August 14-16, 2012

5th International Symposium
on Resilient Control Systems
Salt Lake City, Utah

ISRCS 2012

Conference Sponsors and Organizers

INL
Idaho National Laboratory

THE UNIVERSITY OF UTAH

Idaho State UNIVERSITY

BOISE STATE UNIVERSITY

IEEE

ies

UtahState University

CAES
Center for Advanced Energy Studies

University of Idaho

Table of Contents

Welcome & Keynote Speakers

Opening Remarks

Richard Brown, University of Utah, Dean of the College of Engineering

Bio

Richard B. Brown received his bachelors and masters degrees in electrical engineering from Brigham Young University. Following graduation, he designed computers and instrumentation in California and Missouri. He returned to school at the University of Utah in 1981 and received an electrical engineering Ph.D. in 1985, at which time he joined the faculty of the University of Michigan Department of Electrical Engineering and Computer Science (EECS) where he developed their highly respected integrated circuit design (VLSI) program.

Prof. Brown has conducted major research projects in the development of sensors (for ions, heavy metals and neurochemicals) and microprocessors (high-performance, low-power, and mixed-signal). He holds 17 patents and has authored more than 200 peer-reviewed publications. He was the Micropower Electronics task leader in the University of Michigan's NSF Wireless Integrated Microsystems Engineering Research Center. He has won a variety of teaching and research awards.

At the University of Michigan, Prof. Brown served as Associate Chair for the Electrical Engineering Division of EECS for four years and then as Interim Chair of EECS. He has served on NSF, ASME and DARPA advisory committees for emerging technologies and VLSI education, and on two national advisory committees at other universities. He has been supportive of entrepreneurial activities and personally involved in technology transfer as a founder of Sensicore, i-sens, and Mobius Microsystems.

In July 2004, Prof. Brown was appointed the eleventh Dean of the College of Engineering at the University of Utah. He holds appointments in the School of Computing, the Department of Electrical & Computer Engineering and the Department of Bioengineering as well as an appointment at the University of Michigan Electrical Engineering and Computer Science Department.

Game-Theoretic Framework for Network Resilience, Reliability, and Security (NR2S)

Tamer Başar, University of Illinois at Urbana-Champaign

Abstract

With its rich set of conceptual, analytical and algorithmic tools, game theory has emerged as providing a versatile and effective framework for addressing issues of resilience, reliability and security (R2S) in networked (control) systems. This keynote will introduce the key elements of this modeling paradigm, and discuss various game-theoretic as well as control-theoretic solution concepts of direct relevance to NR2S. It will cover efficiency of these solutions within a non-cooperative mode of decision-making, and their sensitivity to imprecision in modeling. Further, the role of incentive mechanisms in mitigating or totally eliminating the adverse effects of inefficiency and sensitivity will be discussed. The talk will conclude with some specific examples of security games within the context of cyber-physical systems, with one setting involving multi-vehicle coordination in the presence of one or multiple mobile adversaries attempting to disrupt the communication, and thereby break connectivity, among the vehicles.

Bio

Tamer Başar is with the University of Illinois at Urbana-Champaign (UIUC), where he holds the academic positions of Swanlund Endowed Chair, Center for Advanced Study Professor of Electrical and Computer Engineering, Research Professor at the Coordinated Science Laboratory, and Research Professor at the Information Trust Institute. He received a B.S.E.E. from Robert College, Istanbul, and a M.S., M.Phil, and Ph.D. from Yale University. He joined UIUC in 1981 after holding positions at Harvard University and Marmara Research Institute (Turkey). He has published extensively in systems, control, communications, and dynamic games, and has current research interests in modeling and control of communication networks; control over heterogeneous networks; formation in adversarial environments; estimation and control with limited sensing and transmission; security; and cyber-physical systems.

Dr. Başar is currently the Editor-in-Chief of Automatica, Editor of the Birkhäuser Series on Systems & Control, Editor of the Birkhäuser Series on Static & Dynamic Game Theory: Foundations & Applications, Editor of the SpringerBriefs in Electronic and Computer Engineering: Control, Automation and Robotics, Managing Editor of the Annals of the International Society of Dynamic Games (ISDG), and member of editorial and advisory boards of several international journals. He has received several awards over the years, most recently the Isaacs Award of ISDG.

He is a member of the US National Academy of Engineering, a member of the European Academy of Sciences, a Fellow of IEEE, a Fellow of IFAC, a current Council Member of IFAC (2011-14), a past president of CSS, the founding president of ISDG, and current President of AACC (2010-11).

Keynote Speakers *(continued)*

Modeling the Resilience of and Risk to the Power-Grid Infrastructure and the Supportive Human and Organizations as Systems of Systems

Yacov Haimes, University of Virginia

Abstract

This presentation will highlight the complexity of the definitions and quantifications of the multidimensional vulnerability and resilience of and the risk to cyber-physical infrastructures as systems of systems; and building on the following premises: (1) Cyber-physical infrastructures as system of systems, must be studied, modeled, their effective operation measured with appropriate data collection, and be subjected to a regular process of risk assessment, management, and communication; (2) The above systemic process cannot be achieved without reliance on the centrality of the states of a system and the time frame; (3) The vulnerability and resilience of cyber-physical infrastructure systems of systems are manifestations of their states; (4) The shared and unshared state variables play prominent harmonizing roles among the interdependent subsystems of the cyber-physical infrastructures; (5) The significance of risk of low probability and extreme consequences to the cyber-physical infrastructures ought to be recognized and acted upon; (6) Unanticipated, undetected, misunderstood or ignored emergent forced changes, whether they originate from within or from outside a system, are likely to affect a multitude of states of that system with potentially adverse consequences. Therefore, it is imperative to be able--through scenario structuring, modeling and risk analysis--to envision, discover, and track emergent forced changes; (7) The vulnerability and resilience of the electric-power grid to cyber and physical emergent forced changes must be studied, modeled, and managed as systems of systems; (8) Prudent risk management calls for a continuous process of measuring the performance of a system, assessing whether observed changes are sufficiently significant, developing metrics with which to measure performance, and designing a data-collection mechanism—all are requisites for effective risk modeling, assessment, management, and communication.

Bio

Yacov Y. Haimes is the L.R. Quarles Professor of Systems and Information Engineering, and Founding Director (1987) of the Center for Risk Management of Engineering Systems at the University of Virginia. He received his M.S. and Ph.D. (with Distinction) degrees in Systems Engineering from UCLA, and his B.S. degree in Mathematics, Physics, and Chemistry from the Hebrew University, Jerusalem.

He is a Fellow of seven societies: ASCE, IEEE, INCOSE, AWRA, IWRA, AAAS, and Society for Risk Analysis (SRA). The Third Edition of his most recent book, Risk Modeling, Assessment, and Management, was published by Wiley & Sons in 2009. He has authored (and co-authored) six books and 300 technical publications, over 200 of which were published in archival refereed journals.

Air Force Cyber Vision 2025 (CV25)

Mark Maybury, US Air Force

Abstract

Cyber Vision 2025 (CV25) is the Air Force wide cyberspace S&T vision that articulates a path forward in the near-, mid-, and far-term to provide the assured cyber advantage. CV25 forecasts future threats, identifies principled mitigations of vulnerabilities, and indicates opportunities to assure, empower, and sustain resilience of core Air Force missions. It considered both traditional information technology and networks as well as cyber systems embedded in air, space, C2 and ISR mission systems. CV25 was formulated by the Office of the Chief Scientist, in partnership with air staff, MAJCOMs, and key stakeholders. Experts from across government, industry, national laboratories, FFRDCs, and academia helped review and refine the vision. In addition to articulating where the Air Force should lead, follow, or watch in S&T, CV25 also addressed DOTMLPF considerations, especially cyber accessions, training and education, cyber acquisition, and cyber test and evaluation.

Bio

Dr. Mark T. Maybury is Chief Scientist of the U.S. Air Force, Washington, D.C. He serves as chief scientific adviser to the Chief of Staff and Secretary of the Air Force, and provides assessments on a wide range of scientific and technical issues affecting the Air Force mission. In this role he identifies and analyzes technical issues and brings them to attention of Air Force leaders, and interacts with other Air Staff principals, operational commanders, combatant commands, acquisition, and science and technology communities to address cross-organizational technical issues and solutions. He also interacts with other services and the Office of the Secretary of Defense on issues affecting the Air Force in-house technical enterprise. He serves on the Steering Committee and Senior Review Group of the Air Force Scientific Advisory Board, or SAB. He also is the principal science and technology representative of the Air Force to the civilian scientific and engineering community and to the public at large.

Dr. Maybury served on the SAB as Vice Chair of Science and Technology, Vice Chair of a study on remotely piloted aircraft, and member on SAB studies on commercial space, rapid on-orbit checkout, and operating in contested cyberspace. He also chaired a SAB Information S&T review and vice chaired a human effectiveness S&T review at the Air Force Research Laboratory. He has additionally served on studies for the Defense Science Board and the Intelligence Science Board. A former Air Force officer, Dr. Maybury is currently on a leave of absence as an Executive Director at the MITRE Corporation. He has edited or co-authored 10 books, authored more than 60 refereed publications, and been awarded several U.S. patents.

Cyber-Physical Meets Cybertrust

Jeannette M. Wing, Carnegie Mellon University

Abstract

Cyber-physical systems are engineered systems that require tight conjoining of and coordination between the computational (discrete) and the physical (continuous). Cyber-physical systems are rapidly penetrating every aspect of our lives, with potential impact on sectors critical to U.S. security and competitiveness, including aerospace, automotive, chemical production, civil infrastructure, energy, finance, healthcare, manufacturing, materials, and transportation. Cybertrust means making computing systems reliable, secure, privacy-preserving, and usable. This talk will look at cyber-physical systems from the lens of trustworthy computing and look at trustworthy computing from the lens of cyber-physical systems. It will raise research challenges for how to make cyber-physical systems trustworthy and highlight new directions for trustworthy computing more generally.

Bio

Jeannette M. Wing is the President's Professor of Computer Science and Head of the Computer Science Department at Carnegie Mellon University. She received her S.B. and S.M. degrees in Computer Science and Engineering and her Ph.D. in Computer Science, all from the Massachusetts Institute of Technology. From 2004-2007 she served as Department Head at Carnegie Mellon, and from 2007-2010 she was the Assistant Director of the Computer and Information Science and Engineering Directorate at the National Science Foundation.

Professor Wing's general research interests are in the areas of trustworthy computing, specification and verification, concurrent and distributed systems, programming languages, and software engineering. Her current interests are on the foundations of trustworthy computing, with a focus on the science of security and privacy.

Professor Wing has published extensively in top journals and major conferences and has given nearly 300 invited, keynote, and distinguished lectures. During her career, she has been, or currently is, on the editorial board of twelve journals, including the Journal of the ACM and Communications of the ACM.

Professor Wing is a member of the Computing Research Association Board and the Microsoft Trustworthy Computing Academic Advisory Board.

She was on faculty at the University of Southern California, and has worked at USC/Information Sciences Institute and Xerox Palo Alto Research Laboratories. She spent sabbaticals at MIT in 1992 and at Microsoft Research 2002-2003. She has consulted for Digital Equipment Corporation, the Mellon Institute (Carnegie Mellon Research Institute), System Development Corporation, and the Jet Propulsion Laboratory. She received the CRA Distinguished Service Award in 2011. She is a Fellow of the American Academy of Arts and Sciences, American Association for the Advancement of Science, the Association for Computing Machinery (ACM), and the Institute of Electrical and Electronic Engineers (IEEE).

From Identification to Data Mining - Handling Massive Datasets

Vojislav Kecman,
Virginia Commonwealth University

Abstract

The origins of present data mining (DA) and machine learning (ML) are in the good old System Identification. Many control algorithms depend heavily on deriving models from system data. What is new today? First, the concept of data is changed and data have departed from engineering processes records to all possible data collections including images, sounds, and digital records of all kinds. Next, the amount of data has exploded and collections of millions of records are normal today. Massive data challenges our beliefs about the relations between the data and knowledge. The keynote will present some novel techniques to handle massive datasets. Some basic similarities and differences between neural networks and support vector machines (SVMs) will be presented. More will be said about basic algorithms for SVMs, because they are possibly the most feasible tools for handling massive datasets. Novelty detection by SVMs will be introduced as the possible way to increase the resilience of control systems.

Bio

Vojislav Kecman is the tenured associate professor with a Computer Science Department at the Virginia Commonwealth University (VCU) in Richmond, VA, USA, where he directs the Learning Algorithms and Applications Laboratory (LAAL).

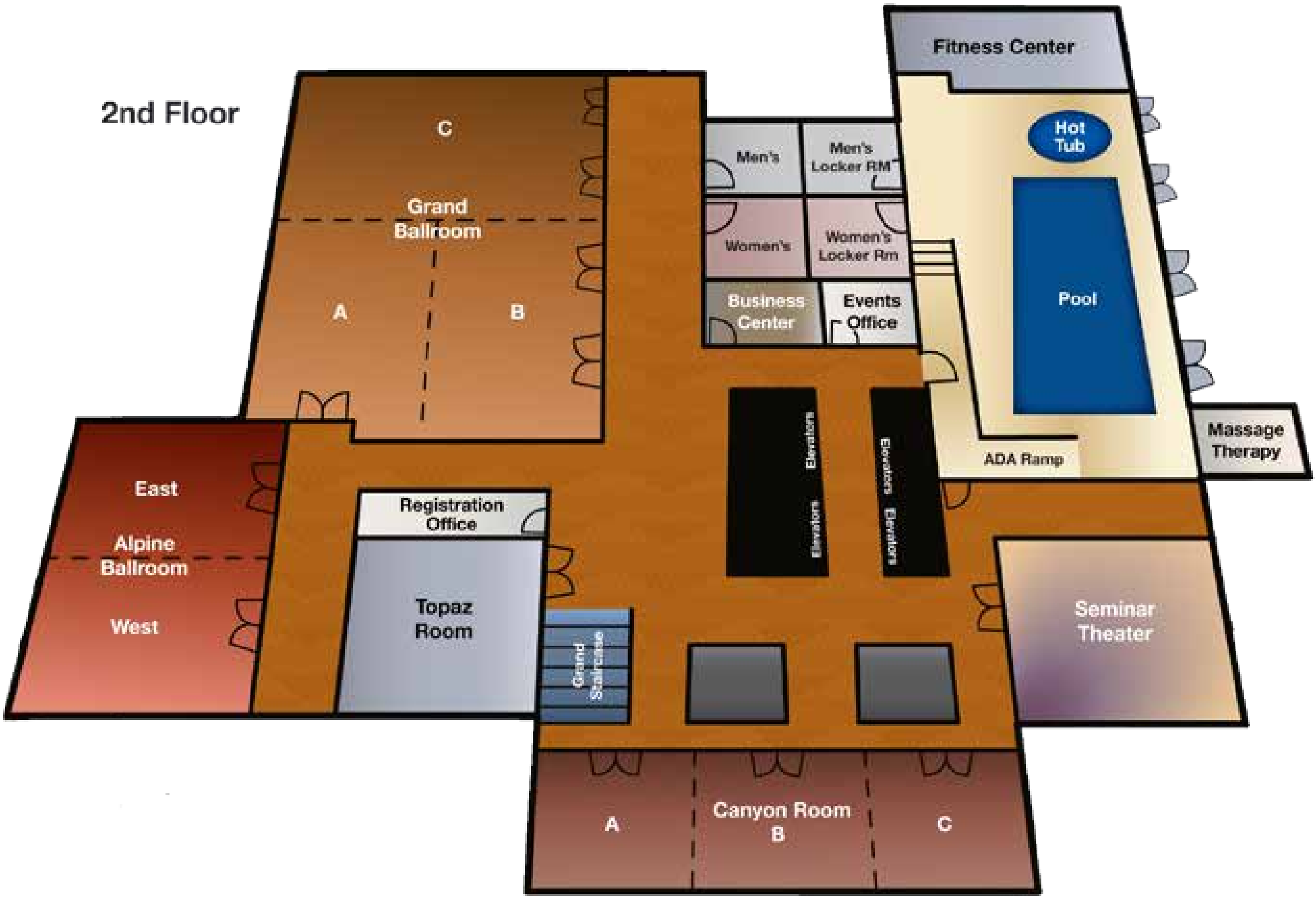
He was Fulbright Professor at MIT, Cambridge, MA, USA; DFG Professor at TH Darmstadt; DAAD Konrad Zuse Professor at FH Heilbronn, FHTW Berlin and SWFH Soest; Research Fellow at Drexel University, Philadelphia, PA and at Stuttgart University, as well as the associate professor at both The University of Auckland and Zagreb University.

Professor Kecman authored several books in the areas of machine learning (data mining) and in the fields of mathematical modeling and simulation of system dynamics, notably, 'Learning and Soft Computing - Support Vector Machines, Neural Networks, and Fuzzy Logic Models' published by The MIT Press, Cambridge, MA,

Professor Kecman's current research interests include: machine learning from experimental data (knowledge discovery, data mining) by support vector machines and neural networks, as well as modeling human knowledge by fuzzy logic systems. Theory, practice, philosophy and versatility of these soft computing tools is used in broad fields of different (nonlinear) regression and pattern recognition (classification, decision making) tasks in – e-commerce, bioinformatics, vision systems, computer graphics, data and signal processing, numerical mathematics, credit assignment problems, (financial) time series analysis, image compression, expert and decision systems and computer intelligence.

Professor Kecman's life long commitment is fighting AIDS disease by HIV infection modeling, which is a part of his modeling of biological systems devotion for many years.

Hilton Salt Lake City Center Map & Agenda



Tuesday, August 14 - *Tutorials & Workshops*

7:00 a.m.	**Light Continental Breakfast and Registration (2nd Floor Atrium)**	
8:00 a.m.	**Welcome and Opening Remarks** Welcome: Richard Brown, University of Utah (Alpine Ballroom) Introductions & Logistics: Jodi Grgich (Alpine Ballroom)	
8:30 a.m.	**Game-Theoretic Framework for Network Resilience, Reliability, and Security (NR²S)** Tamer Başar, University of Illinois Urbana-Champaign (Alpine Ballroom)	
9:30 a.m.	**Morning Break (Grand Ballroom)**	
10:00 a.m.	**Session 1:Tutorials & Workshops**	
	SS03: Tutorial on Static and Dynamic Game Theory for Resilient Control Systems (Canyon A) Chairs: Tamer Başar and Quanyan Zhu, Univ. of Illinois Urbana Champaign	**Experimental Security Panoramas** (Canyon B and C) Detailed Schedule, pg. 26
11:30 a.m.	**Hosted Lunch with Keynote (Alpine Ballroom)** **"Emerging Computational Methods for Smart Grid" Robert Osborn, NNSA**	
1:00 p.m.	**Session 2:Tutorials & Workshops**	
	ReSia Technical Committee (Canyon A) Chairs: Craig Rieger, INL Milos Manic, University of Idaho	Detailed Schedule, pg. 26
2:30 p.m.	**Afternoon Break**	
3:00 p.m.	**Session 3: Tutorials & Workshops**	
	RCS University Challenge (Canyon A) Chairs: Frank Ferrese, NSWC Craig Rieger, INL	Detailed Schedule, pg. 26
4:30 p.m.	**Adjourn**	

Detailed Agenda *(continued)*

Wednesday, August 15 - *Papers & Presentations*

7:30 a.m.	**Light Continental Breakfast and Registration (2nd Floor Atrium)**	
8:15 a.m.	**Opening Remarks and Daily Agenda** Jodi Grgich (Alpine Ballroom)	
8:30 a.m.	**Modeling the Resilience of and Risk to the Power-Grid Infrastructure and the Supportive Human Organizations as Systems of Systems** Yacov Haimes, University of Virginia (Alpine Ballroom)	
9:30 a.m.	**Morning Break (Grand Ballroom)**	
	Complex Networked Control Systems (Canyon A) Chairs: Frank Ferrese, Naval Surface Warfare Center David Scheidt, Johns Hopkins University	**Cyber Awareness** (Canyon B) Chairs: Marco Carvalho, Florida Institute of Technology Jonathan Butts, Air Force Institute of Technology
10:00 a.m.	A Resilient Condition Assessment Monitoring System* Humberto Garcia, Idaho National Laboratory	Improving Cyber-Security of Smart Grid Systems via Anomaly Detection and Linguistic Domain Knowledge Milos Manic, University of Idaho
10:20 a.m.	Resiliency of Linear System Consensus in the Presence of Channel Noise Qing Dong, US Navy	Towards Characterization of Cyber Attacks on Industrial Control Systems: Emulating Field Devices Using Gumstix Technology Jonathan Butts, Air Force Institute of Technology
10:40 a.m.	Adaptive Neural Replication and Resilient Control Despite Malicious Changes to the Plant Chang-Hee Won, Temple University	Agent-based Cyber Control Strategy Design for Resilient Control Systems: Concepts, Architecture and Methodologies Quanyan Zhu, University of Illinois at Urbana-Champaign
11:00 a.m.	Data Quality Assessment: Modeling and Application in Resilient Monitoring Systems Maruthi Ravichandran, University of Michigan	Systematic Analysis of Cyber-Attacks on CPS – Evaluating Applicability of DFD-based Approach Mark Yampolskiy, Vanderbilt University
11:30 a.m.	**Hosted Lunch (Alpine Ballroom)** **Air Force Cyber Vision 2025 (CV25)** Mark Maybury, US Air Force	

* Symposium Best Paper

Light Continental Breakfast and Registration (2nd Floor Atrium)

Opening Remarks and Daily Agenda
Jodi Grgich (Alpine Ballroom)

Modeling the Resilience of and Risk to the Power-Grid Infrastructure and the Supportive Human Organizations as Systems of Systems
Yacov Haimes, University of Virginia (Alpine Ballroom)

Morning Break (Grand Ballroom)

Data Fusion (Canyon C) Chairs: Devendra Garg, Duke University Manish Kumar, University of Cincinnati	**Human Systems** (Seminar Theater) Chairs: Barrett Caldwell, Purdue University Scott Kerick, Army Research Laboratory
Computational Intelligence based Anomaly Detection for Building Energy Management Systems Dumidu Wijayasekara, University of Idaho	A Dual-Process Cognitive Model for Testing Resilient Control Systems Jim Blythe, University of Southern California
Musings on Persistent Excitation Prompt New Weighted Least Squares SysID Method for Nonlinear Differential Equation Based Systems Charles Tolle, SDSMT	Simulation and Human Factors in Modeling of Spaceflight Mission Control Teams Barrett Caldwell, Purdue University
Augmenting Probabilistic Risk Assessment with Malevolent Initiators Curtis Smith, Idaho National Laboratory	WESBES: A Wireless Embedded Sensor for Improving Human Comfort Metrics Using Temporospatially Correlated Data Joel Hewlett, University of Idaho
Collective Perception in Large-Scale Networked Systems Manish Kumar, University of Cincinnati	Resilience in Control Room Modernization Ron Boring and Vivek Agarwal, Idaho National Laboratory

Hosted Lunch (Alpine Ballroom)
Air Force Cyber Vision 2025 (CV25)
Mark Maybury, US Air Force

Detailed Agenda *(continued)*

Wednesday, August 15 - *Papers & Presentations*

	Complex Networked Control Systems (Canyon A) Chairs: Frank Ferrese, Naval Surface Warfare Center David Scheidt, Johns Hopkins University	**SS02: Smart Grid Security, Resiliency, and Privacy** (Canyon B) Chairs: Robin Berthier and Rakesh Bobba, University of Illinois Urbana Champaign Álvaro A. Cárdenas, Fujitsu Laboratories of America
1:00 p.m.	Passivity-Based Trajectory Tracking Control with Adaptive Sampling Over a Wireless Network Emeka Eyisi, Vanderbilt University	Cyber-Physical Systems Security for Smart Grid Manimaran Govindarasu, Iowa State University
1:20 p.m.	Time Scale Analysis and Control of Wind Energy Conversion Systems D.S. Naidu, Idaho State University	
1:40 p.m.	A Novel Numerical Integrator for Structural Health Monitoring Suresh Thenozhi, CINVESTAV-IPN	Towards Addressing Common Security Issues in Smart Grid Specifications Apurva Mohan, Honeywell International
2:00 p.m.	Resilient Control System Execution Agent (ReCoSEA) Kris Villez, Purdue University	A Case for Validating Remote Application Integrity for Data Processing Systems Jonathan M. Chu, University of Illinois at Urbana-Champaign
2:30 p.m.	**Afternoon Break (Grand Ballroom)**	

SS04: Co-Robotics and Tele-Presence (Canyon C) Chairs: Corrie Nichol, Idaho National Laboratory Prof. Mark Colton, Brigham Young University	**SS01: Science of Test** (Seminar Theater) Chairs: Col Reed F. Young, Yuma Proving Ground Bob Von Dell, Yuma Proving Ground
Supporting Human Interaction with Robust Robot Swarms Sean Kerman, Brigham Young University	The Science of Test at the US Army Yuma Proving Ground COL Reed F. Young, Yuma Proving Ground
A Payload Verification and Management Framework forSmall UAV-Based Personal Remote Sensing Systems Calvin Coopmans, Utah State University	Autonomous Systems Test and Evaluation Requirements Study: A Roadmap to Robust Testing of Autonomous Systems Tracy Sheppard, Aberdeen Test Center
Force Control and Nonlinear Master-Slave Force Profile to Manage an Admittance Type Multi-Fingered Haptic User Interface Anthony L. Crawford, Idaho National Laboratory	US Army Test and Evaluation Command’s Reliability Growth Lessons Learned Michael Cushing, US Army
How to Keep Smart Agents Smart in Off-Normal Situations Keith Daum, Idaho National Laboratory	Characterization of Complex Geographic Terrain to Support Testing of Autonomous Systems Eric McDonald, Desert Research Institute
Afternoon Break (Grand Ballroom)	

Detailed Agenda *(continued)*

Wednesday, August 15 - *Papers & Presentations*

	Invitation Only Sessions	
3:00 p.m.		
3:30 p.m.	**Multi-Agent Analysis Workshop** (Canyon A) Chair: Craig Rieger, Idaho National Laboratory	**Cyber Awareness Symposium and ESP Planning** (Canyon B) Chairs: Miles McQueen, Idaho National Laboratory Marco Carvalho, Florida Institute of Technology Carl Kutsche, Idaho National Laboratory
5:00 p.m.	**Adjourn**	
6:00 p.m.	**Hosted Dinner with Keynote Presentation** **(University of Utah - The Tower of Rice-Eccles Stadium, Scholarship Room)** **Cyber-Physical Meets Cybertrust** Jeannette Wing, Carnegie Mellon University	

Concurrent Poster Session (Grand Ballroom AB)	**SS01- Science of Test (continued)**
Featured Posters Presenters Michael Balchanos, Georgia Tech Barrett Caldwell, Purdue University Calvin Coopsman, Utah State University David Gertman, Idaho National Laboratory Peter Hawrylak, University of Tulsa Peter Horvath, Vanderbilt University Kevin McCarthy, University of Idaho Erik Reed, Carnegie Mellon University	Continuation of SS01- Science of Test

Adjourn

Hosted Dinner with Keynote Presentation
(University of Utah- The Tower of Rice-Eccles Stadium, Scholarship Room)
Cyber-Physical Meets Cybertrust
Jeannette Wing, Carnegie Mellon University

Detailed Agenda *(continued)*

Thursday, August 16 - *Panel Discussion*

7:30 a.m.	**Breakfast and Registration (2nd Floor Atrium)**
8:15 a.m.	**Opening Remarks and Daily Agenda** Daily Agenda: Jodi Grgich (Alpine Ballroom)
8:30 a.m.	**From Identification to Data Mining - Handling Massive Datasets** Vojislav Kecman, Virginia Commonwealth University (Alpine Ballroom)
9:30 a.m.	**Morning Break (Grand Ballroom)**
10:00 a.m.	**Panel Discussion** **Government Panel** (Alpine Ballroom) Moderator: Larry Rohrbough, UC Berkeley
11:30 a.m.	**Concluding Remarks** Craig Rieger, Idaho National Laboratory
11:40 a.m.	**Adjourn**
1:30 p.m.	**University of Utah Tour (Optional)*** Algorithmic Robotics Lab Center of Excellence for Smart Sensors TreadPort Lab Applied Cognition Lab
3:30 p.m.	**End of Tour**

*See page 45 for map of TRAX system to navigate to University of Utah

Tour Descriptions

Algorithmic Robotics Lab

Presenter: Jur van den Berg, Assist. Prof. of Computer Science

In the Algorithmic Robotics Lab, we are interested in developing new algorithms with strong theoretical foundations for relevant practical applications in mobile robotics, medical robotics, artificial intelligence, crowd simulation, virtual environments and computer games, autonomous transportation, and personal robotics. Particular areas of research are motion planning under uncertainty, reciprocal collision avoidance, and information-theoretic decision making for autonomous virtual and real-world agents. The goal throughout these areas is to develop algorithms whose applicability extend beyond perfect virtual environments into the real world.

Center for Excellence for Smart Sensors

Presenter: Cynthia Furse, Associate Vice President for Researcher, Professor of Electromagnetics

Intermittent Live Fault Location for Aircraft Wiring

- Detect and locate open and short circuits to within a few centimeters
- Detect and locate arc fault damage
- Detect faults on live wires in flight
- SSTDR chip for fault location
- Acousto-optical methods for aircraft wiring faults

TreadPort Lab

Presenters: John Hollerbach, Mark Minor, Jake Abbott

The TreadPort Active Wind Tunnel (TPAWT) augments the existing TreadPort system with controllable wind, olfactory display, and radiant heat display in order to provide a truly submersive virtual environment. As a user walks on the Sarcos Treadport, the virtual world is displayed on the screens and an environmental computational fluid dynamics (CFD) model determines the wind and odors the user will experience as they travel through their virtual world. The graphical environment displays artifacts of the wind while the wind generation system creates and controls the wind flow. The wind generation system is essentially an actively controlled wind tunnel that allows wind speed and angle at the user to be regulated (the first of its kind).

Applied Cognition Lab

Presenters: David Strayer, Professor, Cognition and Neural Science

Over the last decade, the University of Utah has been studying driver distraction to better understand how and why people can become overloaded while multitasking. We use sophisticated equipment, including driving simulators, eye trackers, and we also measure brain activity (electroencephalography) and use neuroimaging technology (functional magnetic resonance imaging) to understand the cognitive neuroscience of driver distraction.

Tracks & Special Sessions *(in chronological order)*

Experimental Security Panoramas (ESP) for Critical System Protection Workshop

Chairs: Miles McQueen, INL
Annarita Giani, LANL
Eugene Santos, Jr., Dartmouth College

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

Special Session 3: Tutorial on Static and Dynamic Game Theory for Resilient Control Systems

Chairs: Tamer Başar and Quanyan Zhu, University of Illinois at Urbana-Champaign

In many critical infrastructures, the growing complexity of interconnected systems requires a new set of tools for analysis and design. Security and resilience are important system attributes of these systems, which are often subject to exogenous disturbances and exposed to unexpected adversarial attacks or events. Game theory is a versatile quantitative tool and has been commonly used to model different types of interactions among players or subsystems at multiple layers of the system. In this tutorial, we introduce game theoretic methods and discuss their application to resilient control systems. In the first part of the tutorial, we present static one-shot games and their basic solution concepts such as Nash equilibrium and Stackelberg equilibrium. In the second part, we introduce games that can capture system dynamics either in extensive forms or by differential equations and through stochastic dynamics. We draw examples from power systems and smart grids to illustrate various applications of game theory.

Track 1: Complex Control System Networks

Track Chairs: Frank Ferrese, NSWC
David Scheidt, Johns Hopkins University

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.

Track 2: Cyber Awareness

Track Chairs: Marco Carvalho, Floridia Insitute of Technology
Jonathan Butts, Air Force Institute of Technology

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.

Track 3: Data Fusion

Track Chairs: *Devendra Garg, Duke University*
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.

Track 4: Human Systems

Track Chairs: *Barrett Caldwell, Purdue University*
Scott Kerick, Army Research Laboratory

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 1: Science of Test

Chairs: *COL Reed Young and Bob Von Dell,*
Yuma Proving Ground

Just as investment today in fundamental and advanced research sets the stage for the procurement of future generations of materiel, so must we explore the "science of test" to enable and enhance the test community's ability to find effective, streamlined, and cost efficient test methodologies and technologies to support test requirement definition and subsequent test execution. Examples exist within data collection technologies such as exploring multispectral or hyperspectral sensor beyond electro-optic/infrared data collection. They also exist for test data reporting enhancement such as inclusion of complex terrestrial characterization coincident to phenomenologies. Finally, the Science of Test might also explore methodologies to characterize and evaluate autonomous, multi-agent robotic systems beyond simple mobility or communications throughput metrics. The goal of this session is to provide a forum for researchers to discuss test sciences that span commodity or instrumentation boundaries and provide potential for leap-ahead advancements.

Special Session 2: Smart Grid Security, Resiliency, and Privacy

Chairs: Robin Berthier and Rakesh Bobba,
University of Illinois at Urbana-Champaign
Álvaro A. Cárdenas, Fujitsu
Laboratories of America

Power grid is a critical national infrastructure crucial to the nation's economic security and public safety. The upgrade of such a large system to integrate digital communication technologies is driven by the important need to meet new efficiency and automation requirements. The security and resiliency of this infrastructure as it transforms into a smarter grid, and the privacy of the customers that depend on this infrastructure are paramount. However, given the complex and interconnected nature of the grid where the cyber and physical systems interact at varying time-scales (real-time to hours or days) achieving security, resiliency and privacy properties is a challenging problem that requires multi-disciplinary approach. This session aims to bring together a community of researchers and practitioners from academia, industry and the government to discuss the security, resiliency, and privacy aspects of the smart grid.

Special Session 4: Co-Robotics and Tele-Presence

Chair: Corrie Nichol, Idaho National Laboratory
Co-Chair: Mark Colton, Brigham Young University

Because humans are inherently capable of tremendous levels of resilience, system resilience can be greatly enhanced by the inclusion of a human in the loop. This may include humans sharing the operating space with the robot (Co-Robotics), or humans involved in the control and operation of a remote robotic system (Tele Presence). Examples in co-robotics and tele-presence include resilience to unstructured and/or dynamic operating environments, resilience to communication latency or disruption, task variation, dynamic task assignment, etc. This session solicits papers addressing these topics.

Panel Discussion

Government Plenary Panel

Abstract:

This year's panel is intended to provide a cross-agency, multi-disciplinary government perspective on the challenges and funding priorities in cyber security, automation integration and complexity, human systems, and areas associated with control system resilience. Each panelist will be provided opportunity to give a 5-10 minute perspective from their extensive background in guiding strategy in this area, followed by moderated questions and concluding with questions from the audience.

Panelists:

Larry Rohrbourgh, University of California, Berkeley (Moderator)

Bio

Mr. Rohrbough has over 15 years of experience in software engineering, technology consulting, program management, and business development for commercial, military, and government customers. Mr. Rohrbough has particular expertise in the Telecommunications and Department of Defense industries, Science and Technology research and development initiatives, and large-scale Operations Support System (OSS) development, deployment, and support.

Prior to joining ESCHER, Mr. Rohrbough held technical and management positions with CACI International, Accenture, and Delex Systems. At CACI International, Mr. Rohrbough provided technical program management support to the Defense Advanced Research Projects Agency (DARPA). In this role, Mr. Rohrbough managed the day-to-day activities of multiple research and development programs valued at more than $100M. Mr. Rohrbough provided domain expertise and technical analysis in the areas of wireless sensor networks, embedded systems, and complex, software-intensive systems. Mr. Rohrbough helped DARPA launch new research and development programs and supported the successful transition of DARPA-funded technology to the Department of Defense and commercial companies. Prior to that, Mr. Rohrbough was a manager with Accenture leading major engagements for communications and high-tech clients. At Accenture, Mr. Rohrbough led development and release management teams through full life-cycle implementation of large-scale billing, customer care, and order management systems, developed and implemented release management and software configuration management procedures and tools, and performed day-to-day management and client facing activities for multiple engagements. Prior to that, Mr. Rohrbough was a software engineer with Delex Systems. At Delex, Mr. Rohrbough developed sophisticated, computer-based weapons training systems for the U.S. military and foreign governments, researched, designed, and developed modeling algorithms to support multiple DoD weapon systems, implemented weapon training systems at customer sites, and conducted system administrator and end user training sessions.

Mr. Rohrbough holds a B.S. in Systems Analysis from Miami University and an M.S. in Software Systems Engineering from George Mason University. He is a member of ACM and IEEE.

Colonel Reed Young, Yuma Proving Ground

Bio

COL Young serves as the Senior Commander of the U.S. Army Yuma Proving Ground (YPG) responsible for a wide variety of developmental, environmental, and production testing across nearly every military commodity with a workforce of over 3,200 military, civilian, and contract personnel and an annual budget of $455 million. YPG is composed of three test centers including the Cold Regions Test Center located in Fort Greely, Alaska, the Tropic Regions Test Center headquartered in Panama and with sites in Honduras, Hawaii, and Suriname; and the Yuma Test Center located in Yuma, Arizona. COL Young's command also extends to the YPG Garrison including public works, housing, police, network enterprise, safety, and logistics divisions.

COL Young's awards and decorations include the Defense Meritorious Service Medal, Army Meritorious Service Medal (with four oak leaf clusters), Joint Service Commendation Medal, Army Commendation Medal, Joint Service Achievement Medal, Army Achievement Medal, Afghanistan Campaign Medal, Global War on Terrorism – Expeditionary Medal, Korean Defense Service Medal, Joint Meritorious Unit Award (with oak leaf cluster), Army Superior Unit Award, Parachutist Badge, Air Assault Badge, and Army Staff Identification Badge. He also wears the 82nd Airborne Division shoulder sleeve insignia for former wartime service.

Michael Kretzer, Air Force

Bio

J. Michael Kretzer, a member of the Senior Executive Service, is Technical Director, 688th Information Operations Wing, Lackland Air Force Base, Texas. In this position, Mr. Kretzer assists the commander by providing technical guidance and reviewing, evaluating and formulating policies, as well as developing concepts and objectives governing the mission of the Wing. The 688th IOW is a subordinate unit of 24th Air Force and Air Force Space Command and is responsible for executing the information warfare, and command and control warfare capabilities supporting operations, campaign planning, and acquisition and testing. The wing comprises more than 1,200 military and civilian personnel trained in operations, engineering, operations research, intelligence, installation, communications and computer applications.

Mr. Kretzer has also served at various positions within Air Force Intelligence, Surveillance, and Reconnaissance Agency and its predecessor units. His positions have included communications engineer, electronics engineer, program manager, division chief and director. He has a BS EET from Bradley University and a MS Management from Stanford University.

Robert Osborn, National Nuclear Security Administration

Bio available on page 27.

Rajeev Ram, ARPA-E

Bio

Rajeev Ram's primary focus at ARPA-E is in advanced electrical components and systems ranging from transportation to the generation and transmission of electric power.

He has worked in the areas of semiconductor devices, microscopic heat transfer, and bioprocess development for much of his career. In the early 1990's, he developed the III-V wafer bonding technology that led to the fist telecom wavelength surface-emitting laser and record brightness light emitting devices at Hewlett-Packard Laboratory in Palo Alto.

Since 1997, Ram has been on the Electrical Engineering faculty at the Massachusetts Institute of Technology (MIT) and a member of the Research Laboratory of Electronics. While at MIT, he founded two companies in the areas of bioprocess development for biofuels and advanced thermal imaging. He has served on the Defense Sciences Research Council advising DARPA on new areas for investment. His group's work on small-scale solar thermoelectric generation is being deployed for rural electrification in the developing world as SolSource and was recognized with the St. Andrews Prize for Energy and the Environment in 2009.

Ram holds degrees in Applied Physics from California Institute of Technology and Electrical Engineering from the University of California, Santa Barbara.

Experimental Security Panoramas Workshop

ESP Detailed Agenda

	Morning ESP Session and Welcome Session Chair: Eugene Santos, Dartmouth College
10:00 a.m.	Evaluating a ROP Defense Mechanism Professor Angelos Kermoytis, Columbia
10:30 a.m.	The Importance of Realistic Quantitative Studies of Malware Detection Dr. Mihai Christodorescu, IBM-T.J. Watson Research Center
11:00 a.m.	Coactive Emergence as a Sensemaking Strategy for Cyber Defense Dr. Jeffrey Bradshaw, Florida Institute for Human and Machine Cognition
11:30 a.m.	**Hosted Lunch with Keynote (Alpine Ballroom)** **Emerging Computational Methods for Smart Grid** Robert Osborn, National Nuclear Security Administration
	Session Chair: Miles McQueen
1:00 p.m.	Experimenting with Live Cyberattacks for Testing Deceptions Professor Neil C. Rowe, Naval Postgraduate School
1:30 p.m.	Empirical Analysis of System-Level Vulnerability Metrics Through Actual Attacks Mathias Ekstedt, KTH
2:00 p.m.	Lessons Learned and an Experimental Framework for Access Control Biometric Usability Dr. Alex Kilpatrick, Tactical Information Systems
2:30 p.m.	**Afternoon Break**
	Session Chair: Annarita Giani
3:00 p.m.	Big Data for Security: Challenges, Opportunities, and Experiments Dr. Pratyusa Manadhata, HP Labs
3:30 p.m.	Testing the Edge: Cyber Security Testing in the Smart Grid Professor David Nicol, University of Illinois at Urbana-Champaign
4:00 p.m.	Trustworthy Transportation Networked Control Systems Professor Saurabh Amin, Massachusetts Institute of Technology
4:30 p.m.	**Workshop Adjourns**

Experimental Security Panoramas (ESP) for Critical System Protection Workshop

Chairs: Miles McQueen, INL
Annarita Giani, LANL
Eugene Santos, Dartmouth College

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

The second ESP for Critical System Protection workshop will consist of a set of invited "experimentation focused" presentations related to critical system protection, detection, and response to cyber attacks. This will be followed by open discussion. Each presentation will emphasize the experimental aspect of the security research, explicitly discuss the strengths and weaknesses of the chosen approach, and discuss potential improvements. 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 aiding protection of our nation's critical systems from cyber attack. At the end of the workshop the need, focus, and form of the 3rd ESP workshop will be drafted.

Workshop Keynote

Emerging Computational Methods for Smart Grid

Robert Osborn,
National Nuclear
Security Administration

Abstract

The Department of Energy Cyber Sciences Laboratory (DOE CSL) brings together the scientific research excellence, technical assets, innovation capacity, and intellectual strengths of the DOE/NNSA research community in a focused effort to address the one of the Nation's greatest national security challenges: the growing cyber threat. The DOE and NNSA CIOs, and the DOE Director of Intelligence have established the DOE CSL to provide a process in support of a coordinated cyber security research agenda. DOE CSL will focus on the protection of NNSA nuclear weapons information, the national electric grid and the DOE/NNSA information enterprise. Attend this luncheon keynote to hear Bob Osborn, Associate Administrator of Information Management and Chief Information Officer of the NNSA, speak about this exciting initiative and his vision for the future of information security.

Bio

Robert J. Osborn II, a member of the Senior Executive Service, is currently the Associate Administrator for Information Management and Chief Information Officer for the National Nuclear Security Administration under the Department of Energy. Mr. Osborn has recently been appointed to be the NNSA Transformation Executive and will lead the agency's move to "OneNNSA." Mr. Osborn's previous assignment was as the Deputy Director for Distribution Portfolio Management, Command, Control, Communications and Computer Systems, U.S. Transportation Command, Scott Air Force Base, Ill.

As a U.S. Marine, Mr. Osborn held assignments in batteries, battalions and squadrons as well as on division and fleet service support group staffs. He has served in a number of specialties, including C-130 radio operator, field artilleryman and NCO school instructor. He has also been a combat cargo officer aboard the USS Dubuque and Amphibious Squadron 11 staff. Mr. Osborn served in the Marine Security Guard Program at the U.S. Embassy in Tokyo, Japan, and provided personal protection for the Chief of Naval Operations.

Prior to his retirement in 2001, Mr. Osborn was Chief of the Logistics Automation Branch at Headquarters U.S. Marine Corps. He has since held a number of positions of increasing responsibility within Headquarters Department of the Army, Office of the Deputy Chief of Staff (G4), last serving as the Logistics Chief Information Officer.

Abstracts

Evaluating A ROP Defense Mechanism

Professor Angelos Keromytis, Columbia

An "in-place code randomization" was recently developed, and is a practical mitigation technique against return oriented programming (ROP) attacks that can be applied directly on third-party software. Our method uses various narrow-scope code transformations that can be applied statically, without changing the location of basic blocks, allowing the safe randomization of stripped binaries even with partial disassembly coverage. These transformations effectively eliminate about 10%, and probabilistically break about 80% of the useful instruction sequences found in a large set of PE files. Since no additional code is inserted, in-place code randomization does not incur any measurable runtime overhead, enabling it to be easily used in tandem with existing exploit mitigations such as address space layout randomization. Both real ROP exploits and two ROP code generation toolkits were used. In this talk the challenges in evaluating this probabilistic software detection mechanism and the various metrics that are applicable, and why some of those were impossible or difficult to obtain will be discussed.

The Importance of Realistic Quantitative Studies of Malware Detection

Dr. Mihai Christodorescu, IBM-T.J. Watson Research Center

A running theme among existing detection techniques is the similar promises of high detection rates, in spite of the wildly different models of malicious activity used. In addition, the lack of a common testing methodology and the limited datasets used in the experiments make it difficult to compare these models in order to determine which ones yield the best detection accuracy, especially when exposed to a diverse set of previously-unseen, real-world applications that operate on realistic inputs. This is particularly problematic as most previous work has used only a small set of programs to measure their technique's false positive rate. Moreover, these programs were run for a short time, often by the authors themselves.

I will describe a study of the diversity of system calls based on a large-scale data collection (compared to previous efforts) on hosts that run applications for regular users on actual inputs. The analysis of the data demonstrates that simple malware detectors, such as those based on system call sequences, face significant challenges in realistic environments. This suggests that commonly held beliefs about simple models are incorrect in how they relate changes in complexity to changes in detection accuracy. To address these limitations, an alternative detection model that characterizes the general interactions between benign programs and the operating system (OS) will be discussed. Our experiments enabled by the large-scale data set demonstrate that this approach captures well the behavior of benign programs and raises very few (even zero) false positives while being able to detect a significant fraction of today's malware.

Coactive Emergence as a Sensemaking Strategy for Cyber Defense

Dr. Jeffrey Bradshaw, Florida Institute for Human and Machine Cognition

In this talk, how we are applying the concept of coactive emergence as an approach to the design of work methods for distributed sensemaking in cyber defense applications will be described. Distributed sensemaking is a process whereby understanding and anticipation of complex situations is achieved through the collaboration of analysts and software agents working in tandem. As rationale for the principles used in the work design, a series of background studies will be presented. We show how coactive emergence as a strategy for threat understanding relates to Klein's Data/Frame theory of sensemaking. An explanation of the similarities and differences of coactive emergence from the basic form of second-order emergence will be provided, followed by an outline of a set of considerations for resilient human-automation teamwork. These desiderata address the teamwork requirements of observability, directability, interpredictability, adaptation, and multiplicity. Recent results and future plans for empirical studies addressing some of the issues raised in this talk will be described.

Experimenting with Live Cyberattacks for Testing Deceptions

Professor Neil C. Rowe, Naval Postgraduate School

An experimental approach to finding deceptive tactics for computer system defense has been developed. This approach tries a variety of tactics against live Internet traffic and observes the responses. These experiments are easiest to do on a honeypot, a computer system designed solely as an attack target. We report on three kinds of experiments with deceptive honeypots: one with packet modifications on packets provided by attackers using Snort Inline, one on scripted responses to attacks using Honeyd, and one on a fake Web site. Evidence of responses to deceptions in the form of increased session lengths, and the disappearance of attackers was found . Some benefit was obtained by varying the deceptions over time. These results are encouraging for developing more comprehensive automated deception strategies for defending computer systems, and providing a new experimentation methodology for systematically developing deception plans.

Empirical Analysis of System-Level Vulnerability Metrics Through Actual Attacks

Professor Mathias Ekstedt, KTH

The Common Vulnerability Scoring System (CVSS) is a widely used and well established standard for classifying the severity of security vulnerabilities. For instance, all vulnerabilities in the US National Vulnerability Database are scored according to this system. As systems typically have multiple vulnerabilities it is often desirable to aggregate the score of individual vulnerabilities to a system level. Several such metrics have been proposed, but their quality has not been studied. The presentation describes a statistical analysis of how a number of security estimation metrics using CVSS data relate to the time-to-compromise of 41 successful attacks. The empirical data originates from an international cyber defense exercise involving over 100 participants. Utilized data was collected through studying network traffic logs, attacker logs, observer logs, and network vulnerabilities. Results suggest that security modeling through CVSS data alone doesn’t accurately portray the security of a system. However, the results also imply that the amount of CVSS information which is used by the metric is of relevance to its accuracy: a metric employing more CVSS data also explains time-to-compromise better.

Lessons Learned and an Experimental Framework for Access Control Biometric Usability

Dr. Alex Kilpatrick, Tactical Information Systems

The presenter will discuss lessons learned from the deployment of operational biometric systems for access control and security in Iraq and Afghanistan, and the special challenges faced with a non-English speaking population and high-threat environments. The presentation will also include the results of a comprehensive study of biometric usability in DoD and commercial environments, as well as an experimental framework for future biometric usability experiments.

Big Data for Security: Challenges, Opportunities, and Expierments

Dr. Pratyusa Manadhata, HP Labs

This is the age of big data. Big data for security, i.e., the analysis of very large data sets to identify actionable security relevant information, however, is a relatively unexplored area. Our research group has undertaken an initiative on big data for security in enterprise settings, i.e., our goal is to design algorithms and systems to analyze large data sets routinely collected by enterprises for compliance and other reasons. The presentation will highlight some of the challenges and opportunities in big data for security, and present a few experimental results.

Testing the Edge: Cyber Security Testing in the Smart Grid

Professor David Nicol, University of Illinois at Urbana-Champaign

The presenter considers issues related to performing security testing of Smart Grid components and subsystems within the context of an evaluation testbed. Methodologies for assessing components and and component ensembles, in conjunction with metrics that help guide understanding of the testing outcomes are discussed. Useful hardware and software tools for evaluation studies will be identified. Points will be illustrated by stepping through a case study, of meters and theircommunication within an Advanced Metering Infrastructure.

Trustworthy Transportation Networked Control Systems

Professor Saurabh Amin,
Massachusetts Institute of Technology

Networked control systems (NCS) are increasingly being deployed to facilitate monitoring and control of large-scale transportation systems, including vehicular traffic and public transit networks. In recent years, the deployment of advanced sensing technologies has caused a considerable increase in both heterogeneity and volume of real-time measurement data. Transportation agencies are now employing the public communication network (Internet) in addition to private (back-haul) networks for most of their routine tasks, such as monitoring, data processing, and distributed control. The significant drawback of this information technology (IT) modernization is lowered security of transportation NCS caused by the exposure to IT insecurities. The security threats primarily come from four channels: (i) off-the-shelf IT devices; (ii) open communication networks; (iii) multi-party data management; (iv) large number of field devices (sensors, displays, and actuators). This work focuses on experiment design for improving the trustworthiness of transportation NCS. Our goal is to improve NCS operational resilience against security failures (attacks) and reliability failures (faults).

Paper and Poster Abstracts *(listed by track or special session)*

Track 1- Complex Networked Control Systems

International Symposium • Resilient Control Systems • ISRCS

A Resilient Condition Assessment Monitoring System*

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

An architecture and supporting methods are presented for the implementation of a resilient condition assessment monitoring system that can adaptively accommodate both cyber and physical anomalies to a monitored system under observation. In particular, the architecture includes three layers: information, assessment, and sensor selection. The information layer estimates probability distributions of process variables based on sensor measurements and assessments of the quality of sensor data. Based on these estimates, the assessment layer then employs probabilistic reasoning methods to assess the plant health. The sensor selection layer selects sensors so that assessments of the plant condition can be made within desired time periods.

Resiliency of Linear System Consensus in the Presence of Channel Noise

By Frank Ferrese, Saroj Biswas, **Qing Dong** *(US Navy), and Li Bai*

This paper presents multi-agent based control of networked linear time invariant systems in a noisy environment. The control protocol is based on output information received from other subsystems through the communication channel, which imparts noise to the sensor data. We show that the sum of the mean square state errors between various subsystems converges to a small bound for the multi-agent system. It is apparent that a higher controller gain tends to make the networked system arrive at a consensus faster, while at the same time has the detrimental effect of enlarging the radius of consensus. Resilience of consensus is demonstrated in that the controller maintains collective stability in the event of communication or subsystem failures.

Adaptive Neural Replication and Resilient Control Despite Malicious Attacks

By Salvatore Giorgi, Firdous Saleheen, Frank Ferrese, and **Chang-Hee Won** *(Temple University)*

In this paper, an Adaptive Neural Control (ANC) architecture is used for system replication and control within a Resilient Control framework. A dynamic model is chosen for our plant and a "maliciously attacked" plant. A Model Reference Adaptive Control (MRAC) architecture is used to replicate and control the plant to match an ideal reference system. At certain time, we replicate a malicious attack by changing plant parameters, injecting false data, or altering sensor data. This attacked plant is then replicated and controlled to match the reference system. Simulations were carried out to show that accurate system replication and resilient control is possible using adaptive neural networks.

* Symposium Best Paper

Data Quality Assessment: Modeling and Application in Resilient Monitoring Systems

By Humberto Garcia, Wen-Chiao Lin, Semyon Meerkov, and **Maruthi Ravichandran** *(University of Michigan)*

This paper presents a novel data quality model as part of a monitoring system that degrades gracefully under attacks on its sensors. The attacker is assumed to manipulate the sensor data's variance or mean, with the aim of projecting a false state of the plant. Each sensor's data is assigned a level of trust, termed data quality, as part of assessing the states of the process variables. For the variance-based attacker, it is established that the concept of data quality is not, in fact, necessary to obtain the best possible assessment. For the mean-based attacker, it is recognized that statistical means are not sufficient to discern data quality. To combat this problem, the so-called method of probing signals is proposed. The efficacy of this method is illustrated by numerical experiments categorized into two parts. The first deals with individual process variable assessment, while the second deals with the adaptation of the sensor network to obtain the best possible plant assessment.

Passivity-Based Trajectory Tracking Control with Adaptive Sampling Over a Wireless Network

By **Emeka Eyisi** *(Vanderbilt University), Xenofon Koutsoukos, and Nicholas Kottenstette*

Uncertainty in wireless networks, such as time-varying delays and packet loss, often leads to instability and degraded performance in Networked Control Systems (NCS). Further, limited network resources impose constraints on communication between plants and controllers. In this paper, we use passivity combined with adaptive sampling to design a control architecture for trajectory tracking. The proposed architecture can tolerate time-varying delays and packet loss while efficiently utilizing network bandwidth. We provide analytical results to show passivity of the proposed networked control architecture and trajectory tracking. We demonstrate our approach using a case study on the trajectory tracking control of a robotic manipulator over a wireless network. The simulation results show the efficient utilization of network resources as well as robustness to network uncertainties.

Time Scale Analysis and Control of Wind Energy Conversion Systems

By Hoa M. Nguyen and **D. Subbaram Naidu** *(Idaho State University)*

This paper presents a control method to design loworder optimal controllers for a high-order Wind Energy Conversion Systems (WECS) with Permanent Magnet Synchronous Generators (PMSG). Based on the nature of the WECS which consists of different time-scale (slow and fast) dynamics, the WECS is decoupled into slow and fast subsystems using timescale analysis. Separate low-order optimal controllers are then designed for the slow and fast subsystems based on the Linear Quadratic Regulator (LQR) theory. The reduced-order optimal control of separate subsystems is compared with the high-order optimal control of the original system to show the superiority of the proposed method in terms of separation of dynamics and reduced computational effort.

A Novel Numerical Integrator for Structural Health Monitoring

By **Suresh Thenozhi** *(CINVESTAV-IPN), Wen Yu, and Ruben Garrido*

Accelerometers are one of the most commonly used sensor in structural control and health monitoring applications. However the accelerometer output is polluted with noise and bias signals. Obtaining velocity and position from these acceleration measurements are not trivial. Direct integration will result in an output drift. In this paper baseline correction and filtering techniques are used to overcome these problems. Experimental results on a linear actuator illustrates the effectiveness of the proposed method.

Resilient Control System Execution Agent (ReCoSEA)

By Craig Rieger and **Kris Villez** *(Purdue University)*

In an increasingly connected world, critical infrastructure systems suffer from two types of vulnerability. The first is the traditionally recognized problem of monitoring the systems for faults and failures, recognizing and analyzing data, and responding with real understanding to the problems of the system. Increasingly complex systems create the opportunity for single points of failure to cascade when inaccurate assessment of system health increases response time or leads to faulty analysis of the problems involved. A second problem involves vulnerability to cyber intrusion, in which malignant actors can mask system degradation or present false data about system status. A resilient system will protect stability, efficiency, and security. To ensure these three states, the system must react to changing conditions within the system with coordination: no one component of the system can be allowed to react to problems without real consideration of the effects of that action on other components within the system. Systems with multi-agent design typically have three layers of action, a management layer, a coordination layer, and an execution layer. A resilient multi-agent system will emphasize functions of the execution layer, which has the responsibility of initiating actions, monitoring, analyzing, and controlling its own processes, while feeding information back to the higher levels of management and coordination. The design concept of a resilient control system execution agent (ReCoSEA) grows out of these underpinnings, and through the use of computational intelligence techniques, this paper suggests an associated design methodology.

Track 2-Cyber Awareness

Improving Cyber-Security of Smart Grid Systems via Anomaly Detection and Linguistic Domain Knowledge

By Ondrej Linda and **Milos Manic** *(University of Idaho)*

The planned large scale deployment of smart grid network devices will generate a large amount of information exchanged over various types of communication networks. The implementation of these critical systems will require appropriate cyber-security measures. A network anomaly detection solution is considered in this paper. In common network architectures multiple communications streams are simultaneously present, making it difficult to build an anomaly detection solution for the entire system. In addition, common anomaly detection algorithms require specification of a sensitivity threshold, which inevitably leads to a tradeoff between false positives and false negatives rates. In order to alleviate these issues, this paper proposes a novel anomaly detection architecture. The designed system applies a previously developed network security cyber-sensor method to individual selected communication streams allowing for learning accurate normal network behavior models. In addition, an Interval Type-2 Fuzzy Logic System (IT2 FLS) is used to model human background knowledge about the network system and to dynamically adjust the sensitivity threshold of the anomaly detection algorithms. The IT2 FLS was used to model the linguistic uncertainty in describing the relationship between various network communication attributes and the possibility of a cyber attack. The proposed method was tested on an experimental smart grid system demonstrating enhanced cyber-security.

Towards Characterization of Cyber Attacks on Industrial Control Systems: Emulating Field Devices Using Gumstix Technology

By Dustin Berman and **Jonathan Butts** *(Air Force Institute of Technology)*

Industrial control systems (ICS) have an inherent lack of security and situational awareness capabilities at the field device level. Yet these systems comprise a significant portion of the nation's critical infrastructure. Currently, there is little insight into the characterization of attacks on ICS. Stuxnet provided an initial look at the type of tactics that can be employed to create physical damage via cyber means. The question still remains, however, as to the extent of malware and attacks that are targeting the critical infrastructure, along with the various methods employed to target systems associated with the ICS environment. This paper presents a device using Gumstix technology that emulates an ICS field device. The emulation device is low-cost, adaptable to myriad ICS environments and provides logging capabilities at the field device level. The device was evaluated to ensure conformity to RFC standards and that the operating characteristics are consistent with actual field devices.

Agent-based Cyber Control Strategy Design for Resilient Control Systems: Concepts, Architecture and Methodologies

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

The implementation of automated regulatory control has been around since the middle of the last century through analog means. This has removed the burden from human its earliest inception, allowing them to operate the plant more consistently by focusing on overall operations and settings instead of individual monitoring of local instruments (inside and outside of a control room). A similar approach is proposed for cyber security, where current border-protection designs have been inherited from information technology developments that lack consideration of the high-reliability, high consequence nature of industrial control systems. Instead of an independent development, however, an integrated approach is taken to develop a holistic understanding of performance. This performance takes shape inside a multi-agent design, which provides a notional context to model highly decentralized and complex industrial process control systems, the nervous system of critical infrastructure. The resulting strategy will provide a framework for researching solutions to security and unrecognized interdependencies concerns with industrial control systems.

Systematic Analysis of Cyber-Attacks on CPS – Evaluating Applicability of DFD-based Approach

By **Mark Yampolskiy** *(Vanderbilt University), Peter Horvath, Xenofon Koutsoukos, Yuan Xue, and Janos Sztipanovits*

Cyber-Physical Systems (CPSs) consist of as well as interact with cyber and physical elements. This creates multiple vectors for CPS-internal (i.e., within CPS) as well as for CPSexternal (i.e., between CPS itself and its environment) Cyber- Physical Attacks. We argue that an effective Cyber-Physical Defense can only be elaborated if possible attacks on CPS can be identified and assessed in a systematic manner. In this paper, we focus on cyber-attacks only. Our contribution in this paper is the following. We assess the applicability of Data Flow Diagrams (DFD) for the systematic analysis of cyber-attacks against CPS. In this context, we introduce several extensions to DFD. We evaluate the analysis procedure by applying it on a comparatively simple example of a quad-rotor UAV. The selected UAV is fully functioning and contains multiple structural elements representative for more complex systems. At the same time, its simplicity enables an in-depth manual analysis. Our analysis shows that cyber-attacks executed against CPS can lead to various cyber-physical interactions. This, in turn, creates novel challenges for CPS defense. Finally, we outline the preliminary results of our work towards a Taxonomy of Cyber-Physical Attacks.

Track 3: Data Fusion

Computational Intelligence based Anomaly Detection for Building Energy Management Systems

By Ondrej Linda, **Dumidu Wijayasekara** *(University of Idaho), Milos Manic, and Craig Rieger*

In the past several decades Building Energy Management Systems (BEMSs) have become vital components of most modern buildings. BEMSs utilize advanced microprocessor technology combined with extensive sensor data collection and communication to minimize energy consumption while maintaining high human comfort levels. When properly tuned and operated, BEMSs can provide significant energy savings. However, the complexity of the acquired sensory data and the overwhelming amount of presented information renders them difficult to adjust or even understand by responsible building managers. This inevitably results in suboptimal BEMS operation and performance. To address this issue, this paper reports on a research effort that utilizes Computational Intelligence techniques to fuse multiple heterogeneous sources of BEMS data and to extract relevant actionable information. This actionable information can then be easily understood and acted upon by responsible building managers. In particular, this paper describes the use of anomaly detection algorithms for improving the understandability of BEMS data and for increasing the state-awareness of building managers. The developed system utilizes modified nearest neighbor clustering algorithm and fuzzy logic rule extraction technique to automatically build a model of normal BEMS operations and detect possible anomalous behavior. In addition, linguistic summaries based on fuzzy set representation of the input values are generated for the detected anomalies which increase the understandability of the presented results.

Musings on Persistent Excitation Prompts New Weighted Least Squares SysID Method for Nonlinear Differential Equation Based Systems

By **Charles Tolle**, *SDSMT*

The Control community relies heavily on good System Identification (SysID) for finding the plant models needed to develop a good controller. However over time the SysID process and controller development process have remained generally separate activities. One reason for this is that SysID and Control are disparate in their fundamental nature. For good SysID, one is faced with the challenge of persistently exciting plant dynamics; while a good control system attempts to constrain or suppress much of a plant's natural dynamics with desired dynamics. It is this inherent conflict that separates the two practices. But for many plants, their inherent instabilities makes trajectory collection difficult, thus there is a desire to perform data collection while under some simple form of control. Nevertheless, in order to perform solid SysID one must sample the very dynamics one might need to suppress; how then can this be achieved? This paper will explore the notation of persistent excitation, its relationship to phase space trajectories, and how one might recover the most nonlinear dynamics information for SysID while remaining under the linearizing based control region– the very place that those dynamics are most suppressed.

Track 4: Human Systems

A Dual-Process Cognitive Model for Testing Resilient Control Systems

By **Jim Blythe**, *University of Southern California*

We describe an agent-based model of individual human behavior that combines a dual-process architecture with reactive planning and mental models in order to capture a wide range of human behavior, including both behavioral and conceptual errors. Human operator behavior is an important factor in resilient control of systems that has received relatively little attention. Models of human behavior and decision making are needed in order to test existing control systems under a range of conditions or analyze possible new approaches. While the model we describe has been developed and applied in the area of cyber security, it is relevant to a wide range of resilient control systems that include human operation. We discuss an application to modeling operator behavior in a nuclear power plant.

Simulation and Human Factors in Modeling of Spaceflight Mission Control Teams

By **Barrett Caldwell** *(Purdue University) and Jeffrey Onken*

This paper describes a recently completed project to develop a human factors informed simulation of team-based expert coordination and knowledge sharing tasks in a complex and resilient control system. The project explores processes of anomaly response in NASA spaceflight mission control teams, using as a baseline example the mission profile and anomalies experienced during the final Space Shuttle flight, STS-135. While controllers in this simulation work to detect and resolve anomalies using technical decision criteria, their performance is subject to stochastic and non-rational dynamics of information availability and flow affecting situation awareness and hypothesis generation. The initial goal of this work is to assist in analysis of alternatives for future mission control room designs, and to develop increased simulation capability in the area of distributed expertise and problem solving in teams.

WESBES: A Wireless Embedded Sensor for Improving Human Comfort Metrics using Temporospatially Correlated Data

By **Joel Hewlett** *(University of Idaho), Milos Manic, and Craig Rieger*

When utilized properly, energy management systems (EMS) can offer significant energy savings by optimizing the efficiency of heating, ventilation, and air-conditioning (HVAC) systems. However, difficulty often arises due to the constraints imposed by the need to maintain an acceptable level of comfort for a building's occupants. This challenge is compounded by the fact that human comfort is difficult to define in a measurable way. One way to address this problem is to provide a building manager with direct feedback from the building's users. Still, this data is relative in nature, making it difficult to determine the actions that need to be taken, and while some useful comfort correlations have been devised, such as ASHRAE's Predicted Mean Vote index, they are rules of thumb that do not connect individual feedback with direct, diverse feedback sensing. As they are a correlation, quantifying effects of climate, age of buildings and associated defects such as draftiness, are outside the realm of this correlation. Therefore, the contribution of this paper is the Wireless Embedded Smart Block for Environment Sensing (WESBES); an affordable wireless sensor platform that allows subjective human comfort data to be directly paired with temporospatially correlated objective sensor measurements for use in EMS. The described device offers a flexible research platform for analyzing the relationship between objective and subjective occupant feedback in order to formulate more meaningful measures of human comfort. It could also offer an affordable and expandable option for real world deployment in existing EMS.

Special Session 2: Smart Grid Security, Resilience, and Privacy

Towards Addressing Common Security Issues in Smart Grid Specifications

By **Apurva Mohan** *(Honeywell ACS Labs) and Himanshu Khurana*

Smart grid standards initiatives aim to coordinate the development of protocols and model standards for interoperability. The smart grid derives its functionality from several existing technologies and standards. At issue is that most of these base standards were developed for specific functionality and security was added later. As such, most standards do not have a unified and comprehensive approach to security, which results in security gaps in these standards. In this paper, we investigate common security issues in smart grid standards that employ communication protocols and the common causes for these issues. We then propose security considerations for developing these standards; to address them, we develop guidelines for drafting security into smart grid standards either when they are updated or when new standards are developed. We draw examples from the ZigBee Smart Energy Profile standard for security requirements, objectives, and to make recommendations for designing security in similar standards. We finally present a retrospective discussion of how following our recommendations would have improved the ZigBee Smart Energy Profile standard by including security in a unified and comprehensive way.

A Case for Validating Remote Application Integrity for Data Processing Systems

By **Jonathan Chu** *(University of Illinois at Urbana-Champaign), Mirko Montanari, and Roy Campbell*

There has been a great increase in recent years as to the amount of data from the grid that has been going to online systems. As more smart meters get installed into the AMI(advanced metering infrastructure), there is a need to mitigate the potential security threats in the collection system. There are a multitude of attack vectors that an adversary may take to compromise the confidentiality of user data and it may take much time and effort for developers to securely cover all such attack vectors. In this paper, we analyze the architecture of AMI systems and how data moves from one end to the other. In particular, we discuss the need for more research in safe program validation that protects against information leaks. Security problems can arise when programs do not perform as intended and may reveal confidential information or take unexpected actions. We discuss a theoretical network architecture that could take advantage of such secure program validation. The model minimizes attack vectors by containing data in one secure location that we call a DBPC(database processing center) instead of transporting data to multiple locations through a traditional DBMS(database management system). When outside parties want access to the data, they can send verified secure applications to the DBPC to run their applications remotely without direct access to the data. We describe the design of the AMI simulator and DBPC prototype module that we implemented.

Paper and Poster Abstracts *(continued)*

Special Session 4: Co-Robotics and Tele-Presence

Supporting Human Interaction with Robust Robot Swarms

By **Sean Kerman** *(Brigham Young University), Daniel Brown, and Michael Goodrich*

In this paper we propose a bio-inspired model for a decentralized swarm of robots, similar to the model proposed by Couzin [5], that allows for dynamic task assignment and is robust to limited communication from a human. We provide evidence that the model has two fundamental attractors: a torus attractor and a flock attractor. Through simulation and mathematical analysis we investigate the stability of these attractors and show that a control input can be used to force the system to change from one attractor to the other. Finally, we generalize another of Couzin's ideas [4] and present the idea of a stakeholder agent. We show how a human operator can use stakeholders to responsively influence group behavior while maintaining group structure.

A Payload Verification and Management Framework for Small UAV-based Personal Remote Sensing Systems

By **Calvin Coopmans** *(Utah State University), Brandon Stark, and Christopher Coffin*

Small, unmanned aerial systems are becoming more important in many fields, including civilian, scientific applications. Affordable systems that allow remote sensing at a small scale—personal remote sensing—are possible with proper system design. To assure data mission success (i.e., reliable and safe data collection) with low-cost or consumer-level sensor hardware, a well-designed payload management system is needed, along with sensor interface development and standardized testing frameworks for verification. This payload management system ensures a level of airworthiness for Data Mission Assurance. This paper presents such a system, along with motivations and choices such as system architecture and implementation, as well as standardized testing and verification. Data results from flight of a fixed-wing example payload is also included.

Force Control and Nonlinear Master-Slave Force Profile to Manage an Admittance Type Multi-Fingered Haptic User Interface

By **Anthony Crawford**, Idaho National Laboratory

Natural movements and force feedback are important elements in using tele-operated equipment if complex and speedy manipulation tasks are to be accomplished in remote and/or hazardous environments, such as hot cells, glove boxes, decommissioning, explosive disarmament, and space to name a few. In order to achieve this end the research presented in this paper has developed an admittance-type exoskeleton like multi-fingered haptic hand user interface that secures the user's palm and provides 3-dimensional force feedback to the user's fingertips. Atypical to conventional haptic hand user interfaces that limit themselves to integrating the human hand's characteristics just into the system's mechanical design, this system also perpetuates that inspiration into the designed user interface's controller.

Poster Abstracts

(in alphabetical order by last name)

Towards A Method for Assessing Resilience of Complex Dynamical Systems

By **Michael Balchanos** *(Georgia Tech), Yongchang Li, and Dimitri Mavris*

System survivability is one of the key requirements for the conceptual design of an Integrated Reconfigurable Intelligent (IRIS) system. Current approaches in survivability engineering may not effectively address the challenges in designing revolutionary, large scale complex and multi-capable systems. The main objective of this study is to investigate the concept of resilience in the context of system safety and survivability and suggest a technique for assessing resilience in systems engineering. Resilience is expected to be the enabler for integrating safety and survivability in the early conceptual design. For this purpose, a small scale cooling network system architecture has been utilized to demonstrate the technique, both for a 32-valve baseline, as well as for six other configurations. The application of the technique allowed for the comparative assessment and tradeoff investigation of resilience function capacities, as well for the identification of solution feasibility, under adaptability and robustness constraints.

Increasing and Supporting Operator Awareness in Control of Complex Systems

By Jacob Viraldo and **Barrett Caldwell** *(Purdue University)*

Increased complexity of modern control rooms, especially those of nuclear power plants (NPPs), require additional attention to the demands for collaborative sharing of expertise and knowledge to manage dynamic situations and alarms. NPP environments represent a unique challenge due to the needs for technology upgrading, and the problems of alarm flooding, in a highly proceduralized and expert-driven environment. This paper addresses some of these issues, including those of incorporating doctoral dissertation research students into these complex socio-technical settings.

A Framework for Analyzing Human Factors inUnmanned Aerial Systems

By Brandon Stark, **Calvin Coopmans***, and YangQuan Chen (Utah State University)*

The human factors involved in an unmanned aerial system (UAS) come in a variety of forms that has largely gone poorly represented in literature. In this paper, a holistic approach is taken to identify not only the individual aspects but the interconnection of the human-UAS interaction. First, an examination of human factors involved in a UAS are presented. Next, the metrics of human performance, such as cognitive load, situational awareness and complacency are introduced. Finally, a framework is developed to form the interconnection

of human factors with human performance metrics in a UAS. With this framework in place, the intended goal is that an optimal level of cognitive workload for the humans involved in an UAS can be designed and implemented by the utilization of this framework during the development of advanced automation systems and human interface devices.

Complexity: Application to Human Performance Modeling and HRA for Dynamic Environments

By **David Gertman** *(Idaho National Laboratory)*

Although the argument has been made quite strongly and perhaps convincingly that advanced, highly automated control rooms consisting of advanced digital information and control systems will be simpler to operate and maintain; the case can be made that this potential benefit will only be true to the extent that we successfully control the amount of complexity present for the operating crew. Borrowing from complexity theory and human reliability analysis literature, we review the aspects of complexity that should be considered, discuss the implications, and review the extent to which we find current human reliability analysis (HRA) methods sensitivity to complexity in advanced digital environments. Next, we identify 3 complexity factors related to human performance and propose a rating scale approach that allows the analyst to more clearly allocate complexity levels for HRA purposes. These factor scores are used to form the basis of a composite complexity score (CCS) that can be used to support HRA. Although one method, the Simplified Plant Analysis Risk Model Human Reliability Analysis (SPAR-H), is selected for purposes of mapping the 3 complexity elements, the results are thought to support the qualitative and quantitative portions of most HRA methods.

Using Hybrid Attack Graphs to Model Cyber-Physical Attacks in the Smart Grid

By **Peter Hawrylak** *(University of Tulsa) and Michael Haney*

The Smart Grid is a large networked cyber-physical control system that is part of the critical infrastructure. This paper presents a cyber-physical attack against a substation where the attacker causes a transformer to overheat. The attack is modeled using a hybrid attack graph (HAG), which provides a means to model both the physical and cyber components of the attack. The HAG provides insight into potential attack vectors. Based on this information, key points in the system can be identified where security can be strengthened. Direction for future work to expand the capabilities of HAGs for modeling cyber-physical attacks is presented.

An Integrated System Simulation Approach for Wireless Networked Control Systems

By **Peter Horvath** *(Vanderbilt University), Mark Yampolskiy, Yuan Xue, Xenofon Koutsoukos, and Janos Sztipanovits*

Cyber-Physical Systems (CPS), such as networked control systems, are increasingly deployed over wireless networks. Given the sensitivity of control systems to networking conditions such as packet drops, delays and jitters, it is important to verify and evaluate the control system properties under realistic wireless networking deployment scenarios. However, current research is often based on simplistic models of the wireless network physical layer behaviors. In this paper, we point out deficiencies in the existing simulation methods for the performance evaluation of wireless networked control systems and present a novel simulation framework for wireless network control systems. Our approach aims at capturing the effects in the physical layer more accurately than state-of-art simulators are capable of. An integrated simulation tool, based on open-source solutions, is presented and a case study of a networked control system is also provided to illustrate the capabilities of our simulation tool.

A Proposed Data Fusion Architecture for Micro-Zone Analysis and Data Mining

By **Kevin McCarty** *(University of Idaho) and Milos Manic*

-zone analysis involves use of data fusion and data mining techniques in order to understand the relative impact of many different variables. Data Fusion requires the ability to combine or "fuse" date from multiple data sources. Data mining involves the application of sophisticated algorithms such as Neural Networks and Decision Trees, to describe micro-zone behavior and predict future values based upon past values. One of the difficulties encountered in developing generic time series or other data mining techniques for micro-zone analysis is the wide variability of the data sets available for analysis. This presents challenges all the way from the data gathering stage to results presentation. This paper presents an architecture designed and used to facilitate the collection of disparate data sets well suited for data fusion and data mining. Results show this architecture provides a flexible, dynamic framework for the capture and storage of a myriad of dissimilar data sets and can serve as a foundation from which to build a complete data fusion architecture.

Adaptive Control of Bayesian Network Computation

By **Erik Reed** *(Carnegie Mellon University), Abe Ishihara, and Ole Mengshoel*

This paper considers the problem of providing, for computational processes, soft real-time (or reactive) response without the use of a hard real-time operating system. In particular, we focus on the problem of reactively computing fault diagnosis by means of different Bayesian network inference algorithms on non-real-time operating systems where low-criticality (background) process activity and system load is unpredictable. To address this problem, we take in this paper a reconfigurable adaptive control approach. Computation time is modeled using an ARX model where the input consists of the maximum number of background processes allowed to run at any given time. To ensure that the reactive (high-criticality) diagnosis is computed within a set time frame, we introduce a minimum degree pole placement controller to impose a limit on the maximum number of low-criticality processes. Experimentally, we perform electrical power system diagnosis using a Bayesian network model of and data from a NASA electrical power network. The Bayesian network inference algorithms likelihood weighting and junction tree propagation are successfully applied and changed mid-simulation to investigate how inference computation time changes in an unpredictable operating system, as well as how the controller reacts to inference algorithm changes.

ISRCS Committees

Symposium Leadership Team

- Craig Rieger, Symposium Chair, INL (208.851.8839)
- Milos Manic, Symposium Co-Chair, University of Idaho
- Jodi Grgich, Organizing Chair, INL (208.201.2006)
- Saurabh Amin, Massachusetts Institute of Technology
- Miles McQueen, Idaho National Laboratory
- John Chiasson, Boise State University

Technical Program Committee

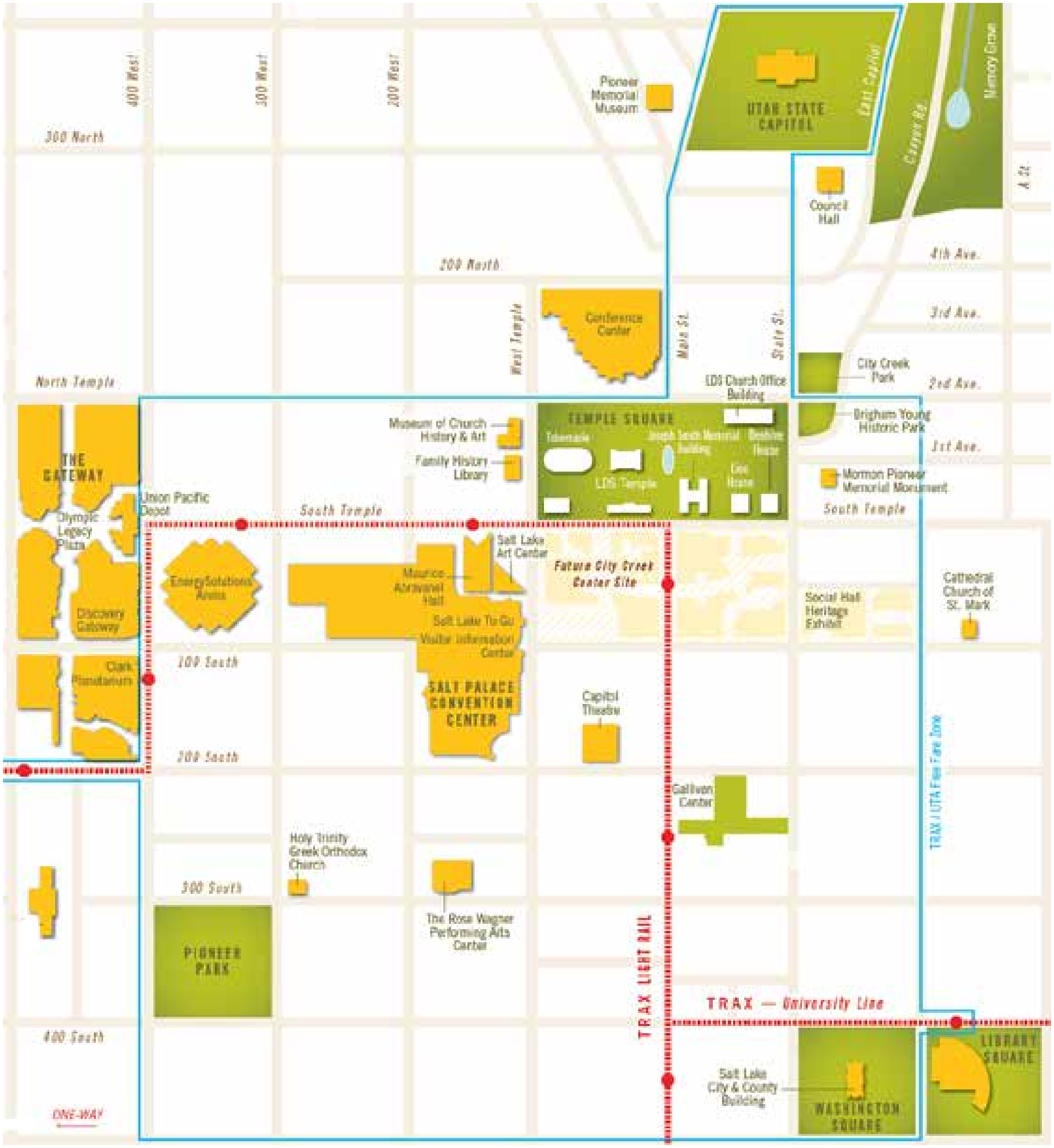
- Juan Jose Rodriguez Andina, University of Vigo
- Azad Azadmanesh, University of Nebraska, Omaha
- Ron Boring, Idaho National Laboratory
- Jonathan Butts, Air Force Institute of Technology
- Barrett Caldwell, Purdue University
- Álvaro A. Cárdenas, Fujitsu Laboratories of America
- Marco Carvahlo, Florida Institute of Technology
- YangQuan Chen, Utah State University
- Mo-Yuen Chow, North Carolina State University
- Michael Condry, INTEL
- John Doyle, California Institute of Technology
- Frank Feresse, NAVSEA
- 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, NETL
- Scott Kerick, Army Research Laboratory
- Nicholas Kottenstette, Vanderbilt University
- 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
- 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, Clarkson University
- Eugene Santos, Dartmouth College
- Marco Schoen, Idaho State University
- 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
- Bogdan Wilamowski, Auburn University
- David Woods, The Ohio State University
- Reed Young, U.S. Army ATEC
- Said Ahmed-Zaid, Boise State University

Symposium Organizing Team

- Andrew Thomas, ISRCS Logistics
- Jody Henley, ISRCS Lead Facilitator
- Desiree Reagan, ISRCS Web Developer
- David Combs, ISRCS Graphics
- Kristyn St. Clair, ISRCS Graphics

Publication Chair

- Debbie McQueen, University of Idaho


400 West
300 West
200 West
300 North
Pioneer Memorial Museum
UTAH STATE CAPITOL
East Capitol
Canyon Rd.
Memory Grove
A St.
Council Hall
200 North
4th Ave.
3rd Ave.
West Temple
Conference Center
Main St.
State St.
City Creek Park
2nd Ave.
North Temple
LDS Church Office Building
Museum of Church History & Art
Family History Library
TEMPLE SQUARE
Tabernacle
Joseph Smith Memorial Building
Beehive House
LDS Temple
Lion House
Brigham Young Historic Park
1st Ave.
Mormon Pioneer Memorial Monument
THE GATEWAY
Olympic Legacy Plaza
Union Pacific Depot
South Temple
South Temple
Salt Lake Art Center
Future City Creek Center Site
EnergySolutions Arena
Maurice Abravanel Hall
Salt Lake Tu Gu Visitor Information Center
Discovery Gateway
Social Hall Heritage Exhibit
Cathedral Church of St. Mark
Clark Planetarium
100 South
SALT PALACE CONVENTION CENTER
Capitol Theatre
200 South
Gallivan Center
Holy Trinity Greek Orthodox Church
300 South
The Rose Wagner Performing Arts Center
PIONEER PARK
TRAX LIGHT RAIL
TRAX / UTA Free Fare Zone
TRAX — University Line
400 South
LIBRARY SQUARE
Salt Lake City & County Building
WASHINGTON SQUARE
ONE-WAY

Capitol Theatre

Wicked

Tuesday, August 14th, 7:30 p.m.

Long before Dorothy drops in, two other girls meet in the Land of Oz! One, born with emerald green skin, is smart, fiery & misunderstood. The other is beautiful, ambitious and very popular. How these two unlikely friends end up as the Wicked Witch of the West and Glinda the Good Witch makes for the most spellbinding new musical in years.

Wicked explores the life of the Wicked Witch of the West, also known as Elphaba Thropp, a misunderstood, victimized person whose behavior was merely a reaction against a charlatan wizard's corrupt government.

Wicked follows Maguire's novel, a re-imagining of L. Frank Baum's classic story, The Wonderful Wizard of Oz, from the point of view of the witches of Oz, set mostly prior to Dorothy's arrival from Kansas.

Watch the story unfolds as you discover Elphaba's relationship with the beautiful and ambitious Galinda Upland, who ultimately becomes Glinda the Good Witch of the North, and how their friendship struggles to endure extreme personality conflicts, opposing viewpoints, rivalry over the same love interest, and of course, Elphaba's eventual fall from grace.

Captiol Theatre
50 West 200 South
Salt Lake City, UT. 84101
801.355.2787

Coming Soon

6th International Symposium on Resilient Control Systems

ISRCS 2013

San Francisco, California

August 13-15, 2013

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. For 2013, the Human Factors and Ergonomics Society will be initiating a co-located symposium on resilient cognizant systems known as "Resilience Week". 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 three symposia:

- International Symposium on Resilient Control Systems
- International Symposium on Resilient Cyber Systems
- International Symposium on Resilient Cognizant Systems

ISRCS 2012