor Design / Networks:** *Montgomery* Chair: Li Bai, Temple University	**Mixed Initiative Response:** *Washington* Chair: Zaruhi Mnatsakanyan, Johns Hopkins University
10:00 a.m.	Infrastructure Resilience Using Cyber-Physical Game Theoretic Approach - Nageswara Rao, ORNL	Resilient Monitoring System for Boiler/Turbine Plant - Seymon Meerkov, University of Michigan	Non-Destructive State Machine Reverse Engineering - Jessica Smith, PNNL
10:30 a.m.	A Mathematical Framework for the Analysis of Cyber-Resilient Control Systems - Alexander Melin, ORNL		A Micro-Grid Simulator Tool (SGridSim) using Effective Node-to-Node Complex Impedance (EN2NCI) Models - Udhay Ravishankar, U of I

11:00 a.m.	Multi-Objective Consensus of Interconnected System of Multi-Agent Systems - Saroj Biswas, Temple University	Inclusion of Game-Theoretic Formulations for Resilient Condition Assessment Monitoring - Humberto Garcia, INL	
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Dane Egli, The Johns Hopkins University *(Grand Ballroom) Sponsored by* ***TRUST, UC Berkeley***		
	Complex Networked Control Systems Chair: Chika Nwankpa, Drexel University	Data Fusion Chair: Jeff Bradshaw, Florida Institute for Human & Machine Cognition	Complex Networked Control Systems Chair: Frank Ferrese, NSWC
1:00 p.m.	On Analysis and Design of Stealth-Resiliant Control Systems - Shaunak Bopardikar, UTRC	Computational Intelligence Based Data Fusion Algorithm for Dynamic sEMG and Skeletal Muscle Force Modelling - Chandrasekhar Potluri, ISU	Resilient Control of Cyber-Physical Systems against Denial-of-Service Attacks - Yuan Yuan, Tsinghua University
1:30 p.m.	Distributed Fuzzy Logic Price Negotiation in Market Based Mutli-agent Control - Li Bai, Temple University	Fuzzy Linguistic Knowledge Based Behavior Extraction for Building Energy Management Systems - Dumidu Wijayasekara, U of I	Variations of Converter's Control Parameters and its Effects on DC Multi-Converter Power Systems - Chika Nwankpa, Drexel
2:00 p.m.	A Hierarchical Multi-Agent Dynamical System Architecture for Resilient Control Systems - Quanyan Zhu, U. Illinois, UC		
2:30 p.m.	**Afternoon Break**		
3:00 p.m.	**Poster Session**		
4:30 p.m.	**Adjourn**		
6:00 p.m.	**Hoster Dinner with Plenary Speaker:** Declan Ganley, Rivada Networks *(The Dining Room)*		

Thursday, August 15 - Panel Discussions

8:30 a.m.	**Keynote:** David Scheidt, Johns Hopkins University APL *(Mason I/II)*
10:00 a.m.	**Panel Discussion** - open to all attendees *(Grand Ballroom)*
1:30 p.m.	**Tour -** UC Berkeley *(Optional)*

Control Systems Tracks

Complex Networked Control Systems

As control systems become more decentralized, the ability to characterize interactions, performance and security becomes more critical to ensuring resilience. While more decentralization can provide additional reliability due to implicit redundancy and diversity, it may also provide more avenues or vectors to cyber attack. Therefore, the design of complex networks needs to consider all factors that influence resilience, and optimize for multiple considerations.

Global stability is often perceived as something that can be achieved by local minimization of all process unit operations, many of which are contained in a facility. However, there is no assurance that global stability can be achieved in this manner, and in addition, this philosophy maintains a reactionary control paradigm by its nature. However, considering the latencies in digital control systems, there is a tendency as well as a desire to provide faster responses when the feedback and response occur close to the point of interaction with the application. Therefore, it is suggested that a true global optimization coupled with a local interaction can achieve both the assurance of a global minima, and an acceptable response when designing control system architecture.

Data Fusion

The nature of the various data types associated with proper operation or performance of critical infrastructure, including cyber and physical security, process efficiency and stability, and process compliancy is diverse. How these data are consumed to generate information will help determine whether appropriate judgments are made, whether by automated and/or human mechanisms. There are several issues that are addressed by data fusion, including the following ones:

Reduction - The reduction of data to provide only that information necessary for the human or automation scheme to provide the appropriate response, i.e., to prevent a common issue of information overload.

Identification - Validation and invalidation of causes for events, e.g., a process upset is due to a failed valve and not a cyber attack.

Improved characterization and knowledge - Development of new information that helps to better characterize the process application, e.g., mining of process temperatures along with process flows provides a better interpretation of stability.

While many of the techniques required to perform data fusion are well known, application to the diverse types of data represented within the measures of performance provide a distinct challenge. This is nowhere more evident than the fusion of cyber and process data to not only indicate whether an event is cyber specific, whether due to an adversary or network problem, or actually represents a process upset. The effort to address this situation could be split into two parts: i) developing the appropriate data to characterize the cyber threat, and ii) combining the spatial and temporal aspects of both process and cyber data to confirm the cause of the process upset.

Sensor Design/Networks

Sensor systems are a critical element in the implementation of both control systems and human / machine interfaces. One of the biggest challenges in the control of large scale systems is maintaining situational awareness for both the operator and the autonomy. Issues such as sensor failure, noise, and cyber spoofing of sensor systems blur the understanding of system state thereby impacting the efficacy of control decisions.

Resilient control design is dependent upon the ability to deploy sensor systems that provide the right information at the right time. Intelligent sensor systems should be able to fuse data into information, provide context for the data they are reporting, detect when individual sensors may be compromised, and perform self calibration. They should provide information that is in the appropriate format for the user to whom it is being provided, whether that is the control system, the operator, or another party who is a stakeholer in the operation of the system. Methods of designing intelligent sensor systems, ensuring the reliability of sensor data, fusing sensor data, and providing intelligence at the sensor level are of interest.

Mixed Initiative Response

In defining the automation of process control operations, it is necessary to understand the impact of the human input. Depending on how human input is interleaved, the human operator can provide tremendous benefit or become the greatest threat to operability. While it is understood that the human is always going to play a "supervisory" role in the

interaction with the control system and process application, there is a need to determine not only what level of interaction is needed to complement automation, but the far more interesting question of how these levels of human and machine initiative can adapt dynamically based on changing needs and limitations. The proposed project will develop a mixed initiative control framework for sharing control between the human and the autonomous portions of the control system architecture.

Many previous attempts to build and use autonomous systems have failed to acknowledge the inevitable boundaries to what intelligent systems can perceive, understand, and decide apart from human input. The framework developed by the grand challenge will build upon the strengths of the intelligent system and the human working as a cohesive team. The intelligent system will support a spectrum of control from the human operator(s). Rather than conceive of the system as a passive tools or as a totally autonomous entity, it is more effective to consider the machine as part of a dynamic human-machine team. The result will be a control system that allows the user to configure autonomy on the fly, activating "channels of initiative" that crosscut broad categories.

Symposia Keynotes

Critical Infrastructure Security and Protection: R&D Challenges in Infrastructure Security and Defense

Dr. S. Massoud Amin, University of Minnesota

Bio

Dr. S. Massoud Amin is the Honeywell/H.W. Sweatt Chair in Technological Leadership, a University Distinguished Teaching Professor, a full professor of electrical and computer engineering, and directs the Technological Leadership Institute (TLI) at the University of Minnesota.

His research focuses on two areas: 1) Global transition dynamics to enhance the resilience, security, and efficiency of systems of critical national infrastructures, and 2) Technology scanning, mapping, and valuation to identify new technology-based opportunities that meet the needs and aspirations of today's consumers and companies.

Dr. Amin pioneered RD&D in smart grids and self-healing infrastructures in 1998 and has led the development of over 24 technologies transferred to industry.

Abstract

The existing power-delivery system is vulnerable to natural disasters and intentional attacks. Regarding the latter, a successful terrorist attempt to disrupt the power-delivery system could have adverse effects on national security, the economy, and the lives of every citizen. Secure and reliable operation of the system is fundamental to national and international economy, security, and quality of life. Their very interconnectedness makes them more vulnerable to global disruption, initiated locally by material failure, natural calamities, intentional attack, or human error.

From a strategic R&D viewpoint, a major challenge is posed by the lack of a unified mathematical framework with robust tools for modeling, simulation, control and optimization of time-critical operations in smart electric power grids (spanning from fuel source to end-use) as complex multi-component and multi-scaled networks. How can systems be developed or even retrofitted that can sense, identify and build realistic models and anticipate impending failures? Will they be able to adapt, control and mitigate disturbances to achieve their goals?

In this keynote address, an intelligent distributed secure control architecture is presented for distribution systems to provide greater adaptive protection, with the ability to proactively reconfigure, and rapidly respond to disturbances. Applying this comprehensive systems approach, performance results for several end-to-end systems as well as distribution system test cases utilizing several control architectures are simulated, validated and analyzed. The models integrate aspects of cyber-physical security, dynamic price and demand response, sensing, communications, and dynamic optimization and reconfiguration. The results show the trade-offs between system reliability, availability, operational

constraints, and costs involved. This work represents a novel strategy toward developing an analytical and multi-domain methodology to assess the effects of smart grid technologies on distribution system operations and performance.

From a broader viewpoint, agility and robustness/ survivability of smart grids as large-scale dynamic networks that face new and unanticipated operating conditions is presented.

Computational Intelligence

Applications to Prognostics and Health Management (PHM) - How the Industrial Internet has Transformed My Job

Dr. Piero P. Bonissone, General Electric Global Research

Bio

A Chief Scientist at GE Global Research, Dr. Piero Bonissone has been a pioneer in the fields of fuzzy logic, AI, soft computing, and approximate reasoning systems applications since 1979. His current interests are the development of multi-criteria decision-making systems for prognostics and health management (PHM) and the automation of predictive model ensembles, via dynamic fusion.

Piero received the PhD in EECS from UC Berkeley in 1979. He is a Fellow of the IEEE, AAAI, and IFSA. He is also a Coolidge Fellow at GE Global Research for lifetime achievements. He is the recipient of the 2012 Fuzzy Systems Pioneer Award from IEEE CIS. In 2010, he became President of the Scientific Committee of the European Centre of Soft Computing. In 2008, he received the II Cajastur International Prize for Soft Computing from the European Centre of Soft Computing. In 2005, he received the Meritorious Service Award from the IEEE CIS. He served as Editor in Chief of the International Journal of Approximate Reasoning for 13 years. He is in the editorial board of five technical journals and is Editor-at-Large of the IEEE Computational Intelligence Magazine. He has co-edited six books and has over 150 publications in refereed journals, book chapters, and conference proceedings, with an H-Index of 30 (by Google Scholar). He received 65 patents issued from the US Patent Office (plus 15 pending patents). From 1982 until 2005 he was an Adjunct Professor at Rensselaer Polytechnic Institute, in Troy NY, where he supervised 5 PhD theses and 33 Master theses. He co-chaired 12 scientific conferences (nine of which sponsored by CIS) focused on Multi-Criteria Decision-Making, Fuzzy sets, Diagnostics, Prognostics, and Uncertainty Management in AI. Dr. Bonissone is very active in the IEEE, where he served as a member of the Fellow Evaluation Committee from 2007 to 2009. In 2002, while President of the IEEE Neural Networks Society (now CIS), he was also a member of the IEEE Technical Activities Board (TAB). He has been an IEEE CIS Distinguished Lecturer from 2004 to 2011.

Abstract

We describe the process of building Computational Intelligence (CI) models for Prognostics and Health Management (PHM) of industrial assets. We use offline metaheuristics to design the models' run-time architectures and online metaheuristics to control/ aggregate the object-level models (base models) in these architectures. CI techniques complement more traditional statistical and Machine Learning techniques. In the first part of our talk, we describe two PHM case studies. In the first one, we address anomaly detection for aircraft engines. Anomaly detection typically uses unsupervised learning techniques to define normal structures and regions, and identify departures from such regions. In our hybrid approach we use a fuzzy supervisory system and an ensemble of locally trained auto associative neural networks (AANN's). In the second case, we rank locomotives in a fleet according to their expected remaining useful life, using similarity-based models trained by evolutionary algorithms.

In the second part of our talk, we explore current trends in which the critical issues are model ensemble selection and fusion, rather than model generation. We also emphasize the need for injecting diversity during the model generation phase. We present a model-agnostic fusion mechanism, which can be used with commoditized models obtained from crowdsourcing, cloud-based evolution, in-house development and other sources. We show the test results of this type

of fusion in a regression problem for power plant management using two different sources of models: bootstrapped neural networks, and cloud-evolved, Genetic Programming symbolic regression models.

Finally, we explore research trends, future challenges, and opportunities for CI techniques in the emerging context of big data, cloud computing, and Industrial Internet.

Reasoning with Cyber-Physical Systems

David H. Scheidt, Johns Hopkins University's Applied Physics Laboratory

Bio

David Scheidt David H. Scheidt is Principal Professional Staff at Johns Hopkins University's Applied Physics Laboratory where for the last 15 years he has been conducting research on distributed intelligent control systems, autonomous unmanned vehicles and command and control. After receiving a B.S. in Computer Engineering from Case Western Reserve University, Mr. Scheidt spent 14 years in industry researching and developing development of information management and process control systems including: hydro-electric power-distribution control, locomotive control, railroad dispatching and mass transit dispatching systems. Mr. Scheidt also led the early development of several wide-area records management systems, including leading the development of immunization records tracking systems for five U.S. states and the second multi-level secure information system to achieve operational status. Throughout his career Mr. Scheidt has conducted research in concert with his development efforts, publishing over 50 peer reviewed publications for research funded by the National Computer Security Center (NCSC), ONR, NASA, DISA, OSD NII and the US Army. Mr. Scheidt's current research interests are autonomous systems and intelligent controls and intelligent cyber-physical systems including ship auxiliary systems, spacecraft and unmanned vehicles. Mr. Scheidt is an awardee of the National Performance Review's Hammer Award (twice) and the Hart Prize for outstanding research (twice).

Abstract

To be resilient, a system must be capable of satisfying performance goals in the presence of unanticipated faults. Fault tolerance requires a resilient design, and an ability to rapidly diagnose and reconfigure during damage events. Modern distribution systems are dependent on control infrastructures that include: sensors, processors, software and networks. Unfortunately, components within the control system can also fail, often with devastating effects. In addition, since the control infrastructure is itself the mechanism that provides information used for state estimation understanding the root cause of complex cyber-physical failures is problematic. This talk discusses the issues associated with developing automated fault tolerant control systems that manage failures within the physical plant and the control infrastructure. Specific subtopics that are discussed include: cyber-physical modeling, cyber-physical reasoning strategies, system complexity and its relationship to control strategies, automation vs. supervisory control trade-offs.

Tutorial and Paper Sessions

Tutorial Description

Tuesday, August 13, 10:00 a.m.-4:30 p.m. Mason I/II

This series of talks provides insight into several topics relevant to the design and development of resilient control systems. It is our privilege to have leading experts on hand to present their work. While the topics originate from a diverse set of fields, so do the issues one faces when attempting to build resilience into a control system. It is in the this spirit that these topics have been selected. Our first speaker, Dr. Damian Rouson, will discuss issues relating to modeling of dynamic systems in software. The modeling process is central to any control design. When models are relied upon to measure system resilience our understanding of the details of the model become even more important. Our second speaker, Mr. Wayne Cantrell, will address the issues of cyber security in industrial control systems. The ability to secure our control systems from cyber attack is central to the topic of resilient control. Finally, Dr. Saroj

Biswas will present his work on the design of resilient coordinated control. His work is based upon the theme of connected stability for resilient coordinated systems.

Track 1: Complex Networked Control Systems

Wednesday, August 14 10:00 a.m.-2:30 p.m. Mason I/II
Chair: Chika Nwankpa, Drexel University

Infrastructure Resilience Using Cyber-Physical Game-Theoretic Approach
Nageswara S. V. Rao *(Oak Ridge National Laboratory), Steve W. Poole, Chris Y. T. May, Fei Hez, Jun Zhuangz, and David K. Y. Yaux*

We consider a class of infrastructures supported by cyber and physical components, which are subject to disruptions. We study reinforcement strategies for cyber and physical components to achieve resilience, specified by the probability of infrastructure survival, against disruptions using a game-theoretic formulation. The game utility function is a sum of the infrastructure survival probability term and a cost term. We account for cyber-physical interactions at two different levels: (i) the conditional survival probability of cyber sub-infrastructure is specified by a linear function of the marginal probability, and (ii) the survival probabilities of components are determined by the numbers of cyber and physical component attacks as well as reinforcements. At Nash Equilibrium, we identify 12 performance regions based on cyber-physical correlations and component costs, where each is determined by a lower survival probability of either cyber or physical sub-infrastructure. We also derive sensitivity functions that highlight the dependence of infrastructure survival probability on cost parameters and component probabilities as well as cyber-physical correlations, under statistical independence conditions. We apply this approach to models of the energy grid derived at different levels of abstraction.

A Mathematical Framework for the Analysis of Cyber-Resilient Control Systems
Alexander M. Melin *(Oak Ridge National Laboratory), Erik M. Ferragut, Jason A. Laska, David L. Fugate, and Roger Kisner*

The increasingly recognized vulnerability of industrial control systems to cyber-attacks has inspired a considerable amount of research into techniques for cyber-resilient control systems. The majority of this effort involves the application of well-known information security techniques to protect system networks. These techniques are primarily concerned with the prevention of unauthorized access and the protection of data integrity. While these efforts are important to protect the control systems that operate critical infrastructure, they are never perfectly effective thus motivating a need to develop control systems that will operate successfully during a cyber attack. Little research has focused on the design of control systems with closed-loop dynamics that are resilient to cyber-attack. An understanding of the types of modifications to the system and signals that could be employed by an attacker after they have gained access to the control system and the effects of these attacks on the behavior of the control systems can guide efforts to develop attack detection and mitigation strategies. To formulate this problem, consistent mathematical definitions of concepts within resilient control need to be established to enable a mathematical analysis of the vulnerabilities and resiliencies of a particular control system design methodology and architecture.

In this paper, we propose rigorous definitions for state awareness, operational normalcy, and resiliency as they relate to real-time control systems. We will also discuss some mathematical consequences that arise from the proposed definitions. The goal is to begin to develop a mathematical framework and testable conditions for resiliency that can be used to build a sound theoretical foundation for resilient control research.

Multi-Objective Consensus of Interconnected System of Multi-Agent Systems
Saroj Biswas *(Temple University), Li Bai, and Qing Dong*

This paper presents consensus control of a system of multi-agent systems represented as an interconnection of platoons. The agents in each platoon are interconnected through their own communication network while only the platoon leaders are connected to global system level leader network. It is assumed that all agents are identical and are linear time invariant. For consensus control, we assume a two stage protocol: an intra-platoon protocol for platoon consensus, and an inter-platoon protocol for global system-wide consensus. The intra-platoon control is based on output information received from agents within the platoon

while the inter-platoon control uses only output information of platoon leaders. We show that the system of multi-agent systems arrives at a collective consensus in the sense that each platoon arrives its own platoon consensus and at the same time all platoons collectively achieve global system-wide consensus. Simulation results are presented to illustrate the methodology.

On Analysis And Design Of Stealth-Resilient Control Systems

Shaunak D. Bopardikar *(United Technologies Research Center) and Alberto Speranzon*

The interest in cyber-physical system security has been growing exponentially in the last five years as the research community has realized that control loops embedded in complex systems can be compromised once attackers are capable to breach the cyber intrusion protection and detection systems. In this paper, we consider the class of attacks known as stealth attacks where the attacker can compromise information flow between all remotely located components of a closed-loop control system. We develop design strategies that can prevent or make stealth attacks difficult to be carried out. Our methods enhance a legacy system, so that stealth attacks can be detected and counteracted at the cost of an increased system complexity.

Distributed Fuzzy Logic Price Negotiation in Market Based Multi-Agent Control

Brian Thibodeau, Qiangguo Ren, **Li Bai** *(Temple University), Saroj Biswas , Frank Ferrese, and Qing Dong*

Market-based models in Multi-Agent systems that use fuzzy logic are not new ideas, but most solutions focus on learning and optimization without regards to the resilience of the system. In this paper we present two agent fuzzy inference systems that enable producer and consumer agents in the market to negotiate on the price of the desired resource until a unique allocation is achieved. By constraining consumers to a budget and providing redundant producers capable of meeting market demand under stress conditions, fuzzy price negotiation allows consumer agents to reason alternative solutions should a producing agent fail in the market.

A Hierarchical Multi-Agent Dynamical System Architecture for Resilient Control Systems

Craig Rieger and **Quanyan Zhu** *(University of Illinois at Urbana-Champaign)*

Resilient control systems refers to the ones that maintain state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. In this paper, we propose a notional research philosophy and resulting framework based on a three-layer architecture of hierarchical multi-agent dynamic systems (HMADS). While a number of different alternatives have been proposed for distributed control system design, few provide the level of integration necessary to support claims of superior performance over traditional designs. We discuss multiple notional attributes associated with HMADS, namely, their functionalities, hardware independence and intelligence. We provide a framework for design of HMADS, and use power systems as a notional example as an illustration of the HMADS design philosophy.

Track 2: Sensor Design/Networks

Wednesday August 14, 10:00 a.m.-11:30 a.m. Montgomery
Chair: Li Bai, Temple University

Resilient Monitoring System for Boiler/Turbine Plant

Humberto E. Garcia, Wen-Chiao Lin, **Semyon M. Meerkov** *(University of Michigan), and Maruthi T. Ravichandran*

The previous work (references [1], [2]) developed methods for design of resilient plant monitoring systems. In the current paper these methods are applied to a specific plant – a simplified model of boiler/turbine (B/T) system. The main difference of the system considered here is that, unlike the previous work, process variables that describe the B/T plant are not independent, which leads to a possibility of inferring the state of one variable using measurements of the other. The resulting monitoring system is evaluated using simulations and shown to be effective in all attack scenarios considered.

Inclusion of Game-Theoretic Formulations for Resilient

Condition Assessment Monitoring
Wen-Chiao Lin and **Humberto E. Garcia**
(Idaho National Laboratory)

Monitoring systems collect information from sensors distributed around a monitored plant to assess its health condition. These sensors are prone to be compromised by an attacker. Consequently, two clearly distinct agents exist, namely, a monitoring system and an attacker, both having opposite objectives regarding the accuracy of plant condition assessments. Under this context, a game between these two players arises. This paper considers the inclusion of game-theoretic formulations into resilient condition assessment monitoring (ReCAM) systems. In particular, proposed game calculations periodically identify best sensor networks to be used by the ReCAM system for sensor adaptation based on estimated attacks that an attacker may use. The resulting ReCAM system is then applied to a simplified power plant model and its performance is evaluated via simulations.

Track 3: Data Fusion

Wednesday, August 14, 1:00 p.m.-2:30 p.m. Montgomery
Chair: Jeff Bradshaw, Florida Institute for Human & Machine Cognition

Computational Intelligence Based Data Fusion Algorithm for Dynamic sEMG and Skeletal Muscle Force Modelling
Chandrasekhar Potluri *(Idaho State University), Madhavi Anugolu, Marco P. Schoen, D. Subbaram Naidu, Alex Urfer, and Craig Rieger*

In this work, an array of three surface Electrography (sEMG) sensors are used to acquired muscle extension and contraction signals for 18 healthy test subjects. The skeletal muscle force is estimated using the acquired sEMG signals and a Non-linear Wiener Hammerstein model, relating the two signals in a dynamic fashion. The model is obtained from using System Identification (SI) algorithm. The obtained force models for each sensor are fused using a proposed fuzzy logic concept with the intent to improve the force estimation accuracy and resilience to sensor failure or misalignment. For the fuzzy logic inference system, the sEMG entropy, the relative error, and the correlation of the force signals are considered for defining the membership functions. The proposed fusion algorithm yields an average of 92.49% correlation between the actual force and the overall estimated force output. In addition, the proposed fusion-based approach is implemented on a test platform. Experiments indicate an improvement in finger/hand force estimation.

Fuzzy Linguistic Knowledge Based Behavior Extraction for Building Energy Management Systems
Dumidu Wijayasekara *(University of Idaho), Milos Manic, and Craig Rieger*

Significant portion of world energy production is consumed by building Heating, Ventilation and Air Conditioning (HVAC) units. Thus along with occupant comfort, energy efficiency is also an important factor in HVAC control. Modern buildings use advanced Multiple Input Multiple Output (MIMO) control schemes to realize these goals. However, since the performance of HVAC units is dependent on many criteria including uncertainties in weather, number of occupants, and thermal state, the performance of current state of the art systems are sub-optimal. Furthermore, because of the large number of sensors in buildings, and the high frequency of data collection, large amount of information is available. Therefore, important behavior of buildings that compromise energy efficiency or occupant comfort is difficult to identify. This paper presents an easy to use and understandable framework for identifying such behavior. The presented framework uses human understandable knowledge-base to extract important behavior of buildings and present it to users via a graphical user interface. The presented framework was tested on a building in the Pacific Northwest and was shown to be able to identify important behavior that relates to energy efficiency and occupant comfort.

Track 4: Mixed Initiative Response

Wednesday, August 14, 10:00 a.m.-11:30 a.m. Washington
Chair: Zaruhi Mnatsakanyan, Johns Hopkins University

Non-Destructive State Machine Reverse Engineering
Jessica Smith *(Pacific Northwest National Laboratory)*

Most of the integrated circuits (ICs) that are in electronic systems today are based on state machines. We are taking advantage of this to develop a hardware reverse engineering method that discovers the ICs underlying state machine, rather than its transistors and gates. While there are other methods for destructively reverse engineering ICs or for nondestructively characterizing

ICs, our method offers a fast and accurate analysis while remaining non-destructive. To do this, we present an intelligent brute-force method of exploring the logic of the IC using only the input and outputs designed into the IC - the I/O pins. From this exploration, we can apply a folding algorithm to discover the designed state machine.

A Micro-Grid Simulator Tool (SGridSim) using Effective Node-to-Node Complex Impedance (EN2NCI) Models
Udhay Ravishankar *(University of Idaho), Milos Manic, and Craig Rieger*

This paper presents a micro-grid simulator tool useful for implementing and testing multi-agent controllers (SGridSim). As a common engineering practice it is important to have a tool that simplifies the modeling of the salient features of a desired system. In electric micro-grids, these salient features are the voltage and power distributions within the micro-grid. Current simplified electric power grid simulator tools such as PowerWorld, PowerSim, Gridlab, etc, model only the power distribution features of a desired micro-grid. Other power grid simulators such as Simulink, Modelica, etc, use detailed Ordinary Differential Equation (ODE) modeling to accommodate the voltage distribution features. This paper presents a SGridSim micro-grid simulator tool that simplifies the modeling of both the voltage and power distribution features in a desired micro-grid. The SGridSim tool accomplishes this simplified modeling by using Effective Node-to-Node Complex Impedance (EN2NCI) models of components that typically make-up a micro-grid. The term EN2NCI models means that the impedance based components of a micro-grid are modeled as single impedances tied between their respective voltage nodes on the micro-grid. The benefit of the presented SGridSim tool are 1) simulation of a micro-grid is performed strictly in the complex-domain; 2) faster simulation of a micro-grid by avoiding ODE solving. An example micro-grid model was built using the SGridSim tool and tested to simulate both the voltage and power distribution features with a total absolute relative error of less than 6%.

Track 1: Complex Networked Control

Systems (continued)

1:00 p.m.-2:30 p.m. Washington
Chair: Frank Ferrese, Navy Surface Warfare Center

Resilient Control of Cyber-Physical Systems against Denial-of-Service Attacks
Yuan Yuan *(Tsinghua University), Quanyan Zhu, Fuchun Sun, Qinyi Wang and Tamer Başar*

The integration of control systems with modern information technologies has posed potential security threats for critical infrastructures. The communication channels of the control system are vulnerable to malicious jamming and Denial-of-Service (DoS) attacks, which lead to severe time-delays and degradation of control performances. In this paper, we design resilient controllers for cyber-physical control systems under DoS attacks. We establish a coupled design framework which incorporates the cyber configuration policy of Intrusion Detection Systems (IDSs) and the robust control of dynamical system. We propose design algorithms based on value iteration methods and linear matrix inequalities for computing the optimal cyber security policy and control laws. We illustrate the design principle with an example from power systems. The results are corroborated by numerical examples and simulations.

Variations of Converter's Control Parameters and its Effects on DC Multi-Converter Power Systems
Juan C. Jimenez and **Chika O. Nwankpa** *(Drexel University)*

Different dynamic and static relations are possible in multi-converter power systems where electromechanical and power electronic equipment interact with each other. Harmful operational situations due to control limit violations can rise during system disturbances. The development of control strategies, be it local or system-wide, are key issues to maintain desired behavior of the system. This work concentrates on the modeling and simulation of a DC multi-converter power system to analyze the effects of load and control parameter variations in the overall behavior of the system and provides insight to possible issues to be included in the development of appropriate control strategies.

Symposia Committee

Symposia Chairs:

Frank Ferrese, Naval Surface Warfare Center
David Scheidt, Johns Hopkins Applied Physics Laboratory

Technical Program Chairs

Prof. Juan Rodriguez-Andina, University of Vigo
Dr. Aleksander Malinowski, Bradley University

Technical Program Committee

- Said Ahmed-Zaid, Boise State University
- Saurabh Amin, Massachusetts Institute of Technology
- Juan Jose Rodriguez Andina, University of Vigo
- Azad Azadmanesh, University of Nebraska, Omaha
- Ron Boring, Idaho National Laboratory
- Jonathan Butts, Air Force Institute of Technology
- Barrett Caldwell, Purdue University
- Álvaro A. Cárdenas, Fujitsu Laboratories of America
- Marco Carvalho, Florida Institute of Technology
- YangQuan Chen, Utah State University
- John Chiasson, Boise State University
- Mo-Yuen Chow, North Carolina State University
- Michael Condry, INTEL
- John Doyle, California Institute of Technology
- Frank Ferrese, Naval Surface Wafare Center
- Douglas Few, Idaho National Laboratory
- John Gardner, Boise State University
- Devendra Garg, Duke University
- David Gertman, Idaho National Laboratory
- Annarita Giani, Los Alamos National Laboratory
- Diane Hooie, National Energy Technology Laboratory
- Scott Kerick, Army Research Laboratory
- Nicholas Kottenstette, WW Technology Group
- Axel Krings, University of Idaho
- Manish Kumar, University of Cincinnati
- Parag Lala, Texas A&M
- Nathan Lau, University of Virginia
- Timothy McJunkin, Idaho National Laboratory
- Miles McQueen, Idaho National Laboratory
- Mark Minor, University of Utah
- Kevin Moore, Colorado School of Mines
- Subbaram Naidu, Idaho State University
- Xinming Ou, Kansas State University
- Brian Powell, National Instruments
- Raghunathan Rengasamy, Texas Tech
- Eugene Santos, Dartmouth College
- Marco Schoen, Idaho State University
- Galina Schwartz, UC Berkeley
- William Smart, Washington University
- Charles Tolle, South Dakota School of Mines and Technology
- Zachary Tudor, SRI International
- Venkat Venkatasubramanian, Purdue University
- I-Jeng Wang, John Hopkins University, Applied Physics Laboratory
- Bogdan Wilamowski, Auburn University
- David Woods, Ohio State University
- Reed Young, U.S. Army ATEC

COGNITIVE

Overview

A growing number of cyber, physical, and hybrid work environments exhibit critical interplays of engineering systems design with human factors and ergonomics research applications. The Cognitive Systems track will explore how people, individually and teams, engage in cognitive work in complex, high consequence settings. We will emphasize technology designs, operating concepts and procedures, and decision-making strategies that improve time-critical human and engineering system performance. Joint sessions with the Control Systems and Cyber Systems Symposia will address multi-function aspects of resilience and robustness of systems integrating humans, automation, and system management resources.

Symposia: Cognitive

Cognitive Systems At-A-Glance

Tuesday, August 13 - Papers & Presentations

8:30 a.m.	**Keynote:** Kyle Hultgren, Center for Medication Safety Advancement *(Columbus I/II)*
9:30 a.m.	**Morning Break**
	Cognitive Session 1: *Columbus I/II* Concepts and Processes of Resilient Cognitive Operations Chair: Barrett Caldwell, Purdue University
10:00 a.m.	Is Performance Variability Necessary? A Qualitative Study on Cognitive Resilience in Forestry Work - Jennifer Colman and Heather Kahle, WorkSafeBC
10:30 a.m.	Considering Quantitative Metrics for Resilience - Barrett Caldwell, Purdue University
11:00 a.m.	Process for Control Room Modernization Using Digital Control Systems at Nuclear Power Plants - Ron Boring, Idaho National Laboratory
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Norman Whitaker, DARPA *(Grand Ballroom)*
	Teams in Resilient Performance Settings Chair: Ron Boring, Idaho National Laboratory
1:00 p.m.	Resilience in Robot-Assisted Surgical Teams - E. Asher Balkin , The Ohio State University
1:30 p.m.	Robust Flight Deck Systems: Harnessing the Synergistic Power of the Crew - Mike Stasio, United Airlines
2:00 p.m.	Differences in Trust Between Two Types of Alarms and Events within a Nuclear Plant and Control Simulation - Ron Boring, Idaho National Laboratory
2:30 p.m.	**Afternoon Break**
3:00 p.m.	Quantitative Modeling of Social Systems Dynamics and Resilience Prior to 1990: Lessons for Today - Barrett Caldwell, Purdue University
4:30 p.m.	**Adjourn**

Wednesday, August 14 - Tutorials & Workshops

8:30 a.m.	**Keynote:** Stephen Rottler, Sandia National Laboratories *(Columbus I/II)*
9:30 a.m.	**Morning Break**
	Cognitive Session 1: *Columbus I/II* Chair: David Woods, The Ohio State University
10:00 a.m.	**Path to Autonomous, Resilient Systems -** John Doyle, Caltech David Woods, The Ohio State University
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Dane Egli, The Johns Hopkins University *(Grand Ballroom) Sponsored by* ***TRUST, UC Berkeley***
1:00 p.m.	**Path to Autonomous, Resilient Systems -** Doyle/Woods cont.
2:30 p.m.	**Afternoon Break**
3:00 p.m.	**Poster Session**
4:30 p.m.	**Adjourn**
6:00 p.m.	**Hoster Dinner with Plenary Speaker:** Declan Ganley, Rivada Networks *(The Dining Room)*

Thursday, August 15 - Panel Discussions

10:00 a.m.	**Panel Discussion** - open to all attendees *(Grand Ballroom)*
1:30 p.m.	**Tour -** UC Berkeley *(Optional)*

Cognitive Systems Tracks

Cognitive Systems

Highlighted by a track at the 2008 Frontiers of Engineering conference, the past decade has seen a substantial increase in the respect and visibility of cognitive engineering systems approaches to the study of healthcare, infrastructure management, manufacturing, process control, and other critical operational systems. While many researchers will applaud newly announced White House initiatives addressing cognitive systems in terms of brain structures, functions, and direct brain interfaces, others may see these approaches as divergent from our growing understanding of "knowledge in context" or "embedded expertise" or "shared cognition". How do we combine basic research investigations with broader investigations of emergent properties and application-focused advances? Where are additional areas for innovation and implementation in the development of cognitive systems approaches to human and technology systems performance? What are the challenges in moving from a specialized subgroup to a dominant force in professional societies such as the Human Factors and Ergonomics Society? We welcome both specific contributions in the area of Cognitive Systems research, as well as broader thought pieces to examine the state and future of what is still a young scientific and engineering subdiscipline.

Human-Centered Resilience

Across a range of complex and high-reliability work settings, humans are seen as critical components of both maintaining system stability in the face of external challenges, and recovering system functions after breakdowns or catastrophes. From Apollo 13 to everyday stories of worker ingenuity and creativity, humans can be the primary source of expanding the range of system capabilities through intuition, innovation, and imagination. A research paradigm focusing only on human error as operator failure to perform acceptably according to previously defined and designed standards is insufficient to examine these creative responses to environmental and operational variances. The goal of papers in the Human-Centered Resilience track is to describe and investigate systematic research approaches to understand these contributions to system resilience, as well as theoretical or basic conceptualizations appropriate for an improved understanding of how wisdom and experience at "the sharp end" can help to improve the performance of complex systems.

Symposia Keynotes

Simulating the Medication Use Process

Dr. Kyle Hultgren, Center for Medication Safety Advancement

Bio

Kyle Hultgren is the Managing Director for the Purdue University College of Pharmacy's Center for Medication Safety Advancement in Indianapolis, Indiana. Dr. Hultgren also serves as a Clinical Assistant Professor of Pharmacy Practice at Purdue where he pursues the development of innovative safe medication use practices as well as engaging methods to educate healthcare practitioners. During his current tenure as Managing Director, the Center has experienced exponential growth that includes work in safety education and competency, innovative safety measurement systems, the creation of an International Medication Safety Fellowship, and an award-winning initiative in electronic prescribing. He lectures extensively on the topics of safe medication use practices and process improvement across the country and internationally. He received his Doctor of Pharmacy from Purdue University College of Pharmacy in West Lafayette, Indiana.

Abstract

Healthcare in the United States is a large and complex system that is all too often fraught with unintended adverse events. Within this large system is the medication use process that will be discussed in greater detail as a subsystem of healthcare. This system can often be difficult to measure and quantify, but through new research targeted at tablet-based computer simulation that will be discussed in this session we will begin to identify methods of educating, training, and instilling a culture of safety within healthcare professionals.

Human Cognition and Operational Safety

Dr. Stephen Rottler, Sandia National Laboratories

Bio

Steve Rottler Dr. J. Stephen (Steve) Rottler is vice president of Sandia's California laboratory and serves as lead for the Laboratories' Energy, Climate, and Infrastructure Security business unit. The California laboratory's principal programs include nuclear weapons stewardship; homeland security with a focus on defending against weapons of mass destruction; combustion, transportation and hydrogen energy research; biology; and advanced computational and information systems.

Prior to moving to Sandia's California laboratory, Dr. Rottler guided corporate research and development efforts as Chief Technology Officer and Vice President, Science and Technology. He also managed technology transfer and strategic research relationships with universities, industry, and the State of New Mexico.

Dr. Rottler has also held a number of leadership roles within Sandia's Nuclear Weapons mission, including, most recently, Chief Engineer for Nuclear Weapons and Vice President, Weapon Engineering and Product Realization where he was the Central Technical Authority for nuclear weapons and led all nuclear weapon engineering and production activities at Sandia. He has been responsible for nuclear warhead system engineering and integration, development of high-performance electronic systems, and system analyses and assessments for Sandia and National Nuclear Security Administration senior management. He also managed organizations and programs responsible for the research, development, and application of advanced computational and experimental techniques in the engineering sciences. As a member of technical staff at Sandia, Dr. Rottler was part of a research team that developed multidimensional radiation-hydrodynamics simulation codes for nuclear weapon applications, and he led projects that supported the development of advanced nuclear and conventional weapon concepts.

Dr. Rottler is a Fellow of the American Institute of Aeronautics and Astronautics, a member of the Institute's Board of Directors, and a past chair of the Institute's Technical Committee on Management. He is a recipient of the Department of the Air Force Award for Exemplary Civilian Service. Dr. Rottler is a Fellow of Seminar XXI at the Massachusetts Institute of Technology. He is currently serving or has served on the Board of Directors of the United Kingdom Atomic Weapons Establishment, New Mexico Humanities Council, the Albuquerque Explora Science Museum, and Technology Ventures Corporation. Additionally, he has served as a member of the external advisory board for the Texas A&M University Dwight Look College of Engineering, and he has led or served on independent review panels for the U.S. Navy Strategic Systems Programs Office and the United Kingdom Atomic Weapons Establishment.

Dr. Rottler received his B.S., M.S., and Ph.D. degrees in Nuclear Engineering from Texas A&M University in 1980, 1982, and 1984, respectively. He has published papers, reports, and conference presentations on the development and application of computational radiation-hydrodynamics codes.

Dr. Rottler and his wife have two children. In his spare time, he finds relaxation through long-distance running and researching his family's history, and he is an avid reader of U.S. and English history.

Abstract

This talk will explore the intersection of operational safety and human cognition. Understanding and accounting for human behavior is a critical component to any safety framework, yet it is often overlooked. Sandia National Laboratories vice president Steve Rottler will explain operational safety in the context of the Lab's ongoing safety journey from a culture that ignored the "human factor" to one that places human cognition at the forefront.

Tutorial and Paper Sessions

Session 1: Concepts and Processes of Resilient Cognitive Operations

Chair: Barrett Caldwell, Purdue University

Is Performance Variability Necessary? A Qualitative Study on Cognitive Resilience in Forestry Work
Jennifer Colman and Heather Kahle *(WorkSafeBC)*

In forestry work, conditions exist and develop that are complex, unpredictable and highly consequential and therefore cannot be handled entirely by following static work procedures. Cognitive adjustments are necessary. The objective of this research was to determine whether performance (cognitive) variability is actually necessary to safely fell trees in the coastal region of British Columbia (B.C.). In this paper two perspectives were contrasted: The traditional view of safety and the resilience perspective. A collection of empirical evidence established that while safe work procedures provide a good foundation, it is individual performance variability shaped by experience and "know-how" that guides the application of technical skills in such a complex, dynamic, high risk environment.

Considering Quantitative Metrics for Resilience
Barrett Caldwell *(Purdue University)*

The current emphasis on Resilience Week and International Symposium on Resilient Cognitive Systems highlights a growing awareness of the importance of designing and operating engineering systems in a variety of environmental conditions and in response to dynamic events. Although there has been considerable confusion and drift in the use of the term, "resilience" as a concept dates back to dynamic systems study of complex ecological systems in the 1970s. This original definition relates clearly to quantitative metrics that link also to statistical process control techniques describing system performance as affected by external, "assignable" causes. This paper discusses important elements to consider resilience as a quantitative metric to improve consistency and clarity of evaluation in engineering systems. Rather than simply a binary attribute of systems, resilience should be considered in terms of system performance measures as affected by environmental conditions or events, energy flow couplings, and statistical process control limits. Our estimations of system resilience are seriously compromised when process control estimates are extrapolated beyond linear ranges of environmental conditions or when including discontinuous performance / event outliers exceeding appropriate forecasting estimates.

Process for Control Room Modernization Using Digital Control Systems at Nuclear Power Plants
Ronald Boring *(Idaho National Laboratory)*

The U.S. nuclear industry, like similar process control industries, has moved toward upgrading its control rooms. The upgraded control rooms typically feature digital control system (DCS) displays embedded in the panels. These displays gather information from the system and represent that information on a single display surface. In this manner, the DCS combines many previously separate analog indicators and controls into a single digital display, whereby the operators can toggle between multiple windows to monitor and control different aspects of the plant. The design of the DCS depends on the function of the system it monitors, but revolves around presenting the information most germane to an operator at any point in time. DCSs require a carefully designed human system interface. This paper centers on redesigning existing DCS displays for an example chemical volume control system (CVCS) at a U.S. nuclear power plant.

Session 2: Teams in Resilient Performance Settings

Chair: Ron Boring, Idaho National Laboratory

Resilience in Robot-Assisted Surgical Teams
E. Asher Balkin *(The Ohio State University), Rene Lewis, Ronney Abaza, Jordan Angel, and Lynda Jay John*

The performance of high-consequence work in situations of high conditional variability demands the development and implementation of mechanisms for resilience to assure desirable outcomes in the face of challenge events. The paper explores the four types of challenge events which surgical teams encounter in robot-assisted surgery (RAS). Specifically they are: equipment failure, patient anatomical and/or physiological variation, emergent medical situations, and team member changes. Differences between robot-assisted and other surgical modalities are also presented.

Robust Flight Deck Systems: Harnessing the Synergistic Power of the Crew
Mike Stasio *(United Airlines)*

Robust flight decks are possible in both normal and novel operations. Existing crew resource and error management programs can improve team centered resilience with Oshry's Organization Development (OD) principles. The need on the flight deck is to diminish the invisible behavioral gap between espoused theory and theory-in-use by balancing Oshry's four basic elements that make up robust human systems—differentiation, homogenization, integration, and individuation.

This low-cost OD vision is offered as a guide for organizations to tailor existing aircrew recurrent training modules. Assessment and diagnosis measures are recommended for continuous improvement, so this OD framework includes adaptive feedback interventions and soft-skills behavioral markers for organizations to consider.

Difference in Trust Between Two Types of Alarms and Events Within a Nuclear Power Plant Control Simulation
Austin Ragsdale, Roger Lew, and **Ronald Boring**
(Idaho National Laboratory)

This research addresses how different types of alarms and events can affect an operator's trust for an alarm system. The experiment examined the effect of two types of alarm systems (two-state and three-state alarms) on trust, alarm compliance, and diagnosis for two types of faults differing in complexity. Two-state alarms typically represent a simple 'alarm'/'no alarm' condition, while three-state alarms represent 'alarm'/'warning'/'no alarm' conditions. We hypothesized that participants would have more trust and would perform better when using three-state alarms. We used sensitivity based on Signal Detection Theory to measure performance. The findings from this research showed participants performed better and had more trust in three-state alarms compared to two-state alarms. Furthermore, these findings have significant theoretical implications and practical applications as they apply to improving the efficiency and effectiveness of nuclear power plant operations.

Session 3: History of Resilience Metrics Discussion

Chair: Barrett Caldwell, Purdue University

Quantitative Modeling of Social Systems Dynamics and Resilience Prior to 1990: Lessons for Today
The papers that comprise the "Resilient Cognitive Systems" track of Resilience Week emphasize the importance of how human experience, knowledge, and skill affect the performance of complex systems. Factors such as information availability, implicit and tacit knowledge, and knowledge sharing and trust significantly affect the nature of tasks, success criteria, and strategic responses to system degradation. However, creating a single standard of resilience is both infeasible across performance domains, and inconsistent with the history of quantitative work in the area. "History of Resilience Metrics," provides a background discussion of attempts at quantitative metrics and models of resilience prior to 1990, with potential implications for the study of resilience affected by cognitive and team processes.

Tutorial Description- Outmaneuvering Complexity with John Doyle and David Woods

Wednesday, August 14, 10:00 a.m.-2:30 p.m.
Columbus I/II

The challenge of brittleness and fragilility in complex networked systems is our common theme, and we offer complementary but somewhat different perspectives. The starting motivation is that efforts to achieve efficient, safe, sustainable, infrastructure across sectors (energy, transport, health, water, waste, communications) collides with complexity to produce unintended effects, brittleness, and sudden collapses in these systems operated to support various human stakeholders and purposes. Efforts to improve systems produce more extensive and hidden interdependencies, and current system design frameworks for large scale efficiency and automation do an inadequate job of managing the unavoidable tradeoffs of complexity and robustness that result. Each effort to improve promises to resolve current problems, but, after fielding, turns out

to generate new and unanticipated difficulties.

John's research has focused on progress towards a more "unified" theory of universal laws and architectures: hard limits, tradeoffs, and constraints on achievable robust performance ("laws"), the organizing principles that succeed or fail in achieving them (architectures and protocols), the resulting high variability data and "robust yet fragile" behavior observed in real systems and case studies (behavior, data), and the processes by which systems adapt and evolve (variation, selection, design). He will leverage a series of case studies from technology but also neuroscience, particularly vision and sensorimotor control, and also cell biology and human physiology to illustrate the implications of recent theoretical developments.

For David, the journey began with observations of various high stakes human systems and the finding that failure is due to brittle systems. His work develops answers to questions such as: How to overcome the risk of brittle systems? What are the basic failure modes of all complex adaptive systems? How do people act as the generic stop gap to fill adaptive shortfalls in complex systems? How does change trigger adaptive reverberations that start to fluoresce and then stall out? What are the common patterns of adaptive stalls following insertionsof new technology, infrstsructures, and automation? The answers to these questions connect to John's theory development in terms of the risk of control saturation, how some systems are able to regulate capacity for maneuver, and how some architectures escape the dilemmas that arise from how th efundamental trade-offs are expressed in human systems.

The central technical difficulty is that basic systems design frameworks from controls, communications, and computing remain too fragmented to fully address the looming challenges. They do have in common the role of their basic "laws" or tradeoffs that address domain specific issues in isolation. But what is needed is a more integrated theory of these limits and how to tradeoff efficiency and robustness more completely. What is needed is a more coherent approach to designing architectures that manage these tradeoffs. The live dialogue will explore the current state of inquiry, highlight areas of progress, break off for mini-talks to provide context for the audience, reflect on the common emergent themes, and point to promising directions.

Symposia Committee

General Chair

- Barrett Caldwell, Purdue University
- Technical Program Committee
- Conne Bazley, NuScale Power
- Ron Boring, Idaho National Laboratory
- Marco Carvalho, Florida Institute of Technology
- David Gertman, Idaho National Laboratory
- Scott Kerick, Army Research Laboratory
- Huafei (Harry) Liao, Sandia National Laboratories
- Timothy McJunkin, Idaho National Laboratory
- Apurva Mohan, Honeywell International
- Jeffrey Onken, Northrup Grumman
- David Woods, Ohio State University

Organizing Chair

- Jodi Grgich, Idaho National Laboratory

CYBER

Overview

The overwhelming majority of engineered systems in use today are highly dependent on computation and communication resources. This includes system at all levels, ranging for example, from our vehicles, to large-scale industrial systems and national critical infrastructures. The resilience of the underlying computational systems and infrastructures underlying these technologies is of great importance for mission continuity and success. Resilience, in this context, is understood as the ability of a system to anticipate, withstand, recover and evolve from external attacks or failures. In this symposium we will focus on the topic of resilience of cyber systems. Among others, the concepts of cyber awareness, anticipation, avoidance, protection, detection, and response to cyber attacks will be promoted and will help set the tone of the event. A better understanding and development of these concepts ad its supporting technologies will help provide some of the key underlying capabilities for the design and development of resilient cyber systems.

Symposia: Cyber Systems

Cyber Systems At-A-Glance

Tuesday, August 13 - Tutorials & Workshops

8:30 a.m.	**Keynote:** Vipin Swarup, MITRE *(Jackson)*
9:30 a.m.	**Morning Break**
10:00 a.m.	**Cyber Session 1:** *Jackson* Chair: Marco Carvalho, Florida Institute of Technology
	Cyber Resilience Theory - Nick Multari and Chris Oehmen, Pacific Northwest National Laboratory
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Norman Whitaker, DARPA *(Grand Ballroom)*
1:00 p.m.	**Cyber Resilience Frameworks and Applications** - Deb Bodeau, MITRE
2:30 p.m.	**Afternoon Break**
3:00 p.m.	**Cyber Resilience Metrics** - Marco Carvalho, Florida Institute of Technology and Sean Peisert, UC Davis
4:30 p.m.	**Adjourn**

Wednesday, August 14 - Papers & Presentations

8:30 a.m.	**Keynote:** Thomas Longstaff, National Security Agency *(Jackson)*	
9:30 a.m.	**Morning Break**	
	Resilient Cyber Systems: *Jackson* Chair: Marco Carvalho, Florida Institute of Technology	**Systems Intelligence for Resilience:** *Sansome* Chair: Dipankar Dasgupta, University of Memphis
10:00 a.m.	**The language of behavior: Exploring a new formalism for resilient response** - Glenn Fink, PNNL	**Information Security Analysis for CKMS Using Game Theory and Simulation** - Rick Sheldon, ORNL
10:30 a.m.	**Towards Improved Detection of Attackers in Computer Networks: New Edges, Fast Updating, and Host Agents** - John Neil, LANL	**Modeling and Cyber Security Vulnerabilities Analyzing for Smart Grid Transmission Subsystem** - Yi Deng, Virginia Tech
11:00 a.m.	**A Command and Control Framework for Moving Target Defense and Cyber Resilience** - Marco Carvalho, FIT	**Adaptive Selection of Multi-Factor Modalities for Continuous Authentication** - Dipankar Dasgupta- University of Memphis

11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Dane Egli, The Johns Hopkins University *(Grand Ballroom) Sponsored by* ***TRUST, UC Berkeley***	
	Resilient Cyber Systems *(Jackson)* Chair: Marco Carvalho, FIT	Cyber Resilience Theory *(Sansome)* Chair: Nick Multari, PNNL
1:00 p.m.	Statistical detection of malicious web sites through time proximity to existing detection events - Alexander Kent, LANL	Supply Chain Integration for Integrity: Policy and architecture for built-in supply chain integrity of trusted components - Rick Sheldon, ORNL
1:30 p.m.	Scalable Machine Learning Framework for Behavior-Based Access Control - Michael Atighetchi, Raytheon BNN Tech.	Increasing Cyber System Resilience Through Predictability-Based Defense - Rich Colbaugh, Sandia National Laboratory
2:00 p.m.	A Combined Discriminative and Generative Behavior Model for Cyber Physical System Defense - Owen McCusker, Sonalysts, Inc.	Metrics and Analysis Techniques for Cyber Defensibility, Resiliency, and Security: Looking Across Different Evaluation Environments - Bill Heinbockel, MITRE
2:30 p.m.	**Afternoon Break**	
3:00 p.m.	Simulation Tool for Evaluation and Design of Resilience Strategies - Dung Lam, University of Texas, Austin	Towards a Unified Theoretical Framework for Reconstitution of Cyber Systems - Mahantesh Halappanavar, PNNL
	Cooperation Models Between Humans and Artificial Self-Organizing Systems: motivations, issues, and perspectives - Gabriel Rey, PUJ	Measuring Success in Complex System Models using Formal Concept Analysis and Probability Models - Jennifer Davidson, Iowa State
4:00 p.m.	**Poster Session**	
4:30 p.m.	**Adjourn**	
6:00 p.m.	**Hoster Dinner with Plenary Speaker:** Declan Ganley, Rivada Networks *(The Dining Room)*	

Thursday, August 15 - Panel Discussions

8:30 a.m.	Keynote: Doug Tygar, UC Berkeley *(Grand Ballroom)*
10:00 a.m.	Panel Discussion - open to all attendees *(Grand Ballroom)*
1:30 p.m.	**Tour -** UC Berkeley *(Optional)*

Symposia Keynotes

Cyber System Keynote Speakers

Dr. Thomas Longstaff, National Security Agency

Dr. Tom Longstaff is currently on a two-year assignment as the Technical Director of the Systems Behavior office within the DOD National Security Agency. Prior to coming to NSA in 2012, Tom was the Chief Scientist for the Cyber Missions Branch of the Applied Physics Laboratory (APL). Tom joined APL in 2007 to work with a wide variety of infocentric operations projects on behalf of the U.S. Government to include technology transition of cyber R&D, information assurance, intelligence, and global information networks.

Tom is currently the chair of the Computer Science, Information Assurance, and Information Systems Engineering Programs within the Whiting School at The Johns Hopkins University. Tom's academic publications span topics such as malware analysis, information survivability, insider threat, intruder modeling, and intrusion detection. He maintains an active role in the information assurance community and regularly advises organizations on the future of network threat and information assurance. Tom is also a fellow of the International Information Integrity Institute and editor of the IEEE Security & Privacy magazine.

Prior to coming to APL, Tom was the deputy director for technology for the CERT at Carnegie Mellon University's Software Engineering Institute. In his 15-year tenure at CERT, Tom helped to create many of the projects and centers that enabled CERT to become an internationally recognized network security organization. His work included assisting the Department of Homeland Security and other agencies to use response and vulnerability data to define and direct a research and operations program in analysis and prediction of network security and cyber terrorism events.

Managing Adversarial Change with Cyber Resilience

Dr. Vipin Swarup, MITRE

Dr. Vipin Swarup is the Chief Scientist for Mission Assurance in MITRE's Cyber Security Division. He leads MITRE's corporate cybersecurity research program focused on mission assurance against advanced cyber threats, which includes over 25 research projects in mobile computing security, cloud computing security, network security, cyber analytics, active cyber defense, and resiliency.

In the past, Dr. Swarup has led research projects in trust management, cross-boundary information sharing, context-aware security, security guards, and mobile agent security, and has published extensively in these and other areas. His work for agencies such as AFRL, NSA, DARPA, and OSD have resulted in significant outcomes. His security guard filter technology, called Felt, has been integrated and deployed on several military security guard products worldwide. In 2008, he played a lead role on a US Department of Defense (DOD) team that developed a DOD Science and Technology (S&T) strategy for cyber conflict defense against advanced cyber threats -- based on this strategy, DOD substantially reshaped its funding priorities in cybersecurity research.

Dr. Swarup holds a B.Tech. in Computer Science and Engineering from Indian Institute of Technology, Bombay, and an MS and Ph.D. in Computer Science from the University of Illinois at Urbana-Champaign.

Abstract

Enterprise networks are under constant attack and network defenders must contend with the expectation that persistent cyber adversaries will eventually penetrate standard perimeter defenses and cause adverse cyber effects. Cyber resilience is essential to managing the unexpected changes that such cyber adversaries can cause. This talk will present a framework

for cyber resiliency in the context of cyber security and defendability, and will explore it via an architecture that protects against adversaries who have acquired an initial foothold within enterprise or enclave networks. The talk will then highlight some pressing challenges in making cyber systems resilient to advanced persistent threats.

Adversarial Machine Learning

Dr. Doug Tygar, UC Berkeley

Dr. Doug Tygar is Professor of Computer Science at UC Berkeley and also a Professor of Information Management at UC Berkeley. He works in the areas of computer security, privacy, and electronic commerce. His current research includes privacy, security issues in sensor webs, digital rights management, and usable computer security. His awards include a National Science Foundation Presidential Young Investigator Award, an Okawa Foundation Fellowship, a teaching award from Carnegie Mellon, and invited keynote addresses at PODC, PODS, VLDB, and many other conferences.

Doug Tygar has written three books; his book Secure Broadcast Communication in Wired and Wireless Networks (with Adrian Perrig) is a standard reference and has been translated to Japanese. He designed cryptographic postage standards for the US Postal Service and has helped build a number of security and electronic commerce systems including: Strongbox, Dyad, Netbill, and Micro-Tesla. He served as chair of the Defense Department's ISAT Study Group on Security with Privacy, and was a founding board member of ACM's Special Interest Group on Electronic Commerce. He helped create and remains an active member of TRUST (Team for Research in Ubiquitous Security Technologies). TRUST is a new National Science Foundation Science and Technology Center with headquarters at UC Berkeley and involving faculty from Berkeley, Carnegie Mellon, Cornell, Stanford, and Vanderbilt.

Before coming to UC Berkeley, Dr. Tygar was tenured faculty at Carnegie Mellon's Computer Science Department, where he continues to hold an Adjunct Professor position. He received his doctorate from Harvard and his undergraduate degree from Berkeley.

Abstract

Machine learning is an important tool for cyber-security, but in its current form it is poorly adapted for adversarial machine learning. In this talk, I'll explore some of the problems with conventional machine learning applications in security, and will discuss research towards a theory of adversarial machine learning. This talk reports on joint work with the Security Machine Learning group at UC Berkeley.

Tutorial and Papers Sessions

Tutorial Description- "Cyber Resilience Theory, Applications, and Metrics"

Tuesday, August 13, 10:00 a.m.-4:30 p.m. Jackson
Chair: Marco Carvalho, Florida Institute of Technology

The first day of the Resilient Cyber Systems Symposium will include plenary talks covering each of the three main thrusts of the symposium. The first presentation will focus on the Theory of Cyber Resilience, followed by a prevention on Cyber Resilience Framework and Architectures. The third presentation will focus on Cyber Resilience Metrics. Combined, the presentations will help provide the necessary background, and will help set the tone for the subsequent presentations and discussions on resilient cyber systems.

Session 1: Resilient Cyber Systems

Wednesday, August 14, 10:00 a.m.-3:30 p.m. Jackson
Chair: Marco Carvalho, Florida Institute of Technology

The language of behavior: Exploring a new formalism for resilient response

Glenn Fink *(Pacific Northwest National Laboratory) and Marco Carvalho*

Historically, behavior-based computer security has relied on automatic classification of the activities of persons and programs to determine whether these activities should be restricted. In this paper, we argue that classification that relies exclusively upon observation of low-level events (either via signatures or anomalies)

is insufficient to infer higher-level behavior correctly. However, ordering these events into linguistic structures according to a finite set of grammar rules may be sufficient. We present an argument that formal language theory offers a bridge between primitive observables and high-level behaviors in cyber systems. We believe that this restatement of the behavior recognition challenge in cyber systems will enable reasoning about the components of automated behavior recognition. Our application area is resilient systems that will identify unusual behaviors (whether good or bad) and employ limited-time, partial quarantines on the actors responsible. We wish to classify based on behaviors of actors rather than bit patterns of actions and events.

To do this, we propose a definition of computer-mediated human behaviors and discuss whether these behaviors can be described via a formal language. If this is possible, then we may be able to classify these behaviors as desirable or undesirable, normal or abnormal. This classification would facilitate the creation of behavioral models that could be used to take automatic actions to stop actors who appear to be acting in ways that may be threatening.

Towards Improved Detection of Attackers in Computer Networks: New Edges, Fast Updating, and Host Agents
Joshua Neil *(Los Alamos National Laboratory), Benjamin Uphoff, Curtis Hash, and Curtis Storlie*

This paper focuses on several important topics related to sub-graph anomaly detection for computer networks. First, we briefly discuss a graph based view of a computer network consisting of nodes (computers) and edges (time-series of communications between computers), and how stochastic models of groups of edges can be used to identify local anomalous areas of the network indicating the traversal of attackers. Next, the concept of a new edge, an edge between two computers that have never communicated before, is introduced, and a model for establishing the probability of such an event is provided. We follow this with a discussion of exponentially weighted moving averages for updating models of edges. Next, as measuring network data for the purposes of anomaly detection is difficult we discuss a host agent designed specifically to gather this type of data. Finally, the performance of anomaly detection using this host agent to collect data is compared with that of DNS data.

MTC2: A Command and Control Framework for Moving Target Defense and Cyber Resilience
Marco Carvalho *(Florida Institute of Technology), Thomas C. Eskridge, Larry Bunch, Adam Dalton, Robert Hoffman, Jeffrey M. Bradshaw, Paul J. Feltovich, Daniel Kidwell, and Teresa Shanklin*

In this paper we discuss the need for a new command and control (C2) approach to Moving Target Defenses (MTDs). We describe some of the requirements and constraints associated with the proposed approach, and introduce a human-agent teamwork concept called MTC2. We discuss specific concepts and technologies that could play an important role in the further development of this capability, and conclude by describing implementation details of the prototype being developed to demonstrate and study MTC2 concepts.

Statistical Detection of Malicious Web Sites Through Time Proximity to Existing Detection Events
Alexander D. Kent *(Los Alamos National Laboratory), and Lorie M. Liebrocky*

We present a novel method of combining and aggregating disparate computer security events with web browsing activity to produce new and extended intrusion information with low false positives. This method integrates web browsing and intrusion-related security events as an unevenly spaced time series, and then aggregates commonalities from these integrated events across a population of monitored computers. This aggregation enables not only increased validation and knowledge about known security events, but also reveals new and previously unknown activity of security concern with very low false positives. This source-oriented information enables more effective defensive measures and increased enterprise-wide security. Using data covering over 24,000 computers and spanning 6 months, we demonstrate the value of our approach. Most importantly, we show a data reduction from 6.4 billion web requests to just 19 from 10 Internet domains requiring a security analyst's review given our real world data set.

Scalable Machine Learning Framework for Behavior-Based Access Control
Jeffrey Cleveland, Michael Jay Mayhew, Aaron Adler, and **Michael Atighetchi** *(Raytheon BBN Technologies)*

Today's activities in cyber space are more connected than ever before, driven by the ability to dynamically interact and share information with a changing set of partners over a wide variety of networks. The success

of approaches aimed at securing the infrastructure has changed the threat profile to point where the biggest threat to the US cyber infrastructure is posed by targeted cyber attacks. The Behavior-Based Access Control (BBAC) effort has been investigating means to increase resilience against these attacks. Using statistical machine learning, BBAC (a) analyzes behaviors of insiders pursuing targeted attacks and (b) assesses trustworthiness of information to support real-time decision making about information sharing. The scope of this paper is to describe the challenge of processing disparate cyber security information at scale, together with an architecture and work-in-progress prototype implementation for a cloud framework supporting a strategic combination of stream and batch processing.

A Combined Discriminative and Generative Behavior Model for Cyber Physical System Defense
Owen McCusker *(Sonalysts, Inc), Scott Brunza, Dipankar Dasgupta, Marco Carvalho, and Setu Vora*

In this position paper we explore the use of behavior models as an enabling methodology in the promotion of a more holistic understanding of CPS that can bridge both cyber and physical domains. Thus, we investigate the use of aggregate behavior analysis techniques combined in both cyber and physical domains. Ultimately, our work focuses on the development of a cyber-physical behavior model that leverages behavior aggregation promoting the creation of a long-view sense-making capability driven by both cyber and physical observations. We look to the use of this approach to establish the ability to anticipate malicious activity in CPS, rather that react.

Simulation Tool for Evaluation and Design of Resilience Strategies
Dung Lam *(University of Texas, Austin), Erik Skiles, and Paul Grisham*

A resilient system is designed to survive and recover from failure or attack. Evaluating resilience strategies for a computer network is difficult because their effectiveness depends on numerous, complex, and interacting factors. This paper presents a simulation prototype for experimenting with resilience strategies, demonstrates scoring metrics for comprehensive evaluations, and highlights simulation results that reveal important parameters and trade-offs that influence resilience strategy performance. Experimental results supported expectations about resilience strategies and revealed strategy assumptions, unexpected emergent situations, and insights into strategy configurations that should be considered when designing a resilient network system.

Cooperation Models Between Humans and Artificial Self-Organizing Systems: Motivations, Issues and Perspectives
Gabriel Rey *(Pontificia Universidad Javeriana), Marco Carvalho, and Damien Trentesaux*

In this paper we introduce and discuss some of the concepts, motivations and requirements for cooperative models between humans and artificial self-organizing systems. After a brief review of alternative cooperation methods, an implicit cooperation-based approach through parameterization and incentives is proposed for human-agent collaboration. Our case study is based on self-organizing, flexible manufacturing control systems.

Session 2- Systems Intelligence for Resilience

Wednesday, August 14, 10:00 a.m.- 11:30 a.m. Sansome
Chair: Dipankar Dasgupta (University of Memphis)

Overview

Intelligent systems and bio-inspired approaches are appearing to be very promising in building robust cyber defense systems. These approaches have increasingly being applied in designing secure protocols, intrusion detection systems, user authentication, cloud security, etc. This invited session presents such techniques in designing resilient and adaptive systems in order to protect cyber and critical infrastructures against unknown threats and dynamic attacks."

Session 3-Cyber Resilience Theory

Wednesday, August 14, 1:00 p.m.-3:30 p.m. Sansome
Chair: Nick Multari (Pacific Northwest National Lab)

Overview

This session will focus on the investigation and discussion of the principles and theory associated with the ability of general system to anticipate, withstand, recover, and evolve in response to localized failures or attacks. The session will cover important topics including the establishment of roots of trust for system resilience, predictability-based defense, and the study of metrics and analysis techniques for system defense. During the session, we will explore these foundations from a theory point of view.

Symposia Committee

General Chairs

- Marco Carvalho, Florida Institute of Technology
- Miles McQueen, Idaho National Laboratory
- Annarita Giani, Los Alamos National Laboratory
- Eugene Santos, Dartmouth College

Technical Program Committee

- Himanshu Khurana – Honeywell
- Rick Sheldon – Oak Ridge National Laboratory
- Marco Carvalho, Florida Institute of Technology
- Miles McQueen, Idaho National Laboratory
- Annarita Giani, Los Alamos National Laboratory
- Eugene Santos, Dartmouth College
- Dipankar Dasgupta, University of Memphis
- Micahel Grimaila, Air Force Institute of Technology
- Michael Atighetchi, BBN Technologies
- Thomas Haigh, Adventium Labs
- Ronda Henning, Harris Corporation
- Owen McCusker, Sonalysts
- Michael Van Putte, MOD-2 Systems
- Gregory Frazier, Apogee Research
- Ben Cook, Sandia National Laboratories
- David Manz, Pacific Northwest Laboratory
- Pratyusa Manadhatta, HP labs
- Xinming Ou, Kansas State University
- Wayne Boyer, Idaho National Laboratory
- Nick Multari, Pacific Northwest Laboratory

Organizing Chair

- Jodi Grgich, Idaho National Laboratory

Publication Chair

- Miles McQueen, Idaho National Laboratory

COMMUNICATION

Overview

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 an anti-access area denial 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.

Symposia- Communications

Communication Systems At-A-Glance

Tuesday, August 13 - Tutorials & Workshops

8:30 a.m.	Open to attend keynotes
9:30 a.m.	**Morning Break**
10:00 a.m.	**Communication Tutorials:** *Pine* Chair: Juan Deaton, Idaho National Laboratory
	Learning form Disasters: Sandy, Communications, and Manifold Resiliency - Lee Vinsel, Steven Institute
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Norman Whitaker, DARPA *(Grand Ballroom)*
1:00 p.m.	Resilience, Survivability, and Disruption Tolerance for the Future Internet and Global Information Grid - James Sterbenz, University of Kansas
2:30 p.m.	**Afternoon Break**
3:00 p.m.	James Sterbenz cont.
4:30 p.m.	**Adjourn**

Wednesday, August 14 - Papers & Presentations

8:30 a.m.	**Keynote:** Rangam Subramanian, Idaho National Laboratory *(Pine)*
9:30 a.m.	**Morning Break**
10:00 a.m.	**Communication Session 1:** *Pine* Chair: Juan Deaton, Idaho National Laboratory
	Efficient and Resilient Communication in Error-prone Wireless Networks - Jie Wu, Temple University
11:30 a.m.	**Hosted Lunch with Plenary Speaker:** Dane Egli, The Johns Hopkins University *(Grand Ballroom) Sponsored by* ***TRUST, UC Berkeley***
1:00 p.m.	**Communication Session 2** Space-polarization MIMO Testbed - Jun Chen, University of Notre Dame
1:30 p.m.	Throughput and Fairness-Aware Dynamic Network Coding in Wireless Communication Networks - Pouya Ostovari , Temple University
2:30 p.m.	**Afternoon Break**
3:00 p.m.	**Poster Session**
4:30 p.m.	**Adjourn**
6:00 p.m.	**Hoster Dinner with Plenary Speaker:** Declan Ganley, Rivada Networks *(The Dining Room)*

Thursday, August 15 - Panel Discussions

10:00 a.m.	**Panel Discussion** - open to all attendees *(Grand Ballroom)*
1:30 p.m.	**Tour -** UC Berkeley *(Optional)*

Symposia Keynote

Resilient Communications - Current Challenges and the Critical Need for Impactful Innovation

Dr. Rangam Subramanian, Idaho National Laboratory

Bio

Dr. Subramanian is a Chief Wireless Technology and Business Strategist, National and Homeland Security Directorate, Idaho National Laboratory, Idaho Falls, ID. His primary responsibilities include: developing and executing on secure wireless business development and strategy; delivering on wireless technology leadership for research and testing programs of national importance; building collaborations across the stakeholders in the government, industry, entrepreneurs and the academia; and defining the direction and roadmap for the INL wireless research center. He is currently serving the White House/ OSTP (Office of the Science and Technology Policy) Senior Steering Group (SSG) on Wireless Spectrum Sharing R&D (WSRD).

Dr. Subramanian has more than 20 years of international experience across multiple Telecommunications OEMs, carriers, investors, government and the academic community. Dr. Subramanian holds an MBA from Northwestern University; a PhD in Computer & Systems Engineering from Oakland University; an MS in Telecommunications from the Asian Institute of Technology, Bangkok, Thailand; and a BS in Electronics Engineering from the National Institute of Technology, Calicut, India.

Abstract

Communications systems and technologies have been a major contributor to transforming human life. However, along with the increasing complexity of these critical infrastructure systems, devices and networks, global communications are becoming virtually wireless, impacting several sectors of the economy, including defense, homeland security, cellular, energy, transportation systems, industrial systems and medical systems. The ability to operate and maintain these complex networks and systems to achieve optimum performance with multiple considerations, such as availability, stability, efficiency, quality of service and security, have thrown enormous research challenges to resilient communications under normal and emergency scenarios.

This keynote will discuss the current challenges, critical needs and driving factors for impactful resilient communications innovation and address why collaborative inter-disciplinary research and implementation in multiple areas, reaching across different stakeholders is needed to build resilient communication systems of the future.

Tutorials and Paper Sessions

Tutorial Description

Tutorials in resilient communications will first explore the realities of communications during disasters, followed by a tutorial in cutting edge research in resilient networks. In our first tutorial, Lee Vinsel will deliver his breaking research on "Learning form Disasters: Sandy, Communications, and Manifold Resiliency" and explore the role of communications technologies, disaster response, and social resiliency during Hurricane Sandy. His analysis will focus on the perspective of science and technology studies and "manifold resiliency," the dynamic interplay that arises between different forms of coping, responding, and recovering that arise during disasters. In our second tutorial, James Sterbenz will present "Resilience, Survivability, and Disruption Tolerance for the Future Internet and Global Information Grid". This tutorial provides a broad overview of the architecture and analysis of resilient networks. This tutorial will present a taxonomy of challenges, explore the sub-disciplines of resilience, architectures, and approaches for modeling and analyzing these networks. At the conclusion of this day, the audience will have an excellent understanding of real-world challenges with communications and the future technologies and techniques to address these challenges.

Session 1: Communications

Wednesday, August 14, 10:00 a.m.-2:00 p.m. Pine
Chair: Juan Deaton, Idaho National Laboratory

Space-polarization MIMO Test-bed
Jun Chen *(University of Notre Dame) and Thomas Pratt*

Space-polarization multiple input multiple output (SP-MIMO) communication systems can provide improved reliability, increased data rates, and higher energy efficiency as compared to conventional co-polarized MIMO (CP-MIMO) systems. To achieve these gains relative to CP-MIMO arrays, SP-MIMO architectures employ a dual-polarized (DP) antenna at each of the antenna locations, effectively doubling the number of ports without substantially increasing the footprint of antenna arrays. CP-MIMO schemes have been explored rigorously in literature, however very few results are available for DPMIMO and SP-MIMO systems, particularly over realistic and imperfect channels. In this paper, we present the design of a state-of-the-art 44 SP-MIMO wireless communications system test-bed to enable comparative performance studies. The test-bed incorporates baseband generators, MIMO channel emulators, a coherent multi-channel receiver, and a host computer for signal processing. We consider full spatial multiplexing schemes involving the simultaneous transmission of either two or four data streams through emulated physical channels for CP-MIMO and SP-MIMO, respectively. Operation, control and signal processing are performed on a host computer within a Matlab environment, giving a powerful, flexible, and efficient platform for analyzing MIMO algorithms in emulated channels. Examples show that SP-MIMO architectures achieve performance shifts in capacity (bit/s/Hz), bit-error-rate (BER), packet-error-rate (PER) and energy efficiencies (Joule/bit) relative to CP-MIMO systems.

Throughput and Fairness-Aware Dynamic Network Coding in Wireless Communication Networks
Pouya Ostovari *(Temple University) and Jie Wu*

Network coding techniques have received a lot of attention from the research community for providing reliable broadcasting in error-prone wireless networks. The most common network coding approach is segment coding, in which the packets are partitioned into segments, and linear network coding is performed inside each segment. In order to increase the throughput of network coding and decrease the decoding delay, dynamic coding schemes have been recently proposed. However, these methods incur many feedback messages. In this paper, we propose two dynamic network coding schemes that achieve the maximum throughput and reduce the number of required feedback messages. Moreover, we propose a fair dynamic network coding scheme that performs a trade-off between the throughput and the fairness in terms of decoding delay and the number of decodable packets at different destination nodes. Our simulation results show that our proposed dynamic network coding method provides the same throughput as the ANC method, with up to 90% less feedback messages. Moreover, our fair dynamic network coding can increase decoding delay fairness by about 80%.

Symposia Committee

General Chairs

- Scott Rothermel, United States Air Force
- Juan Deaton, Idaho National Laboratory
- Darrell Apilado, United States Air Force

Organizing Chair

- Jodi Grgich, Idaho National Laboratory

City Map


Hyde St. Pier
Aquatic Park
Fort Mason
Ghirardelli Square
The Cannery
The Anchorage
Beach St.
Jefferson
FISHERMAN'S WHARF
Pier 39
Aquarium of the Bay
Pier 35
Alcatraz Landing
Hilton
San Francisco Financial District
North Point
Bay St.
Francisco
Chestnut
To Golden Gate Bridge, Fort Mason
Lombard St.
Crookedest St.
TELEGRAPH HILL
Coit Tower
NORTH BEACH
Washington Square
Filbert Street Steps
Levi's Plaza
Greenwich
Filbert
Union
Green
Vallejo
Broadway
RUSSIAN HILL
Broadway Tunnel
Hyde Cable Car Line
Mason Cable Car Line
The Embarcadero
LEGEND
BART STATION
MUNI
CABLE CAR LINE
LIGHT RAIL (F LINE)
San Francisco Bay
Pacific
Jackson
Washington
Clay
Sacramento
California
Pine
Bush
Sutter
Post
Geary
O'Farrell
Ellis
Eddy
Turk
Golden Gate
Van Ness Ave.
Cable Car Museum
Cable Car Line
NOB HILL
Grace Cathedral
Masonic Auditorium
CHINATOWN
Transamerica Bldg.
Walton Park
Safeway
Maritime Plaza
Ferry Building
Embarcadero Center
Old St. Mary's
B of A Bldg.
Stockton Tunnel
Chinatown Gate
Hornblower Cruises
Pier 2
Amtrak
Golden Gate Transit
Rincon Center
UNION SQUARE
Macy's
Maiden Lane
Crocker Galleria
Curran Theatre
ACT Theatre
Visitors' Center
Yerba Buena Gardens
MOMA
MoAD
Moscone Convention Center
Zeum
Westfield S.F. Centre
SOMA
(South of Market)
Transbay Terminal
To: Bay Bridge
CIVIC CENTER
City Hall
Asian Art Museum
Library
Opera House
Davies Sym. Hall
Grove
Hayes
Fell
Market St.
Mission
Howard
Folsom
Harrison
Bryant
Brannan
Townsend
King
South Park
AT&T Giants Ballpark
© 2011 City Maps Inc.

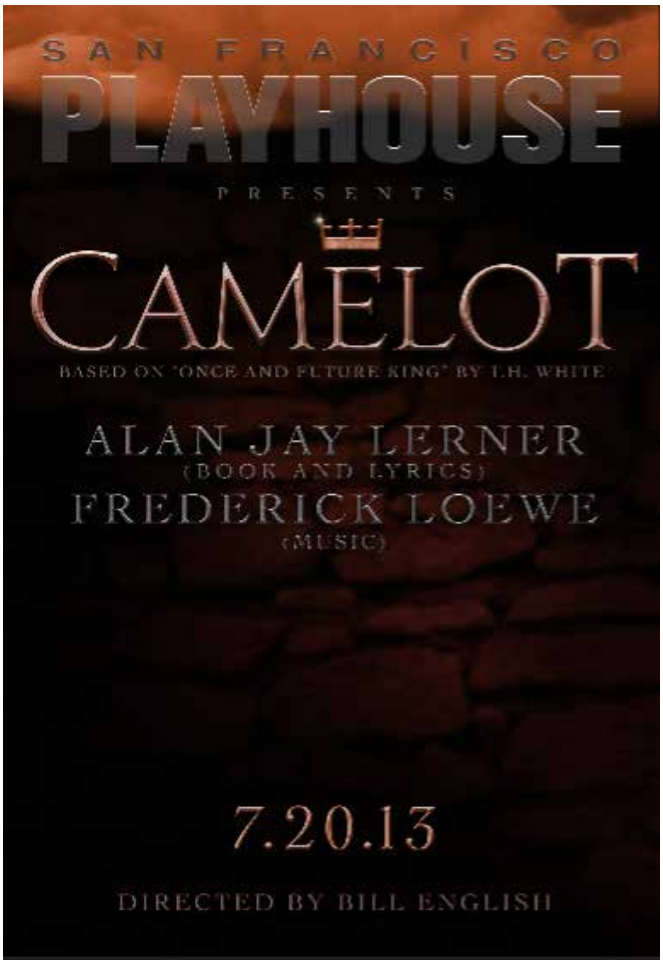
Special Events

Camelot is the timeless and powerful love triangle between legendary King Arthur, his Queen Guenevere and his best friend Lancelot. With one of Broadway's most enchanting scores featuring the hauntingly romantic "If Ever I Would Leave You", "I Loved You Once in Silence", and "Follow Me", Camelot is the definitive musical theatre fable.

Inspired by the extraordinary success of Bill English's re-imagination of My Fair Lady, currently nominated for 13 Bay Area Critics' Awards, this production will delve into the gritty side of Camelot, by anchoring it in a much more barbaric world where shining knights are little more than bikers with clubs, Arthur is a dreamer with a crazy idea, Guenevere an angry goth princess, Modred, a budding Richard III, and Lancelot, a religious zealot unaware of his sexual nature. We've cast our leads from My Fair Lady— Johnny Moreno and Monique Hafen as Arthur and Guenevere and bring back Charles Dean to play Merlin/Pelinore. Nina Ball designs the set. Think "Camelot" meets "Game of Thrones".

Date: Tuesday, August 13
Time: 7:00 pm

Cost: $30 per person



Resilience Week Organizers

Organizing Committee

- Jodi Grgich, Idaho National Laboratory
- Larry Rohrbough, UC Berkeley
- Aimee Tabor, UC Berkeley

Steering Committee

- Barrett Caldwell, Purdue University
- Marco Carvalho, Florida Institute of Technology
- Frank Ferrese, Temple University
- Milos Manic, University of Idaho
- Craig Rieger, Idaho National Laboratory
- Shankar Sastry, UC Berkeley

Resilience Week 2014

Denver, Colorado
August 19-21, 2014

As the symposium has grown, the diversity of the contributors has also expanded, precipitating a need to cultivate the individuality of these distinct areas of resilience research. Planning sessions will be held during this year's event to discuss this evolution, as well as a similar evolution of a resilient cyber systems symposium. Resilience Week will feature four symposia:

- International Symposium on Resilient Control Systems
- International Symposium on Resilient Cyber Systems
- International Symposium on Resilient Cognitive Systems
- International Symposium on Resilient Communication Systems

Resilience Week 2013

09-50094-R2