August 9-11, 2011

**4th International Symposium
on Resilient Control Systems**

ISRCS 2011

Conference Sponsors

Table of Contents

Welcome Remarks

Cheryl B. Schrader, Boise State University

Dr. Cheryl B. Schrader became Associate Vice President for Strategic Research Initiatives and Professor of Electrical and Computer Engineering at Boise State University after 27 years of leadership in academia and industry. She most recently served as Dean of the College of Engineering at Boise State University. Dr. Schrader also has served as Associate Dean for Graduate Studies and Research in the College of Sciences and the College of Engineering at The University of Texas at San Antonio, and has held positions at Rice University, Valparaiso University, Chimera Research and McDonnell Douglas Astronautics Company. Dr. Schrader has received several best paper awards; authored approximately 100 publications in the areas of systems and control, robotics, and intelligent systems, with biomedical, networking and aircraft applications; and delivered over 70 invited presentations and keynote addresses. Her grant and contract funding exceeds eleven million dollars.

The Valparaiso University Alumni Association recently conferred its prestigious Alumni Achievement Award on Dr. Schrader, and named her one of the 150 Most Influential People in the history of the university during its 150th anniversary celebration. In 2005 the White House presented Dr. Schrader with The Presidential Award for Excellence in Science, Mathematics, and Engineering Mentoring for an enduring, strong and personal commitment to underrepresented engineering students and faculty. Other awards include the Hewlett-Packard/Harriett B. Rigas Award from the Institute of Electrical and Electronics Engineers (IEEE) Education Society in recognition of her contribution to the profession; Idaho Women Making History Award from the Women's Center for extraordinary accomplishments that change the face of Idaho; Exemplary Online Course Award from WebCT for teaching abstract concepts online; Engineering Excellence Award from Steven Myers & Associates for excellence in engineering; and the 40 Under 40 Rising Stars Award from the San Antonio Business Journal for leadership, career success and community involvement.

Dr. Schrader currently serves on the Board of Directors for the Discovery Center of Idaho, the Board of Directors for the Boise Valley Economic Partnership, and the Advisory Board for Highway 12 Ventures. She is a Past President of the IEEE Control Systems Society, a professional organization with 9,000 members worldwide. For her many contributions to the Society, she received its Distinguished Member Award. She is a member of five societies of the IEEE, American Society for Engineering Education, Society of Women Engineers, and Tau Beta Pi.

Dr. Schrader completed her PhD and MS degrees in control systems at the University of Notre Dame and received her BS degree in electrical engineering with high distinction from Valparaiso University, where she was an honors college graduate.

Enabling a Resilient and Secure North American Electric Power Grid

Massoud Amin, University of Minnesota

Abstract

Planning has already begun to replace much of the antiquated electric infrastructure of the current power grid with digital systems providing the grid with the capability to reconfigure itself and prevent widespread outages. This transformation of the end-to-end power grid to a digitalized, intelligent, self-healing system presents many new modeling, sensing, communications, and control challenges that must be addressed before extensive deployment can begin. Increasing the security, robustness, and efficiency of electric power infrastructure requires utilizing these automation technologies in order to continually assess and optimize system performance.

For deeper and layered protection, an intelligent distributed secure control is required, which would enable parts of the network to remain operational and even automatically reconfigure in the event of local failures.

With communication technologies providing a system-wide integration infrastructure, the smart grid will represent a prototypical "system of systems." Multiple and often conflicting criteria will need to be coordinated: profits, grid reliability, environmental impacts, equipment constraints, policies, technologies and consumer preferences.

Furthermore, upgrading the power grid presents many new security challenges. The digitalization of the electric grid may enable remote attacks to grow rapidly, potentially spanning countries or even continents. While digitalization of the electric grid will present many new security challenges, it will also provide the gird with increased flexibility and possibly added resilience to prevent and withstand potential threats.

In this keynote we shall focus on the advances, challenges and opportunities for control systems to enhance the resilience and security of the infrastructure.

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 more than 24 technologies transferred to industry. He is the author or co-author of more than 190 peer reviewed research papers, and is the editor of seven collections of manuscripts.

Making the Concepts of Robustness, Resilience and Sustainability Useful Tools for Power System Planning, Operation and Control

Lamine Mili, Virginia Tech

Abstract

Advances in power electronics, computer and communications have opened new avenues for the monitoring, control and protection of critical infrastructures. For instance, the advent of low-cost computer-based sensors and actuators together with wireless communications devices are making possible the development of a new form of control based on multiagent technologies. If the latter are endowed with the ability to take collective actions geared toward a common goal, then control actions exhibiting emergent properties may result. Another level of complexity is attained if the common goal is defined by the agents themselves as a response to an environment evolving in an unexpected way. In this talk, we will define the concepts of robustness, resilience and sustainability for critical infrastructures and we will outline a future research agenda that fosters a paradigm shift in interacting electric power and communications systems using multiagent technologies, microgrids, and power electronic interfaces. Furthermore, in contrast with the definitions of robustness and resilience given in ecology or in complex systems, which are inclusive to each other in that robustness includes resilience or vice versa, we argue that for designed systems such as infrastructures, the definitions of these two concepts should be distinct from each other to become a useful tool during the design/planning process. The robustness of a system to a given class of perturbations is defined as the ability of this system to maintain its function when it is subject to a set of perturbations of this class, which may induce changes in its structure. By contrast, the resilience of a system to a class of unexpected extreme perturbations is defined as the ability of this system to (i) gracefully degrade its function by altering its structure in an agile way when it is subject to a set of perturbations of this class and (ii) quickly recover it once the perturbations have ceased.

Bio

Professor Lamine Mili received an Electrical Engineering Diploma from the Swiss Federal Institute of Technology, Lausanne, in 1976, and the Ph. D. degree from the University of Liege, Belgium, in 1987. He is presently a Professor at the Bradley Department of Electrical and Computer Engineering and a Program Director at the Northern Virginia Center of Virginia Tech. He worked at the Planning Department and the Test and Meter Laboratories of the Tunisian electric utility, STEG, in Tunisia, from 1976 till 1981. Dr. Mili is a co-founder and co-editor of the International Journal of Critical Infrastructures. His research interests include risk management of catastrophic failures in complex networks, enhancement of the resilience and sustainability of coupled electric power and communications systems, distributed and coordinated control of large-scale systems, bifurcation theory in electric power systems, and robust statistics as applied to signal processing.

Wrestling With Reality -- Integrating New Security Solutions into Existing Control Systems

David M. Nicol, University of Illionois, Urbana-Champaign

Abstract

One of the more significant challenges we face when developing security solutions for existing control systems is to integrate with the existing culture, technology, and users.

This talk touches on some of the issues we've encountered working with industry to extend their product lines, developing next generation security solutions for their existing customers. The issues are made concrete in the context of extending Role-based Access Control mechanisms to existing control systems, where we find that some of the hardest constraints faced aren't technical.

Bio

William David M. Nicol is Professor of Computer and Electrical Engineering at the University of Illinois, Urbana-Champaign, where he also serves as the Director of the Information Trust Institute.

Previously he held faculty positions at the College of William and Mary, and Dartmouth College. His research interests include high performance computing, simulation modeling and analysis, and security. He was elected Fellow of the IEEE, and Fellow of the ACM for his contributions in these areas. He is co-author of the widely used textbook "Discrete-Event Systems Simulation", and was the inaugural awardee of the ACM Special Interest Group on Simulation's Distinguished Contributions Award, for his contributions in research, teaching, and service in the field of simulation.

Towards a Theory of High Confidence Networked Control Systems: Action Webs

S. Shankar Sastry, University of California, Berkeley

Abstract

There has been a great deal of excitement in recent years concerning the evolution of sensor webs. There has been very substantive active worldwide activity in this area and in particular at Berkeley. There have now been over six generations of "motes" for these sensor webs, and several new start ups have arisen to commercialize these developments.

The primary use of sensor networks to date has been on information gathering and threshold detection. However, it is fair to say that the greatest impact of sensor webs will be from what we call Action Webs, involving "closing the loop" around these networked embedded systems. We believe that this closing the loop brings into sharp focus the real time constraints issues inherent in the use of networked embedded systems. A very large number of societal scale systems such as physical infrastructures, energy and building infrastructures are now being instrumented by these Action Webs. Consequently the use of Action Webs in these Cyber Physical Systems will need the high confidence attributes of robustness, fault tolerance and resistance to cyber attacks.

In this talk I will provide the rudiments of a theory for modeling confidentiality, integrity and availability attackers on action webs and tools for defending them in depth.

Further, we will discuss how we can provide economic incentives to the private entities which own individual action webs to address the issues of "under investment in the common good." More technically, this is a procedure for helping bridge the gap between the non-cooperative Nash equilibrium of multiple players and the societal optimum strategy. The work is primarily based on the doctoral dissertation of Dr. Saurabh Amin and joint work with Dr. Galina Schwartz.

Bio

S. Shankar Sastry is currently the Dean of Engineering at University of California, Berkeley. From 2004 to 2007 he was the Director of CITRIS (Center for Information Technology in the Interests of Society) an interdisciplinary center spanning UC Berkeley, Davis, Merced and Santa Cruz. In February 2007, he was appointed the faculty director of the Blum Center for Developing Economies. He has served as Chairman, Department of Electrical Engineering and Computer Sciences, University of California, Berkeley from January 2001 through June 2004. From 1999-early 2001, he served as Director of the Information Technology Office at DARPA. From 1996-1999, he was the Director of the Electronics Research Laboratory at Berkeley.

Dr. Sastry received his Ph.D. degree in 1981 from the University of California, Berkeley. He was on the faculty of MIT as Asst. Professor from 1980-82 and Harvard University as a chaired Gordon Mc Kay professor in 1994. Most recently he has been concerned with cybersecurity and critical infrastructure protection, and has helped establish an NSF Science and Technology Center, TRUST (Team for Research in Ubiquitous Secure Technologies).

He has coauthored over 400 technical papers and 9 books. He is currently an Associate Editor of the IEEE Proceedings.

Emerging Computational Methods for Smart Grid

G. Kumar Venayagamoorthy, Missouri University of Science and Technology

Abstract

The smart electric power grid will evolve into a very complex adaptive system under semi-autonomous distributed control. Its spatial and temporal complexity, non-convexity, non-linearity, non-stationarity, variability and uncertainties exceed the characteristics found in today's traditional power system. The distributed integration of intermittent sources of energy and plug-in electric vehicles to a smart grid further adds complexity and challenges to its modeling, control and optimization. Innovative technologies are needed to handle the growing complexity of the smart grid and stochastic bidirectional optimal power flows, to maximize the penetration of renewable energy, and to provide maximum utilization of available energy storage, especially plug-in electric vehicles.
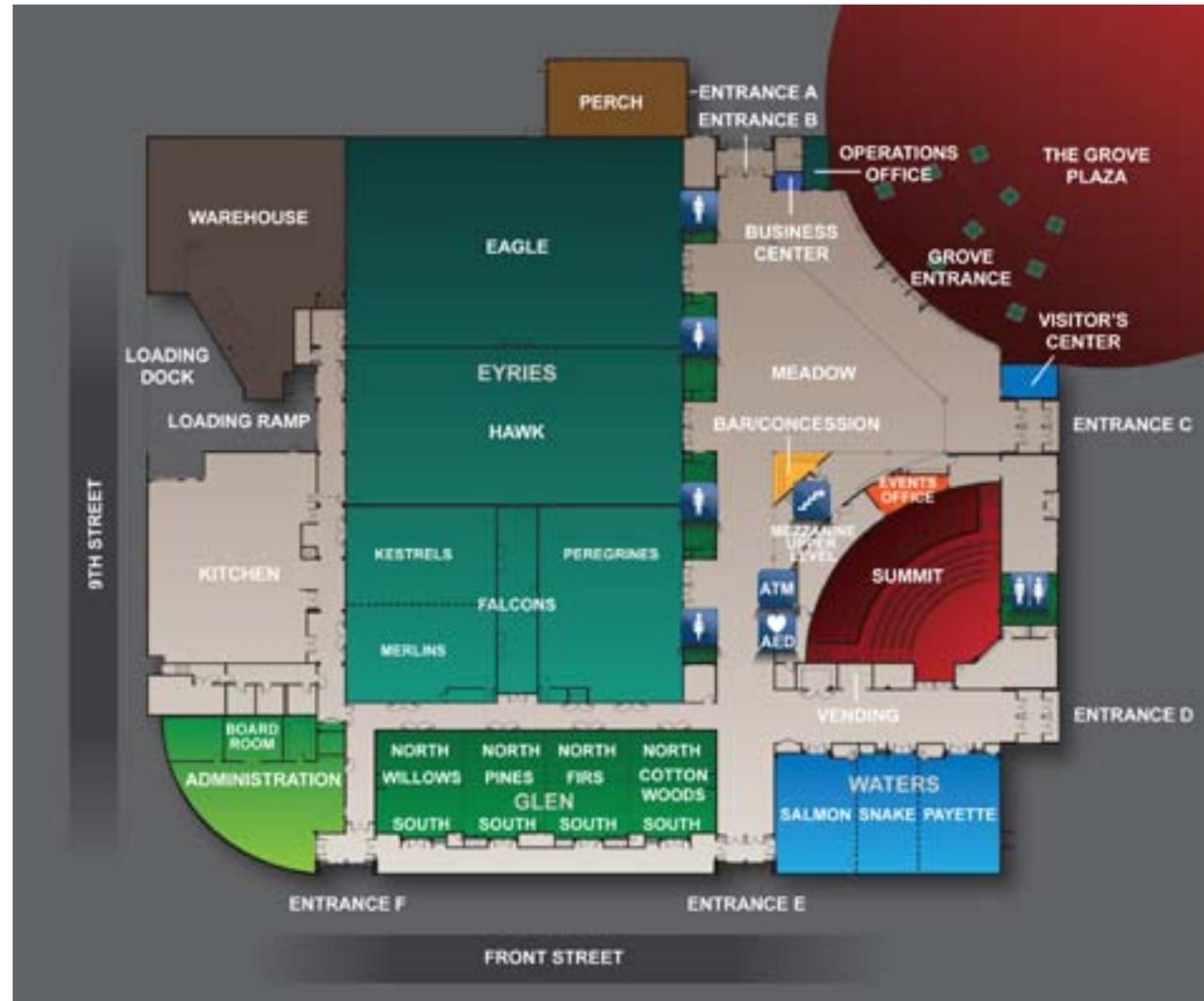
Smart grids will need to be monitored continuously to maintain stability, reliability and efficiency under normal and abnormal operating conditions and disturbances. A combination of capabilities for system state prediction, dynamic stochastic power flow, system optimization, and solution checking will be necessary. The optimization and control systems for a smart-grid environment will require innovative computational paradigms to handle the uncertainties and variability that exist. Emerging computational paradigms and methods that enable dynamic, stochastic, and scalable technologies, and needed for sense-making, situational awareness, control and optimization in smart grids will be presented in this keynote.

Bio

Professor Ganesh Kumar Venayagamoorthy received his Ph.D. degree in electrical engineering from the University of Natal, Durban, South Africa, in 2002. He is the Founder and Director of the Real-Time Power and Intelligent Systems (RTPIS) Laboratory at Missouri University of Science and Technology (Missouri S&T), and has been recently promoted to Professor of Electrical and Computer Engineering, effective September 1, 2011. He was a Visiting Researcher with ABB Corporate Research, Sweden, in 2007. His research interests are in the development and applications of advanced computational algorithms for real-world applications, including power systems stability and control, smart grid applications, sensor networks and signal processing. He has published 2 edited books, 6 book chapters, and more than 90 refereed journal papers and 290 refereed conference proceeding papers.

Dr. Venayagamoorthy is a recipient of several awards including a 2008 US National Science Foundation (NSF) Emerging Frontiers in Research and Innovation Award, a 2007 US Office of Naval Research Young Investigator Program Award, a 2004 NSF CAREER Award, the 2010 Innovation Award from St. Louis Academy of Science, the 2010 IEEE Region 5 Outstanding Member Award, the 2006 IEEE Power and Energy Society Outstanding Young Engineer Award, the 2005 South African Institute of Electrical Engineers (SAIEE) Young Achievers Award, a 2008, 2007 and 2005 Missouri S&T Faculty Excellence Award and a 2009 Missouri S&T Faculty Research Award.

Tuesday, August 9 - *Tutorials & Workshops*

Time				
8:00 a.m.	**Registration**			
8:15 a.m.	**Welcome and Opening Remarks** Welcome: Cheryl Schrader, BSU Introductions & Logistics: Margie Jeffs (Summit)			
8:30 a.m.	**Emerging Computational Methods for Smart Grid** G. Kumar Venayagamoorthy, Missouri Science & Technology (Summit)			
9:30 a.m.	**Morning Break**			
10:00 a.m.	**Session 1:** Tutorials & Workshops			
	Experimental Security Panoramas Workshop (Willows) Chairs: Miles McQueen, INL Annarita Giani, UC Berkely Detailed schedule, pg. 26	**Building Resilience through the Art of Maneuver: Architectures for Polycentric Governance** (Payette) David Woods, The Ohio State University	**Workshop on Game Theoretic Approach to Network Security and Reliability (SS05)** (Salmon) Galina Schwartz & Saurabh Amin, UC Berkeley	**ReSia Technical Committee** (Snake) Chair: Milos Manic, University of Idaho
11:30 a.m.	**Hosted Lunch**	**Lunch Break** - No Host		
1:00 p.m.	**Session 2:** Tutorials & Workshops			
	Detailed schedule, pg. 26	**Continuation of Tracks**		**ReSia Technical Committee** (continued)
2:30 p.m.	**Afternoon Break**			
3:00 p.m.	**Session 3:** Tutorials & Workshops			
3:30 p.m.	**Detailed Schedule, pg. 26**	**Round Table Discussion: Communicating Perspectives on Resilience** Chair: Ronald Boring, INL	**Continuation of Track**	**Tutorial on Quantitative Methods for Resilient Control Systems** (Snake) Quanyan Zhu, U. of Illinois Dong Wei, Siemens
4:30 p.m.	**Adjourn**			
6:30 p.m.	**Shakespeare Festival**			

Wednesday, August 10 - *Papers & Presentations*

8:15 a.m.	**Opening Remarks** Daily Agenda: Margie Jeffs (Summit)		
8:30 a.m.	**Towards a Theory of High Confidence Networked Control Systems: Action Webs** Shankar Sastry, UC Berkeley (Summit)		
9:30 a.m.	**Morning Break**		
	Special Session: Resilient Control of Shipboard Systems (Snake)	**Track 1: Complex Network Control Systems** (Payette)	**Track 2: Cyber Awareness** (Willows)
10:00 a.m.			
10:20 a.m.		**Resilient Control System University Challenge** Facilitator: Craig Rieger, INL	
10:40 a.m.			
11:00 a.m.			
11:30 a.m.	**Hosted Lunch** **Enabling a Resilient and Secure North American Electric Power Grid** Massoud Amin, University of Minnesota		

Opening Remarks Daily Agenda: Margie Jeffs (Summit)		
Towards a Theory of High Confidence Networked Control Systems: Action Webs Prof. Shankar Sastry, UC Berkeley (Summit)		
Morning Break		
Track 3: Human Systems (Pines)	**Track 4: Data Fusion** (Salmon)	**Track 5: Robotics** (Salmon)
Tutorial: **Complexity, Robutstness, and Sociotechnical Systems Modeling** Chairs: Barrett Caldwell and Venkat Venkatasubramanian, Purdue University		*Addressing the Top 3 Challenges in Robotics Development* Brian Powell, National Instruments *Architectures and Platforms for Resilient Robotics* Derek Wadsworth, INL *Increasing the Resilience of Autonomous Robots by Keeping Humans in the Loop* William Smart, Washington University *Passive and Active Techniques for Resilient Control of Ground Vehicle Systems* Mark Minor, U. of Utah
Hosted Lunch **Enabling a Resilient and Secure North American Electric Power Grid** Massoud Amin, University of Minnesota		

Wednesday, August 10 - *Papers & Presentations*

	Special Session: Resilient Control of Shipboard Systems (Snake)	Track 1: Complex Network Control Systems (Payette)	Track 2: Cyber Awareness (Willows)		Track 3: Human Systems (Pines)	Track 4: Data Fusion (Salmon)	Track 5: Robotics (Salmon)
1:00 p.m.	*Reference-free Detection of Spike Faults in Wireless Sensor Networks* Jerome Lynch, University of Michigan	*Supervisory Control of a Pilot-Scale Cooling Loop* Kris Villez, Purdue University	*A Hierarchical Security Architecture for Cyber-Physical Systems* Quanyan Zhu, University of Illinois		**Tutorial** (continued) Chairs: Barrett Caldwell and Venkat Venkatasubramanian, Purdue University	*Correction of Erroneously-Trained Adaptive Neural Networks* Reza Khosravani, American University of Dubai	
1:20 p.m.	*Fuel Optimization Under Quality of Service Constraints for Shipboard Hybrid Electric Drive* Sudipta Lahiri, Drexel University	*Remote Output Feedback Stabilization for Fractional-Order Systems via Communication Networks* YangQuan Chen, Utah State University	*Towards Resilient Critical Infrastructures: Application of Type-2 Fuzzy Logic in Embedded Network Security Cyber Sensor* Ondrej Linda, University of Idaho			*Aggregation of Heterogeneous Units in a Swarm of Robotic Agents* Manish Kumar, University of Cincinnati	
1:40 p.m.	*Multi-agent Based Federated Control of Large-Scale Systems with Application to Ship Roll Control* Qing Dong, Temple University	*Resilient Monitoring System: Design and Performance Analysis* Humberto Garcia, INL	*Co-Active Emergence for Human-Automation Cyber Security Awareness* Marco Carvalho, Institute for Human and Machine Cognition			*Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine* Ondrej Linda, University of Idaho	
2:00 p.m.	*Decentralized Agent-based Control of Chilled Water Plants using Wireless Sensor and Actuator Networks* Jerome Lynch, University of Michigan	*Resilient Design of Recharging Station Networks for Electric Transportation Vehicles* Kris Villez, Purdue University				**Work In Progress**	
2:30 p.m.	**Afternoon Break**				**Afternoon Break**		

Wednesday, August 10 - *Papers & Presentations*

	Special Session: Resilient Control of Shipboard Systems (Snake)	Track 1: Complex Network Control Systems (Payette)	Track 2: Cyber Awareness (Willows)	Track 3: Human Systems (Pines)	Track 4: Data Fusion (Salmon)	Track 5: Robotics (Salmon)
3:00 p.m.	*A Measure of Observability for Multi-converter Shipboard Power Systems* Chika Nwankpa, Drexel University	*Distributed Multi-Agent Microgrids: A Decentra-ized Approach to Resiient Power System Self-Healing * Chris Colson, Montana State University	*Towards Flexible, Distributed Autonomy* Barrett S. Caldwell, Purdue University	*Toward Providing Guideance for Porcedure Design: Formal Definitions of Procedure Characteristics* Steven Landry, Purdue University		**Round Table Discussion** *Defining Resiliency in Robotics: Planning for Failure*
3:20 p.m.	**Work in Progress**	*High Quality Integration of Alternate Energy Sources into Electric Power Grids* Osama Mohammed, Flordia International University	*Information Sharing Issues with Control System Security Incident Reports* Paul Thompson, Dartmouth College	*Measuring Situation Awareness in Representative Process Control Environment* Nathan Lau, University of Toronto		**Chair:** Brian Powell, National Instruments **Panelists:** • Derek Wadsworth, INL
3:40 p.m.		**Work in Progress**	*Adaptive Bio-Inpired Resilient Cyber-Physical Ssytems: R&D Prospective* Frederick Sheldon, Oak Ridge National Laboratory	*Information Foraging Theory for Control Room Resilience* Ronald Boring, INL		• William Smart, Washington University at St. Louis • Mark A. Minor, University of Utah
4:00 p.m.			*First Experimental Security Panora-mas Workshop: A Need for Improved Experimentation?* Miles McQueen, INL Annarita Giani, UC Berkeley			• YangQuan Chen, Utah State University
4:30 p.m.	**Poster Session**			**Poster Session**		
6:00 p.m.	**Hosted Dinner with Keynote Presentation** **Wrestling with Reality: Integrating New Security Solutions into Existing Control Systems** David Nichol, University of Illinois Urbana-Champaign			**Hosted Dinner with Keynote Presentation** **Wrestling with Reality: Integrating New Security Solutions into Existing Control Systems** David Nichol, University of Illinois Urbana-Champaign		

* Symposium Best Paper

Thursday, August 11 - *Panel Discussion*

Time	Event
8:15 a.m.	**Opening Remarks** Daily Agenda: Margie Jeffs
8:30 a.m.	**Making the Concepts of Robustness, Resilience, and Sustainability Useful Tools for Power System Planning, Operation and Control** Lamine Mili, Virginia Tech (Summit)
9:30 p.m.	**Morning Break**
10:00 a.m.	**Panel Discussion** **Smart Grid Resilience and Cyber Security: What are the issues and how do we address them?** (Summit) Chair: Marco Carvahlo, Institute for Human and Machine Cognition
11:50 p.m.	**Concluding Remarks** Margie Jeffs: Thanks and next year
	Optional Afternoon Tour Tour of Hewlett-Packard Usability Labs Facilitator: Ron Boring, INL

Friday, August 12 - Train Ride and River Rafting Trip

Time	Event
10:30 a.m.	Bus Departs from Downtown Boise
11:30 a.m.	Arrive at Horseshoe Bend
11:30 a.m.	Scenic Train Ride
1:00 p.m.	**Lunch**
2:00 p.m.	Whitewater Rafting/Train Ride Back to Horseshoe Bend
4:00 p.m.	Bus Leaves Horseshoe Bend for Downtown Boise
5:00 p.m.	Van Picks Up Rafters and Returns to Downtown Boise

Tuesday, August 9

Experimental Security Panoramas (ESP) Workshop

Chairs: Miles McQueen, Idaho National Laboratory
Annarita Giani, UC Berkeley

A detailed schedule and workshop descirption of the Experimental Security Panoramas Workshop is available on page 26.

Resilience and Security for Industrial Applications (ReSia) Technical Committee Establishment

Chair: Milos Manic, University of Idaho
Co-chair: Michael Condry, Intel Corporation
Secretary: Craig Rieger, Idaho National Laboratory

During these meetings, prior working group charter attributes will be refined for the ReSia Technical Committee proposal, which will be presented to the next administrative committee (AdCom) meeting of the IEEE Industrial Electronics Society (IES).

Special Session 3: Tutorial on Quantitative Methods for Resilient Control Systems

Chair: Quanyan Zhu, University of Illinois at Urbana-Champaign
Co-chair: Dong Wei, Siemens Research

The integration of the cyber-computing with the physical control systems in many critical infrastructures brings a multitude of security and resilience issues at the cyber and physical interface. This session gives a tutorial on the emerging quantitative methods used to study these issues, which are fundamental and essential for the analysis and design of resilient systems. This session surveys the proposed metrics and heuristic methods for assessing the resilience and security metrics of control systems in the literature as well as in practice. Security is a pivotal aspect of resilience. We introduce concepts from game theory and their applications in network security and privacy. The game-theoretic modeling provides insights to the optimal defense mechanisms, attacker incentives and performance limits. The recent development from the game-theoretical perspective offers emerging opportunities for the system-wide assessment of large-scale systems. The session concludes with recent results and future work.

Special Session 10: Building Resilience through the Art of Maneuver: Architectures for Polycentric Governance

Chair: David Woods, The Ohio State University

Investigations into complex adaptive systems (CAS) have identified multiple trade-offs that place hard limits on the behavior of adaptive systems of any type (Alderson and Doyle, 2010). Resilience Engineering (RE) also arose from the recognition that basic trade-offs placed hard limits on the safety performance of teams and organizations in the context of pressures for these systems to be "faster, better, cheaper" (Woods, 2006; Hollnagel, 2009). The question to be answered is: what kinds of control architectures allow multi-scale interdependent networks dynamically balance the conflicts, risks and pressures that arise from the fundamental trade-offs--the problem of what are resilient control strategies?

Round Table Discussion: Communicating Perspectives on Resilience

Chair: Ronald L. Boring, Idaho National Laboratory

A roundtable discussion on how industry, academia, and government human factors groups understand, implement, and communicate resilience throughout their organizations. The roundtable will offer the opportunity to learn from experts how resilience is used and what challenges there are in putting resilience concepts into practice.

Panelists:

David Woods- The Ohio State University

Barrett Caldwell- Purdue University

David Gertman- Idaho National Laboratory

Michael Hildebrandt- Halden Reactor Project

Special Session 5: Workshop on Game Theoretic Approach to Network Security and Reliability

Chairs: Galina A. Schwartz, TREAT, UC Berkeley
Saurabh Amin, TREAT, UC Berkeley
S. Shankar Sastry, TREAT, UC Berkeley

This session will focus on research ideas for analyzing and improving security and reliability of interdependent infrastructure networks. We will discuss the progress made over the past year at the TRUST Science and Technology Research Center in applying game theoretic tools to security assessment and improvement. Topics include security and reliability metrics for large-scale networks, analysis of network interdependencies, managing residual risks for critical infrastructure systems, and incentive mechanisms for security.

Wednesday, August 10

Special Session 4: Resilient Control of Shipboard Systems

Chair: Frank Ferrese, Naval Surface Warfare Center, Carderock Division
Co-Chair: David Scheidt, Johns Hopkins Applied Physics Lab

Naval systems are becoming increasingly complex, with mission success depending on the correct operation of in excess of 20,000 coupled components. Because naval platforms are placed in harm's way, this control of ship systems is confounded, requiring shipboard systems address multiple, unpredictable component failures. Even when damaged, ships are required to function, therefore shipboard systems need to be resilient, managing complex damage events in real time. In situ sensor and communications equipment are also subject to damage shipboard system control infrastructures must themselves be resilient. Also, reduced workload and manning

commitments limit the availability of human operators, forcing ship systems to address damage events autonomously. This session will focus on research that enables resilient ship systems.

Track 1: Complex Control System Networks

Track Chair: YangQuan Chen, Utah State University
Track Co-chair: Charles Tolle, South Dakota School of Mines and Technology

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. 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.

Special Session 1: Smart Grid

Chair: John Gardner, Boise State University

In terms of complexity, spatial distribution and importance, the electric distribution grid is arguable the most important network in the history of civilization. The integration of information exchange and automatic control to the grid (i.e the Smart Grid) brings with it the potential for great benefits to society but with that brings increased potential for catastrophic failures. This session addresses the Smart Grid in the context of resilient control theory. Topics include Smart Grid, integration of intermittent generation, fault detection and resilient control of distributed networks.

Track 2: Cyber Awareness

Track Chair: Eugene Santos, Dartmouth College
Track Co-chair: Marco Carvalho, Institute for Human and Machine Cognition

Because of the human element of a malicious actor, traditional methods of achieving reliability cannot be used to characterize cyber awareness and resilience. Dynamic mechanisms of probabilistic risk analysis that can link human reliability with the system state are still maturing. The intellectual level and background of the adversary makes stochastic methods unusable due to the variability of both the objective and the motives. In addition, the strength of the adversary is increased because the existing control system architecture is not random, and response characteristics are reproducible. Therefore, a resilient design can find strength in similar fashion by becoming atypical of normal control system architectural design, and appearing random in response and characteristics to the adversary.

Special Session 7: Collaborative Approach to Systems Resilience

Chairs: Eugene Santos, Dartmouth College
Marco Carvalho, Institute for Human and Machine Cognition

The security and resilience of our critical infrastructures depend on our ability to effectively monitor, understand and control large cyber physical systems (CPS). Large volumes of data associated with very short time scales have traditionally demanded the extensive use of automation and abstract visualizations for cyber situation awareness and response. In most cases, the roles and responsibilities attributed to humans (analysts) and autonomous systems have been fixed by design, with little flexibility for online changes in operational context and unexpected situations. Collaborative Human-Automation control infrastructures are likely to be more resilient, and may enable the new capabilities that may change the future of CPS security. In this session we will bring together experts from different areas and backgrounds to present and discuss their views in collaborative approaches for large-scale systems resilience.

Track 3: Human Systems

Track Chair: Barrett Caldwell, Purdue University
Track Co-chair: Nathan Lau, University of Toronto

The human ability to quickly understand novel situations, employ heuristics and analogy can provide additional control system resilience. On the other hand there are situations in which we may have a general inability to reproducibly predict human behavior. This may be true in situations of fatigue or high stress or decision making under high levels of uncertainty. Bayesian methods provide one method by which to take into account evidence regarding human response, but this is one among many approaches. The literature in human reliability analysis provides an orientation regarding ergonomics, workload, complexity, training, experience, etc., which may be used to characterize and quantify human actions and decisions.

Special Session 9: Tutorial on Integrating Human Performance Concerns in RCS Systems Engineering Analysis

Chairs: Barrett Caldwell, Purdue University
Nathan Lau, University of Toronto

Although there is a long history of systems engineering tools and attempts to model human and system performance in complex task environments, many of these tools address the "human factor" using simplistic or inappropriate assumptions. Realistic studies of human performance may consider issues of appropriate and inappropriate noncompliance with procedures; non-rational elements of information sharing and decision making; impacts of human expertise on system recovery (and not only human error); and the interplay of human factors and system simulation topics. Topics include System of systems engineering; human factors influences on simulation and system dynamics; human performance and recovery from system degradation; knowledge sharing and distributed expertise; digital human modeling of cognitive and team performance; simulation-informed human factors research design.

Track 4: Data Fusion

Track Chair: Devendra Garg, Duke University
Track Co-chair: Manish Kumar, University of Cincinnati

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.

Special Session 2: Multi-Sensor Fusion and Cooperative Robot Control

Chair: Devendra Garg, Duke University
Co-chair: Manish Kumar, University of Cincinnati

With the increasing need for resilience, flexibility, efficiency, performance, product diversity and accuracy, modern control systems are required to operate in an inherently complicated, uncertain, and dynamic world. Consequently, these systems are complex networks of sensors, machines, and other resources. Two of the most critical issues in these systems include fusion of information to develop consistent knowledge, and cooperative control of resources for optimizing metrics such as plant throughput.

Track 5: Robotics Applications

Track Chair: William Smart, Washington University
Track Co-chair: Timothy McJunkin, Idaho National Laboratory

The nature of the various data types associated with proper operation or performance of critical infrastructure, including cyber and physical security, process efficiency Resilience is the ability for a system to regain its "shape" to some degree: for a system to retain functionality to the extent possible when a disruption occurs. In robotics, resilience may take on many connotations and forms. The resilience of a system can be analyzed from the perspective of the effect that various disruptions have on the system and what the desired outcome in the presence of the disturbance may be. The strategy for achieving that outcome is the design element of resilience in robotics. To achieve resilient robotics systems, designers, vendors and researchers will consider hardware, control systems (including humans in the loop), and algorithms for producing outcomes within bounds of operational success and safety of equipment, facilities, and people. Awareness of the degree of degradation and the probability of operational success is a goal of resilience from a supervisory and stake holder perspective.

Special Session 8: Resilient Control of Robots in Complex Networks

Chair: Brian Powell, National Instruments
Co-chair: Tim McJunkin, Idaho National Laboratory

Increasingly networked components of robotic systems yield a control problem where fully characterizing the system as a whole becomes a daunting task during design and deployment. Consideration of the effects of latencies and disconnects in the initial design becomes a key ingredient to creating a successful resilient architecture. For systems that have grown organically the analysis and retrofit is again difficult. Producing designs that may continue to function when communication is slowed or severed or methods for analyzing the hazards of deteriorating conditions provides the basis for resilient designs or measures of the resilience of a networked robotic system.

Panel Discussion

Smart Grid Resilience and Cyber Security: What are the Issues and How Do We Address them?

Abstract: Smart grid technologies are gaining significant attention in the modernization of the national electric grid. Central to concept of smart grids is the coordinated use of advanced electricity transmission, distributed generation and data communication technologies to maintain a reliable, efficient and secure electricity infrastructure. While a deep integration of renewable energy poses a threat to reliability, the use of storage and responsive load may be used to mitigate the uncertainty introduced by renewable generation. The goal of 20% wind energy by 2030 in the US shows how aggressive the electricity market is in relation to renewable energy and how serious the problem of resilience must be taken.

In this panel we will discuss the security and resilience aspects of smart grids, highlighting the potential threats, vulnerabilities and consequences of smart girds technologies.

Panelists:

Marco Carvahlo - Institute for Human and Machine Cognition

Milos Manic - University of Idaho

Annarita Giani - University of California, Berkeley

David Cartes - Flordia State University

Rita Wells- Idaho National Laboratory

Fred Cohen- Fred Cohen and Associates

Lamine Mili- Virginia Tech

ESP Detailed Agenda

Time	Session
10:00 a.m.	**Morning ESP Session and Welcome** Chair: Miles McQueen
10:30 a.m.	*Scientific Experimentation for Cyber Security--Mission Impossible?* Xinming Ou, Kansas State University
11:00 a.m.	*Challenges in Cyber Security Experiments: Our Experience* Annarita Giani, University of California, Berkeley
11:30 a.m.	*The Dynamics and Threats of End-Point Software Portfolios* Stefan Frei, Secunia
12:00 p.m.	**Hosted Lunch Keynote** (Workshop Attendees Only) **DARPA Initiatives in the Cyber Experimentation Domain** David Robinson, Air Force Institute of Technology
1:00 p.m.	*Security Science and Measurement* Fred Cohen, Fred Cohen & Associates
1:30 p.m.	*Information Markets for Security Experiments and Metrics* George Cybenko, Dartmouth College
2:00 p.m.	*Effectiveness of Information Disclosure* Rahul Telang, Carnegie Mellon University
2:30 p.m.	**Afternoon Break**
3:00 p.m.	*Panel on Security and Recovery Challenges in Industry Systems* Michael Condry, Intel Corporation
4:30 p.m.	**Workshop Adjourns**

Experimental Security Panoramas (ESP)

Sponsored by INL Cyber Security Research, Experimental Security, and Instrumentation, Control, and Intelligent Systems (ICIS) groups

Chairs: Miles McQueen, Idaho National Laboratory
Annarita Giani, University of California Berkeley

In general, scientific experimentation refers to the iterative process of observation, hypothesis formation, test and measurement, followed by assessment. Experiments may be executed in tightly controlled settings such as an experimental network in a laboratory, or consist of observational studies of a phenomena in the naturally occurring eco system. The ESP workshop will focus on all forms of experimentation which relate to cyber system security including both software and human vulnerabilities.

Workshop Format

This first workshop will consist of a set of invited cyber security and experimentation presentations followed by open discussion. The breadth of cyber security experimentation will be explored with some focus on defining the needs and possibilities for improvement in the use of experiments in cyber security. At the end of the workshop the need, focus, and form of the 2nd ESP workshop--to include the solicitation and selection of research papers--will be drafted. The workshop will provide lunch for all participants.

Workshop Keynote

DARPA Initiatives in the Cyber Experimentation Domain

David J. Robinson, Lt. Col., USAF
Defense Advanced Research Projects Agency

Abstract

The focus of this talk will be to address DARPA's role in enhancing the CNCI through advanced testing and experimentation operations. The presentation will focus on the National Cyber Range initiative and how technologies from this program may be used to produce qualitative and quantitative assessments of the Nation's cyber research and development technologies.

Bio

Dr. David J. Robinson is a deputy Program Manager at the Defense Advanced Research Projects Agency (DARPA) and an assistant professor of computer engineering at the Air Force Institute of Technology. He earned a Master of Science degree in Computer Engineering from the Air Force Institute of Technology in 2000, and a Ph.D. in Computer Engineering from Dartmouth College in 2010. David is an active duty Lieutenant Colonel in the United States Air Force with 18 years of service and offensive and defensive cyber related experience at operational, staff, and command levels. In 2005, he completed the National Security Agency's (NSA) premier System and Network Interdisciplinary Program, a 3-year immersion into graduate-level computer network defense/exploitation research, development and operations. He has conducted research for the NSA, United States Strategic Command, Department of Homeland Secu-

rity, Air Force Research Laboratory, Air Force Office of Scientific Research, and the Defense Advanced Research Projects Agency. His current research initiatives include quantitatively defining aspects of cyber space as it relates to the Department of Defense operations (Science of Cyber), characterization, prediction, and change detection of users cyber behaviors (cyber-based behavioral modeling), secure design of Cyber Physical Systems (CPS), and proactive network defense.quantitative assessments of the Nation's cyber research and development technologies.

Workshop Panel Discussion

Panel on Security and Recovery Challenges in Industry Systems

Michael Condry, Intel Corporation, Intel Architecture Group

Abstract

Security and Recovery are critical elements to building a sustainable industry computing infrastructure. Today we have some core technologies that are used in building security solutions and this technology base is growing. However, the diverse threats are also increasing with more aggressive attacks and more calculating than simpler outbreaks of the past. The growth of cloud connectivity to industry systems with its diversity of devices (many not secured) has even expanded these risks. Finally, the existence of security and recovery technologies does not imply their adoption across the products in the cloud; allowing for exposures to industry systems using unexpected sources such as consumer devices.

This session overviews the core technologies in security and recovery, and then examines some of the data on vulnerabilities that groups including NIST are tracking. It

also observes the lack of adoption of security technologies and the key elements that appear to be causing this lack of adoption including scientific based metrics, usability, market conditions, and user understanding.

After an introduction scoping the problem space and challenges the session will move to a panel where its members will discuss their views and supporting data to the different aspects of security and recovery, with a particular emphasis on experimentation and its impact on security solution development and adoption.

Bio

After receiving his Ph.D. from Yale University Computer Science in 1980, Michael's career has followed a mixture of academic and industry positions, mostly industry. He had teaching and research positions at Princeton and University of Illinois and industry roles AT&T Bell-Labs, Sun Microsystems, and Intel. His background includes projects in computer architecture, software, firmware, operating systems, networking, internet applications, and computer security. Currently, Michael is focused on challenges of adoption with security technologies and methodologies to improve how our security features are valued across the ecosystem compute continuum from cloud to client to control.

Michael is also a senior board member for the IEEE Industrial Electronics Society (IES), for IES he chairs Industry Forum conference series and co-chairs Technical Committee on standards. Michael is also a board member for the IEEE Technology Management Council.

Abstracts

Security Science and Measurement

Fred Cohen, Fred Cohen & Associates

This talk will discuss the physics of digital information and, in that context, measurement theory and actual measurements applied using the described framework.

Information Markets for Security Experiments and Metrics

George Cybenko, Thayer School of Engineering, Dartmouth

Inferences about security properties of cyber systems involve reasoning about many different types and sources of information. So-called information markets have been getting increasing attention as mechanisms for fusing different kinds of information from different sources, with the goal of more informed decision-making. Information markets have had successful impact across many domains but are rather new to cyber security.

This presentation will review several experiments that have used information markets for cyber security. A short tutorial on information markets will be given and details of the experiments will reveal lessons learned and possible paths forward.

The Dynamics and Threats of Endpoint Software Portfolios

Stefan Frei, Secunia

In this talk we look at the evolution of the security threats and the complexity of keeping a typical end-user's PC and organizations secure over the last five years. The study is based on data from more than 3.5 million users

of the Secunia Personal Software Inspector (PSI), which provides unique insights into the distribution and dynamics of programs typically present on end-user PCs, and corporate software portfolios. Analyzing the data, we find an alarming development - vulnerabilities affecting the portfolio of the Top-50 programs typically present on end-user PCs almost quadrupled in the last three years. Further analysis identifies third party (non-Microsoft) programs to be almost exclusively responsible for this alarming trend. Patches are found to be an effective means to escape the arms race with cybercriminals and the majority of vulnerabilities have patches ready on the day of disclosure. We quantify the dynamics of critical programs and compare patching strategies to maximize risk reduction with limited resources.

Challenges in Cyber Security Experiments: Our Experience

Annarita Giani, University of California-Berkeley

Scientific experimentations are based on observations, hypotheses and evaluation of results. Cyber security experiments present the challenge that often the ground truth is unknown so that it must be artificially created with the particular experimental purpose in mind. In this talk we present our direct experience in implementing a cyber security experiment with emphases on the challenges we faced.

Scientific Experimentation for Cyber Security -- Mission Impossible?

Xinming Ou, Kansas State University

Recently there has been significant discussion on creating a scientific foundation for cyber security. As all science disciplines, one cannot be called a science unless there

is a rigorous way to evaluate theories through controlled, repeatable experiments. Such experiments are almost non-existence in today's cyber security literature, especially in a few critical areas lacking practical solutions, such as intrusion detection and security risk estimation. A key reason for this difficulty is the human-aspects in cyber security that makes experimentation results hard to generalize, and makes it extremely difficult to obtain data for experiments.

In this talk, I will discuss our experience of carrying out experiments in the specific areas of intrusion detection and risk analysis, and share a number of key observations of what we can do in scientific experimentation for cyber security with such limitations. I will also discuss some ideas on how the research community can foster the growth of a "habit" of scientific experiments in cyber-security research, to form a virtuous circle that provides positive feedback to mitigate the challenges for experimentation in cyber security.

Effectiveness of Information Disclosure

Rahul Telang, Carnegie Mellon Unversity

This presentation will discuss the theory as well as practice of information disclosure regarding software vulnerabilities and data breaches. In particular, I will discuss the rationale for why the firms do (or do not) voluntarily disclose such information and when is it effective for society to force the firms to disclose such information. I will also discuss the role of regulations in controlling the disclosure process.

I will then highlight some empirical studies that examine the effectiveness of disclosures. In particular, I will discuss studies that examine how vulnerability disclosure affect software vendors' patch release behavior and data breach disclosures affect instances of identity thefts.

Track 1- Complex Networked Control Systems

Supervisory Control of a Pilot-Scale Cooling Loop

By Kris Villez *and Venkat Venkatasubramanian (Purdue University), Humberto Garcia and Craig Rieger (INL)*

We combine a previously developed strategy for Fault Detection and Identification (FDI) with a supervisory controller in closed loop. The combined method is applied to a model of a pilot-scale cooling loop of a nuclear plant, which includes Kalman filters and a model-based predictive controller as part of normal operation. The system has two valves available for flow control meaning that some redundancy is available. The FDI method is based on likelihood ratios for different fault scenarios which in turn are derived from the application of the Kalman filter. A previously introduced extension of the FDI method is used here to enable detection and identification of non-linear faults like stuck valve problems and proper accounting of the time of fault introduction. The supervisory control system is designed to take different kinds of actions depending on the status of the fault diagnosis task and on the type of identified fault once diagnosis is complete. Some faults, like sensor bias and drift, are parametric in nature and can be adjusted without need for reconfiguration of the regulatory control system. Other faults, like a stuck valve problem, require reconfiguration of the regulatory control system. The whole strategy is demonstrated for several scenarios.

Remote Output Feedback Stabilization for Fractional-Order Systems via Communication Networks

By Xiaona Song, Ines Tejado, and YangQuan Chen *(Utah State University)*

The problem of remote output feedback stabilization for fractional-order (FO) systems with input time-varying delay via communication networks is investigated. The order of the FO system denoted by ® considered in this paper is in the range of 0 to 2. Additionally, the network induced time-varying delay is considered as being generated by a known FO dynamic system. We design static output feedback and dynamic output feedback controller, respectively, and show how the delay dynamics can be explicitly incorporated into the Networked Control System controller design. The basic idea is to use linear matrix inequality and receding horizon control framework. We use the receding horizon method to design a stabilizing control law that sets the poles of the closedloop system. The proposed control law explicitly takes into account an estimation of the delay dynamics. Finally, numerical examples are offered to demonstrate the effectiveness of the proposed method.

Resilient Monitoring System: Design and Performance Analysis

By Humberto Garcia *(INL), Naman Jhamaria, Heng Kuang, Wen-Chiao Lin, and Semyon M. Meerkov*

This paper is devoted to the design and performance analysis of an autonomous decentralized monitoring system that degrades gracefully under natural or malicious sensor malfunctioning. Along with their measurements, the sensors are characterized by data quality, and a method for estimating process variables, based on sensor measurements and data quality, is developed. Using these estimates, the plant status assessment is carried out, and the entropy of the resulting pmf, augmented by the Kullback-Leibler divergence of sensor measurements, is used to drive the so-called rational controllers that force the monitoring system to operate in the optimal state. Along with analytical results, the paper presents numerical examples, which illustrate the system performance.

Resilient Design of Recharging Station Networks for Electric Transportation Vehicles

By Kris Villez*, Akshya Gupta, Venkat Venkatasubramanian, (Purdue University) and Craig Rieger (INL)*

As societies shift to "greener" means of transportation using electricity-driven vehicles one critical challenge we face is the creation of a robust and resilient infrastructure of recharging stations. A particular issue here is the optimal location of service stations. In this work, we consider the placement of battery replacing service station in a city network for which the normal traffic flow is known. For such known traffic flow, the service stations are placed such that the expected performance is maximized without changing the traffic flow. This is done for different scenarios in which roads, road junctions and service stations can fail with a given probability. To account for such failure probabilities, the previously developed facility interception model is extended. Results show that service station failures have a minimal impact on the performance following robust placement while road and road junction failures have larger impacts which are not mitigated easily by robust placement.

Distributed Multi-Agent Microgrids: A Decentralized Approach to Resilient Power System Self-Healing *

By Chris Colson*, M.H. Nehrir, and R.W. Gunderson (Montana State University)*

The predominance of recent self-healing power system research has been directed towards centralized command and control functions. In this paper, a decentralized multi-agent control method for distributed microgrids is introduced. Given the complexity of a large power system spanning hundreds of miles and comprised of numerous microgrids, it is potentially unrealistic to expect that centralizing total system control functions is feasible. Therefore, the authors are particularly interested in dispersing decision-making by utilizing smart microgrid control agents that cooperate during normal and emergency situations. The combination of microgrids and agent-based control can improve power system resiliency. The method described herein lays the groundwork for a comprehensive microgrid control architecture that strikes a balance between the multiple intra-microgrid objectives defined by local operator and the situational demands of the microgrid collective as part of the power system. In this way, both self-interest and cooperation

* Symposium Best Paper

can arise, allowing microgrid agents to successfully transition from normal operations to an emergency condition and back again when conditions have resolved, independent of a central supervisor. The decentralized multi-agent methods for microgrids explored in this paper help to support what may be an enabling technology of future smart grids.

High Quality Integration of Alternate Energy Sources into Electric Power Grids

By Osama Mohammed *(Florida Interntional University), Ahmed Mohamed, and Mohamed A. Elshaer*

This paper investigates different converter topologies, and their control, that can be used as an interface between fuel cells and the DC bus in a power system. As an example, the integration of fuel cells energy to the DC bus in a DC zonal electric distribution system (DC ZEDS) will be focused on. Among the two topologies presented, one is new and its performance is compared to that of the conventional boost converter. The proposed topology is a form of the boost converter that has been modified by adding some components such that an enhancement of sustainable energy integration to the system is achieved. It gives continuous output current and some other advantages over the conventional one. However, it is more complex. A prototype system has been designed and simulated in MATLAB/SIMULINK to validate the proposed technique. Moreover, it has been examined experimentally to verify the results and conclusions deduced out of the study. Both simulation and experimental results show the effectiveness of the proposed technique and its validity as a DC-DC converter for fuel cells integration to DC ZEDS and its outper-

formance over conventional DC-DC boost converters.

Track 2: Cyber Awareness

A Hierarchical Security Architecture for Cyber-Physical Systems

By Quanyan Zhu *(University of Illinois at Urbana-Champaign), Craig Rieger (INL), and Tamer Basar*

Security of control systems is becoming a pivotal concern in critical national infrastructures such as the power grid and nuclear plants. In this paper, we adopt a hierarchical viewpoint to these security issues, addressing security concerns at each level and emphasizing a holistic cross-layer philosophy for developing security solutions. We propose a bottom-up framework that establishes a model from the physical and control levels to the supervisory level, incorporating concerns from network and communication levels. We show that the game-theoretical approach can yield cross-layer security strategy solutions to the cyber-physical systems.

Towards Resilient Critical Infrastructures: Application of Type-2 Fuzzy Logic in Embedded Network Security Cyber Sensor

By Ondrej Linda, *Milos Manic, Jim alves-Foss, (University of Idaho), and Todd Vollmer (INL)*

Resiliency and cyber security of modern critical infrastructures is becoming increasingly important with the growing number of threats in the cyber-environment. This paper proposes an extension to a previously devel-

oped fuzzy logic based anomaly detection network security cyber sensor via incorporating Type-2 Fuzzy Logic (T2 FL). In general, fuzzy logic provides a framework for system modeling in linguistic form capable of coping with imprecise and vague meanings of words. T2 FL is an extension of Type-1 FL which proved to be successful in modeling and minimizing the effects of various kinds of dynamic uncertainties. In this paper, T2 FL provides a basis for robust anomaly detection and cyber security state awareness. In addition, the proposed algorithm was specifically developed to comply with the constrained computational requirements of low-cost embedded network security cyber sensors. The performance of the system was evaluated on a set of network data recorded from an experimental cyber-security test-bed.

Track 3: Human Systems

A Framework for Understanding Procedure-Following

By Deepti Surabattula *and Steven J. Landry (Purdue University)*

A framework was developed that identifies factors that influence procedure following behavior. In addition, formal definitions of the factors are introduced, as well as tradeoffs between factors that can be controlled by procedure designers.This framework, along with the formal definitions, should help enable comparisons across experiments and provide more concrete guidance for researchers and practitioners concerning the design of procedures for human-machine systems.

Track 4: Data Fusion

Correction of Erroneously-Trained Adaptive Neural Networks

By Reza Khosravani *(American University of Dubai)*

Applications of adaptive neural network models, i.e. models that are updated while they are used, are becoming more widespread. Adjustments to an adaptive model are based on a feedback which is collected while the model is in operation. The feedback is generally gathered by comparing the model output and the actual target. While changing model parameters in production can improve the performance, it comes with inherent risks. In particular, any erroneous adjustment to an online model may reduce the performance and be costly to the business. At the same time, mistakes in feedback are sometimes unavoidable. In the financial services industry for example, the target of a model may be corrected/revised at a later time. Therefore, an adaptively trained model with old data is sub-optimal unless the new revisions are taken into account.

In this paper, we investigate the effect of a faulty feedback on the performance of an e-commerce customer identification neural network model. We first investigate the impact of feedback error on an adaptive model's performance. We then examine a technique to undo the incorrect adjustments to the model by re-training the adaptive model by a corrected feedback. Our results show the majority of loss (97%) in model performance due to the feedback error is recovered by re-training the adaptive model with the new corrected data.

Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural Data Fusion Engine

By Ondrej Linda (University of Idaho) and Timothy R. McJunkin (INL)

Resilient control systems in critical infrastructures require increased cyber-security and state-awareness. One of the necessary conditions for achieving the desired high level of resiliency is timely reporting and understanding of the status and behavioral trends of the control system. This paper describes the design and development of a neural-network based data-fusion system for increased state-awareness of resilient control systems. The proposed system consists of a dedicated data-fusion engine for each component of the control system. Each data-fusion engine implements three-layered alarm systems consisting of: 1) conventional threshold-based alarms, 2) anomalous behavior detector using self-organizing maps, and 3) prediction error based alarms using neural network based signal forecasting. The proposed system was integrated with a model of the Idaho National Laboratory Hytest facility, which is a testing facility for hybrid energy systems. Experimental results demonstrate that the implemented data fusion system provides timely plant performance monitoring and cyber-state reporting.

Aggregation of Heterogeneous Units in a Swarm of Robotic Agents

By Manish Kumar (University of Cincinnati) and Devendra P. Garg (Duke University)

Formation of patterns in a system of interacting units of heterogeneous types is a self-organized behavior which is seen in many biological systems. Earlier research in this area has indicated that such pattern formation behaviors in biological cells and tissues are made possible because of difference in the adhesivity between different types of cells or tissues. Inspired by this differential adhesivity model, in our earlier research, we had presented a decentralized approach based on differential artificial potential to achieve the segregation behavior in a swarm of heterogeneous robotic agents in which agents of different types formed spatially separate clusters. In this paper, we extend that work by presenting an approach to achieve aggregation in which agents of different types get uniformly mixed with each other. The method is based on the proposition that agents of different types experience different magnitude of potential while they are interacting with the agents of different types. An analysis of the system with the proposed approach in Lyapunov sense is carried out for stability. Extensive simulation studies and numerical analysis suggest that the proposed method would lead a population of heterogeneous agents to the aggregated configuration.

Special Session 4: Resilient Control of Shipboard Systems

Reference-free Detection of Spike Faults in Wireless Sensor Networks

By Chun Lo, Jerome Lynch, and Mingyan Liu (University of Michigan)

In recent years, wireless sensor networks have been applied to many applications. These sensors are usually simple, low-cost devices, deployed in large quantities, and prone to failure. This paper presents a model-free and reference-free spike fault identification method based on pair-wise verification. When the input of a system comes from a common source, there is a linear relationship between the output of any pair of sensors. This linear relationship between sensor pairs can be obtained through training. We present a method which is able to find faulty sensors suffering from sparse spikes in their outputs by pairwise comparisons even though there is no knowledge of which sensor is normal or abnormal, and no knowledge of the common input. The performance and limitations of the algorithm are discussed. Simulation results show that our algorithm has good performance, even when the spike fault power is comparable to the output signal power or observation noise power.

Fuel Optimization Under Quality of Service Constraints for Shipboard Hybrid Electric Drive

By Sudipta Lahiri, Karen Miu, Harry Kwatny (Drexel University) and Gaurav Bajpai, Adam Beytin, Jaymit Patel (Techno Sciences Inc.)

This paper presents an approach to optimize fuel costs of a hybrid electric ship propulsion system under different mission considerations. The static optimization problem is to commit and dispatch the generation sources such that fuel cost is minimized, while meeting load demands and complying to dynamic Quality of Service (QOS) constraints. A simulation platform capable of representing a continuous time differential algebraic model of the power system and discrete switching events has been developed. A generation commitment list is prepared for each mission requirement and commitments satisfying QOS constraints are determined by simulation. The feasible commitments are economically dispatched based on quadratic fuel cost curves, and the commitment with the lowest cost per unit time is selected as optimal for that mission. Comparative cost benefits of an optimal commitment over a non-optimal commitment are enumerated.

Multi-Agent Based Federated Control of Large-Scale Systems with Application to Ship Roll Control

By *Qing Dong, Kristen Bradshaw, and Stephen Chaves (Naval Surface Warfare Center) and Li Bai and Saroj Biswas (Temple University)*

Large-scale systems refer to systems that consist of many interconnected local systems. Conventional centralized control schemes are not suitable for such large-scale systems because of their complex local and global dynamic behavior as well as computational difficulties. This paper introduces the general framework of an agent-based federated control motivated by the political structure where partially self-governing states are united by a federal government. Likewise, a multi-agent based federated control system is composed of local autonomous subsystems (agent-based controllers) that cooperate to provide an overall (large-scale) system behavior. In this concept, each agent has partial observations of the state of other agents and executes the local control law correspondingly to satisfy the performance requirements at the overall system level. Preliminary results are presented on the general architecture of multi-agent federated control for local and global connective stability.

Decentralized Agent-based Control of Chilled Water Plants using Wireless Sensor and Actuator Networks

By *Michael B. Kane, Jerome Lynch (University of Michigan), and Andrew Zimmerman (Civionics, LLC)*

The resiliency of a ship is dependent upon the resiliency of the various engineering plants that operate the ship.

Especially for combatant ships, engineering plants must be reconfigurable when damage occurs to ensure the ship has fight-through capabilities. Furthermore, reduced manning on ships necessitates the automated operation of engineering plants, especially their reconfiguration during times of battle damage. Wireless telemetry has been proposed in lieu of traditional tethered architectures for the monitoring and control of shipboard engineering plants. In this study, wireless nodes capable of sensing and actuation are explored for the automated control of a chilled water plant. An agent-based approach based on marketplace utility is proposed as a scalable and robust approach to the automated configuration of a chilled water plant. To illustrate the performance of the proposed control and reconfiguration architecture, a small-scale chilled water demonstrator is utilized. A network of wireless sensing and actuation nodes are shown to be highly effective in monitoring and reconfiguring the chilled water plant under varying operational conditions to achieve its operational objectives.

A Measure of Observability for Mutli-converter Shipboard Power Systems

By *Juan C. Jimenez, Chris J. Dafis, Karen Miu, and Chika Nwankpa (Drexel University)*

Perturbations in shipboard power systems can make controllers useless if improper control strategies are used. Incorporating the nonlinear dynamics of the shipboard power system in the control methodology is the solution to this problem. Before this solution is designed, the concept of nonlinear observability should be first investigated. A measure of observability of such systems will allow one to quantify their operational performance. This paper attempts to account for an observability measure of these multiconverter systems through the inclusion of other dynamics such as electro-mechnical behavior of generators and loads, providing a more comprehensive view of system performance. In the example section the observability condition number will lead to an indicator of how far the system is from being unobservable based on the system load profile.

State-Based Adjoint Model Reduction for Large Scale Control Problems

By Youngsuk Bang and Hany Abdel-Khalik (North Carolina State University)

Design of robust control systems requires efficient ways to compute variations of responses of interest with respect to a wide range of variations for a large number of initial conditions. This is necessary in order to perform engineering oriented applications such as design optimization, inverse studies, and sensitivity analysis. A reduced order model based on an adjoint approach that takes advantage of the contraction in the state rather than the response phase space is developed to calculate the variations in responses of interest with respect to input parameters. The approach is designed to combat the explosion in the state phase space often limiting the design of reduced order models. We show that the developed adjoint approach is independent of the given response, and is only dependent on the constraint equations relating initial conditions to the state variables. The mathematical framework hybridizes sampling techniques with adjoint methods to find the reduced order model. Its construction permits a general applicability to linear and nonlinear dynamical systems with general initial conditions variations. A proof of principle linear problem is demonstrated in this summary. The details of its general applicability to nonlinear models is left to a full journal article.

Consensus Control for Linear Systems in the Presence of Environmental and Channel Noise

By Saroj Biswas (Temple University), Qing Dong, and Li Bai

This paper uses multi-agent concepts for the development of a decentralized control law for networked large scale systems in the presence of environmental noise and noise in the communication channel. The subsystems are assumed to be linear time invariant with Gaussian white noise appearing as an exogenous input. Each subsystem receives output information of other subsystems through communication channel, which is then used to synthesize the control. The communication channels are also assumed to corrupt the signal with additive Gaussian White noise. Using the Lyapunov's approach, we develop a consensus protocol so that the various subsystems arrive at a weak consensus in the sense that the leader-follower state error remains within a small neighborhood of the origin. Simulation results are presented to illustrate the method.

Performance of Soft-Switched DC-DC Resonant Converter for Electrolyzer

By P. Chandrasekhar (Bharath University, Chennai, Jerusalem) and S. Rama Reddy (Jerusalem Engineering College, Chennai)

Electrolyzer produces hydrogen and oxygen from off-peak electricity generated by the renewable energy sources (wind turbine and photovoltaic array), for later use in the fuel cell to produce on-peak electricity. A power conditioning system, usually a DCDC converter is required to couple the Electrolyser to the system bus. This paper presents the design of three soft-switched high-frequency transformer isolated dc-to-dc resonant converters for this application based on the given specifications. Due to the wide variation in input voltage and load current, no converter can maintain zero-voltage switching for the complete operating range. Based on an extensive comparison of all the selected converters, LLC resonant converter will be studied in the future.

A Reference Architecture Approach to ICS Security

By Fred Cohen (Fred Cohen & Associates)

This paper describes the potential for use of a reference architecture for industrial control system (ICS) security as a method for moving toward improved protection through better decision-making. Reference architectures have been applied to enterprise information protection programs for about 10 years, [1] and the results have started to filter into common practice in improved decision-making for protection in enterprises of all sizes and from a wide range of different industries. Unfortunately, the most common reference architectures today for information protection are based on enterprise models of computing that are largely inadequate to the needs of automated control systems.

Feasibility of LabVIEW as a Scalable Robot Programming Language

By Karl Muecke and Brian Powell, National Instruments

LabVIEW has long been used as a graphical programming language for test, measurement, and control. LabVIEW's graphical data flow paradigm and tight coupling with hardware make it well suited for data acquisition applications. While robot applications rely on good, reliable hardware interfaces, they also frequently require scalability to multiple heterogeneous targets and complex architectures. This work seeks to test the feasibility of using LabVIEW as a programming language for a complex robot application, using a multi-robot search-and-rescue scenario as a case study.

Trust and Reputation Approach to Smart Grid Security

By Omkar Pradhan, Muhammad Awan, Kimberly Newman, and Frank Barnes (University of Colorado)

The electric grid in the US is aging and needs to be upgraded. Solutions involve the use of equipment with wireless communication capability for monitoring of generation, transmission and distribution. These systems introduce vulnerabilities to attack that can lead to blackouts and damage to equipment. In order to increase the reliability of the power systems, it is important to detect sources of risk at the system and individual level. The approach described in this paper applies trust and reputation management at the home based meter to detect when false reports occur.

Towards Agile Control of Ship Auxiliary Systems

By Kevin Schultz (Johns Hopkins University)

An agile control system is a set of distributed controllers designed for the management of complex, interconnected systems that are able to change their structure in response to faults and damage events. Structural changes include dynamic reconfiguration of communication, agent scoping, and control algorithms. We propose that information theory will be a valuable tool in the design

and analysis of such a controller, in that the information-theoretic characteristics of the system affect the utility of the information gathered and processed in the course of generating a control strategy. In particular, the rate at which the information content of a prior observation becomes irrelevant to the current state of the system is studied, called entropic drag. This paper summarizes recent work by researchers at the Johns Hopkins University Applied Physics Lab into components of an agile control system for ship auxiliary systems.

Ecologically Inspired Cooperative Control of Multi-Robot Systems

By Nagini Devarakonda and Rama Yedavalli (The Ohio State University)

In this paper we propose a new ecologically inspired control methodology for cooperative control of multi-robot systems. In this method we identify each individual robot as a subsystem of a large system and build the interactions between these subsystems to satisfy the design requirements. Interactions between these subsystems are built such that they mimic the interspecific (between species) interactions in an ecosystem. In the mathematical formulation of the control design, the subsystems and interactions between these subsystems are matrices whereas, interspecific interaction principles in an ecosystem are scalar in dimension. The novelty of this method lies in extending ecological principles that defined for scalars to matrices and then using these results in the design of the controller. Since we define the block matrices on the diagonal as the subsystems, the off-block-diagonal matrices clearly represent the interactions between these subsystems. Since control design involves determination of the off-block-diagonal matrices, it is seen that there is sufficient flexibility in the design of the controller.

ISRCS Committees

Symposium Leadership Team

- Craig Rieger, Symposium Chair, INL
- Milos Manic, Symposium Co-Chair,
  University of Idaho
- Michelle Blacker, Organizing Chair, INL
- Eugene Santos, Dartmouth College
- YangQuan Chen, Utah State University
- Barrett Caldwell, Purdue
- Devendra Garg, Duke University
- Miles McQueen, Idaho National Laboratory
- John Chiasson, Boise State University

Technical Program Committee

- Juan Jose Rodriguez Andina, University of Vigo
- Azad Azadmanesh, University of Nebraska, Omaha
- Ron Boring, Idaho National Laboratory
- Barrett Caldwell, Purdue University
- YangQuan Chen, Utah State University
- Devendra Garg, Duke University
- David Gertman, Idaho National Laboratory
- Diane Hooie, NETL
- Nicholas Kottenstette, Vanderbilt University
- Axel Krings, University of Idaho
- Manish Kumar, University of Cincinnati
- Parag Lala, Texas A&M
- Douglas Few, Idaho National Laboratory
- Kevin Moore, Colorado School of Mines
- Xinming Ou, Kansas State University
- Raghunathan Rengasamy, Clarkson University
- Eugene Santos, Dartmouth College
- Marco Schoen, Idaho State University
- Charles Tolle, South Dakota School of
  Mines and Technology

- Zachary Tudor, SRI International
- I-Jeng Wang, John Hopkins University
- Ernesto Bustamante, University of Idaho
- John Gardner, Boise State University
- Timothy McJunkin, Idaho National Laboratory
- Venkat Venkatasubramanian, Purdue University
- Subbaram Naidu, Idaho State University
- Said Ahmed-Zaid, Boise State University
- Saurabh Amin, University of California, Berkeley
- William Smart, Washington University
- Miles McQueen, Idaho National Laboratory

Symposium Organizing Team

- Jodi Grgich, ISRCS Logistics
- Andrew Thomas, ISRCS Logistics
- Margie Jeffs, ISRCS Lead Facilitator
- Desiree Reagan, ISRCS Web Developer
- Kristyn St. Clair, ISRCS Graphics
- Debra Leatherman, ISRCS Graphics

Publication Chair

- Debbie McQueen, University of Idaho

ISRCS Contacts

- Craig Rieger – 208.851.8839
- Michelle Blacker – 208.757.7642

Local Hospital

St. Luke's Boise
190 E. Bannock Street
Boise, Idaho. 83712
For an emergency call 911

Special Events

Idaho Shakespeare Festival
Taming of the Shrew

As you enter the outdoor amphitheater and habitat reserve, you'll be embarking upon a theatrical experience like no other! In addition to all the magic, drama and passion of professional theater, and a 770-seat, state-of-the-art facility that was built to feature the human voice, the Festival Amphitheater & Reserve is nestled in a unique habitat that is home to an astonishing variety of plant and animal species. The Festival operates under an agreement with the Idaho Foundation for Parks & Lands and the Idaho Department of Parks & Recreation. As you wend your way into the theater proper, you'll enjoy native plants, the songs of water birds and glimpses of deer, heron, ducks, geese and an occasional fox.

We encourage you to bring blankets and low-backed lawn chairs with seats no higher than 6 inches from the ground for both reserved and general admission lawn seating. And you may, of course, bring your own picnic and beverages or purchase food and beverage from Café Shakespeare By Lisa Peterson. Chairs are also available for rental at the souvenir stand for $2 (subject to availability.)

Dress for the weather, as the theater is outdoors and evenings along the river may start off warm but can quickly cool down as the sun sets. Or purchase a blanket or sweatshirt from the ISF Souvenir stand.

Directions to Idaho Shakespeare Festival
From Downtown Boise:

- Start going northwest on W. Front St
- Take the 1st left on S. 9th St.
- Take a left onto W. Myrtle St.
- W. Myrtle becomes E. Park Blvd.
- Stay straight onto W. Parkcenter Blvd.
- W. Parkcenter Blvd becomes E. Warm Springs Ave.
- Idaho Shakespeare Festival is on the right

Thunder Mountain Lines
Horsebend Route

The history of the Thunder Mountain Line dates back to more than a century ago. The prospects for the railroad were originally to serve the Thunder Mountain Mining District, which was full of gold and ore. The current roads could not handle the incoming freight for these areas. Prospectors were filling the Long Valley area as mining districts and camps were forming. Gold fever soon spread and an entrepreneur named Colonel W. Dewey formed a railroad syndicate due to the suspected wealth in the areas.

The railroad was built to Smiths Ferry on July 10, 1913 and an inaugural run was made in August 1913 and regularservice began later that month from Nampa. The railroad was completed on July 1914 with regular service beginning to McCall on Mondays, Wednesdays, and Fridays. The trains were mixed with freight, mail, and passengers. Many people were excited to have access to the mountain lakes and rivers for their vacations.

The Horseshoe Bend Route begins in historic Horseshoe Bend and travels along the scenic Payette River. The route is on the Old Wagon Road to the settlement of Banks. Enjoy the fresh mountain air and visit our refreshment car on this train ride. Local musicians will accompany your trip during special events.

Directions to Horsebend Depot
From Downtown Boise:

- Start going West on W. Front St.
- Merge onto W. Chinden Blvd toward Garden City/ Fairgrounds
- Turn right onto N. Glenwood St.
- Turn left onto W. State St.
- Turn slight right onto ID-55
- Stay on ID-55 for about 20 miles
- Thunder Mountain Line is on the right